

# SCCE Compliance & Ethics Essentials Workshop

## Resources

Resource 1

**Acronyms**

## **Acronyms**

ADA	Americans with Disabilities Act
AML	Anti Money Laundering
APEC	Asian-Pacific Economic Cooperation
ARS	Auction Rate Securities
AUSA	Assistant U.S. Attorney
BNA	Bureau of National Affairs
BOD	Board of Directors
BSA	Bank Secrecy Act
CAE	Chief Audit Executive
CBT	Computer Based Training
CCO	Chief Compliance Officer
CCEP	Certified Compliance & Ethics Professional
CCEP-I	Certified Compliance & Ethics Professional - International
CCPA	California Consumer Privacy Act
CIS	Commonwealth of Independent States
CLO	Chief Legal Officer
COSO	Committee of Sponsoring Organizations
CP	Compliance Program
CPI	Corruption Perception Index
DEA	Drug Enforcement Agency
DFARS	Defense Federal Acquisition Regulations
DII	Defense Industry Initiative
DOE	Department of Energy
DOI	Department of Insurance
DOJ	Department of Justice
DPA	Deferred Prosecution Agreement
E&C	Ethics & Compliance
ECOA	Equal Credit Opportunity Act
EEOC	Equal Employment Opportunity Commission
EPA	Environmental Protection Agency
ERISA	Employee Retirement Income Security Act
ERM	Enterprise Risk Management
EU	European Union
FACTA	Fair and Accurate Credit Transactions Act
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FCA	False Claims Act
FCPA	Foreign Corrupt Practices Act
FCRA	Fair Credit Reporting Act
FDIC	Federal Deposit Insurance Corporation
FERC	Federal Energy Regulatory Commission
FERPA	Family Education Rights and Privacy Act
FLSA	Fair Labor Standards Act
FMLA	Family Medical Leave Act
FOIA	Freedom of Information Act
FSG	Federal Sentencing Guidelines
FTC	Federal Trade Commission
GDPR	General Data Protection Regulations
GINA	Genetic Information Non-Discrimination Act
GLBA	Gramm-Leach-Bliley Act

HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IASB	International Accounting Standards Board
IFRS	International Financial Reporting Standards
IIA	Institute of Internal Auditors
IPSIG	Independent Private Sector Inspector General
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulations
KPI	Key Performance Indicator
LCA	Law Council Australia
M&A	Mergers and Acquisitions
NASDAQ	National Association of Securities Dealers Automated Quotations
NCRA	National Credit Reporting Agency
NIH	National Institute of Health
NIST	National Institute of Standards and Technology
NLRA	National Labor Relations Act
NLRB	National Labor Relations Board
NPA	Non-Prosecution Agreement
NSF	National Science Foundation
NYSE	New York Stock Exchange
OECD	Organization for Economic Cooperation and Development
OFAC	US Treasury - Office of Foreign Assets Control
OIG	Office of Inspector General
OSHA	Occupational Safety and Health Administration
PCAOB	Public Company Accounting Oversight Board
PCI	Payment Card Industry Standard
PEP	Politically Exposed Person
PETA	People for the Ethical Treatment of Animals
PHI	Protected Health Information
PII	Personally Identifiable Person
PIPED Act	Personal Information Protection and Electronic Documents Act
RCRA	Resource Conservation and Recovery Act
ROI	Return on Investment
SCCE	Society of Corporate Compliance & Ethics
SEC	Securities and Exchange Commission
SFO	Serious Fraud Office
SOX	Sarbanes Oxley Act
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act - 2001
USSC	United States Sentencing Commission
USSG	United States Sentencing Guidelines
USAID	US Agency for International Development



**Guidelines Manual – Effective Compliance and Ethics Program**

**§8B1.4. Order of Notice to Victims - Organizations**

Apply §5F1.4 (Order of Notice to Victims).

Historical Note: Effective November 1, 1991 (see Appendix C, amendment 422).

**2. EFFECTIVE COMPLIANCE AND ETHICS PROGRAM**

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673).

**§8B2.1. Effective Compliance and Ethics Program**

- (a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (c)(1) of §8D1.4 (Recommended Conditions of Probation - Organizations), an organization shall—

- (1) exercise due diligence to prevent and detect criminal conduct; and
- (2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

- (b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:
- (1) The organization shall establish standards and procedures to prevent and detect criminal conduct.
  - (2)
    - (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.
    - (B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.

- (C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.
- (3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.
- (4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subdivision (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.  
  
(B) The individuals referred to in subdivision (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.
- (5) The organization shall take reasonable steps—
  - (A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;
  - (B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and
  - (C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.
- (6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in

criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

- (7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program.
- (c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

Commentary

Application Notes:

1. Definitions.—For purposes of this guideline:

*"Compliance and ethics program" means a program designed to prevent and detect criminal conduct.*

*"Governing authority" means the (A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing body of the organization.*

*"High-level personnel of the organization" and "substantial authority personnel" have the meaning given those terms in the Commentary to §8A1.2 (Application Instructions - Organizations).*

*"Standards and procedures" means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct.*

2. Factors to Consider in Meeting Requirements of this Guideline.—

(A) In General.—Each of the requirements set forth in this guideline shall be met by an organization; however, in determining what specific actions are necessary to meet those requirements, factors that shall be considered include: (i) applicable industry practice or the standards called for by any applicable governmental regulation; (ii) the size of the organization; and (iii) similar misconduct.

(B) Applicable Governmental Regulation and Industry Practice.—An organization's failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.



(C) The Size of the Organization.—

- (i) In General.—The formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization's standards and procedures, depend on the size of the organization.
- (ii) Large Organizations.—A large organization generally shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization. As appropriate, a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs.
- (iii) Small Organizations.—In meeting the requirements of this guideline, small organizations shall demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations. However, a small organization may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems.

Examples of the informality and use of fewer resources with which a small organization may meet the requirements of this guideline include the following: (I) the governing authority's discharge of its responsibility for oversight of the compliance and ethics program by directly managing the organization's compliance and ethics efforts; (II) training employees through informal staff meetings, and monitoring through regular "walk-arounds" or continuous observation while managing the organization; (III) using available personnel, rather than employing separate staff, to carry out the compliance and ethics program; and (IV) modeling its own compliance and ethics program on existing, well-regarded compliance and ethics programs and best practices of other similar organizations.

- (D) Recurrence of Similar Misconduct.—Recurrence of similar misconduct creates doubt regarding whether the organization took reasonable steps to meet the requirements of this guideline. For purposes of this subdivision, "similar misconduct" has the meaning given that term in the Commentary to §8A1.2 (Application Instructions - Organizations).

3. Application of Subsection (b)(2).—High-level personnel and substantial authority personnel of the organization shall be knowledgeable about the content and operation of the compliance and ethics program, shall perform their assigned duties consistent with the exercise of due diligence, and shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

If the specific individual(s) assigned overall responsibility for the compliance and ethics program does not have day-to-day operational responsibility for the program, then the individual(s) with day-to-day operational responsibility for the program typically should, no less than annually, give the governing authority or an appropriate subgroup thereof information on the implementation and effectiveness of the compliance and ethics program.

4. Application of Subsection (b)(3).—

(A) Consistency with Other Law.—Nothing in subsection (b)(3) is intended to require conduct inconsistent with any Federal, State, or local law, including any law governing employment or hiring practices.

(B) Implementation.—In implementing subsection (b)(3), the organization shall hire and promote individuals so as to ensure that all individuals within the high-level personnel and substantial authority personnel of the organization will perform their assigned duties in a manner consistent with the exercise of due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law under subsection (a). With respect to the hiring or promotion of such individuals, an organization shall consider the relatedness of the individual's illegal activities and other misconduct (*i.e.*, other conduct inconsistent with an effective compliance and ethics program) to the specific responsibilities the individual is anticipated to be assigned and other factors such as: (i) the recency of the individual's illegal activities and other misconduct; and (ii) whether the individual has engaged in other such illegal activities and other such misconduct.

5. Application of Subsection (b)(6).—Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

6. Application of Subsection (c).—To meet the requirements of subsection (c), an organization shall:

(A) Assess periodically the risk that criminal conduct will occur, including assessing the following:

(i) The nature and seriousness of such criminal conduct.

(ii) The likelihood that certain criminal conduct may occur because of the nature of the organization's business. If, because of the nature of an organization's business, there is a substantial risk that certain types of criminal conduct may occur, the organization shall take reasonable steps to prevent and detect that type of criminal conduct. For example, an organization that, due to the nature of its business, employs sales personnel who have flexibility to set prices shall establish standards and procedures designed to prevent and detect price-fixing. An organization that, due to the nature of its business, employs sales personnel who have flexibility to represent the material characteristics of a product shall establish standards and procedures designed to prevent and detect fraud.

(iii) The prior history of the organization. The prior history of an organization may indicate types of criminal conduct that it shall take actions to prevent and detect.

(B) Prioritize periodically, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b), in order to focus on preventing and detecting the criminal conduct identified under subdivision (A) of this note as most serious, and most likely, to occur.



- (C) *Modify, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b) to reduce the risk of criminal conduct identified under subdivision (A) of this note as most serious, and most likely, to occur.*

Background: *This section sets forth the requirements for an effective compliance and ethics program. This section responds to section 805(a)(2)(5) of the Sarbanes-Oxley Act of 2002, Public Law 107-204, which directed the Commission to review and amend, as appropriate, the guidelines and related policy statements to ensure that the guidelines that apply to organizations in this chapter "are sufficient to deter and punish organizational criminal misconduct."*

*The requirements set forth in this guideline are intended to achieve reasonable prevention and detection of criminal conduct for which the organization would be vicariously liable. The prior diligence of an organization in seeking to prevent and detect criminal conduct has a direct bearing on the appropriate penalties and probation terms for the organization if it is convicted and sentenced for a criminal offense.*

Historical Note: Effective November 1, 2004 (see Appendix C, amendment 673).

Resource 3

**2018 Federal Sentencing Guidelines Manual**



## CHAPTER EIGHT

# SENTENCING OF ORGANIZATIONS

### Introductory Commentary

The guidelines and policy statements in this chapter apply when the convicted defendant is an organization. Organizations can act only through agents and, under federal criminal law, generally are vicariously liable for offenses committed by their agents. At the same time, individual agents are responsible for their own criminal conduct. Federal prosecutions of organizations therefore frequently involve individual and organizational co-defendants. Convicted individual agents of organizations are sentenced in accordance with the guidelines and policy statements in the preceding chapters. This chapter is designed so that the sanctions imposed upon organizations and their agents, taken together, will provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct.

This chapter reflects the following general principles:

*First*, the court must, whenever practicable, order the organization to remedy any harm caused by the offense. The resources expended to remedy the harm should not be viewed as punishment, but rather as a means of making victims whole for the harm caused.

*Second*, if the organization operated primarily for a criminal purpose or primarily by criminal means, the fine should be set sufficiently high to divest the organization of all its assets.

*Third*, the fine range for any other organization should be based on the seriousness of the offense and the culpability of the organization. The seriousness of the offense generally will be reflected by the greatest of the pecuniary gain, the pecuniary loss, or the amount in a guideline offense level fine table. Culpability generally will be determined by six factors that the sentencing court must consider. The four factors that increase the ultimate punishment of an organization are: (i) the involvement in or tolerance of criminal activity; (ii) the prior history of the organization; (iii) the violation of an order; and (iv) the obstruction of justice. The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, co-operation, or acceptance of responsibility.

*Fourth*, probation is an appropriate sentence for an organizational defendant when needed to ensure that another sanction will be fully implemented, or to ensure that steps will be taken within the organization to reduce the likelihood of future criminal conduct.

These guidelines offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program. The prevention and detection of criminal conduct, as facilitated by an effective compliance and ethics program, will assist an organization in encouraging ethical conduct and in complying fully with all applicable laws.

#### Historical Note

Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673).

## PART A — GENERAL APPLICATION PRINCIPLES

---

### §8A1.1. Applicability of Chapter Eight

---

This chapter applies to the sentencing of all organizations for felony and Class A misdemeanor offenses.

#### Commentary

#### Application Notes:

1. “**Organization**” means “a person other than an individual.” 18 U.S.C. § 18. The term includes corporations, partnerships, associations, joint-stock companies, unions, trusts, pension funds, unincorporated organizations, governments and political subdivisions thereof, and non-profit organizations.
2. The fine guidelines in §§8C2.2 through 8C2.9 apply only to specified types of offenses. The other provisions of this chapter apply to the sentencing of all organizations for all felony and Class A misdemeanor offenses. For example, the restitution and probation provisions in Parts B and D of this chapter apply to the sentencing of an organization, even if the fine guidelines in §§8C2.2 through 8C2.9 do not apply.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
----------------------------	---

---

### §8A1.2. Application Instructions — Organizations

---

- (a) Determine from Part B, Subpart 1 (Remedying Harm from Criminal Conduct) the sentencing requirements and options relating to restitution, remedial orders, community service, and notice to victims.
- (b) Determine from Part C (Fines) the sentencing requirements and options relating to fines:
  - (1) If the organization operated primarily for a criminal purpose or primarily by criminal means, apply §8C1.1 (Determining the Fine — Criminal Purpose Organizations).
  - (2) Otherwise, apply §8C2.1 (Applicability of Fine Guidelines) to identify the counts for which the provisions of §§8C2.2 through 8C2.9 apply. For such counts:
    - (A) Refer to §8C2.2 (Preliminary Determination of Inability to Pay Fine) to determine whether an abbreviated determination of the guideline fine range may be warranted.

- (B) Apply §8C2.3 (Offense Level) to determine the offense level from Chapter Two (Offense Conduct) and Chapter Three, Part D (Multiple Counts).
- (C) Apply §8C2.4 (Base Fine) to determine the base fine.
- (D) Apply §8C2.5 (Culpability Score) to determine the culpability score. To determine whether the organization had an effective compliance and ethics program for purposes of §8C2.5(f), apply §8B2.1 (Effective Compliance and Ethics Program).
- (E) Apply §8C2.6 (Minimum and Maximum Multipliers) to determine the minimum and maximum multipliers corresponding to the culpability score.
- (F) Apply §8C2.7 (Guideline Fine Range — Organizations) to determine the minimum and maximum of the guideline fine range.
- (G) Refer to §8C2.8 (Determining the Fine Within the Range) to determine the amount of the fine within the applicable guideline range.
- (H) Apply §8C2.9 (Disgorgement) to determine whether an increase to the fine is required.

For any count or counts not covered under §8C2.1 (Applicability of Fine Guidelines), apply §8C2.10 (Determining the Fine for Other Counts).

- (3) Apply the provisions relating to the implementation of the sentence of a fine in Part C, Subpart 3 (Implementing the Sentence of a Fine).
- (4) For grounds for departure from the applicable guideline fine range, refer to Part C, Subpart 4 (Departures from the Guideline Fine Range).
- (c) Determine from Part D (Organizational Probation) the sentencing requirements and options relating to probation.
- (d) Determine from Part E (Special Assessments, Forfeitures, and Costs) the sentencing requirements relating to special assessments, forfeitures, and costs.

## Commentary

### Application Notes:

1. Determinations under this chapter are to be based upon the facts and information specified in the applicable guideline. Determinations that reference other chapters are to be made under the standards applicable to determinations under those chapters.
2. The definitions in the Commentary to §1B1.1 (Application Instructions) and the guidelines and commentary in §§1B1.2 through 1B1.8 apply to determinations under this chapter unless otherwise specified. The adjustments in Chapter Three, Parts A (Victim-Related Adjustments), B (Role in the Offense), C (Obstruction and Related Adjustments), and E (Acceptance of Responsibility) do not apply. The provisions of Chapter Six (Sentencing Procedures, Plea Agreements, and Crime Victims' Rights) apply to proceedings in which the defendant is an organization. Guidelines and policy statements not referenced in this chapter, directly or indirectly, do not apply when the defendant is an organization; *e.g.*, the policy statements in Chapter Seven (Violations of Probation and Supervised Release) do not apply to organizations.
3. The following are definitions of terms used frequently in this chapter:
  - (A) “**Offense**” means the offense of conviction and all relevant conduct under §1B1.3 (Relevant Conduct) unless a different meaning is specified or is otherwise clear from the context. The term “**instant**” is used in connection with “offense,” “federal offense,” or “offense of conviction,” as the case may be, to distinguish the violation for which the defendant is being sentenced from a prior or subsequent offense, or from an offense before another court (*e.g.*, an offense before a state court involving the same underlying conduct).
  - (B) “**High-level personnel of the organization**” means individuals who have substantial control over the organization or who have a substantial role in the making of policy within the organization. The term includes: a director; an executive officer; an individual in charge of a major business or functional unit of the organization, such as sales, administration, or finance; and an individual with a substantial ownership interest. “**High-level personnel of a unit of the organization**” is defined in the Commentary to §8C2.5 (Culpability Score).
  - (C) “**Substantial authority personnel**” means individuals who within the scope of their authority exercise a substantial measure of discretion in acting on behalf of an organization. The term includes high-level personnel of the organization, individuals who exercise substantial supervisory authority (*e.g.*, a plant manager, a sales manager), and any other individuals who, although not a part of an organization’s management, nevertheless exercise substantial discretion when acting within the scope of their authority (*e.g.*, an individual with authority in an organization to negotiate or set price levels or an individual authorized to negotiate or approve significant contracts). Whether an individual falls within this category must be determined on a case-by-case basis.
  - (D) “**Agent**” means any individual, including a director, an officer, an employee, or an independent contractor, authorized to act on behalf of the organization.
  - (E) An individual “**condoned**” an offense if the individual knew of the offense and did not take reasonable steps to prevent or terminate the offense.
  - (F) “**Similar misconduct**” means prior conduct that is similar in nature to the conduct underlying the instant offense, without regard to whether or not such conduct violated the same statutory provision. For example, prior Medicare fraud would be misconduct similar to an instant offense involving another type of fraud.

- (G) “**Prior criminal adjudication**” means conviction by trial, plea of guilty (including an *Alford* plea), or plea of *nolo contendere*.
- (H) “**Pecuniary gain**” is derived from 18 U.S.C. § 3571(d) and means the additional before-tax profit to the defendant resulting from the relevant conduct of the offense. Gain can result from either additional revenue or cost savings. For example, an offense involving odometer tampering can produce additional revenue. In such a case, the pecuniary gain is the additional revenue received because the automobiles appeared to have less mileage, *i.e.*, the difference between the price received or expected for the automobiles with the apparent mileage and the fair market value of the automobiles with the actual mileage. An offense involving defense procurement fraud related to defective product testing can produce pecuniary gain resulting from cost savings. In such a case, the pecuniary gain is the amount saved because the product was not tested in the required manner.
- (I) “**Pecuniary loss**” is derived from 18 U.S.C. § 3571(d) and is equivalent to the term “loss” as used in Chapter Two (Offense Conduct). *See* Commentary to §2B1.1 (Theft, Property Destruction, and Fraud), and definitions of “tax loss” in Chapter Two, Part T (Offenses Involving Taxation).
- (J) An individual was “**willfully ignorant of the offense**” if the individual did not investigate the possible occurrence of unlawful conduct despite knowledge of circumstances that would lead a reasonable person to investigate whether unlawful conduct had occurred.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422); November 1, 1997 (amendment 546); November 1, 2001 (amendment 617); November 1, 2004 (amendment 673); November 1, 2010 (amendment 747); November 1, 2011 (amendment 758).
------------------------	---

## PART B — REMEDYING HARM FROM CRIMINAL CONDUCT, AND EFFECTIVE COMPLIANCE AND ETHICS PROGRAM

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673).
------------------------	---

### 1. REMEDYING HARM FROM CRIMINAL CONDUCT

<i>Historical Note</i>	Effective November 1, 2004 (amendment 673).
------------------------	---

#### Introductory Commentary

As a general principle, the court should require that the organization take all appropriate steps to provide compensation to victims and otherwise remedy the harm caused or threatened by the offense. A restitution order or an order of probation requiring restitution can be used to compensate identifiable victims of the offense. A remedial order or an order of probation requiring community service can be used to reduce or eliminate the harm threatened, or to repair the harm caused by the offense, when that harm or threatened harm would otherwise not be remedied. An order of notice to victims can be used to notify unidentified victims of the offense.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

### §8B1.1. Restitution — Organizations

---

- (a) In the case of an identifiable victim, the court shall—
  - (1) enter a restitution order for the full amount of the victim’s loss, if such order is authorized under 18 U.S.C. § 2248, § 2259, § 2264, § 2327, § 3663, or § 3663A; or
  - (2) impose a term of probation or supervised release with a condition requiring restitution for the full amount of the victim’s loss, if the offense is not an offense for which restitution is authorized under 18 U.S.C. § 3663(a)(1) but otherwise meets the criteria for an order of restitution under that section.
- (b) *Provided*, that the provisions of subsection (a) do not apply—
  - (1) when full restitution has been made; or
  - (2) in the case of a restitution order under § 3663; a restitution order under 18 U.S.C. § 3663A that pertains to an offense against property described in 18 U.S.C. § 3663A(c)(1)(A)(ii); or a condition of restitution

imposed pursuant to subsection (a)(2) above, to the extent the court finds, from facts on the record, that (A) the number of identifiable victims is so large as to make restitution impracticable; or (B) determining complex issues of fact related to the cause or amount of the victim's losses would complicate or prolong the sentencing process to a degree that the need to provide restitution to any victim is outweighed by the burden on the sentencing process.

- (c) If a defendant is ordered to make restitution to an identifiable victim and to pay a fine, the court shall order that any money paid by the defendant shall first be applied to satisfy the order of restitution.
- (d) A restitution order may direct the defendant to make a single, lump sum payment, partial payments at specified intervals, in-kind payments, or a combination of payments at specified intervals and in-kind payments. *See* 18 U.S.C. § 3664(f)(3)(A). An in-kind payment may be in the form of (1) return of property; (2) replacement of property; or (3) if the victim agrees, services rendered to the victim or to a person or organization other than the victim. *See* 18 U.S.C. § 3664(f)(4).
- (e) A restitution order may direct the defendant to make nominal periodic payments if the court finds from facts on the record that the economic circumstances of the defendant do not allow the payment of any amount of a restitution order, and do not allow for the payment of the full amount of a restitution order in the foreseeable future under any reasonable schedule of payments.
- (f) Special Instruction
  - (1) This guideline applies only to a defendant convicted of an offense committed on or after November 1, 1997. Notwithstanding the provisions of §1B1.11 (Use of Guidelines Manual in Effect on Date of Sentencing), use the former §8B1.1 (set forth in Appendix C, amendment 571) in lieu of this guideline in any other case.

### Commentary

**Background:** Section 3553(a)(7) of Title 18, United States Code, requires the court, “in determining the particular sentence to be imposed,” to consider “the need to provide restitution to any victims of the offense.” Orders of restitution are authorized under 18 U.S.C. §§ 2248, 2259, 2264, 2327, 3663, and 3663A. For offenses for which an order of restitution is not authorized, restitution may be imposed as a condition of probation.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422); November 1, 1997 (amendment 571).
----------------------------	---

---

**§8B1.2. Remedial Orders — Organizations (Policy Statement)**

---

- (a) To the extent not addressed under §8B1.1 (Restitution — Organizations), a remedial order imposed as a condition of probation may require the organization to remedy the harm caused by the offense and to eliminate or reduce the risk that the instant offense will cause future harm.
- (b) If the magnitude of expected future harm can be reasonably estimated, the court may require the organization to create a trust fund sufficient to address that expected harm.

**Commentary**

**Background:** The purposes of a remedial order are to remedy harm that has already occurred and to prevent future harm. A remedial order requiring corrective action by the organization may be necessary to prevent future injury from the instant offense, *e.g.*, a product recall for a food and drug violation or a clean-up order for an environmental violation. In some cases in which a remedial order potentially may be appropriate, a governmental regulatory agency, *e.g.*, the Environmental Protection Agency or the Food and Drug Administration, may have authority to order remedial measures. In such cases, a remedial order by the court may not be necessary. If a remedial order is entered, it should be coordinated with any administrative or civil actions taken by the appropriate governmental regulatory agency.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

**§8B1.3. Community Service — Organizations (Policy Statement)**

---

Community service may be ordered as a condition of probation where such community service is reasonably designed to repair the harm caused by the offense.

**Commentary**

**Background:** An organization can perform community service only by employing its resources or paying its employees or others to do so. Consequently, an order that an organization perform community service is essentially an indirect monetary sanction, and therefore generally less desirable than a direct monetary sanction. However, where the convicted organization possesses knowledge, facilities, or skills that uniquely qualify it to repair damage caused by the offense, community service directed at repairing damage may provide an efficient means of remedying harm caused.

In the past, some forms of community service imposed on organizations have not been related to the purposes of sentencing. Requiring a defendant to endow a chair at a university or to contribute to a local charity would not be consistent with this section unless such community service provided a means for preventive or corrective action directly related to the offense and therefore served one of the purposes of sentencing set forth in 18 U.S.C. § 3553(a).

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---



---

**§8B1.4. Order of Notice to Victims — Organizations**


---

Apply §5F1.4 (Order of Notice to Victims).

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

\* \* \* \* \*

**2. EFFECTIVE COMPLIANCE AND ETHICS PROGRAM**

<i>Historical Note</i>	Effective November 1, 2004 (amendment 673).
------------------------	---

---

**§8B2.1. Effective Compliance and Ethics Program**


---

- (a) To have an effective compliance and ethics program, for purposes of subsection (f) of §8C2.5 (Culpability Score) and subsection (b)(1) of §8D1.4 (Recommended Conditions of Probation — Organizations), an organization shall—
  - (1) exercise due diligence to prevent and detect criminal conduct; and
  - (2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

Such compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct. The failure to prevent or detect the instant offense does not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct.

- (b) Due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law within the meaning of subsection (a) minimally require the following:
  - (1) The organization shall establish standards and procedures to prevent and detect criminal conduct.
  - (2) (A) The organization's governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the

implementation and effectiveness of the compliance and ethics program.

- (B) High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program, as described in this guideline. Specific individual(s) within high-level personnel shall be assigned overall responsibility for the compliance and ethics program.
- (C) Specific individual(s) within the organization shall be delegated day-to-day operational responsibility for the compliance and ethics program. Individual(s) with operational responsibility shall report periodically to high-level personnel and, as appropriate, to the governing authority, or an appropriate subgroup of the governing authority, on the effectiveness of the compliance and ethics program. To carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority.
- (3) The organization shall use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.
- (4) (A) The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.
- (B) The individuals referred to in subparagraph (A) are the members of the governing authority, high-level personnel, substantial authority personnel, the organization's employees, and, as appropriate, the organization's agents.
- (5) The organization shall take reasonable steps—
  - (A) to ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;
  - (B) to evaluate periodically the effectiveness of the organization's compliance and ethics program; and

- (C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization’s employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.
- (6) The organization’s compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.
- (7) After criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization’s compliance and ethics program.
- (c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.

#### Commentary

##### Application Notes:

##### 1. **Definitions.**—For purposes of this guideline:

**“Compliance and ethics program”** means a program designed to prevent and detect criminal conduct.

**“Governing authority”** means the (A) the Board of Directors; or (B) if the organization does not have a Board of Directors, the highest-level governing body of the organization.

**“High-level personnel of the organization”** and **“substantial authority personnel”** have the meaning given those terms in the Commentary to §8A1.2 (Application Instructions — Organizations).

**“Standards and procedures”** means standards of conduct and internal controls that are reasonably capable of reducing the likelihood of criminal conduct.

##### 2. **Factors to Consider in Meeting Requirements of this Guideline.**—

- (A) **In General.**—Each of the requirements set forth in this guideline shall be met by an organization; however, in determining what specific actions are necessary to meet those requirements, factors that shall be considered include: (i) applicable industry practice or the standards called for by any applicable governmental regulation; (ii) the size of the organization; and (iii) similar misconduct.

(B) **Applicable Governmental Regulation and Industry Practice.**—An organization’s failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective compliance and ethics program.

(C) **The Size of the Organization.**—

- (i) **In General.**—The formality and scope of actions that an organization shall take to meet the requirements of this guideline, including the necessary features of the organization’s standards and procedures, depend on the size of the organization.
- (ii) **Large Organizations.**—A large organization generally shall devote more formal operations and greater resources in meeting the requirements of this guideline than shall a small organization. As appropriate, a large organization should encourage small organizations (especially those that have, or seek to have, a business relationship with the large organization) to implement effective compliance and ethics programs.
- (iii) **Small Organizations.**—In meeting the requirements of this guideline, small organizations shall demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations. However, a small organization may meet the requirements of this guideline with less formality and fewer resources than would be expected of large organizations. In appropriate circumstances, reliance on existing resources and simple systems can demonstrate a degree of commitment that, for a large organization, would only be demonstrated through more formally planned and implemented systems.

Examples of the informality and use of fewer resources with which a small organization may meet the requirements of this guideline include the following: (I) the governing authority’s discharge of its responsibility for oversight of the compliance and ethics program by directly managing the organization’s compliance and ethics efforts; (II) training employees through informal staff meetings, and monitoring through regular “walk-arounds” or continuous observation while managing the organization; (III) using available personnel, rather than employing separate staff, to carry out the compliance and ethics program; and (IV) modeling its own compliance and ethics program on existing, well-regarded compliance and ethics programs and best practices of other similar organizations.

(D) **Recurrence of Similar Misconduct.**—Recurrence of similar misconduct creates doubt regarding whether the organization took reasonable steps to meet the requirements of this guideline. For purposes of this subparagraph, “*similar misconduct*” has the meaning given that term in the Commentary to §8A1.2 (Application Instructions — Organizations).

3. **Application of Subsection (b)(2).**—High-level personnel and substantial authority personnel of the organization shall be knowledgeable about the content and operation of the compliance and ethics program, shall perform their assigned duties consistent with the exercise of due diligence, and shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

If the specific individual(s) assigned overall responsibility for the compliance and ethics program does not have day-to-day operational responsibility for the program, then the individual(s) with day-to-day operational responsibility for the program typically should, no less than annually,

give the governing authority or an appropriate subgroup thereof information on the implementation and effectiveness of the compliance and ethics program.

4. **Application of Subsection (b)(3).—**

- (A) **Consistency with Other Law.**—Nothing in subsection (b)(3) is intended to require conduct inconsistent with any Federal, State, or local law, including any law governing employment or hiring practices.
- (B) **Implementation.**—In implementing subsection (b)(3), the organization shall hire and promote individuals so as to ensure that all individuals within the high-level personnel and substantial authority personnel of the organization will perform their assigned duties in a manner consistent with the exercise of due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law under subsection (a). With respect to the hiring or promotion of such individuals, an organization shall consider the relatedness of the individual’s illegal activities and other misconduct (*i.e.*, other conduct inconsistent with an effective compliance and ethics program) to the specific responsibilities the individual is anticipated to be assigned and other factors such as: (i) the recency of the individual’s illegal activities and other misconduct; and (ii) whether the individual has engaged in other such illegal activities and other such misconduct.

5. **Application of Subsection (b)(6).**—Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

6. **Application of Subsection (b)(7).**—Subsection (b)(7) has two aspects.

First, the organization should respond appropriately to the criminal conduct. The organization should take reasonable steps, as warranted under the circumstances, to remedy the harm resulting from the criminal conduct. These steps may include, where appropriate, providing restitution to identifiable victims, as well as other forms of remediation. Other reasonable steps to respond appropriately to the criminal conduct may include self-reporting and cooperation with authorities.

Second, the organization should act appropriately to prevent further similar criminal conduct, including assessing the compliance and ethics program and making modifications necessary to ensure the program is effective. The steps taken should be consistent with subsections (b)(5) and (c) and may include the use of an outside professional advisor to ensure adequate assessment and implementation of any modifications.

7. **Application of Subsection (c).**—To meet the requirements of subsection (c), an organization shall:

- (A) Assess periodically the risk that criminal conduct will occur, including assessing the following:
  - (i) The nature and seriousness of such criminal conduct.
  - (ii) The likelihood that certain criminal conduct may occur because of the nature of the organization’s business. If, because of the nature of an organization’s business, there is a substantial risk that certain types of criminal conduct may occur, the organization shall take reasonable steps to prevent and detect that type of criminal conduct. For example, an organization that, due to the nature of its business, employs sales per-

## §8B2.1

sonnel who have flexibility to set prices shall establish standards and procedures designed to prevent and detect price-fixing. An organization that, due to the nature of its business, employs sales personnel who have flexibility to represent the material characteristics of a product shall establish standards and procedures designed to prevent and detect fraud.

- (iii) The prior history of the organization. The prior history of an organization may indicate types of criminal conduct that it shall take actions to prevent and detect.
- (B) Prioritize periodically, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b), in order to focus on preventing and detecting the criminal conduct identified under subparagraph (A) of this note as most serious, and most likely, to occur.
- (C) Modify, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b) to reduce the risk of criminal conduct identified under subparagraph (A) of this note as most serious, and most likely, to occur.

**Background:** This section sets forth the requirements for an effective compliance and ethics program. This section responds to section 805(a)(5) of the Sarbanes–Oxley Act of 2002, Public Law 107–204, which directed the Commission to review and amend, as appropriate, the guidelines and related policy statements to ensure that the guidelines that apply to organizations in this chapter “are sufficient to deter and punish organizational criminal misconduct.”

The requirements set forth in this guideline are intended to achieve reasonable prevention and detection of criminal conduct for which the organization would be vicariously liable. The prior diligence of an organization in seeking to prevent and detect criminal conduct has a direct bearing on the appropriate penalties and probation terms for the organization if it is convicted and sentenced for a criminal offense.

*Historical  
Note*

Effective November 1, 2004 (amendment 673). Amended effective November 1, 2010 (amendment 744); November 1, 2011 (amendment 758); November 1, 2013 (amendment 778).

## PART C — FINES

### 1. DETERMINING THE FINE — CRIMINAL PURPOSE ORGANIZATIONS

---

#### §8C1.1. Determining the Fine — Criminal Purpose Organizations

---

If, upon consideration of the nature and circumstances of the offense and the history and characteristics of the organization, the court determines that the organization operated primarily for a criminal purpose or primarily by criminal means, the fine shall be set at an amount (subject to the statutory maximum) sufficient to divest the organization of all its net assets. When this section applies, Subpart 2 (Determining the Fine — Other Organizations) and §8C3.4 (Fines Paid by Owners of Closely Held Organizations) do not apply.

#### Commentary

##### Application Note:

1. “**Net assets**,” as used in this section, means the assets remaining after payment of all legitimate claims against assets by known innocent bona fide creditors.

**Background:** This guideline addresses the case in which the court, based upon an examination of the nature and circumstances of the offense and the history and characteristics of the organization, determines that the organization was operated primarily for a criminal purpose (*e.g.*, a front for a scheme that was designed to commit fraud; an organization established to participate in the illegal manufacture, importation, or distribution of a controlled substance) or operated primarily by criminal means (*e.g.*, a hazardous waste disposal business that had no legitimate means of disposing of hazardous waste). In such a case, the fine shall be set at an amount sufficient to remove all of the organization’s net assets. If the extent of the assets of the organization is unknown, the maximum fine authorized by statute should be imposed, absent innocent bona fide creditors.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

\* \* \* \* \*

### 2. DETERMINING THE FINE — OTHER ORGANIZATIONS

---

#### §8C2.1. Applicability of Fine Guidelines

---

The provisions of §§8C2.2 through 8C2.9 apply to each count for which the applicable guideline offense level is determined under:

- (a) §§2B1.1, 2B1.4, 2B2.3, 2B4.1, 2B5.3, 2B6.1;  
§§2C1.1, 2C1.2;  
§§2D1.7, 2D3.1, 2D3.2;

## §8C2.2

§§2E3.1, 2E4.1, 2E5.1, 2E5.3;  
§2G3.1;  
§§2K1.1, 2K2.1;  
§2L1.1;  
§2N3.1;  
§2R1.1;  
§§2S1.1, 2S1.3;  
§§2T1.1, 2T1.4, 2T1.6, 2T1.7, 2T1.8, 2T1.9, 2T2.1, 2T2.2, 2T3.1; or

- (b) §§2E1.1, 2X1.1, 2X2.1, 2X3.1, 2X4.1, with respect to cases in which the offense level for the underlying offense is determined under one of the guideline sections listed in subsection (a) above.

### Commentary

#### Application Notes:

1. If the Chapter Two offense guideline for a count is listed in subsection (a) or (b) above, and the applicable guideline results in the determination of the offense level by use of one of the listed guidelines, apply the provisions of §§8C2.2 through 8C2.9 to that count. For example, §§8C2.2 through 8C2.9 apply to an offense under §2K2.1 (an offense guideline listed in subsection (a)), unless the cross reference in that guideline requires the offense level to be determined under an offense guideline section not listed in subsection (a).
2. If the Chapter Two offense guideline for a count is not listed in subsection (a) or (b) above, but the applicable guideline results in the determination of the offense level by use of a listed guideline, apply the provisions of §§8C2.2 through 8C2.9 to that count. For example, where the conduct set forth in a count of conviction ordinarily referenced to §2N2.1 (an offense guideline not listed in subsection (a)) establishes §2B1.1 (Theft, Property Destruction, and Fraud) as the applicable offense guideline (an offense guideline listed in subsection (a)), §§8C2.2 through 8C2.9 would apply because the actual offense level is determined under §2B1.1 (Theft, Property Destruction, and Fraud).

**Background:** The fine guidelines of this subpart apply only to offenses covered by the guideline sections set forth in subsection (a) above. For example, the provisions of §§8C2.2 through 8C2.9 do not apply to counts for which the applicable guideline offense level is determined under Chapter Two, Part Q (Offenses Involving the Environment). For such cases, §8C2.10 (Determining the Fine for Other Counts) is applicable.

*Historical  
Note*

Effective November 1, 1991 (amendment 422). Amended effective November 1, 1992 (amendment 453); November 1, 1993 (amendment 496); November 1, 2001 (amendments 617, 619, and 634); November 1, 2005 (amendment 679); November 1, 2018 (amendment 813).

---

## §8C2.2. Preliminary Determination of Inability to Pay Fine

---

- (a) Where it is readily ascertainable that the organization cannot and is not likely to become able (even on an installment schedule) to pay restitution required under §8B1.1 (Restitution — Organizations), a determination of



the guideline fine range is unnecessary because, pursuant to §8C3.3(a), no fine would be imposed.

- (b) Where it is readily ascertainable through a preliminary determination of the minimum of the guideline fine range (*see* §§8C2.3 through 8C2.7) that the organization cannot and is not likely to become able (even on an installment schedule) to pay such minimum guideline fine, a further determination of the guideline fine range is unnecessary. Instead, the court may use the preliminary determination and impose the fine that would result from the application of §8C3.3 (Reduction of Fine Based on Inability to Pay).

#### Commentary

##### Application Notes:

1. In a case of a determination under subsection (a), a statement that “the guideline fine range was not determined because it is readily ascertainable that the defendant cannot and is not likely to become able to pay restitution” is recommended.
2. In a case of a determination under subsection (b), a statement that “no precise determination of the guideline fine range is required because it is readily ascertainable that the defendant cannot and is not likely to become able to pay the minimum of the guideline fine range” is recommended.

**Background:** Many organizational defendants lack the ability to pay restitution. In addition, many organizational defendants who may be able to pay restitution lack the ability to pay the minimum fine called for by §8C2.7(a). In such cases, a complete determination of the guideline fine range may be a needless exercise. This section provides for an abbreviated determination of the guideline fine range that can be applied where it is readily ascertainable that the fine within the guideline fine range determined under §8C2.7 (Guideline Fine Range — Organizations) would be reduced under §8C3.3 (Reduction of Fine Based on Inability to Pay).

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

### §8C2.3. Offense Level

---

- (a) For each count covered by §8C2.1 (Applicability of Fine Guidelines), use the applicable Chapter Two guideline to determine the base offense level and apply, in the order listed, any appropriate adjustments contained in that guideline.
- (b) Where there is more than one such count, apply Chapter Three, Part D (Multiple Counts) to determine the combined offense level.

## §8C2.4

### Commentary

#### Application Notes:

1. In determining the offense level under this section, “*defendant*,” as used in Chapter Two, includes any agent of the organization for whose conduct the organization is criminally responsible.
2. In determining the offense level under this section, apply the provisions of §§1B1.2 through 1B1.8. Do not apply the adjustments in Chapter Three, Parts A (Victim-Related Adjustments), B (Role in the Offense), C (Obstruction and Related Adjustments), and E (Acceptance of Responsibility).

*Historical  
Note*

Effective November 1, 1991 (amendment 422). Amended effective November 1, 2011 (amendment 758).

---

### §8C2.4. Base Fine

---

- (a) The base fine is the greatest of:
- (1) the amount from the table in subsection (d) below corresponding to the offense level determined under §8C2.3 (Offense Level); or
  - (2) the pecuniary gain to the organization from the offense; or
  - (3) the pecuniary loss from the offense caused by the organization, to the extent the loss was caused intentionally, knowingly, or recklessly.
- (b) *Provided*, that if the applicable offense guideline in Chapter Two includes a special instruction for organizational fines, that special instruction shall be applied, as appropriate.
- (c) *Provided, further*, that to the extent the calculation of either pecuniary gain or pecuniary loss would unduly complicate or prolong the sentencing process, that amount, *i.e.*, gain or loss as appropriate, shall not be used for the determination of the base fine.

- (d) OFFENSE LEVEL FINE TABLE

Offense Level	Amount
6 or less	\$8,500
7	\$15,000
8	\$15,000
9	\$25,000
10	\$35,000
11	\$50,000
12	\$70,000
13	\$100,000

14	\$150,000
15	\$200,000
16	\$300,000
17	\$450,000
18	\$600,000
19	\$850,000
20	\$1,000,000
21	\$1,500,000
22	\$2,000,000
23	\$3,000,000
24	\$3,500,000
25	\$5,000,000
26	\$6,500,000
27	\$8,500,000
28	\$10,000,000
29	\$15,000,000
30	\$20,000,000
31	\$25,000,000
32	\$30,000,000
33	\$40,000,000
34	\$50,000,000
35	\$65,000,000
36	\$80,000,000
37	\$100,000,000
38 or more	\$150,000,000.

## (e) Special Instruction

- (1) For offenses committed prior to November 1, 2015, use the offense level fine table that was set forth in the version of §8C2.4(d) that was in effect on November 1, 2014, rather than the offense level fine table set forth in subsection (d) above.

## Commentary

## Application Notes:

1. “*Pecuniary gain*,” “*pecuniary loss*,” and “*offense*” are defined in the Commentary to §8A1.2 (Application Instructions — Organizations). Note that subsections (a)(2) and (a)(3) contain certain limitations as to the use of pecuniary gain and pecuniary loss in determining the base fine. Under subsection (a)(2), the pecuniary gain used to determine the base fine is the pecuniary gain to the organization from the offense. Under subsection (a)(3), the pecuniary loss used to determine the base fine is the pecuniary loss from the offense caused by the organization, to the extent that such loss was caused intentionally, knowingly, or recklessly.
2. Under 18 U.S.C. § 3571(d), the court is not required to calculate pecuniary loss or pecuniary gain to the extent that determination of loss or gain would unduly complicate or prolong the sentencing process. Nevertheless, the court may need to approximate loss in order to calculate offense levels under Chapter Two. See Commentary to §2B1.1 (Theft, Property Destruction, and Fraud).

## §8C2.4

If loss is approximated for purposes of determining the applicable offense level, the court should use that approximation as the starting point for calculating pecuniary loss under this section.

3. In a case of an attempted offense or a conspiracy to commit an offense, pecuniary loss and pecuniary gain are to be determined in accordance with the principles stated in §2X1.1 (Attempt, Solicitation, or Conspiracy).
4. In a case involving multiple participants (*i.e.*, multiple organizations, or the organization and individual(s) unassociated with the organization), the applicable offense level is to be determined without regard to apportionment of the gain from or loss caused by the offense. *See* §1B1.3 (Relevant Conduct). However, if the base fine is determined under subsections (a)(2) or (a)(3), the court may, as appropriate, apportion gain or loss considering the defendant's relative culpability and other pertinent factors. Note also that under §2R1.1(d)(1), the volume of commerce, which is used in determining a proxy for loss under §8C2.4(a)(3), is limited to the volume of commerce attributable to the defendant.
5. Special instructions regarding the determination of the base fine are contained in §§2B4.1 (Bribery in Procurement of Bank Loan and Other Commercial Bribery); 2C1.1 (Offering, Giving, Soliciting, or Receiving a Bribe; Extortion Under Color of Official Right; Fraud Involving the Deprivation of the Intangible Right to Honest Services of Public Officials; Conspiracy to Defraud by Interference with Governmental Functions); 2C1.2 (Offering, Giving, Soliciting, or Receiving a Gratuity); 2E5.1 (Offering, Accepting, or Soliciting a Bribe or Gratuity Affecting the Operation of an Employee Welfare or Pension Benefit Plan; Prohibited Payments or Lending of Money by Employer or Agent to Employees, Representatives, or Labor Organizations); and 2R1.1 (Bid-Rigging, Price-Fixing or Market-Allocation Agreements Among Competitors).

**Background:** Under this section, the base fine is determined in one of three ways: (1) by the amount, based on the offense level, from the table in subsection (d); (2) by the pecuniary gain to the organization from the offense; and (3) by the pecuniary loss caused by the organization, to the extent that such loss was caused intentionally, knowingly, or recklessly. In certain cases, special instructions for determining the loss or offense level amount apply. As a general rule, the base fine measures the seriousness of the offense. The determinants of the base fine are selected so that, in conjunction with the multipliers derived from the culpability score in §8C2.5 (Culpability Score), they will result in guideline fine ranges appropriate to deter organizational criminal conduct and to provide incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct. In order to deter organizations from seeking to obtain financial reward through criminal conduct, this section provides that, when greatest, pecuniary gain to the organization is used to determine the base fine. In order to ensure that organizations will seek to prevent losses intentionally, knowingly, or recklessly caused by their agents, this section provides that, when greatest, pecuniary loss is used to determine the base fine in such circumstances. Chapter Two provides special instructions for fines that include specific rules for determining the base fine in connection with certain types of offenses in which the calculation of loss or gain is difficult, *e.g.*, price-fixing. For these offenses, the special instructions tailor the base fine to circumstances that occur in connection with such offenses and that generally relate to the magnitude of loss or gain resulting from such offenses.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422). Amended effective November 1, 1993 (amendment 496); November 1, 1995 (amendment 534); November 1, 2001 (amendment 634); November 1, 2004 (amendments 666 and 673); November 1, 2015 (amendment 791).
----------------------------	--

---

**§8C2.5. Culpability Score**


---

(a) Start with **5** points and apply subsections (b) through (g) below.

(b) INVOLVEMENT IN OR TOLERANCE OF CRIMINAL ACTIVITY

If more than one applies, use the greatest:

(1) If—

(A) the organization had 5,000 or more employees and

(i) an individual within high-level personnel of the organization participated in, condoned, or was willfully ignorant of the offense; or

(ii) tolerance of the offense by substantial authority personnel was pervasive throughout the organization; or

(B) the unit of the organization within which the offense was committed had 5,000 or more employees and

(i) an individual within high-level personnel of the unit participated in, condoned, or was willfully ignorant of the offense; or

(ii) tolerance of the offense by substantial authority personnel was pervasive throughout such unit,

add **5** points; or

(2) If—

(A) the organization had 1,000 or more employees and

(i) an individual within high-level personnel of the organization participated in, condoned, or was willfully ignorant of the offense; or

(ii) tolerance of the offense by substantial authority personnel was pervasive throughout the organization; or

(B) the unit of the organization within which the offense was committed had 1,000 or more employees and

## §8C2.5

- (i) an individual within high-level personnel of the unit participated in, condoned, or was willfully ignorant of the offense; or
- (ii) tolerance of the offense by substantial authority personnel was pervasive throughout such unit,

add 4 points; or

(3) If—

(A) the organization had 200 or more employees and

- (i) an individual within high-level personnel of the organization participated in, condoned, or was willfully ignorant of the offense; or
- (ii) tolerance of the offense by substantial authority personnel was pervasive throughout the organization; or

(B) the unit of the organization within which the offense was committed had 200 or more employees and

- (i) an individual within high-level personnel of the unit participated in, condoned, or was willfully ignorant of the offense; or
- (ii) tolerance of the offense by substantial authority personnel was pervasive throughout such unit,

add 3 points; or

- (4) If the organization had 50 or more employees and an individual within substantial authority personnel participated in, condoned, or was willfully ignorant of the offense, add 2 points; or
- (5) If the organization had 10 or more employees and an individual within substantial authority personnel participated in, condoned, or was willfully ignorant of the offense, add 1 point.

(c) PRIOR HISTORY

If more than one applies, use the greater:

- (1) If the organization (or separately managed line of business) committed any part of the instant offense less than 10 years after (A) a crim-

inal adjudication based on similar misconduct; or (B) civil or administrative adjudication(s) based on two or more separate instances of similar misconduct, add **1** point; or

- (2) If the organization (or separately managed line of business) committed any part of the instant offense less than 5 years after (A) a criminal adjudication based on similar misconduct; or (B) civil or administrative adjudication(s) based on two or more separate instances of similar misconduct, add **2** points.

(d) VIOLATION OF AN ORDER

If more than one applies, use the greater:

- (1) (A) If the commission of the instant offense violated a judicial order or injunction, other than a violation of a condition of probation; or (B) if the organization (or separately managed line of business) violated a condition of probation by engaging in similar misconduct, *i.e.*, misconduct similar to that for which it was placed on probation, add **2** points; or
- (2) If the commission of the instant offense violated a condition of probation, add **1** point.

(e) OBSTRUCTION OF JUSTICE

If the organization willfully obstructed or impeded, attempted to obstruct or impede, or aided, abetted, or encouraged obstruction of justice during the investigation, prosecution, or sentencing of the instant offense, or, with knowledge thereof, failed to take reasonable steps to prevent such obstruction or impedance or attempted obstruction or impedance, add **3** points.

(f) EFFECTIVE COMPLIANCE AND ETHICS PROGRAM

- (1) If the offense occurred even though the organization had in place at the time of the offense an effective compliance and ethics program, as provided in §8B2.1 (Effective Compliance and Ethics Program), subtract **3** points.
- (2) Subsection (f)(1) shall not apply if, after becoming aware of an offense, the organization unreasonably delayed reporting the offense to appropriate governmental authorities.
- (3) (A) Except as provided in subparagraphs (B) and (C), subsection (f)(1) shall not apply if an individual within high-level personnel of the organization, a person within high-level personnel

of the unit of the organization within which the offense was committed where the unit had 200 or more employees, or an individual described in §8B2.1(b)(2)(B) or (C), participated in, condoned, or was willfully ignorant of the offense.

(B) There is a rebuttable presumption, for purposes of subsection (f)(1), that the organization did not have an effective compliance and ethics program if an individual—

- (i) within high-level personnel of a small organization; or
- (ii) within substantial authority personnel, but not within high-level personnel, of any organization,

participated in, condoned, or was willfully ignorant of, the offense.

(C) Subparagraphs (A) and (B) shall not apply if—

- (i) the individual or individuals with operational responsibility for the compliance and ethics program (*see* §8B2.1(b)(2)(C)) have direct reporting obligations to the governing authority or an appropriate subgroup thereof (*e.g.*, an audit committee of the board of directors);
- (ii) the compliance and ethics program detected the offense before discovery outside the organization or before such discovery was reasonably likely;
- (iii) the organization promptly reported the offense to appropriate governmental authorities; and
- (iv) no individual with operational responsibility for the compliance and ethics program participated in, condoned, or was willfully ignorant of the offense.

(g) SELF-REPORTING, COOPERATION, AND ACCEPTANCE OF RESPONSIBILITY

If more than one applies, use the greatest:

- (1) If the organization (A) prior to an imminent threat of disclosure or government investigation; and (B) within a reasonably prompt time after becoming aware of the offense, reported the offense to appropriate governmental authorities, fully cooperated in the investigation, and clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct, subtract **5** points; or



- (2) If the organization fully cooperated in the investigation and clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct, subtract **2** points; or
- (3) If the organization clearly demonstrated recognition and affirmative acceptance of responsibility for its criminal conduct, subtract **1** point.

### Commentary

#### Application Notes:

1. **Definitions.**—For purposes of this guideline, “*condoned*”, “*prior criminal adjudication*”, “*similar misconduct*”, “*substantial authority personnel*”, and “*willfully ignorant of the offense*” have the meaning given those terms in Application Note 3 of the Commentary to §8A1.2 (Application Instructions — Organizations).  
  
“*Small Organization*”, for purposes of subsection (f)(3), means an organization that, at the time of the instant offense, had fewer than 200 employees.
2. For purposes of subsection (b), “*unit of the organization*” means any reasonably distinct operational component of the organization. For example, a large organization may have several large units such as divisions or subsidiaries, as well as many smaller units such as specialized manufacturing, marketing, or accounting operations within these larger units. For purposes of this definition, all of these types of units are encompassed within the term “unit of the organization.”
3. “*High-level personnel of the organization*” is defined in the Commentary to §8A1.2 (Application Instructions — Organizations). With respect to a unit with 200 or more employees, “*high-level personnel of a unit of the organization*” means agents within the unit who set the policy for or control that unit. For example, if the managing agent of a unit with 200 employees participated in an offense, three points would be added under subsection (b)(3); if that organization had 1,000 employees and the managing agent of the unit with 200 employees were also within high-level personnel of the organization in its entirety, four points (rather than three) would be added under subsection (b)(2).
4. Pervasiveness under subsection (b) will be case specific and depend on the number, and degree of responsibility, of individuals within substantial authority personnel who participated in, condoned, or were willfully ignorant of the offense. Fewer individuals need to be involved for a finding of pervasiveness if those individuals exercised a relatively high degree of authority. Pervasiveness can occur either within an organization as a whole or within a unit of an organization. For example, if an offense were committed in an organization with 1,000 employees but the tolerance of the offense was pervasive only within a unit of the organization with 200 employees (and no high-level personnel of the organization participated in, condoned, or was willfully ignorant of the offense), three points would be added under subsection (b)(3). If, in the same organization, tolerance of the offense was pervasive throughout the organization as a whole, or an individual within high-level personnel of the organization participated in the offense, four points (rather than three) would be added under subsection (b)(2).
5. A “*separately managed line of business*,” as used in subsections (c) and (d), is a subpart of a for-profit organization that has its own management, has a high degree of autonomy from higher managerial authority, and maintains its own separate books of account. Corporate subsidiaries and divisions frequently are separately managed lines of business. Under subsection (c), in determining the prior history of an organization with separately managed lines of business, only the prior conduct or criminal record of the separately managed line of business involved in the

## §8C2.5

instant offense is to be used. Under subsection (d), in the context of an organization with separately managed lines of business, in making the determination whether a violation of a condition of probation involved engaging in similar misconduct, only the prior misconduct of the separately managed line of business involved in the instant offense is to be considered.

6. Under subsection (c), in determining the prior history of an organization or separately managed line of business, the conduct of the underlying economic entity shall be considered without regard to its legal structure or ownership. For example, if two companies merged and became separate divisions and separately managed lines of business within the merged company, each division would retain the prior history of its predecessor company. If a company reorganized and became a new legal entity, the new company would retain the prior history of the predecessor company. In contrast, if one company purchased the physical assets but not the ongoing business of another company, the prior history of the company selling the physical assets would not be transferred to the company purchasing the assets. However, if an organization is acquired by another organization in response to solicitations by appropriate federal government officials, the prior history of the acquired organization shall not be attributed to the acquiring organization.
7. Under subsections (c)(1)(B) and (c)(2)(B), the civil or administrative adjudication(s) must have occurred within the specified period (ten or five years) of the instant offense.
8. Adjust the culpability score for the factors listed in subsection (e) whether or not the offense guideline incorporates that factor, or that factor is inherent in the offense.
9. Subsection (e) applies where the obstruction is committed on behalf of the organization; it does not apply where an individual or individuals have attempted to conceal their misconduct from the organization. The Commentary to §3C1.1 (Obstructing or Impeding the Administration of Justice) provides guidance regarding the types of conduct that constitute obstruction.
10. Subsection (f)(2) contemplates that the organization will be allowed a reasonable period of time to conduct an internal investigation. In addition, no reporting is required by subsection (f)(2) or (f)(3)(C)(iii) if the organization reasonably concluded, based on the information then available, that no offense had been committed.
11. For purposes of subsection (f)(3)(C)(i), an individual has “**direct reporting obligations**” to the governing authority or an appropriate subgroup thereof if the individual has express authority to communicate personally to the governing authority or appropriate subgroup thereof (A) promptly on any matter involving criminal conduct or potential criminal conduct, and (B) no less than annually on the implementation and effectiveness of the compliance and ethics program.
12. “**Appropriate governmental authorities**,” as used in subsections (f) and (g)(1), means the federal or state law enforcement, regulatory, or program officials having jurisdiction over such matter. To qualify for a reduction under subsection (g)(1), the report to appropriate governmental authorities must be made under the direction of the organization.
13. To qualify for a reduction under subsection (g)(1) or (g)(2), cooperation must be both timely and thorough. To be timely, the cooperation must begin essentially at the same time as the organization is officially notified of a criminal investigation. To be thorough, the cooperation should include the disclosure of all pertinent information known by the organization. A prime test of whether the organization has disclosed all pertinent information is whether the information is sufficient for law enforcement personnel to identify the nature and extent of the offense and the individual(s) responsible for the criminal conduct. However, the cooperation to be measured is the cooperation of the organization itself, not the cooperation of individuals within the organization. If, because of the lack of cooperation of particular individual(s), neither the organization nor

law enforcement personnel are able to identify the culpable individual(s) within the organization despite the organization's efforts to cooperate fully, the organization may still be given credit for full cooperation.

14. Entry of a plea of guilty prior to the commencement of trial combined with truthful admission of involvement in the offense and related conduct ordinarily will constitute significant evidence of affirmative acceptance of responsibility under subsection (g), unless outweighed by conduct of the organization that is inconsistent with such acceptance of responsibility. This adjustment is not intended to apply to an organization that puts the government to its burden of proof at trial by denying the essential factual elements of guilt, is convicted, and only then admits guilt and expresses remorse. Conviction by trial, however, does not automatically preclude an organization from consideration for such a reduction. In rare situations, an organization may clearly demonstrate an acceptance of responsibility for its criminal conduct even though it exercises its constitutional right to a trial. This may occur, for example, where an organization goes to trial to assert and preserve issues that do not relate to factual guilt (e.g., to make a constitutional challenge to a statute or a challenge to the applicability of a statute to its conduct). In each such instance, however, a determination that an organization has accepted responsibility will be based primarily upon pretrial statements and conduct.
15. In making a determination with respect to subsection (g), the court may determine that the chief executive officer or highest ranking employee of an organization should appear at sentencing in order to signify that the organization has clearly demonstrated recognition and affirmative acceptance of responsibility.

**Background:** The increased culpability scores under subsection (b) are based on three interrelated principles. First, an organization is more culpable when individuals who manage the organization or who have substantial discretion in acting for the organization participate in, condone, or are willfully ignorant of criminal conduct. Second, as organizations become larger and their managements become more professional, participation in, condonation of, or willful ignorance of criminal conduct by such management is increasingly a breach of trust or abuse of position. Third, as organizations increase in size, the risk of criminal conduct beyond that reflected in the instant offense also increases whenever management's tolerance of that offense is pervasive. Because of the continuum of sizes of organizations and professionalization of management, subsection (b) gradually increases the culpability score based upon the size of the organization and the level and extent of the substantial authority personnel involvement.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673); November 1, 2006 (amendment 695); November 1, 2010 (amendment 744).
------------------------	---

---

## §8C2.6. Minimum and Maximum Multipliers

---

Using the culpability score from §8C2.5 (Culpability Score) and applying any applicable special instruction for fines in Chapter Two, determine the applicable minimum and maximum fine multipliers from the table below.

## §8C2.7

CULPABILITY SCORE	MINIMUM MULTIPLIER	MAXIMUM MULTIPLIER
10 or more	2.00	4.00
9	1.80	3.60
8	1.60	3.20
7	1.40	2.80
6	1.20	2.40
5	1.00	2.00
4	0.80	1.60
3	0.60	1.20
2	0.40	0.80
1	0.20	0.40
0 or less	0.05	0.20.

### Commentary

#### Application Note:

1. A special instruction for fines in §2R1.1 (Bid-Rigging, Price-Fixing or Market-Allocation Agreements Among Competitors) sets a floor for minimum and maximum multipliers in cases covered by that guideline.

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

---

## §8C2.7. Guideline Fine Range — Organizations

---

- (a) The minimum of the guideline fine range is determined by multiplying the base fine determined under §8C2.4 (Base Fine) by the applicable minimum multiplier determined under §8C2.6 (Minimum and Maximum Multipliers).
- (b) The maximum of the guideline fine range is determined by multiplying the base fine determined under §8C2.4 (Base Fine) by the applicable maximum multiplier determined under §8C2.6 (Minimum and Maximum Multipliers).

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

---

## §8C2.8. Determining the Fine Within the Range (Policy Statement)

---

- (a) In determining the amount of the fine within the applicable guideline range, the court should consider:

- (1) the need for the sentence to reflect the seriousness of the offense, promote respect for the law, provide just punishment, afford adequate deterrence, and protect the public from further crimes of the organization;
  - (2) the organization's role in the offense;
  - (3) any collateral consequences of conviction, including civil obligations arising from the organization's conduct;
  - (4) any nonpecuniary loss caused or threatened by the offense;
  - (5) whether the offense involved a vulnerable victim;
  - (6) any prior criminal record of an individual within high-level personnel of the organization or high-level personnel of a unit of the organization who participated in, condoned, or was willfully ignorant of the criminal conduct;
  - (7) any prior civil or criminal misconduct by the organization other than that counted under §8C2.5(c);
  - (8) any culpability score under §8C2.5 (Culpability Score) higher than **10** or lower than **0**;
  - (9) partial but incomplete satisfaction of the conditions for one or more of the mitigating or aggravating factors set forth in §8C2.5 (Culpability Score);
  - (10) any factor listed in 18 U.S.C. § 3572(a); and
  - (11) whether the organization failed to have, at the time of the instant offense, an effective compliance and ethics program within the meaning of §8B2.1 (Effective Compliance and Ethics Program).
- (b) In addition, the court may consider the relative importance of any factor used to determine the range, including the pecuniary loss caused by the offense, the pecuniary gain from the offense, any specific offense characteristic used to determine the offense level, and any aggravating or mitigating factor used to determine the culpability score.

#### Commentary

#### Application Notes:

1. Subsection (a)(2) provides that the court, in setting the fine within the guideline fine range, should consider the organization's role in the offense. This consideration is particularly appropriate if the guideline fine range does not take the organization's role in the offense into account.

## §8C2.8

For example, the guideline fine range in an antitrust case does not take into consideration whether the organization was an organizer or leader of the conspiracy. A higher fine within the guideline fine range ordinarily will be appropriate for an organization that takes a leading role in such an offense.

2. Subsection (a)(3) provides that the court, in setting the fine within the guideline fine range, should consider any collateral consequences of conviction, including civil obligations arising from the organization's conduct. As a general rule, collateral consequences that merely make victims whole provide no basis for reducing the fine within the guideline range. If criminal and civil sanctions are unlikely to make victims whole, this may provide a basis for a higher fine within the guideline fine range. If punitive collateral sanctions have been or will be imposed on the organization, this may provide a basis for a lower fine within the guideline fine range.
3. Subsection (a)(4) provides that the court, in setting the fine within the guideline fine range, should consider any nonpecuniary loss caused or threatened by the offense. To the extent that nonpecuniary loss caused or threatened (*e.g.*, loss of or threat to human life; psychological injury; threat to national security) by the offense is not adequately considered in setting the guideline fine range, this factor provides a basis for a higher fine within the range. This factor is more likely to be applicable where the guideline fine range is determined by pecuniary loss or gain, rather than by offense level, because the Chapter Two offense levels frequently take actual or threatened nonpecuniary loss into account.
4. Subsection (a)(6) provides that the court, in setting the fine within the guideline fine range, should consider any prior criminal record of an individual within high-level personnel of the organization or within high-level personnel of a unit of the organization. Since an individual within high-level personnel either exercises substantial control over the organization or a unit of the organization or has a substantial role in the making of policy within the organization or a unit of the organization, any prior criminal misconduct of such an individual may be relevant to the determination of the appropriate fine for the organization.
5. Subsection (a)(7) provides that the court, in setting the fine within the guideline fine range, should consider any prior civil or criminal misconduct by the organization other than that counted under §8C2.5(c). The civil and criminal misconduct counted under §8C2.5(c) increases the guideline fine range. Civil or criminal misconduct other than that counted under §8C2.5(c) may provide a basis for a higher fine within the range. In a case involving a pattern of illegality, an upward departure may be warranted.
6. Subsection (a)(8) provides that the court, in setting the fine within the guideline fine range, should consider any culpability score higher than ten or lower than zero. As the culpability score increases above ten, this may provide a basis for a higher fine within the range. Similarly, as the culpability score decreases below zero, this may provide a basis for a lower fine within the range.
7. Under subsection (b), the court, in determining the fine within the range, may consider any factor that it considered in determining the range. This allows for courts to differentiate between cases that have the same offense level but differ in seriousness (*e.g.*, two fraud cases at offense level 12, one resulting in a loss of \$21,000, the other \$40,000). Similarly, this allows for courts to differentiate between two cases that have the same aggravating factors, but in which those factors vary in their intensity (*e.g.*, two cases with upward adjustments to the culpability score under §8C2.5(c)(2) (prior criminal adjudications within 5 years of the commencement of the instant offense, one involving a single conviction, the other involving two or more convictions)).

**Background:** Subsection (a) includes factors that the court is required to consider under 18 U.S.C. §§ 3553(a) and 3572(a) as well as additional factors that the Commission has determined may be relevant in a particular case. A number of factors required for consideration under 18 U.S.C. § 3572(a)

(*e.g.*, pecuniary loss, the size of the organization) are used under the fine guidelines in this subpart to determine the fine range, and therefore are not specifically set out again in subsection (a) of this guideline. In unusual cases, factors listed in this section may provide a basis for departure.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673); November 1, 2015 (amendment 797).
------------------------	---

---

## §8C2.9. Disgorgement

---

The court shall add to the fine determined under §8C2.8 (Determining the Fine Within the Range) any gain to the organization from the offense that has not and will not be paid as restitution or by way of other remedial measures.

### Commentary

#### Application Note:

1. This section is designed to ensure that the amount of any gain that has not and will not be taken from the organization for remedial purposes will be added to the fine. This section typically will apply in cases in which the organization has received gain from an offense but restitution or remedial efforts will not be required because the offense did not result in harm to identifiable victims, *e.g.*, money laundering, obscenity, and regulatory reporting offenses. Money spent or to be spent to remedy the adverse effects of the offense, *e.g.*, the cost to retrofit defective products, should be considered as disgorged gain. If the cost of remedial efforts made or to be made by the organization equals or exceeds the gain from the offense, this section will not apply.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

## §8C2.10. Determining the Fine for Other Counts

---

For any count or counts not covered under §8C2.1 (Applicability of Fine Guidelines), the court should determine an appropriate fine by applying the provisions of 18 U.S.C. §§ 3553 and 3572. The court should determine the appropriate fine amount, if any, to be imposed in addition to any fine determined under §8C2.8 (Determining the Fine Within the Range) and §8C2.9 (Disgorgement).

### Commentary

**Background:** The Commission has not promulgated guidelines governing the setting of fines for counts not covered by §8C2.1 (Applicability of Fine Guidelines). For such counts, the court should determine the appropriate fine based on the general statutory provisions governing sentencing. In cases that have a count or counts not covered by the guidelines in addition to a count or counts covered by the guidelines, the court shall apply the fine guidelines for the count(s) covered by the guidelines, and add any additional amount to the fine, as appropriate, for the count(s) not covered by the guidelines.

## §8C3.1

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

\* \* \* \* \*

### 3. IMPLEMENTING THE SENTENCE OF A FINE

---

#### §8C3.1. Imposing a Fine

---

- (a) Except to the extent restricted by the maximum fine authorized by statute or any minimum fine required by statute, the fine or fine range shall be that determined under §8C1.1 (Determining the Fine — Criminal Purpose Organizations); §8C2.7 (Guideline Fine Range — Organizations) and §8C2.9 (Disgorgement); or §8C2.10 (Determining the Fine for Other Counts), as appropriate.
- (b) Where the minimum guideline fine is greater than the maximum fine authorized by statute, the maximum fine authorized by statute shall be the guideline fine.
- (c) Where the maximum guideline fine is less than a minimum fine required by statute, the minimum fine required by statute shall be the guideline fine.

#### Commentary

**Background:** This section sets forth the interaction of the fines or fine ranges determined under this chapter with the maximum fine authorized by statute and any minimum fine required by statute for the count or counts of conviction. The general statutory provisions governing a sentence of a fine are set forth in 18 U.S.C. § 3571.

When the organization is convicted of multiple counts, the maximum fine authorized by statute may increase. For example, in the case of an organization convicted of three felony counts related to a \$200,000 fraud, the maximum fine authorized by statute will be \$500,000 on each count, for an aggregate maximum authorized fine of \$1,500,000.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

#### §8C3.2. Payment of the Fine — Organizations

---

- (a) If the defendant operated primarily for a criminal purpose or primarily by criminal means, immediate payment of the fine shall be required.



- (b) In any other case, immediate payment of the fine shall be required unless the court finds that the organization is financially unable to make immediate payment or that such payment would pose an undue burden on the organization. If the court permits other than immediate payment, it shall require full payment at the earliest possible date, either by requiring payment on a date certain or by establishing an installment schedule.

Commentary

Application Note:

1. When the court permits other than immediate payment, the period provided for payment shall in no event exceed five years. 18 U.S.C. § 3572(d).

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

**§8C3.3. Reduction of Fine Based on Inability to Pay**

---

- (a) The court shall reduce the fine below that otherwise required by §8C1.1 (Determining the Fine — Criminal Purpose Organizations), or §8C2.7 (Guideline Fine Range — Organizations) and §8C2.9 (Disgorgement), to the extent that imposition of such fine would impair its ability to make restitution to victims.
- (b) The court may impose a fine below that otherwise required by §8C2.7 (Guideline Fine Range — Organizations) and §8C2.9 (Disgorgement) if the court finds that the organization is not able and, even with the use of a reasonable installment schedule, is not likely to become able to pay the minimum fine required by §8C2.7 (Guideline Fine Range — Organizations) and §8C2.9 (Disgorgement).

*Provided*, that the reduction under this subsection shall not be more than necessary to avoid substantially jeopardizing the continued viability of the organization.

Commentary

Application Note:

1. For purposes of this section, an organization is not able to pay the minimum fine if, even with an installment schedule under §8C3.2 (Payment of the Fine — Organizations), the payment of that fine would substantially jeopardize the continued existence of the organization.

**Background:** Subsection (a) carries out the requirement in 18 U.S.C. § 3572(b) that the court impose a fine or other monetary penalty only to the extent that such fine or penalty will not impair the ability of the organization to make restitution for the offense; however, this section does not authorize a criminal purpose organization to remain in business in order to pay restitution.

## §8C3.4

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

### §8C3.4. Fines Paid by Owners of Closely Held Organizations

---

The court may offset the fine imposed upon a closely held organization when one or more individuals, each of whom owns at least a 5 percent interest in the organization, has been fined in a federal criminal proceeding for the same offense conduct for which the organization is being sentenced. The amount of such offset shall not exceed the amount resulting from multiplying the total fines imposed on those individuals by those individuals' total percentage interest in the organization.

#### Commentary

##### Application Notes:

1. For purposes of this section, an organization is closely held, regardless of its size, when relatively few individuals own it. In order for an organization to be closely held, ownership and management need not completely overlap.
2. This section does not apply to a fine imposed upon an individual that arises out of offense conduct different from that for which the organization is being sentenced.

**Background:** For practical purposes, most closely held organizations are the alter egos of their owner-managers. In the case of criminal conduct by a closely held corporation, the organization and the culpable individual(s) both may be convicted. As a general rule in such cases, appropriate punishment may be achieved by offsetting the fine imposed upon the organization by an amount that reflects the percentage ownership interest of the sentenced individuals and the magnitude of the fines imposed upon those individuals. For example, an organization is owned by five individuals, each of whom has a twenty percent interest; three of the individuals are convicted; and the combined fines imposed on those three equals \$100,000. In this example, the fine imposed upon the organization may be offset by up to 60 percent of their combined fine amounts, *i.e.*, by \$60,000.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

\* \* \* \* \*

## 4. DEPARTURES FROM THE GUIDELINE FINE RANGE

#### Introductory Commentary

The statutory provisions governing departures are set forth in 18 U.S.C. § 3553(b). Departure may be warranted if the court finds “that there exists an aggravating or mitigating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines that should result in a sentence different from that described.” This subpart sets forth certain factors that, in connection with certain offenses, may not have been adequately taken

into consideration by the guidelines. In deciding whether departure is warranted, the court should consider the extent to which that factor is adequately taken into consideration by the guidelines and the relative importance or substantiality of that factor in the particular case.

To the extent that any policy statement from Chapter Five, Part K (Departures) is relevant to the organization, a departure from the applicable guideline fine range may be warranted. Some factors listed in Chapter Five, Part K that are particularly applicable to organizations are listed in this subpart. Other factors listed in Chapter Five, Part K may be applicable in particular cases. While this subpart lists factors that the Commission believes may constitute grounds for departure, the list is not exhaustive.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

### §8C4.1. Substantial Assistance to Authorities — Organizations (Policy Statement)

---

- (a) Upon motion of the government stating that the defendant has provided substantial assistance in the investigation or prosecution of another organization that has committed an offense, or in the investigation or prosecution of an individual not directly affiliated with the defendant who has committed an offense, the court may depart from the guidelines.
- (b) The appropriate reduction shall be determined by the court for reasons stated on the record that may include, but are not limited to, consideration of the following:
  - (1) the court's evaluation of the significance and usefulness of the organization's assistance, taking into consideration the government's evaluation of the assistance rendered;
  - (2) the nature and extent of the organization's assistance; and
  - (3) the timeliness of the organization's assistance.

#### Commentary

#### Application Note:

1. Departure under this section is intended for cases in which substantial assistance is provided in the investigation or prosecution of crimes committed by individuals not directly affiliated with the organization or by other organizations. It is not intended for assistance in the investigation or prosecution of the agents of the organization responsible for the offense for which the organization is being sentenced.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

## §8C4.2

---

### §8C4.2. Risk of Death or Bodily Injury (Policy Statement)

---

If the offense resulted in death or bodily injury, or involved a foreseeable risk of death or bodily injury, an upward departure may be warranted. The extent of any such departure should depend, among other factors, on the nature of the harm and the extent to which the harm was intended or knowingly risked, and the extent to which such harm or risk is taken into account within the applicable guideline fine range.

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

---

### §8C4.3. Threat to National Security (Policy Statement)

---

If the offense constituted a threat to national security, an upward departure may be warranted.

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

---

### §8C4.4. Threat to the Environment (Policy Statement)

---

If the offense presented a threat to the environment, an upward departure may be warranted.

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

---

### §8C4.5. Threat to a Market (Policy Statement)

---

If the offense presented a risk to the integrity or continued existence of a market, an upward departure may be warranted. This section is applicable to both private markets (*e.g.*, a financial market, a commodities market, or a market for consumer goods) and public markets (*e.g.*, government contracting).

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

---

**§8C4.6. Official Corruption (Policy Statement)**


---

If the organization, in connection with the offense, bribed or unlawfully gave a gratuity to a public official, or attempted or conspired to bribe or unlawfully give a gratuity to a public official, an upward departure may be warranted.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

**§8C4.7. Public Entity (Policy Statement)**


---

If the organization is a public entity, a downward departure may be warranted.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

**§8C4.8. Members or Beneficiaries of the Organization as Victims (Policy Statement)**


---

If the members or beneficiaries, other than shareholders, of the organization are direct victims of the offense, a downward departure may be warranted. If the members or beneficiaries of an organization are direct victims of the offense, imposing a fine upon the organization may increase the burden upon the victims of the offense without achieving a deterrent effect. In such cases, a fine may not be appropriate. For example, departure may be appropriate if a labor union is convicted of embezzlement of pension funds.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
------------------------	---

---

**§8C4.9. Remedial Costs that Greatly Exceed Gain (Policy Statement)**


---

If the organization has paid or has agreed to pay remedial costs arising from the offense that greatly exceed the gain that the organization received from the offense, a downward departure may be warranted. In such a case, a substantial fine may not be necessary in order to achieve adequate punishment and deterrence. In deciding whether departure is appropriate, the court should consider the level and extent of substantial authority personnel involvement in the offense and the degree to which the loss exceeds the gain. If an individual within high-level personnel was involved in the offense, a departure would not be ap-

## §8C4.10

appropriate under this section. The lower the level and the more limited the extent of substantial authority personnel involvement in the offense, and the greater the degree to which remedial costs exceeded or will exceed gain, the less will be the need for a substantial fine to achieve adequate punishment and deterrence.

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

---

### §8C4.10. Mandatory Programs to Prevent and Detect Violations of Law (Policy Statement)

---

If the organization's culpability score is reduced under §8C2.5(f) (Effective Compliance and Ethics Program) and the organization had implemented its program in response to a court order or administrative order specifically directed at the organization, an upward departure may be warranted to offset, in part or in whole, such reduction.

Similarly, if, at the time of the instant offense, the organization was required by law to have an effective compliance and ethics program, but the organization did not have such a program, an upward departure may be warranted.

*Historical  
Note*

Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673).

---

### §8C4.11. Exceptional Organizational Culpability (Policy Statement)

---

If the organization's culpability score is greater than **10**, an upward departure may be appropriate.

If no individual within substantial authority personnel participated in, condoned, or was willfully ignorant of the offense; the organization at the time of the offense had an effective program to prevent and detect violations of law; and the base fine is determined under §8C2.4(a)(1), §8C2.4(a)(3), or a special instruction for fines in Chapter Two (Offense Conduct), a downward departure may be warranted. In a case meeting these criteria, the court may find that the organization had exceptionally low culpability and therefore a fine based on loss, offense level, or a special Chapter Two instruction results in a guideline fine range higher than necessary to achieve the purposes of sentencing. Nevertheless, such fine should not be lower than if determined under §8C2.4(a)(2).

*Historical  
Note*

Effective November 1, 1991 (amendment 422).

## PART D — ORGANIZATIONAL PROBATION

### Introductory Commentary

Section 8D1.1 sets forth the circumstances under which a sentence to a term of probation is required. Sections 8D1.2 through 8D1.4, and 8F1.1, address the length of the probation term, conditions of probation, and violations of probation conditions.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673).
----------------------------	---

---

### §8D1.1. Imposition of Probation — Organizations

---

- (a) The court shall order a term of probation:
  - (1) if such sentence is necessary to secure payment of restitution (§8B1.1), enforce a remedial order (§8B1.2), or ensure completion of community service (§8B1.3);
  - (2) if the organization is sentenced to pay a monetary penalty (*e.g.*, restitution, fine, or special assessment), the penalty is not paid in full at the time of sentencing, and restrictions are necessary to safeguard the organization's ability to make payments;
  - (3) if, at the time of sentencing, (A) the organization (i) has 50 or more employees, or (ii) was otherwise required under law to have an effective compliance and ethics program; and (B) the organization does not have such a program;
  - (4) if the organization within five years prior to sentencing engaged in similar misconduct, as determined by a prior criminal adjudication, and any part of the misconduct underlying the instant offense occurred after that adjudication;
  - (5) if an individual within high-level personnel of the organization or the unit of the organization within which the instant offense was committed participated in the misconduct underlying the instant offense and that individual within five years prior to sentencing engaged in similar misconduct, as determined by a prior criminal adjudication, and any part of the misconduct underlying the instant offense occurred after that adjudication;
  - (6) if such sentence is necessary to ensure that changes are made within the organization to reduce the likelihood of future criminal conduct;

## §8D1.2

- (7) if the sentence imposed upon the organization does not include a fine;  
or
- (8) if necessary to accomplish one or more of the purposes of sentencing set forth in 18 U.S.C. § 3553(a)(2).

### Commentary

**Background:** Under 18 U.S.C. § 3561(a), an organization may be sentenced to a term of probation. Under 18 U.S.C. § 3551(c), imposition of a term of probation is required if the sentence imposed upon the organization does not include a fine.

*Historical  
Note*

Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673).

---

## §8D1.2. Term of Probation — Organizations

---

- (a) When a sentence of probation is imposed—
  - (1) In the case of a felony, the term of probation shall be at least one year but not more than five years.
  - (2) In any other case, the term of probation shall be not more than five years.

### Commentary

#### Application Note:

1. Within the limits set by the guidelines, the term of probation should be sufficient, but not more than necessary, to accomplish the court's specific objectives in imposing the term of probation. The terms of probation set forth in this section are those provided in 18 U.S.C. § 3561(c).

*Historical  
Note*

Effective November 1, 1991 (amendment 422). Amended effective November 1, 2013 (amendment 778).

---

## §8D1.3. Conditions of Probation — Organizations

---

- (a) Pursuant to 18 U.S.C. § 3563(a)(1), any sentence of probation shall include the condition that the organization not commit another federal, state, or local crime during the term of probation.
- (b) Pursuant to 18 U.S.C. § 3563(a)(2), if a sentence of probation is imposed for a felony, the court shall impose as a condition of probation at least one



of the following: (1) restitution or (2) community service, unless the court has imposed a fine, or unless the court finds on the record that extraordinary circumstances exist that would make such condition plainly unreasonable, in which event the court shall impose one or more other conditions set forth in 18 U.S.C. § 3563(b).

- (c) The court may impose other conditions that (1) are reasonably related to the nature and circumstances of the offense or the history and characteristics of the organization; and (2) involve only such deprivations of liberty or property as are necessary to effect the purposes of sentencing.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422). Amended effective November 1, 1997 (amendment 569); November 1, 2009 (amendment 733).
------------------------	---

---

#### **§8D1.4. Recommended Conditions of Probation — Organizations (Policy Statement)**

---

- (a) The court may order the organization, at its expense and in the format and media specified by the court, to publicize the nature of the offense committed, the fact of conviction, the nature of the punishment imposed, and the steps that will be taken to prevent the recurrence of similar offenses.
- (b) If probation is imposed under §8D1.1, the following conditions may be appropriate:
  - (1) The organization shall develop and submit to the court an effective compliance and ethics program consistent with §8B2.1 (Effective Compliance and Ethics Program). The organization shall include in its submission a schedule for implementation of the compliance and ethics program.
  - (2) Upon approval by the court of a program referred to in paragraph (1), the organization shall notify its employees and shareholders of its criminal behavior and its program referred to in paragraph (1). Such notice shall be in a form prescribed by the court.
  - (3) The organization shall make periodic submissions to the court or probation officer, at intervals specified by the court, (A) reporting on the organization's financial condition and results of business operations, and accounting for the disposition of all funds received, and (B) reporting on the organization's progress in implementing the program referred to in paragraph (1). Among other things, reports under subparagraph (B) shall disclose any criminal prosecution, civil litigation, or administrative proceeding commenced against the organization, or any investigation or formal inquiry by governmental authorities of which the organization learned since its last report.

## §8D1.5

- (4) The organization shall notify the court or probation officer immediately upon learning of (A) any material adverse change in its business or financial condition or prospects, or (B) the commencement of any bankruptcy proceeding, major civil litigation, criminal prosecution, or administrative proceeding against the organization, or any investigation or formal inquiry by governmental authorities regarding the organization.
- (5) The organization shall submit to: (A) a reasonable number of regular or unannounced examinations of its books and records at appropriate business premises by the probation officer or experts engaged by the court; and (B) interrogation of knowledgeable individuals within the organization. Compensation to and costs of any experts engaged by the court shall be paid by the organization.
- (6) The organization shall make periodic payments, as specified by the court, in the following priority: (A) restitution; (B) fine; and (C) any other monetary sanction.

### Commentary

#### Application Note:

1. In determining the conditions to be imposed when probation is ordered under §8D1.1, the court should consider the views of any governmental regulatory body that oversees conduct of the organization relating to the instant offense. To assess the efficacy of a compliance and ethics program submitted by the organization, the court may employ appropriate experts who shall be afforded access to all material possessed by the organization that is necessary for a comprehensive assessment of the proposed program. The court should approve any program that appears reasonably calculated to prevent and detect criminal conduct, as long as it is consistent with §8B2.1 (Effective Compliance and Ethics Program), and any applicable statutory and regulatory requirements.

Periodic reports submitted in accordance with subsection (b)(3) should be provided to any governmental regulatory body that oversees conduct of the organization relating to the instant offense.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422). Amended effective November 1, 2004 (amendment 673); November 1, 2010 (amendment 744).
------------------------	---

---

## §8D1.5. [Deleted]

---

<i>Historical Note</i>	Section 8D1.5 (Violations of Conditions of Probation – Organizations (Policy Statement)), effective November 1, 1991 (amendment 422), was moved to §8F1.1 effective November 1, 2004 (amendment 673).
------------------------	---

## PART E — SPECIAL ASSESSMENTS, FORFEITURES, AND COSTS

### §8E1.1. Special Assessments — Organizations

A special assessment must be imposed on an organization in the amount prescribed by statute.

#### Commentary

#### Application Notes:

1. This guideline applies if the defendant is an organization. It does not apply if the defendant is an individual. *See* §5E1.3 for special assessments applicable to individuals.
2. The following special assessments are provided by statute (*see* 18 U.S.C. § 3013):

#### FOR OFFENSES COMMITTED BY ORGANIZATIONS ON OR AFTER APRIL 24, 1996:

- (A) \$400, if convicted of a felony;
- (B) \$125, if convicted of a Class A misdemeanor;
- (C) \$50, if convicted of a Class B misdemeanor; or
- (D) \$25, if convicted of a Class C misdemeanor or an infraction.

#### FOR OFFENSES COMMITTED BY ORGANIZATIONS ON OR AFTER NOVEMBER 18, 1988 BUT PRIOR TO APRIL 24, 1996:

- (E) \$200, if convicted of a felony;
- (F) \$125, if convicted of a Class A misdemeanor;
- (G) \$50, if convicted of a Class B misdemeanor; or
- (H) \$25, if convicted of a Class C misdemeanor or an infraction.

#### FOR OFFENSES COMMITTED BY ORGANIZATIONS PRIOR TO NOVEMBER 18, 1988:

- (I) \$200, if convicted of a felony;
- (J) \$100, if convicted of a misdemeanor.

3. A special assessment is required by statute for each count of conviction.

**Background:** Section 3013 of Title 18, United States Code, added by The Victims of Crimes Act of 1984, Pub. L. No. 98-473, Title II, Chap. XIV, requires courts to impose special assessments on convicted defendants for the purpose of funding the Crime Victims Fund established by the same legislation.

#### Historical Note

Effective November 1, 1991 (amendment 422); November 1, 1997 (amendment 573).

### §8E1.2. Forfeiture — Organizations

Apply §5E1.4 (Forfeiture).

## §8E1.3

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
----------------------------	---

---

### §8E1.3. Assessment of Costs – Organizations

---

As provided in 28 U.S.C. § 1918, the court may order the organization to pay the costs of prosecution. In addition, specific statutory provisions mandate assessment of costs.

<i>Historical Note</i>	Effective November 1, 1991 (amendment 422).
----------------------------	---

## PART F — VIOLATIONS OF PROBATION — ORGANIZATIONS

<i>Historical Note</i>	Effective November 1, 2004 (amendment 673).
------------------------	---

### §8F1.1. Violations of Conditions of Probation — Organizations (Policy Statement)

Upon a finding of a violation of a condition of probation, the court may extend the term of probation, impose more restrictive conditions of probation, or revoke probation and resentence the organization.

#### Commentary

#### Application Notes:

1. **Appointment of Master or Trustee.**—In the event of repeated violations of conditions of probation, the appointment of a master or trustee may be appropriate to ensure compliance with court orders.
2. **Conditions of Probation.**—Mandatory and recommended conditions of probation are specified in §§8D1.3 (Conditions of Probation — Organizations) and 8D1.4 (Recommended Conditions of Probation — Organizations).

<i>Historical Note</i>	Effective November 1, 2004 (amendment 673).
------------------------	---

Resource 4

**U.S. Department of Justice Criminal Division**  
**Evaluation of Corporate Compliance Programs**

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

**Introduction**

The “Principles of Federal Prosecution of Business Organizations” in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include “the adequacy and effectiveness of the corporation’s compliance program at the time of the offense, as well as at the time of a charging decision” and the corporation’s remedial efforts “to implement an adequate and effective corporate compliance program or to improve an existing one.” JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation’s compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company’s risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company’s size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company’s operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three “fundamental questions” a prosecutor should ask:

1. Is the corporation’s compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

3. Does the corporation's compliance program work in practice?

*See JM 9-28.800.*

In answering each of these three “fundamental questions,” prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program both at the time of the offense and at the time of the charging decision and resolution.<sup>1</sup> The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the circumstances of the company.<sup>2</sup> Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

**I. Is the Corporation's Compliance Program Well Designed?**

The critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or permitting employees to engage in misconduct. JM 9-28.800.

Accordingly, prosecutors should examine the comprehensiveness of the compliance program, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

**A. Risk Assessment**

The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks. In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.

Prosecutors should consider whether the program is appropriately “designed to detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business” and “complex regulatory environment[.]” JM 9-28.800.<sup>3</sup> For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.



**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

Prosecutors should also consider “[t]he effectiveness of the company’s risk assessment and the manner in which the company’s compliance program has been tailored based on that risk assessment” and whether its criteria are “periodically updated.” *See, e.g.*, JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c) (“the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct”).

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. Prosecutors should therefore consider, as an indicator of risk-tailoring, “revisions to corporate compliance programs in light of lessons learned.” JM 9-28.800.

- ☐ **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company’s compliance program?
- ☐ **Risk-Tailored Resource Allocation** – Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?
- ☐ **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a “snapshot” in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?
- ☐ **Lessons Learned** – Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company’s own prior issues or from those of other companies operating in the same industry and/or geographical region?

**B. Policies and Procedures**

Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company’s commitment to full compliance with relevant Federal laws that is accessible and applicable to all

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- ☐ **Design** – What is the company’s process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?
- ☐ **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?
- ☐ **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees’ access? Have the policies and procedures been published in a searchable format for easy reference? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?
- ☐ **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees’ understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company’s internal control systems?
- ☐ **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (*e.g.*, those with approval authority or certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

**C. Training and Communications**

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience’s size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise.

**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

Other companies have invested in shorter, more targeted training sessions to enable employees to timely identify and raise issues to appropriate compliance, internal audit, or other risk management functions. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is “truly effective.” JM 9-28.800.

- ☐ **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?
- ☐ **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company’s rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed employees who fail all or a portion of the testing? Has the company evaluated the extent to which the training has an impact on employee behavior or operations?
- ☐ **Communications about Misconduct** – What has senior management done to let employees know the company’s position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company’s policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?
- ☐ **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

**D. Confidential Reporting Structure and Investigation Process**

Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company’s code of conduct, company policies, or suspected or actual

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has established corporate governance mechanisms that can effectively detect and prevent misconduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- ☐ **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism and, if not, why not? How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used? Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?
- ☐ **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?
- ☐ **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?
- ☐ **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? Does the company periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?

**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

**E. Third Party Management**

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.

In sum, a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business." JM 9-28.800.

- ☐ **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?
- ☐ **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?
- ☐ **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third-party relationship managers

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

- ☐ **Real Actions and Consequences** – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company’s due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

**F. Mergers and Acquisitions (M&A)**

A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target’s value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business’s profitability and reputation and risking civil and criminal liability.

The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

- ☐ **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?
- ☐ **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?
- ☐ **Process Connecting Due Diligence to Implementation** – What has been the company’s process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company’s process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities?

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

**II. Is the Corporation’s Compliance Program Adequately Resourced and Empowered to Function Effectively?**

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a “paper program” or one implemented, resourced, reviewed, and revised, as appropriate, in an effective manner. JM 9-28.800. In this regard, prosecutors should evaluate a corporation’s method for assessing and addressing applicable risks and designing appropriate controls to manage these risks. In addition, prosecutors should determine whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation’s compliance efforts. Prosecutors should also determine “whether the corporation’s employees are adequately informed about the compliance program and are convinced of the corporation’s commitment to it.” JM 9-28.800; *see also* JM 9-47.120(2)(c) (criteria for an effective compliance program include “[t]he company’s culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated”).

**A. Commitment by Senior and Middle Management**

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company’s top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company’s ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company’s “*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight” of it; “[h]igh-level personnel ... shall ensure that the organization has an effective compliance and ethics program” (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company’s compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

- ☐ **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (*e.g.*, business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?
- ☐ **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

**B. Autonomy and Resources**

Effective implementation also requires those charged with a compliance program’s day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board’s audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. “A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization.” Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, “a small organization may [rely on] less formality and fewer resources.” *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy, as an indicator of whether compliance personnel are in fact empowered and positioned to effectively detect and prevent misconduct. Prosecutors should also evaluate “[t]he resources the company has dedicated to compliance,” “[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk,” and “[t]he authority and independence of the compliance function and the availability of compliance expertise to the board.” JM 9-47.120(2)(c); *see also* U.S.S.G. § 8B2.1(b)(2)(C) (those with “day-to-day operational responsibility” shall have “adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority”).

- ☐ **Structure** – Where within the company is the compliance function housed (*e.g.*, within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive



**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place? What are the reasons for the structural choices the company has made?

- ☐ **Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company’s strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?
- ☐ **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? How does the company invest in further training and development of the compliance and other control personnel? Who reviews the performance of the compliance function and what is the review process?
- ☐ **Funding and Resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?
- ☐ **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?
- ☐ **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

**C. Compensation Structures and Consequence Management**

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear consequence management procedures (procedures to identify, investigate, discipline and remediate violations of law, regulation, or policy) in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company’s communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) (“the organization’s compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct”).

By way of example, prosecutors may consider whether a company has publicized disciplinary actions internally, where appropriate and possible, which can have valuable deterrent effects. Prosecutors may also consider whether a company is tracking data relating to disciplinary actions to measure effectiveness of the investigation and consequence management functions. This can include monitoring the number of compliance-related allegations that are substantiated, the average (and outlier) times to complete a compliance investigation, and the effectiveness and consistency of disciplinary measures across the levels, geographies, units or departments of an organization.

The design and implementation of compensation schemes play an important role in fostering a compliance culture. Prosecutors may consider whether a company has incentivized compliance by designing compensation systems that defer or escrow certain compensation tied to conduct consistent with company values and policies. Some companies have also enforced contract provisions that permit the company to recoup previously awarded compensation if the recipient of such compensation is found to have engaged in or to be otherwise responsible for corporate wrongdoing. Finally, prosecutors may consider whether provisions for recoupment or reduction of compensation due to compliance violations or misconduct are maintained and enforced in accordance with company policy and applicable laws.

Compensation structures that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance. At the same time,

**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

providing positive incentives, such as promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership, can drive compliance. Prosecutors should examine whether a company has made working on compliance a means of career advancement, offered opportunities for managers and employees to serve as a compliance “champion”, or made compliance a significant metric for management bonuses. In evaluating whether the compensation and consequence management schemes are indicative of a positive compliance culture, prosecutors should consider the following factors:

- ☐ **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? How transparent has the company been with the design and implementation of its disciplinary process? In circumstances where an executive has been exited from the company on account of a compliance violation, how transparent has the company been with employees about the terms of the separation? Are the actual reasons for discipline communicated to employees in all cases? If not, why not? Is the same process followed for each instance of misconduct, and if not, why? Has the company taken steps to restrict disclosure or access to information about the disciplinary process? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?
- ☐ **Disciplinary Measures** – What types of disciplinary actions are available to management when it seeks to enforce compliance policies? Does the company have policies or procedures in place to recoup compensation that would not have been achieved but for misconduct attributable directly or indirectly to the executive or employee? What policies and practices does the company have in place to put employees on notice that they will not benefit from any potential fruits of misconduct? With respect to the particular misconduct at issue, has the company made good faith efforts to follow its policies and practices in this respect?
- ☐ **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency? Are there similar instances of misconduct that were treated disparately, and if so, why? What metrics does the company apply to ensure consistency of disciplinary measures across all geographies, operating units, and levels of the organization?
- ☐ **Financial Incentive System** – Has the company considered the impact of its financial rewards and other incentives on compliance? Has the company evaluated whether commercial targets are achievable if the business operates within a compliant and ethical manner? What role does the compliance function have in designing and awarding financial incentives at senior levels of the organization? How does the company incentivize compliance and ethical behavior? What percentage of executive

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

compensation is structured to encourage enduring ethical business objectives? Are the terms of bonus and deferred compensation subject to cancellation or recoupment, to the extent available under applicable law, in the event that non-compliant or unethical behavior is exposed before or after the award was issued? Does the company have a policy for recouping compensation that has been paid, where there has been misconduct? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied, compensation recouped or deferred compensation cancelled) as a result of compliance and ethics considerations?

- **Effectiveness** – How has the company ensured effective consequence management of compliance violations in practice? What insights can be taken from the management of a company’s hotline that provide indicia of its compliance culture or its management of hotline reports? How do the substantiation rates compare for similar types of reported wrongdoing across the company (*i.e.* between two or more different states, countries, or departments) or compared to similarly situated companies, if known? Has the company undertaken a root cause analysis into areas where certain conduct is comparatively over or under reported? What is the average time for completion of investigations into hotline reports and how are investigations that are addressed inconsistently managed by the responsible department? What percentage of the compensation awarded to executives who have been found to have engaged in wrongdoing has been subject to cancellation or recoupment for ethical violations? Taking into account the relevant laws and local circumstances governing the relevant parts of a compensation scheme, how has the organization sought to enforce breaches of compliance or penalize ethical lapses? How much compensation has in fact been impacted (either positively or negatively) on account of compliance-related activities?

**III. Does the Corporation’s Compliance Program Work in Practice?**

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess “the adequacy and effectiveness of the corporation’s compliance program at the time of the offense, as well as at the time of a charging decision.” JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) (“[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct”). Indeed, “[t]he Department recognizes that no compliance program can prevent all criminal activity by a corporation’s employees.” JM 9-28.800. Of course, if a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

should view the occurrence as a strong indicator that the compliance program was working effectively.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts.

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.

**A. Continuous Improvement, Periodic Testing, and Review**

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47-120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

- ☐ **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?
- ☐ **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?
- ☐ **Culture of Compliance** – How often and how does the company measure its culture of compliance? How does the company’s hiring and incentive structure reinforce its commitment to ethical culture? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management’s commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

**B. Investigation of Misconduct**

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company’s response, including any disciplinary or remediation measures taken.

- ☐ **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?
- ☐ **Response to Investigations** – Have the company’s investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

- **Independence and Empowerment** – Is compensation for employees who are responsible for investigating and adjudicating misconduct structured in a way that ensures the compliance team is empowered to enforce the policies and ethical values of the company? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel or others within the organization that have a role in the disciplinary process generally?

Messaging applications have become ubiquitous in many markets and offer important platforms for companies to achieve growth and facilitate communication. In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications. Policies governing such applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company. Prosecutors should consider how the policies and procedures have been communicated to employees, and whether the corporation has enforced the policies and procedures on a regular and consistent basis in practice. In conducting this evaluation, prosecutors should consider the following factors:

- **Communication Channels** – What electronic communication channels do the company and its employees use, or allow to be used, to conduct business? How does that practice vary by jurisdiction and business function, and why? What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels? What preservation or deletion settings are available to each employee under each communication channel, and what do the company's policies require with respect to each? What is the rationale for the company's approach to determining which communication channels and settings are permitted?
- **Policy Environment** – What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced? What are the relevant code of conduct, privacy, security, and employment laws or policies that govern the organization's ability to ensure security or monitor/access business-related communications? If the company has a "bring your own device" (BYOD) program, what are its policies governing preservation of and access to corporate data and communications stored on personal devices—including data contained within messaging platforms—and what is the rationale behind those policies? How have the company's data retention and business conduct policies been applied and enforced with respect to personal devices and messaging applications? Do the organization's policies permit the company to review business communications on BYOD and/or messaging applications? What exceptions or limitations to these policies have been permitted by

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

the organization? If the company has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto company record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?

- **Risk Management** – What are the consequences for employees who refuse the company access to company communications? Has the company ever exercised these rights? Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications? Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization’s compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies? How does the organization manage security and exercise control over the communication channels used to conduct the organization’s affairs? Is the organization’s approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the company’s business needs and risk profile?

**C. Analysis and Remediation of Any Underlying Misconduct**

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on “the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned.” JM 9-28.800; *see also* JM 9-47.120(3)(c) (“to receive full credit for timely and appropriate remediation” under the FCPA Corporate Enforcement Policy, a company should demonstrate “a root cause analysis” and, where appropriate, “remediation to address the root causes”).

Prosecutors should consider “any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program.” JM 98-28.800; *see also* JM 9-47-120(2)(c) (looking to “[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred” and “any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk”).



**U.S. Department of Justice**  
**Criminal Division**  
**Evaluation of Corporate Compliance Programs**  
**(Updated March 2023)**

- ☐ **Root Cause Analysis** – What is the company’s root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?
- ☐ **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?
- ☐ **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?
- ☐ **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?
- ☐ **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company’s analysis of why such opportunities were missed?
- ☐ **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?
- ☐ **Accountability** – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company’s record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue? Did the company take any actions to recoup or reduce compensation for responsible employees to the extent practicable and available under applicable law?

---

<sup>1</sup> Many of the topics also appear in the following resources:

**U.S. Department of Justice  
Criminal Division  
Evaluation of Corporate Compliance Programs  
(Updated March 2023)**

---


- Justice Manual (“JM”)
  - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual (“JM”), *available at* <https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations>.
  - JM 9-47.120 and the Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, *available at* <https://www.justice.gov/criminal-fraud/file/1562831/download>.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines (“U.S.S.G.”), *available at* [https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/CHAPTER\\_8.pdf](https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/CHAPTER_8.pdf).
- Memorandum entitled “Selection of Monitors in Criminal Division Matters,” issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* <https://www.justice.gov/criminal-fraud/file/1100366/download>; updated Memorandum entitled “Selection of Monitors in Criminal Division Matters,” issued by Assistant Attorney General Kenneth A. Polite, Jr., on March 1, 2023, *available at* <https://www.justice.gov/criminal-fraud/file/1100366/download>.
- Criminal Division corporate resolution agreements, *available at* <https://www.justice.gov/news> (the Department of Justice’s (“DOJ”) Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).
- A Resource Guide to the U.S. Foreign Corrupt Practices Act (2d ed.) (“FCPA Guide”), published in July 2020 by the DOJ and the Securities and Exchange Commission (“SEC”), *available at* <https://www.justice.gov/criminal-fraud/file/1292051/download>.
- Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions, amended by the Organization for Economic Co-operation and Development (“OECD”) Council on November 25, 2021, *available at* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378>.
- Anti-Corruption Ethics and Compliance Handbook for Business (“OECD Handbook”), published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank, *available at* <https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf>.
- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, published in July 2019 by DOJ’s Antitrust Division, *available at* <https://www.justice.gov/atr/page/file/1182001/download>.

**Practical Guidance for Health Care Governing Boards on Compliance Oversight**



# Practical Guidance for Health Care Governing Boards on Compliance Oversight

Office of Inspector General,  
U.S. Department of Health and Human Services  
Association of Healthcare Internal Auditors  
American Health Lawyers Association  
Health Care Compliance Association



# About the Organizations

This educational resource was developed in collaboration between the Association of Healthcare Internal Auditors (AHIA), the American Health Lawyers Association (AHLA), the Health Care Compliance Association (HCCA), and the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS).

AHIA is an international organization dedicated to the advancement of the health care internal auditing profession. The AHLA is the Nation's largest nonpartisan, educational organization devoted to legal issues in the health care field. HCCA is a member-based, nonprofit organization serving compliance professionals throughout the health care field. OIG's mission is to protect the integrity of more than 100 HHS programs, including Medicare and Medicaid, as well as the health and welfare of program beneficiaries.

The following individuals, representing these organizations, served on the drafting task force for this document:

**Katherine Matos**, Senior Counsel, OIG, HHS

**Felicia E. Heimer**, Senior Counsel, OIG, HHS

**Catherine A. Martin**, Principal, Ober | Kaler (AHLA)

**Robert R. Michalski**, Chief Compliance Officer,  
Baylor Scott & White Health (AHIA)

**Daniel Roach**, General Counsel and Chief  
Compliance Officer, Optum360 (HCCA)

**Sanford V. Teplitzky**, Principal, Ober | Kaler (AHLA)

Published on April 20, 2015.

*This document is intended to assist governing boards of health care organizations (Boards) to responsibly carry out their compliance plan oversight obligations under applicable laws. This document is intended as guidance and should not be interpreted as setting any particular standards of conduct. The authors recognize that each health care entity can, and should, take the necessary steps to ensure compliance with applicable Federal, State, and local law. At the same time, the authors also recognize that there is no uniform approach to compliance. No part of this document should be taken as the opinion of, or as legal or professional advice from, any of the authors or their respective agencies or organizations.*

# Table of Contents

Introduction.....	1
Expectations for Board Oversight of Compliance Program Functions.....	2
Roles and Relationships.....	6
Reporting to the Board.....	9
Identifying and Auditing Potential Risk Areas.....	11
Encouraging Accountability and Compliance.....	13
Conclusion.....	15
Bibliography.....	16



# Introduction

Previous guidance<sup>1</sup> has consistently emphasized the need for Boards to be fully engaged in their oversight responsibility. A critical element of effective oversight is the process of asking the right questions of management to determine the adequacy and effectiveness of the organization's compliance program, as well as the performance of those who develop and execute that program, and to make compliance a responsibility for all levels of management. Given heightened industry and professional interest in governance and transparency issues, this document seeks to provide practical tips for Boards as they work to effectuate their oversight role of their organizations' compliance with State and Federal laws that regulate the health care industry. Specifically, this document addresses issues relating to a Board's oversight and review of compliance program functions, including the: (1) roles of, and relationships between, the organization's audit, compliance, and legal departments; (2) mechanism and process for issue-reporting within an organization; (3) approach to identifying regulatory risk; and (4) methods of encouraging enterprise-wide accountability for achievement of compliance goals and objectives.

**A critical element of effective oversight is the process of asking the right questions....**

---

1   OIG and AHHA, *Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors* (2003); OIG and AHHA, *An Integrated Approach to Corporate Compliance: A Resource for Health Care Organization Boards of Directors* (2004); and OIG and AHHA, *Corporate Responsibility and Health Care Quality: A Resource for Health Care Boards of Directors* (2007).

# Expectations for Board Oversight of Compliance Program Functions

A Board must act in good faith in the exercise of its oversight responsibility for its organization, including making inquiries to ensure: (1) a corporate information and reporting system exists and (2) the reporting system is adequate to assure the Board that appropriate information relating to compliance with applicable laws will come to its attention timely and as a matter of course.<sup>2</sup> The existence of a corporate reporting system is a key compliance program element, which not only keeps the Board informed of the activities of the organization, but also enables an organization to evaluate and respond to issues of potentially illegal or otherwise inappropriate activity.

Boards are encouraged to use widely recognized public compliance resources as benchmarks for their organizations. The Federal Sentencing Guidelines (Guidelines),<sup>3</sup> OIG's voluntary compliance program guidance documents,<sup>4</sup> and OIG Corporate Integrity Agreements (CIAs) can be used as baseline assessment tools for Boards and management in determining what specific functions may be necessary to meet the requirements of an effective compliance program. The Guidelines "offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program."<sup>5</sup> The compliance program guidance documents were developed by OIG to encourage the development and use of internal controls to monitor adherence to applicable statutes, regulations, and program requirements. CIAs impose specific structural and reporting requirements to

---

2 *In re Caremark Int'l, Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

3 U.S. Sentencing Commission, *Guidelines Manual* (Nov. 2013) (USSG), [http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2013/manual-pdf/2013\\_Guidelines\\_Manual\\_Full.pdf](http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2013/manual-pdf/2013_Guidelines_Manual_Full.pdf).

4 OIG, *Compliance Guidance*, <http://oig.hhs.gov/compliance/compliance-guidance/index.asp>.

5 USSG Ch. 8, Intro. Comment.



promote compliance with Federal health care program standards at entities that have resolved fraud allegations.

Basic CIA elements mirror those in the Guidelines, but a CIA also includes obligations tailored to the organization and its compliance risks. Existing CIAs may be helpful resources for Boards seeking to evaluate their organizations' compliance programs. OIG has required some settling entities, such as health systems and hospitals, to agree to Board-level requirements, including annual resolutions. These resolutions are signed by each member of the Board, or the designated Board committee, and detail the activities that have been undertaken to review and oversee the organization's compliance with Federal health care program and CIA requirements. OIG has not required this level of Board involvement in every case, but these provisions demonstrate the importance placed on Board oversight in cases OIG believes reflect serious compliance failures.

**Although compliance program design is not a “one size fits all” issue, Boards are expected to put forth a meaningful effort....**

Although compliance program design is not a “one size fits all” issue, Boards are expected to put forth a meaningful effort to review the adequacy of existing compliance systems and functions. Ensuring that management is aware of the Guidelines, compliance program guidance, and relevant CIAs is a good first step.

One area of inquiry for Board members of health care organizations should be the scope and adequacy of the compliance program in light of the size and complexity of their organizations. The Guidelines allow for variation according to “the size of the organization.”<sup>6</sup> In accordance with the Guidelines,

---

6 USSG § 8B2.1, comment. (n. 2).

OIG recognizes that the design of a compliance program will depend on the size and resources of the organization.<sup>7</sup> Additionally, the complexity of the organization will likely dictate the nature and magnitude of regulatory impact and thereby the nature and skill set of resources needed to manage and monitor compliance.

While smaller or less complex organizations must demonstrate the same degree of commitment to ethical conduct and compliance as larger organizations, the Government recognizes that they may meet the Guidelines requirements with less formality and fewer resources than would be expected of larger and more complex organizations.<sup>8</sup> Smaller organizations may meet their compliance responsibility by “using available personnel, rather than employing separate staff, to carry out the compliance and ethics program.” Board members of such organizations may wish to evaluate whether the organization is “modeling its own compliance and ethics programs on existing, well-regarded compliance and ethics programs and best practices of other similar organizations.”<sup>9</sup> The Guidelines also foresee that Boards of smaller organizations may need to become more involved in the organizations’ compliance and ethics efforts than their larger counterparts.<sup>10</sup>

Boards should develop a formal plan to stay abreast of the ever-changing regulatory landscape and operating environment. The plan may involve periodic updates from informed staff or review of regulatory resources made available to them by staff. With an understanding of the dynamic regulatory environment, Boards will be in a position to ask more pertinent questions of management

---

<sup>7</sup> Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. 59434, 59436 (Oct. 5, 2000) (“The extent of implementation [of the seven components of a voluntary compliance program] will depend on the size and resources of the practice. Smaller physician practices may incorporate each of the components in a manner that best suits the practice. By contrast, larger physician practices often have the means to incorporate the components in a more systematic manner.”); Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289 (Mar. 16, 2000) (recognizing that smaller providers may not be able to outsource their screening process or afford to maintain a telephone hotline).

<sup>8</sup> USSG § 8B2.1, comment. (n. 2).

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

and make informed strategic decisions regarding the organizations' compliance programs, including matters that relate to funding and resource allocation. For instance, new standards and reporting requirements, as required by law, may, but do not necessarily, result in increased compliance costs for an organization. Board members may also wish to take advantage of outside educational programs that provide them with opportunities to develop a better understanding of industry risks, regulatory requirements, and how effective compliance and ethics programs operate. In addition, Boards may want management to create a formal education calendar that ensures that Board members are periodically educated on the organizations' highest risks.

Finally, a Board can raise its level of substantive expertise with respect to regulatory and compliance matters by adding to the Board, or periodically consulting with, an experienced regulatory, compliance, or legal professional. The presence of a professional with health care compliance expertise on the Board sends a strong message about the organization's commitment to compliance, provides a valuable resource to other Board members, and helps the Board better fulfill its oversight obligations. Board members are generally entitled to rely on the advice of experts in fulfilling their duties.<sup>11</sup> OIG sometimes requires entities under a CIA to retain an expert in compliance or governance issues to assist the Board in fulfilling its responsibilities under the CIA.<sup>12</sup> Experts can assist Boards and management in a variety of ways, including the identification of risk areas, provision of insight into best practices in governance, or consultation on other substantive or investigative matters.

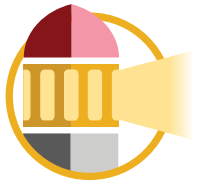
---

11 See Del Code Ann. tit. 8, § 141(e) (2010); ABA Revised Model Business Corporation Act, §§ 8.30(e), (f)(2) Standards of Conduct for Directors.

12 See Corporate Integrity Agreements between OIG and Halifax Hospital Medical Center and Halifax Staffing, Inc. (2014, compliance and governance); Johnson & Johnson (2013); Dallas County Hospital District d/b/a Parkland Health and Hospital System (2013, compliance and governance); Forest Laboratories, Inc. (2010); Novartis Pharmaceuticals Corporation (2010); Ortho-McNeil-Janssen Pharmaceuticals, Inc. (2010); Synthes, Inc. (2010, compliance expert retained by Audit Committee); The University of Medicine and Dentistry of New Jersey (2009, compliance expert retained by Audit Committee); Quest Diagnostics Incorporated (2009); Amerigroup Corporation (2008); Bayer HealthCare LLC (2008); and Tenet Healthcare Corporation (2006; retained by the Quality, Compliance, and Ethics Committee of the Board).

# Roles and Relationships

Organizations should define the interrelationship of the audit, compliance, and legal functions in charters or other organizational documents. The structure, reporting relationships, and interaction of these and other functions (e.g., quality, risk management, and human resources) should be included as departmental roles and responsibilities are defined. One approach is for the charters to draw functional boundaries while also setting an expectation of cooperation and collaboration among those functions. One illustration is the following, recognizing that not all entities may possess sufficient resources to support this structure:



**The compliance function** promotes the prevention, detection, and resolution of actions that do not conform to legal, policy, or business standards. This responsibility includes the obligation to develop policies and procedures that provide employees guidance, the creation of incentives to promote employee compliance, the development of plans to improve or sustain compliance, the development of metrics to measure execution (particularly by management) of the program and implementation of corrective actions, and the development of reports and dashboards that help management and the Board evaluate the effectiveness of the program.

**The legal function** advises the organization on the legal and regulatory risks of its business strategies, providing advice and counsel to management and the Board about relevant laws and regulations that govern, relate to, or impact the organization. The function also defends the organization in legal proceedings and initiates legal proceedings against other parties if such action is warranted.

**The internal audit function** provides an objective evaluation of the existing risk and internal control systems and framework within an organization. Internal audits ensure monitoring functions are working as intended and identify where management monitoring and/or additional

Board oversight may be required. Internal audit helps management (and the compliance function) develop actions to enhance internal controls, reduce risk to the organization, and promote more effective and efficient use of resources. Internal audit can fulfill the auditing requirements of the Guidelines.

**The human resources function** manages the recruiting, screening, and hiring of employees; coordinates employee benefits; and provides employee training and development opportunities.

**The quality improvement function** promotes consistent, safe, and high quality practices within health care organizations. This function improves efficiency and health outcomes by measuring and reporting on quality outcomes and recommends necessary changes to clinical processes to management and the Board. Quality improvement is critical to maintaining patient-centered care and helping the organization minimize risk of patient harm.

Boards should be aware of, and evaluate, the adequacy, independence,<sup>13</sup> and performance of different functions within an organization on a periodic basis. OIG believes an organization's Compliance Officer should neither be counsel for the provider, nor be subordinate in function or position to counsel or the legal department, in any manner.<sup>14</sup> While independent, an organization's counsel and compliance officer should collaborate to further the interests of the organization. OIG's position on separate compliance and legal functions reflects the independent roles and professional obligations of each function;<sup>15</sup>

---

13 Evaluation of independence typically includes assessing whether the function has uninhibited access to the relevant Board committees, is free from organizational bias through an appropriate administrative reporting relationship, and receives fair compensation adjustments based on input from any relevant Board committee.

14 See OIG and AHHA, *An Integrated Approach to Corporate Compliance: A Resource for Health Care Organization Boards of Directors*, 3 (2004) (citing Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,997 (Feb. 23, 1998)).

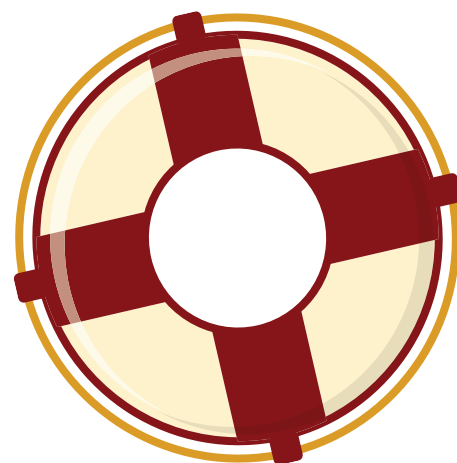
15 See, generally, *id.*

the same is true for internal audit.<sup>16</sup> To operate effectively, the compliance, legal, and internal audit functions should have access to appropriate and relevant corporate information and resources. As part of this effort, organizations will need to balance any existing attorney-client privilege with the goal of providing such access to key individuals who are charged with the responsibility for ensuring compliance, as well as properly reporting and remediating any violations of civil, criminal, or administrative law.

The Board should have a process to ensure appropriate access to information; this process may be set forth in a formal charter document approved by the Audit Committee of the Board or in other appropriate documents. Organizations that do not separate these functions (and some organizations may not have the resources to make this complete separation) should recognize the potential risks of such an arrangement. To partially mitigate these potential risks, organizations should provide individuals serving in multiple roles the capability to execute each function in an independent manner when necessary, including through reporting opportunities with the Board and executive management.

Boards should also evaluate and discuss how management works together to address risk, including the role of each in:

- 1.** identifying compliance risks,
- 2.** investigating compliance risks and avoiding duplication of effort,
- 3.** identifying and implementing appropriate corrective actions and decision-making, and
- 4.** communicating between the various functions throughout the process.



<sup>16</sup> Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,997 (Feb. 23, 1998) (auditing and monitoring function should “[b]e independent of physicians and line management”); Compliance Program Guidance for Home Health Agencies, 63 Fed. Reg. 42,410, 42,424 (Aug. 7, 1998) (auditing and monitoring function should “[b]e objective and independent of line management to the extent reasonably possible”); Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289, 14,302 (Mar. 16, 2000).

Boards should understand how management approaches conflicts or disagreements with respect to the resolution of compliance issues and how it decides on the appropriate course of action. The audit, compliance, and legal functions should speak a common language, at least to the Board and management, with respect to governance concepts, such as accountability, risk, compliance, auditing, and monitoring. Agreeing on the adoption of certain frameworks and definitions can help to develop such a common language.

## Reporting to the Board

The Board should set and enforce expectations for receiving particular types of compliance-related information from various members of management. The Board should receive regular reports regarding the organization's risk mitigation and compliance efforts—separately and independently—from a variety of key players, including those responsible for audit, compliance, human resources, legal, quality, and information technology. By engaging the leadership team and others deeper in the organization, the Board can identify who can provide relevant information about operations and operational risks. It may be helpful and productive for the Board to establish clear expectations for members of the management team and to hold them accountable for performing and informing the Board in accordance with those expectations. The Board may request the development of objective scorecards that measure how well management is executing the compliance program, mitigating risks, and implementing corrective action plans. Expectations could also include reporting information on internal and external investigations, serious issues raised in internal and external audits, hotline call activity, all allegations of material fraud or senior management misconduct, and all management exceptions to the organization's

**The Board should receive regular reports regarding the organization's risk mitigation and compliance efforts....**

code of conduct and/or expense reimbursement policy. In addition, the Board should expect that management will address significant regulatory changes and enforcement events relevant to the organization's business.

Boards of health care organizations should receive compliance and risk-related information in a format sufficient to satisfy the interests or concerns of their members and to fit their capacity to review that information. Some Boards use tools such as dashboards—containing key financial, operational and compliance indicators to assess risk, performance against budgets, strategic plans, policies and procedures, or other goals and objectives—in order to strike a balance between too much and too little information. For instance, Board quality committees can work with management to create the content of the dashboards with a goal of identifying and responding to risks and improving quality of care. Boards should also consider establishing a risk-based reporting system, in which those responsible for the compliance function provide reports to the Board when certain risk-based criteria are met. The Board should be assured that there are mechanisms in place to ensure timely reporting of suspected violations and to evaluate and implement remedial measures. These tools may also be used to track and identify trends in organizational performance against corrective action plans developed in response to compliance concerns. Regular internal reviews that provide a Board with a snapshot of where the organization is, and where it may be going, in terms of compliance and quality improvement, should produce better compliance results and higher quality services.

As part of its oversight responsibilities, the Board may want to consider conducting regular “executive sessions” (i.e., excluding senior management) with leadership from the compliance, legal, internal audit, and quality functions to encourage more open communication. Scheduling regular executive sessions creates a continuous expectation of open dialogue, rather than calling such a session only when a problem arises, and is helpful to avoid suspicion among management about why a special executive session is being called.



# Identifying and Auditing Potential Risk Areas

Some regulatory risk areas are common to all health care providers. Compliance in health care requires monitoring of activities that are highly vulnerable to fraud or other violations. Areas of particular interest include referral relationships and arrangements, billing problems (e.g., upcoding, submitting claims for services not rendered and/or medically unnecessary services), privacy breaches, and quality-related events.

The Board should ensure that management and the Board have strong processes for identifying risk areas. Risk areas may be identified from internal or external information sources. For instance, Boards and management may identify regulatory risks from internal sources, such as employee reports to an internal compliance hotline or internal audits. External sources that may be used to identify regulatory risks might include professional organization publications, OIG-issued guidance, consultants, competitors, or news media. When failures or problems in similar organizations are publicized, Board members should ask their own management teams whether there are controls and processes in place to reduce the risk of, and to identify, similar misconduct or issues within their organizations.



The Board should ensure that management consistently reviews and audits risk areas, as well as develops, implements, and monitors corrective action plans. One of the reasonable steps an organization is expected to take

under the Guidelines is “monitoring and auditing to detect criminal conduct.”<sup>17</sup> Audits can pinpoint potential risk factors, identify regulatory or compliance problems, or confirm the effectiveness of compliance controls. Audit results that reflect compliance issues or control deficiencies should be accompanied by corrective action plans.<sup>18</sup>

Recent industry trends should also be considered when designing risk assessment plans. Compliance functions tasked with monitoring new areas of risk should take into account the increasing emphasis on quality, industry consolidation, and changes in insurance coverage and reimbursement. New forms of reimbursement (e.g., value-based purchasing, bundling of services for a single payment, and global payments for maintaining and improving the health of individual patients and even entire populations) lead to new incentives and compliance risks. Payment policies that align payment with quality care have placed increasing pressure to conform to recommended quality guidelines and improve quality outcomes. New payment models have also incentivized consolidation among health care providers and more employment and contractual relationships (e.g., between hospitals and physicians). In light of the fact that statutes applicable to provider-physician relationships are very broad, Boards of entities that have financial relationships with referral sources or recipients should ask how their organizations are reviewing these arrangements for compliance with the physician self-referral (Stark) and anti-kickback laws. There should also be a clear understanding between the Board and management as to how the entity will approach and implement those relationships and what level of risk is acceptable in such arrangements.

Emerging trends in the health care industry to increase transparency can present health care organizations with opportunities and risks. For example, the Government is collecting and publishing data on health outcomes and quality measures (e.g., Centers for Medicare & Medicaid Services (CMS) Quality Compare Measures), Medicare payment data are now publicly available (e.g.,

---

<sup>17</sup> See USSG § 8B2.1(b)(5).

<sup>18</sup> See USSG § 8B2.1(c).

CMS physician payment data), and the Sunshine Rule<sup>19</sup> offers public access to data on payments from the pharmaceutical and device industries to physicians. Boards should consider all beneficial use of this newly available information. For example, Boards may choose to compare accessible data against organizational peers and incorporate national benchmarks when assessing organizational risk and compliance. Also, Boards of organizations that employ physicians should be cognizant of the relationships that exist between their employees and other health care entities and whether those relationships could have an impact on such matters as clinical and research decision-making. Because so much more information is becoming public, Boards may be asked significant compliance-oriented questions by various stakeholders, including patients, employees, government officials, donors, the media, and whistleblowers.

## Encouraging Accountability and Compliance

Compliance is an enterprise-wide responsibility. While audit, compliance, and legal functions serve as advisors, evaluators, identifiers, and monitors of risk and compliance, it is the responsibility of the entire organization to execute the compliance program.

In an effort to support the concept that compliance is “a way of life,” a Board may assess employee performance in promoting and adhering to compliance.<sup>20</sup> An organization may assess individual, department, or facility-level performance or consistency in executing the compliance program. These assessments can then be used to either withhold incentives or to provide bonuses

**Compliance is an enterprise-wide responsibility.**

19 See Sunshine Rule, 42 C.F.R. § 403.904, and CMS *Open Payments*, <http://www.cms.gov/Regulations-and-Guidance/Legislation/National-Physician-Payment-Transparency-Program/index.html>.

20 Compliance Program Guidance for Nursing Facilities, 65 Fed. Reg. 14,289, 14,298-14,299 (Mar. 16, 2000).

based on compliance and quality outcomes. Some companies have made participation in annual incentive programs contingent on satisfactorily meeting annual compliance goals. Others have instituted employee and executive compensation claw-back/recoupment provisions if compliance metrics are not met. Such approaches mirror Government trends. For example, OIG is increasingly requiring certifications of compliance from managers outside the compliance department. Through a system of defined compliance goals and objectives against which performance may be measured and incentivized, organizations can effectively communicate the message that everyone is ultimately responsible for compliance.

Governing Boards have multiple incentives to build compliance programs that encourage self-identification of compliance failures and to voluntarily disclose such failures to the Government. For instance, providers enrolled in Medicare or Medicaid are required by statute to report and refund any overpayments under what is called the 60 Day Rule.<sup>21</sup> The 60-Day Rule requires all Medicare and Medicaid participating providers and suppliers to report and refund known overpayments within 60 days from the date the overpayment is “identified” or within 60 days of the date when any corresponding cost report is due. Failure to follow the 60-Day Rule can result in False Claims Act or civil monetary penalty liability. The final regulations, when released, should provide additional guidance and clarity as to what it means to “identify” an overpayment.<sup>22</sup> However, as an example, a Board would be well served by asking management about its efforts to develop policies for identifying and returning overpayments. Such an inquiry would inform the Board about how proactive the organization’s compliance program may be in correcting and remediating compliance issues.

---

21 42 U.S.C. § 1320a-7k.

22 Medicare Program; Reporting and Returning of Overpayments, 77 Fed. Reg. 9179, 9182 (Feb. 16, 2012) (Under the proposed regulations interpreting this statutory requirement, an overpayment is “identified” when a person “has actual knowledge of the existence of the overpayment or acts in reckless disregard or deliberate ignorance of the overpayment.”) disregard or deliberate ignorance of the overpayment.”); Medicare Program; Reporting and Returning of Overpayments; Extensions of Timeline for Publication of the Final Rule, 80 Fed. Reg. 8247 (Feb. 17, 2015).

Organizations that discover a violation of law often engage in an internal analysis of the benefits and costs of disclosing—and risks of failing to disclose—such violation to OIG and/or another governmental agency. Organizations that are proactive in self-disclosing issues under OIG’s Self-Disclosure Protocol realize certain benefits, such as (1) faster resolution of the case—the average OIG self-disclosure is resolved in less than one year; (2) lower payment—OIG settles most self-disclosure cases for 1.5 times damages rather than for double or treble damages and penalties available under the False Claims Act; and (3) exclusion release as part of settlement with no CIA or other compliance obligations.<sup>23</sup> OIG believes that providers have legal and ethical obligations to disclose known violations of law occurring within their organizations.<sup>24</sup> Boards should ask management how it handles the identification of probable violations of law, including voluntary self-disclosure of such issues to the Government.

As an extension of their oversight of reporting mechanisms and structures, Boards would also be well served by evaluating whether compliance systems and processes encourage effective communication across the organizations and whether employees feel confident that raising compliance concerns, questions, or complaints will result in meaningful inquiry without retaliation or retribution. Further, the Board should request and receive sufficient information to evaluate the appropriateness of management’s responses to identified violations of the organization’s policies or Federal or State laws.

## Conclusion

A health care governing Board should make efforts to increase its knowledge of relevant and emerging regulatory risks, the role and functioning of the organization’s compliance program in the face of those risks, and the flow and elevation of reporting of potential issues and problems to

---

23 See OIG, *Self-Disclosure Information*, <http://oig.hhs.gov/compliance/self-disclosure-info>.

24 See *id.*, at 2 (“we believe that using the [Self-Disclosure Protocol] may mitigate potential exposure under section 1128J(d) of the Act, 42 U.S.C. 1320a-7k(d).”)

senior management. A Board should also encourage a level of compliance accountability across the organization. A Board may find that not every measure addressed in this document is appropriate for its organization, but every Board is responsible for ensuring that its organization complies with relevant Federal, State, and local laws. The recommendations presented in this document are intended to assist Boards with the performance of those activities that are key to their compliance program oversight responsibilities. Ultimately, compliance efforts are necessary to protect patients and public funds, but the form and manner of such efforts will always be dependent on the organization's individual situation.

## Bibliography

Elisabeth Belmont, et al., "Quality in Action: Paradigm for a Hospital Board-Driven Quality Program," 4 *Journal of Health & Life Sciences Law*. 95, 113 (Feb. 2011).

Larry Gage, *Transformational Governance: Best Practices for Public and Nonprofit Hospitals and Health Systems*, Center for Healthcare Governance (2012).

Tracy E. Miller and Valerie L. Gutmann, "Changing Expectations for Board Oversight of Healthcare Quality: The Emerging Paradigm," 2 *Journal of Health & Life Sciences Law* (July 2009).

Tracy E. Miller, *Board Fiduciary Duty to Oversee Quality: New Challenges, Rising Expectations*, 3 *NYSBA Health L.J.* (Summer/Fall 2012).

Lawrence Prybil, et al., *Governance in Nonprofit Community Health Systems: An Initial Report on CEO Perspectives*, Grant Thornton LLP (Feb. 2008).





Resource 6

**U.S. Department of Justice**

**Individual Accountability for Corporate Wrongdoing Memo**





U.S. Department of Justice

Office of the Deputy Attorney General


The Deputy Attorney General

Washington, D.C. 20530

September 9, 2015

MEMORANDUM FOR THE ASSISTANT ATTORNEY GENERAL, ANTITRUST DIVISION  
THE ASSISTANT ATTORNEY GENERAL, CIVIL DIVISION  
THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION  
THE ASSISTANT ATTORNEY GENERAL, ENVIRONMENT AND  
NATURAL RESOURCES DIVISION  
THE ASSISTANT ATTORNEY GENERAL, NATIONAL  
SECURITY DIVISION  
THE ASSISTANT ATTORNEY GENERAL, TAX DIVISION  
THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION  
THE DIRECTOR, EXECUTIVE OFFICE FOR UNITED STATES  
TRUSTEES  
ALL UNITED STATES ATTORNEYS

FROM:

Sally Quillian Yates   
Deputy Attorney General

SUBJECT:

Individual Accountability for Corporate Wrongdoing

Fighting corporate fraud and other misconduct is a top priority of the Department of Justice. Our nation's economy depends on effective enforcement of the civil and criminal laws that protect our financial system and, by extension, all our citizens. These are principles that the Department lives and breathes—as evidenced by the many attorneys, agents, and support staff who have worked tirelessly on corporate investigations, particularly in the aftermath of the financial crisis.

One of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing. Such accountability is important for several reasons: it deters future illegal activity, it incentivizes changes in corporate behavior, it ensures that the proper parties are held responsible for their actions, and it promotes the public's confidence in our justice system.

There are, however, many substantial challenges unique to pursuing individuals for corporate misdeeds. In large corporations, where responsibility can be diffuse and decisions are made at various levels, it can be difficult to determine if someone possessed the knowledge and criminal intent necessary to establish their guilt beyond a reasonable doubt. This is particularly true when determining the culpability of high-level executives, who may be insulated from the day-to-day activity in which the misconduct occurs. As a result, investigators often must reconstruct what happened based on a painstaking review of corporate documents, which can number in the millions, and which may be difficult to collect due to legal restrictions.

These challenges make it all the more important that the Department fully leverage its resources to identify culpable individuals at all levels in corporate cases. To address these challenges, the Department convened a working group of senior attorneys from Department components and the United States Attorney community with significant experience in this area. The working group examined how the Department approaches corporate investigations, and identified areas in which it can amend its policies and practices in order to most effectively pursue the individuals responsible for corporate wrongs. This memo is a product of the working group's discussions.

The measures described in this memo are steps that should be taken in any investigation of corporate misconduct. Some of these measures are new, while others reflect best practices that are already employed by many federal prosecutors. Fundamentally, this memo is designed to ensure that all attorneys across the Department are consistent in our best efforts to hold to account the individuals responsible for illegal corporate conduct.

The guidance in this memo will also apply to civil corporate matters. In addition to recovering assets, civil enforcement actions serve to redress misconduct and deter future wrongdoing. Thus, civil attorneys investigating corporate wrongdoing should maintain a focus on the responsible individuals, recognizing that holding them to account is an important part of protecting the public fisc in the long term.

The guidance in this memo reflects six key steps to strengthen our pursuit of individual corporate wrongdoing, some of which reflect policy shifts and each of which is described in greater detail below: (1) in order to qualify for any cooperation credit, corporations must provide to the Department all relevant facts relating to the individuals responsible for the misconduct; (2) criminal and civil corporate investigations should focus on individuals from the inception of the investigation; (3) criminal and civil attorneys handling corporate investigations should be in routine communication with one another; (4) absent extraordinary circumstances or approved departmental policy, the Department will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation; (5) Department attorneys should not resolve matters with a corporation without a clear plan to resolve related individual cases, and should

memorialize any declinations as to individuals in such cases; and (6) civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.<sup>1</sup>

I have directed that certain criminal and civil provisions in the United States Attorney's Manual, more specifically the Principles of Federal Prosecution of Business Organizations (USAM 9-28.000 *et seq.*) and the commercial litigation provisions in Title 4 (USAM 4-4.000 *et seq.*), be revised to reflect these changes. The guidance in this memo will apply to all future investigations of corporate wrongdoing. It will also apply to those matters pending as of the date of this memo, to the extent it is practicable to do so.

**1. To be eligible for any cooperation credit, corporations must provide to the Department all relevant facts about the individuals involved in corporate misconduct.**

In order for a company to receive any consideration for cooperation under the Principles of Federal Prosecution of Business Organizations, the company must completely disclose to the Department all relevant facts about individual misconduct. Companies cannot pick and choose what facts to disclose. That is, to be eligible for any credit for cooperation, the company must identify all individuals involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide to the Department all facts relating to that misconduct. If a company seeking cooperation credit declines to learn of such facts or to provide the Department with complete factual information about individual wrongdoers, its cooperation will not be considered a mitigating factor pursuant to USAM 9-28.700 *et seq.*<sup>2</sup> Once a company meets the threshold requirement of providing all relevant facts with respect to individuals, it will be eligible for consideration for cooperation credit. The extent of that cooperation credit will depend on all the various factors that have traditionally applied in making this assessment (*e.g.*, the timeliness of the cooperation, the diligence, thoroughness, and speed of the internal investigation, the proactive nature of the cooperation, etc.).

This condition of cooperation applies equally to corporations seeking to cooperate in civil matters; a company under civil investigation must provide to the Department all relevant facts about individual misconduct in order to receive any consideration in the negotiation. For

---

<sup>1</sup> The measures laid out in this memo are intended solely to guide attorneys for the government in accordance with their statutory responsibilities and federal law. They are not intended to, do not, and may not be relied upon to create a right or benefit, substantive or procedural, enforceable at law by a party to litigation with the United States.

<sup>2</sup> Nor, if a company is prosecuted, will it support a cooperation-related reduction at sentencing. See U.S.S.G. USSG § 8C2.5(g), Application Note 13 ("A prime test of whether the organization has disclosed all pertinent information" necessary to receive a cooperation-related reduction in its offense level calculation "is whether the information is sufficient ... to identify ... the individual(s) responsible for the criminal conduct").

example, the Department's position on "full cooperation" under the False Claims Act, 31 U.S.C. § 3729(a)(2), will be that, at a minimum, all relevant facts about responsible individuals must be provided.

The requirement that companies cooperate completely as to individuals, within the bounds of the law and legal privileges, *see* USAM 9-28.700 to 9-28.760, does not mean that Department attorneys should wait for the company to deliver the information about individual wrongdoers and then merely accept what companies provide. To the contrary, Department attorneys should be proactively investigating individuals at every step of the process – before, during, and after any corporate cooperation. Department attorneys should vigorously review any information provided by companies and compare it to the results of their own investigation, in order to best ensure that the information provided is indeed complete and does not seek to minimize the behavior or role of any individual or group of individuals.

Department attorneys should strive to obtain from the company as much information as possible about responsible individuals before resolving the corporate case. But there may be instances where the company's continued cooperation with respect to individuals will be necessary post-resolution. In these circumstances, the plea or settlement agreement should include a provision that requires the company to provide information about all culpable individuals and that is explicit enough so that a failure to provide the information results in specific consequences, such as stipulated penalties and/or a material breach.

**2. Both criminal and civil corporate investigations should focus on individuals from the inception of the investigation.**

Both criminal and civil attorneys should focus on individual wrongdoing from the very beginning of any investigation of corporate misconduct. By focusing on building cases against individual wrongdoers from the inception of an investigation, we accomplish multiple goals. First, we maximize our ability to ferret out the full extent of corporate misconduct. Because a corporation only acts through individuals, investigating the conduct of individuals is the most efficient and effective way to determine the facts and extent of any corporate misconduct. Second, by focusing our investigation on individuals, we can increase the likelihood that individuals with knowledge of the corporate misconduct will cooperate with the investigation and provide information against individuals higher up the corporate hierarchy. Third, by focusing on individuals from the very beginning of an investigation, we maximize the chances that the final resolution of an investigation uncovering the misconduct will include civil or criminal charges against not just the corporation but against culpable individuals as well.

**3. Criminal and civil attorneys handling corporate investigations should be in routine communication with one another.**

Early and regular communication between civil attorneys and criminal prosecutors handling corporate investigations can be crucial to our ability to effectively pursue individuals in

these matters. Consultation between the Department's civil and criminal attorneys, together with agency attorneys, permits consideration of the full range of the government's potential remedies (including incarceration, fines, penalties, damages, restitution to victims, asset seizure, civil and criminal forfeiture, and exclusion, suspension and debarment) and promotes the most thorough and appropriate resolution in every case. That is why the Department has long recognized the importance of parallel development of civil and criminal proceedings. *See* USAM 1-12.000.

Criminal attorneys handling corporate investigations should notify civil attorneys as early as permissible of conduct that might give rise to potential individual civil liability, even if criminal liability continues to be sought. Further, if there is a decision not to pursue a criminal action against an individual – due to questions of intent or burden of proof, for example – criminal attorneys should confer with their civil counterparts so that they may make an assessment under applicable civil statutes and consistent with this guidance. Likewise, if civil attorneys believe that an individual identified in the course of their corporate investigation should be subject to a criminal inquiry, that matter should promptly be referred to criminal prosecutors, regardless of the current status of the civil corporate investigation.

Department attorneys should be alert for circumstances where concurrent criminal and civil investigations of individual misconduct should be pursued. Coordination in this regard should happen early, even if it is not certain that a civil or criminal disposition will be the end result for the individuals or the company.

#### **4. Absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals.**

There may be instances where the Department reaches a resolution with the company before resolving matters with responsible individuals. In these circumstances, Department attorneys should take care to preserve the ability to pursue these individuals. Because of the importance of holding responsible individuals to account, absent extraordinary circumstances or approved departmental policy such as the Antitrust Division's Corporate Leniency Policy, Department lawyers should not agree to a corporate resolution that includes an agreement to dismiss charges against, or provide immunity for, individual officers or employees. The same principle holds true in civil corporate matters; absent extraordinary circumstances, the United States should not release claims related to the liability of individuals based on corporate settlement releases. Any such release of criminal or civil liability due to extraordinary circumstances must be personally approved in writing by the relevant Assistant Attorney General or United States Attorney.

**5. Corporate cases should not be resolved without a clear plan to resolve related individual cases before the statute of limitations expires and declinations as to individuals in such cases must be memorialized.**

If the investigation of individual misconduct has not concluded by the time authorization is sought to resolve the case against the corporation, the prosecution or corporate authorization memorandum should include a discussion of the potentially liable individuals, a description of the current status of the investigation regarding their conduct and the investigative work that remains to be done, and an investigative plan to bring the matter to resolution prior to the end of any statute of limitations period. If a decision is made at the conclusion of the investigation not to bring civil claims or criminal charges against the individuals who committed the misconduct, the reasons for that determination must be memorialized and approved by the United States Attorney or Assistant Attorney General whose office handled the investigation, or their designees.

Delays in the corporate investigation should not affect the Department's ability to pursue potentially culpable individuals. While every effort should be made to resolve a corporate matter within the statutorily allotted time, and tolling agreements should be the rare exception, in situations where it is anticipated that a tolling agreement is nevertheless unavoidable and necessary, all efforts should be made either to resolve the matter against culpable individuals before the limitations period expires or to preserve the ability to charge individuals by tolling the limitations period by agreement or court order.

**6. Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.**

The Department's civil enforcement efforts are designed not only to return government money to the public fisc, but also to hold the wrongdoers accountable and to deter future wrongdoing. These twin aims – of recovering as much money as possible, on the one hand, and of accountability for and deterrence of individual misconduct, on the other – are equally important. In certain circumstances, though, these dual goals can be in apparent tension with one another, for example, when it comes to the question of whether to pursue civil actions against individual corporate wrongdoers who may not have the necessary financial resources to pay a significant judgment.

Pursuit of civil actions against culpable individuals should not be governed solely by those individuals' ability to pay. In other words, the fact that an individual may not have sufficient resources to satisfy a significant judgment should not control the decision on whether to bring suit. Rather, in deciding whether to file a civil action against an individual, Department attorneys should consider factors such as whether the person's misconduct was serious, whether

it is actionable, whether the admissible evidence will probably be sufficient to obtain and sustain a judgment, and whether pursuing the action reflects an important federal interest. Just as our prosecutors do when making charging decisions, civil attorneys should make individualized assessments in deciding whether to bring a case, taking into account numerous factors, such as the individual's misconduct and past history and the circumstances relating to the commission of the misconduct, the needs of the communities we serve, and federal resources and priorities.

Although in the short term certain cases against individuals may not provide as robust a monetary return on the Department's investment, pursuing individual actions in civil corporate matters will result in significant long-term deterrence. Only by seeking to hold individuals accountable in view of all of the factors above can the Department ensure that it is doing everything in its power to minimize corporate fraud, and, over the course of time, minimize losses to the public fisc through fraud.

### **Conclusion**

The Department makes these changes recognizing the challenges they may present. But we are making these changes because we believe they will maximize our ability to deter misconduct and to hold those who engage in it accountable.

In the months ahead, the Department will be working with components to turn these policies into everyday practice. On September 16, 2015, for example, the Department will be hosting a training conference in Washington, D.C., on this subject, and I look forward to further addressing the topic with some of you then.





Resource 7

**The Relationship between the Board of Directors  
and the Compliance and Ethics Officer**

# The Relationship between the Board of Directors and the Compliance and Ethics Officer

*April 2018*

*A survey by the Society of Corporate Compliance and Ethics  
and the Health Care Compliance Association*



[corporatecompliance.org](http://corporatecompliance.org)  
[hcca-info.org](http://hcca-info.org)



## Introduction

The relationship between the compliance and ethics officer and the board of directors is both essential and often under developed. When the first version of the survey was fielded in 2010, many compliance professionals were struggling with how to manage what was to many a very new relationship.

Since then a number of factors have changed the dynamic. The Yates memo and increased scrutiny of individual (vs. corporate) actions gained the attention of senior leaders. Later, the Criminal Division of the US Department of Justice issued questions for prosecutors to use as guidance when evaluating compliance programs. Included in them were several about the activities of the board in overseeing the compliance and ethics programs.

To assess how the relationship between the compliance team and the board had evolved, as well as to examine issues of compliance officer influence, the Society of Corporate Compliance and Ethics and Health Care Compliance Association fielded this survey in 2014 and again in 2018.

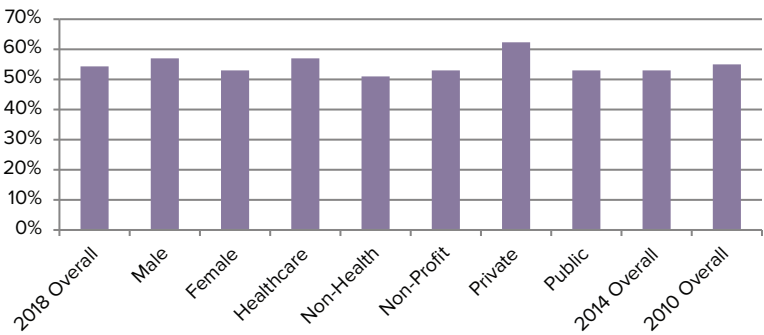
## Executive Summary

The data reveals that relatively little has changed since the survey results were last released in January 2014. In general, the relationship between boards and the compliance team is seen as a good one. Despite those who argue that compliance should fall under the General Counsel and treat it as the norm, that appears to be the case for only the minority of organizations. Compliance most often reports directly to the board and meets with the board at least four times a year.

## Key Findings

- **Approximately half of compliance officers report to the board.** This is true when looking at the data by industry, ownership (for profit and non-profit) and even by the gender of the compliance officer. Privately held companies were most likely to have a compliance officer reporting to the board (62%). Non-healthcare companies were the least likely (51%) but the difference versus the overall number of 54% was very small.

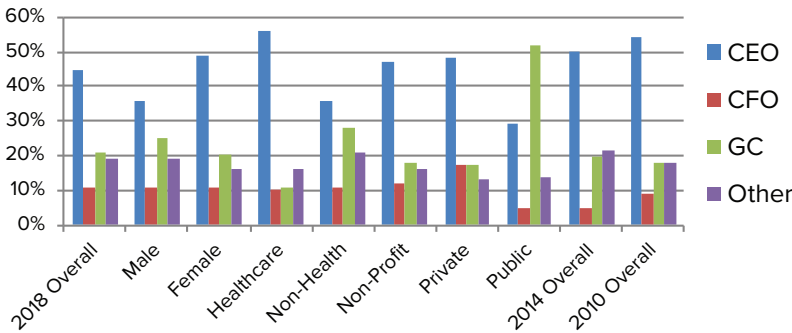
### Does the Chief Compliance and Ethics Officer of your Organization Report Directly to the Board?



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)

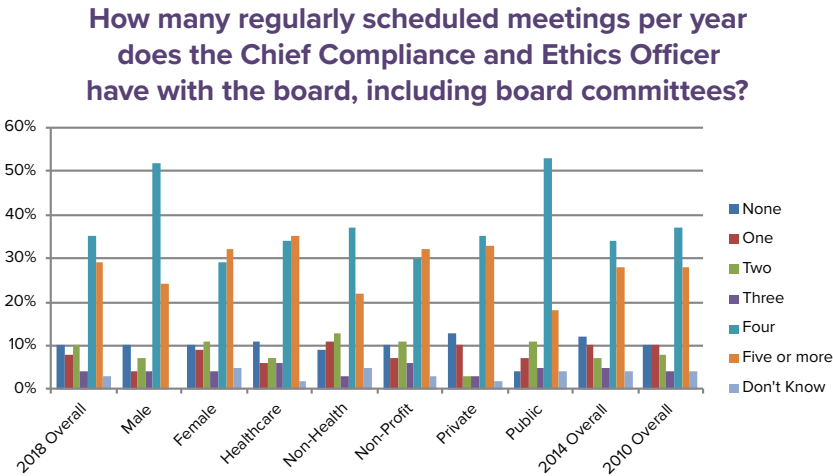
- **Among compliance professionals not reporting to the board, the CEO was the position they were most likely to report to (45%).** There were some notable differences. In healthcare, 56% of those not reporting to the board reported to the CEO. By contrast, for publicly traded companies the figure was just 29%. Women (49%) were more likely to report to the CEO than men (36%). And most notably, only 21% of survey respondents not reporting to the board reported to the GC. Also, potentially of significance, the percentage of respondents who don't report to the board but do report to the CEO has declined over the years from 54% in 2010 to 45% in 2018.

**If not to the board, to what position does the CEO report?**



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)

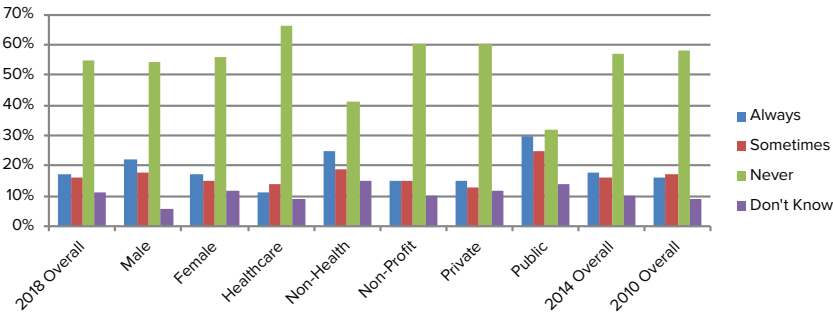
- **Meeting with the board four or more times a year is the norm.** Overall, 35% of respondents reported four regularly scheduled meetings per year, and another 29% reported five or more, bringing the total to 64% with four meetings or more annually.



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)

- **The majority of respondents reported that their reports are not screened by the general counsel or others before being shown to the board.** Healthcare firms particularly stood out in this regard (66% vs. 55%). For publicly traded-firms, though, the likelihood of the report being pre-screened was substantially higher (55% vs 33% of respondents as a whole).

**How often are the Chief Compliance and Ethics Officer's reports to the board screened and substantively edited?**



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)



**SCCE**<sup>TM</sup>  
Society of Corporate  
Compliance and Ethics

## TAKE CHARGE OF YOUR COMPLIANCE CAREER

Stay informed on changes affecting the compliance world.  
Learn from industry experts about emerging best practices  
for effective compliance and ethics programs.

# Join the Society of Corporate Compliance and Ethics



### MEMBERSHIP BENEFITS

- *Compliance & Ethics Professional* magazine, 12 issues exclusively for SCCE members plus full access to the magazine archives
- Be a part of a community of 6,500+ Compliance and Ethics Professionals in more than 95 countries
- Member-only discounts on conferences, manuals, and books
- Network locally and globally with 30+ conferences a year at special member rates
- Save on weekly Web conferences for live learning at your desk
- Receive a discount on Compliance Certification Board (CCB)<sup>®</sup> exam pricing for CCEP and CCEP-I

### *Additional resources*

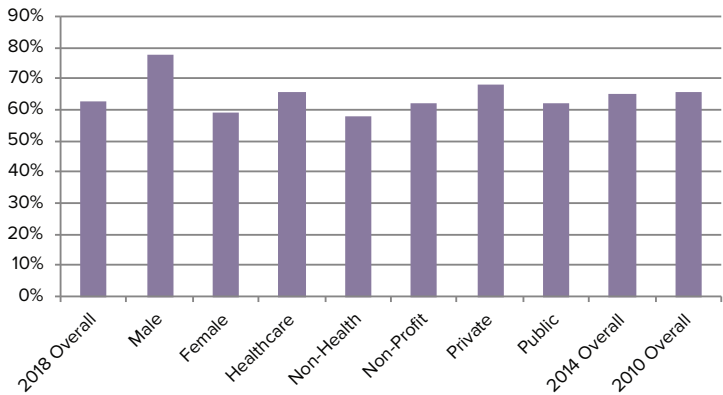
- Weekly newsletters and blog posts from industry experts
- SCCEnet<sup>®</sup> provides access to an online Resource Library and networking

**LEARN MORE AND JOIN TODAY**  
[corporatecompliance.org/join](http://corporatecompliance.org/join)



- **Generally, compliance officers surveyed were satisfied with the number of meetings with the board each year.** Sixty three percent felt that there were sufficient contacts. Men (78%) tended to be more satisfied with the number than women (59%)

**Believe that there are a sufficient number of contacts between the Board and Chief Compliance and Ethics Officer**



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)

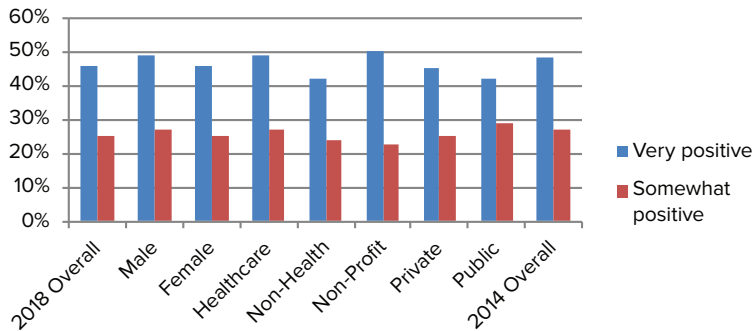
- **One area of possible concern is a declining belief that the board values compliance a great deal.** In 2014, the first year the question was asked, 55% gave the highest mark on this measure. By 2018, the number had declined to 46%. The lowest score (40%) came from survey respondents at privately held companies.



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)

- **In general compliance professionals felt that the quality of the interaction with the board is positive.** The interaction was described as “very positive” by 46% and another 25% rated it as somewhat positive. Only 5% rated it as somewhat or very negative.

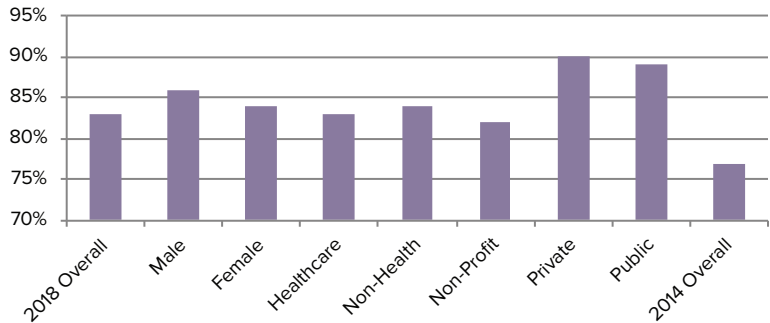
**How positively would you rate the quality of the interaction of the board with the Chief Compliance and Ethics Officer?**



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)

- **Compliance is very much responsible for escalating serious allegations and investigations to the board.** Overall 83% said this was compliance’s responsibility either as required by a formal procedure or as a practice.

**Compliance responsible for escalating to Board**



Society of Corporate Compliance & Ethics / [corporatecompliance.org](http://corporatecompliance.org)

- **When looking at the attributes for a successful compliance professional, men and women generally had similar opinions.** Survey respondents were given a list of attributes and asked to rate their importance on a 1 to 5 scale, with 5 being most important. While one gender or another might rate an attribute higher on the scale than the other, if looking at the top two highest ratings, they generally were very consistent.

ATTRIBUTES	MEN			WOMEN		
	4	5	4 & 5	4	5	4 & 5
Assertiveness/ Decisiveness	41%	48%	89%	26%	65%	91%
Consensus Building	31%	43%	74%	34%	47%	81%
Confidence	33%	61%	94%	27%	68%	95%
Empathy/Ability to Assess Situation	37%	48%	85%	30%	60%	90%
Independence	22%	69%	91%	17%	77%	94%
Relational/ Interpersonal	31%	53%	84%	22%	68%	90%
Ability to Influence	33%	53%	86%	28%	62%	90%

## Conclusions/Implications

- **The role of compliance in organizations seems to be solidified and strong.** The consistency of the data year to year and the overwhelming consistency across the various measures suggests that the position has become an integral one in most organizations with reporting lines to the governing body or very close to it.
- **The idea that compliance reporting to the general counsel is the norm is not born out by the data in the survey or previous ones.** Reporting to the general counsel is the exception, albeit a common one, rather than the rule.
- **Overall the relationship between the board and compliance seems to meet the needs of compliance professionals.** Their general high satisfaction levels with the quality and frequency of the meetings is encouraging.
- **There do appear to be some differences by gender.** Men generally view the relationship more positively and meet with the board more frequently. However, in those cases when compliance does not report to the board, women are much more likely to report to the CEO than elsewhere in the organization

## Methodology

Survey responses were solicited and collected during March and April 2018 from compliance and ethics professionals in the database of the Society of Corporate Compliance and Ethics and the Health Care Compliance Association. Additional outreach via social media was also used. Responses were collected and analyzed using SurveyGizmo, a web-based, third-party system. A total of 386 responses were received.



**HCCA**<sup>TM</sup>  
Health Care Compliance  
Association

LEARN.NETWORK.INSPIRE.



Maximize and grow your compliance program.

Stay informed on privacy issues, Stark compliance, conflicts of interest, False Claims Act, Risk Management, HIPAA, regulatory changes and patient rights, and more. Learn proactive compliance strategies from industry leaders and network with peers.

### **MEMBERSHIP BENEFITS**

- *Compliance Today* magazine, 12 issues exclusively for HCCA members plus full access to the magazine archives
- Join a community of 12,000+ compliance professionals
- Members-only discounts on conferences, publications, and newsletters
- Network and learn at 50+ conferences a year
- Save on weekly Web conferences for live learning at your desk
- Receive a discount on Compliance Certification Board (CCB)<sup>®</sup> exam pricing for CHC, CHRC, and CHPC

### ***Additional resources***

- HCCAnet<sup>®</sup> provides access to an online Resource Library and networking
- Weekly newsletters and blog posts from industry experts

**Learn more and join HCCA's community today.**

**[hcca-info.org/join](http://hcca-info.org/join)**

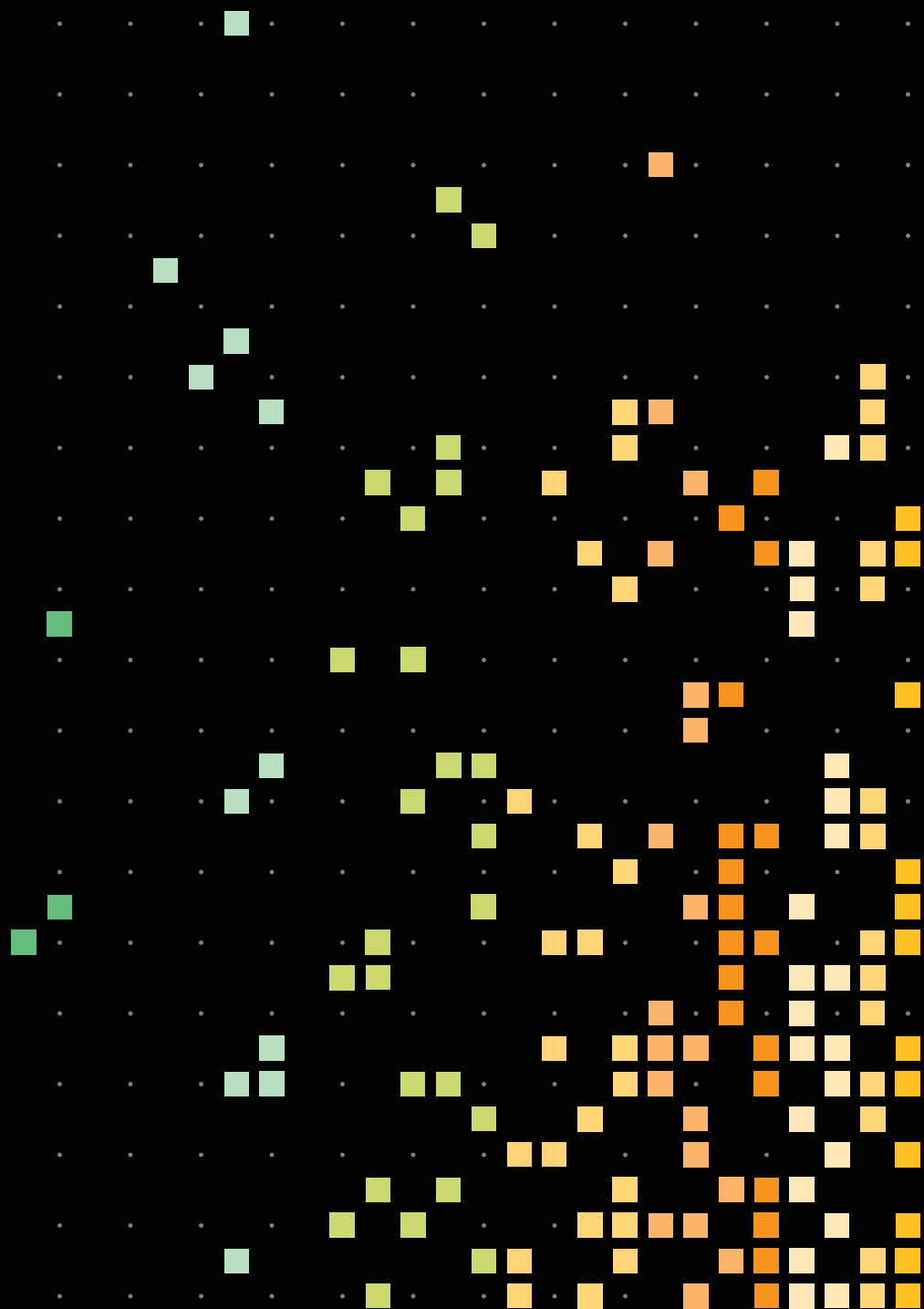
Resource 8

## **2020 Data Breach Investigations Report**





# 2020 Data Breach Investigations Report





# 3,950 breaches

That is what you are seeing. Each of these squares is organized by the 16 different industries and four world regions we cover in this year's report. Each square represents roughly one breach (1.04 to be more exact), for a total of 4,675 squares since breaches can be displayed in both their industry and region.

We also analyzed a record total of 157,525 incidents, 32,002 of which met our quality standards. The data coverage this year is so comprehensive that it shines through the monochromatic front cover, reinforcing the mission of the DBIR as being a data-driven resource. Turn the page to dig into the findings.

# Table of contents

## 01

DBIR Cheat sheet	4
Introduction	6
Summary of findings	7

## 02

<b>Results and analysis</b>	<b>8</b>
Actors	10
Actions	12
Threat action varieties	13
Error	14
Malware	15
Ransomware	16
Hacking	19
Social	24
Assets	26
Attributes	29
How many paths must a breach walk down?	31
Timeline	34
Incident classification patterns and subsets	35

## 03

<b>Industry analysis</b>	<b>39</b>
Accommodation and Food Services (NAICS 72)	44
Arts, Entertainment and Recreation (NAICS 71)	46
Construction (NAICS 23)	48
Educational Services (NAICS 61)	50
Financial and Insurance (NAICS 52)	52
Healthcare (NAICS 62)	54
Information (NAICS 51)	57
Manufacturing (NAICS 31–33)	59
Mining, Quarrying, and Oil & Gas Extraction + Utilities (NAICS 21 + 22)	62
Other Services (NAICS 81)	64
Professional, Scientific and Technical Services (NAICS 54)	66
Public Administration (NAICS 92)	69
Real Estate and Rental and Leasing (NAICS 53)	71
Retail (NAICS 44–45)	73
Transportation and Warehousing (NAICS 48–49)	76

## 04

<b>Does size matter? A deep dive into SMB breaches</b>	<b>78</b>
--	-----------

## 05

<b>Regional analysis</b>	<b>83</b>
Northern America (NA)	86
Europe, Middle East and Africa (EMEA)	90
Asia-Pacific (APAC)	93
Latin America and the Caribbean (LAC)	97

## 06

<b>Wrap-up</b>	<b>100</b>
CIS Control recommendations	101
Year in review	104

## 07

<b>Appendices</b>	<b>107</b>
Appendix A: Methodology	108
Appendix B: VERIS Common Attack Framework (VCAF)	112
Appendix C: Following the money—the key to nabbing the cybercriminal	114
Appendix D: State of Idaho enhances incident response program with VERIS.	116
Appendix E: Contributing organizations	118

# DBIR Cheat sheet

**Hello, and welcome to the 2020 Data Breach Investigations Report (DBIR)! We have been doing this report for a while now, and we appreciate that all the verbiage we use can be a bit obtuse at times. We use very deliberate naming conventions, terms and definitions and spend a lot of time making sure we are consistent throughout the report. Hopefully, this section will help make all of those more familiar.**

---

## VERIS resources

The terms “threat actions,” “threat actors” and “varieties” will be referenced a lot. These are part of the Vocabulary for Event Recording and Incident Sharing (VERIS), a framework designed to allow for a consistent, unequivocal collection of security incident details. Here is how they should be interpreted:

**Threat actor:** Who is behind the event? This could be the external “bad guy” that launches a phishing campaign or an employee who leaves sensitive documents in their seat-back pocket.

**Threat action:** What tactics (actions) were used to affect an asset? VERIS uses seven primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error and Environmental. Examples at a high level are hacking a server, installing malware and influencing human behavior through a social attack.

**Variety:** More specific enumerations of higher-level categories, e.g., classifying the external “bad guy” as an organized criminal group or recording a hacking action as SQL injection or brute force.

---

### Learn more here:

- [github.com/vz-risk/dbir/tree/gh-pages/2020](https://github.com/vz-risk/dbir/tree/gh-pages/2020) includes DBIR facts, figures and figure data.
- [veriscommunity.net](https://veriscommunity.net) features information on the framework with examples and enumeration listings.
- [github.com/vz-risk/veris](https://github.com/vz-risk/veris) features the full VERIS schema.
- [github.com/vz-risk/vcdb](https://github.com/vz-risk/vcdb) provides access to our database on publicly disclosed breaches, the VERIS Community Database.
- [http://veriscommunity.net/veris\\_webapp\\_min.html](http://veriscommunity.net/veris_webapp_min.html) allows you to record your own incidents and breaches. Don't fret, it saves any data locally and you only share what you want.

---

## Incident vs breach

We talk a lot about incidents and breaches and we use the following definitions:

**Incident:** A security event that compromises the integrity, confidentiality or availability of an information asset.

**Breach:** An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

---

## Industry labels

We align with the North American Industry Classification System (NAICS) standard to categorize the victim organizations in our corpus. The standard uses two- to six-digit codes to classify businesses and organizations. Our analysis is typically done at the two-digit level. We will specify NAICS codes along with an industry label. For example, a chart with a label of Financial (52) is not indicative of 52 as a value. “52” is the NAICS code for the Finance and Insurance sector. The overall label of “Financial” is used for brevity within the figures. Detailed information on the codes and classification system is available here:

<https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012>

---

## Dotting the charts and crossing the confidence

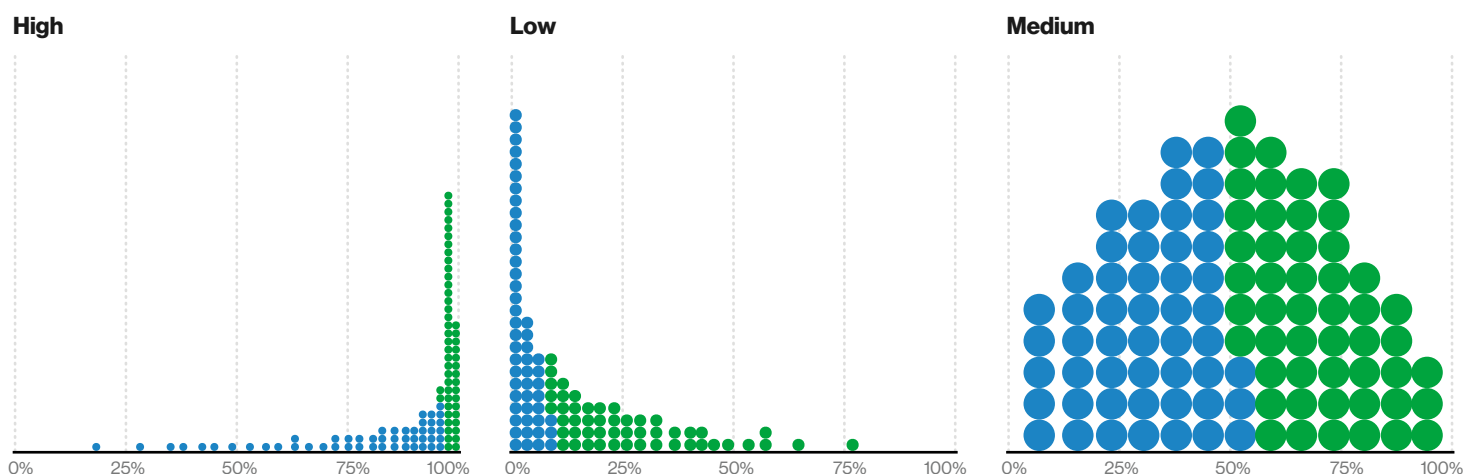
Last year, we introduced our now (in)famous slanted bar charts to show the uncertainty due to sampling bias.<sup>1</sup> One tweak we added this year was to roll up an “Other” aggregation of all the items that do not make the cut on our “Top (whatever)” charts. This will give you a better sense of the things we left out.

Not to be outdone this year, our incredible team of data scientists decided to try dot plots<sup>2</sup> to provide a better way to show how values are distributed.

The trick to understanding this chart is that the dots represent organizations. So if there are 100 dots (like in each chart in Figure 1), each dot represents 1% of organizations.

<sup>1</sup> Check “New chart, who dis?” in the “A couple of tidbits” section on the inside cover of the 2019 DBIR if you need a refresher on the slanted bar charts.

<sup>2</sup> To find out more about dot plots, check out Matthew Kay's paper: <http://www.mjskay.com/papers/chi2018-uncertain-bus-decisions.pdf>



**Figure 1.** Example dot plots

In Figure 1, we have three different charts, each representing common distributions you may find in this report. For convenience, we have colored the first half and the second half differently so it's easier to locate the median.

In the first chart (High), you see that a lot of companies had a very large value<sup>3</sup> associated with them. The opposite is true for the second one (Low), where a large number of the companies had zero or a low value. On the third chart (Medium), we got stuck in the middle of the road and all we can say is that most companies have that middle value. Using the Medium chart, we could probably report an average or a median value. For the High and Low ones, an average is statistically undefined and the median would be a bit misleading. We wouldn't want to do you like that.

**Questions? Comments? Still mad because VERIS uses the term “Hacking”?**

**Let us know! Drop us a line at [dbir@verizon.com](mailto:dbir@verizon.com), find us on LinkedIn, tweet @VerizonBusiness with the #dbir. Got a data question? Tweet @VZDBIR!**

<sup>3</sup> Don't worry about what the value is here. We made it up to make the charts pretty. And don't worry later either, we'll use a real value for the rest of the dot plots.

# Introduction

**Experience is merely the name men gave to their mistakes.**

**—Oscar Wilde, *The Picture of Dorian Gray***

Here we are at another edition of the DBIR. This is an exciting time for us as our little bundle of data turns 13 this year. That means that the report is going through a lot of big changes right now, just as we all did at that age. While some may harbor deeply rooted concerns regarding the number 13 and its purported associations with mishap, misadventure and misfortune, we here on the team continue to do our best to shine the light of data science into the dark corners of security superstition and dispel unfounded beliefs.

With that in mind, we are excited to ask you to join us for the report's coming-of-age party. If you look closely, you may notice that it has sprouted a few more industries here and there, and has started to grow a greater interest in other areas of the world. This year, we analyzed a record total of 157,525 incidents. Of those, 32,002 met our quality standards and 3,950 were confirmed data breaches. The resultant findings are spread throughout this report.

This year, we have added substantially more industry breakouts for a total of 16 verticals (the most to date) in which we examine the most common attacks, actors and actions for each. We are also proud to announce that, for the first time ever, we have been able to look at cybercrime from a regional viewpoint—thanks to a combination of improvements in our statistical processes and protocols, and, most of all, by data provided by new contributors—making this report arguably the most comprehensive analysis of global data breaches in existence.

We continue to use the VERIS framework to classify and analyze both incidents and breaches, and we have put additional focus on this

process in order to improve how VERIS connects and interacts with other existing standards. We also aligned with the Center for Internet Security (CIS)<sup>4</sup> Critical Security Controls and the MITRE ATT&CK<sup>5</sup> framework to improve the types of data we can collect for this report, and to map them to appropriate controls.

A huge “thank you” is in order to each and every one of our 81 contributors representing 81 countries, both those who participated for the first time in this year's report, and those tried-and-true friends who have walked this path with us for many years. This document, and the data and analysis it contains, would not be possible without you, and you have our most sincere thanks and heartfelt gratitude. And while we are on that topic, the way to continue to grow and improve is to have more quality organizations like yours join us in this fight against the unknown and the uncertain. Therefore, we urge you to consider becoming a data contributor and help us to continue to shed light into dark places.

Finally, thank you, our readers, for sticking with us these many years and for sharing your expertise, advice, encouragement and suggestions so that we can continue to make this report better each year.

Sincerely,  
The DBIR Team

(in alphabetical order)

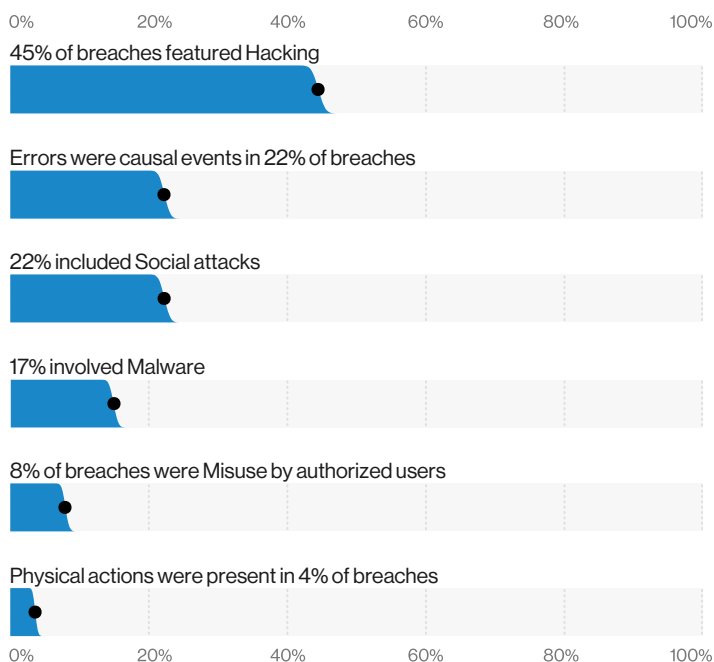
Gabriel Bassett  
C. David Hylender  
Philippe Langlois  
Alexandre Pinto  
Suzanne Widup

<sup>4</sup> <https://www.cisecurity.org/>

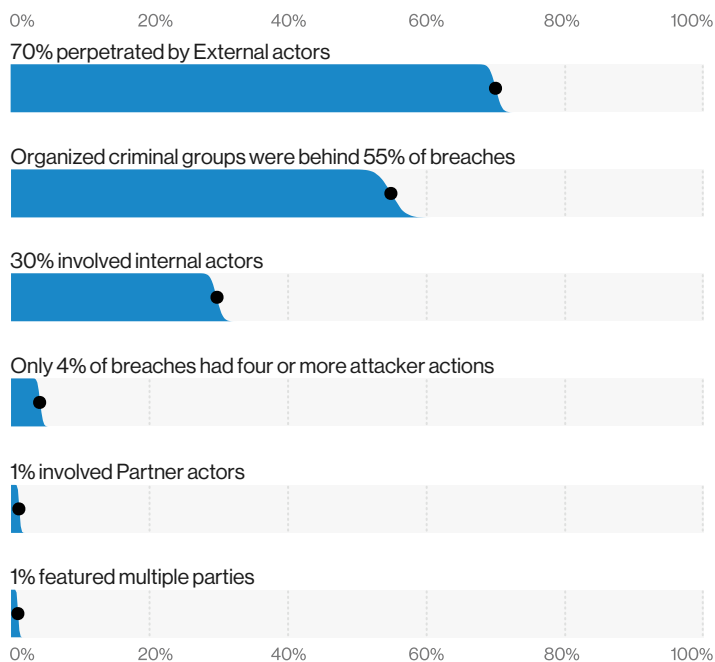
<sup>5</sup> <https://attack.mitre.org/>

# Summary of findings

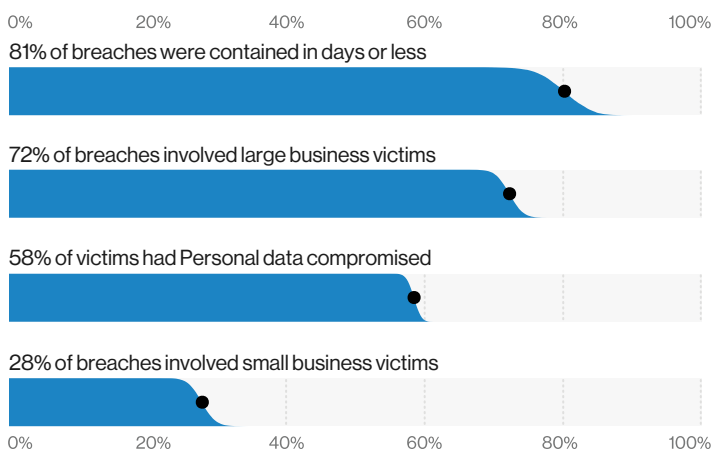
**Figure 2.** What tactics are utilized? (Actions)



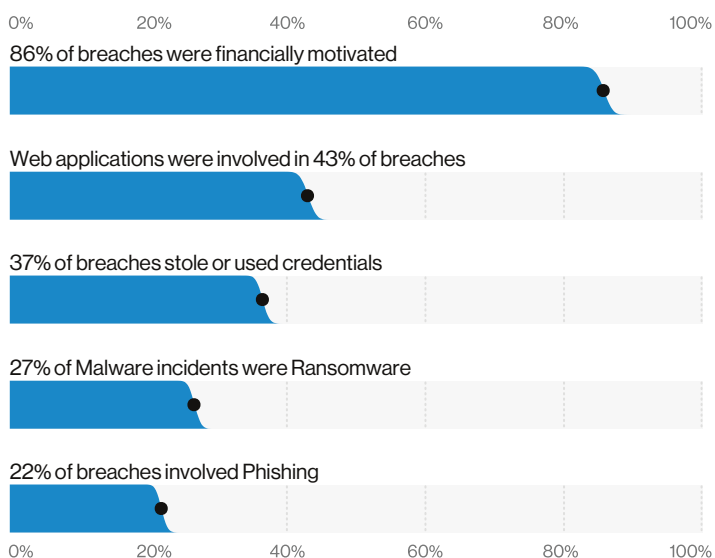
**Figure 3.** Who's behind the breaches?



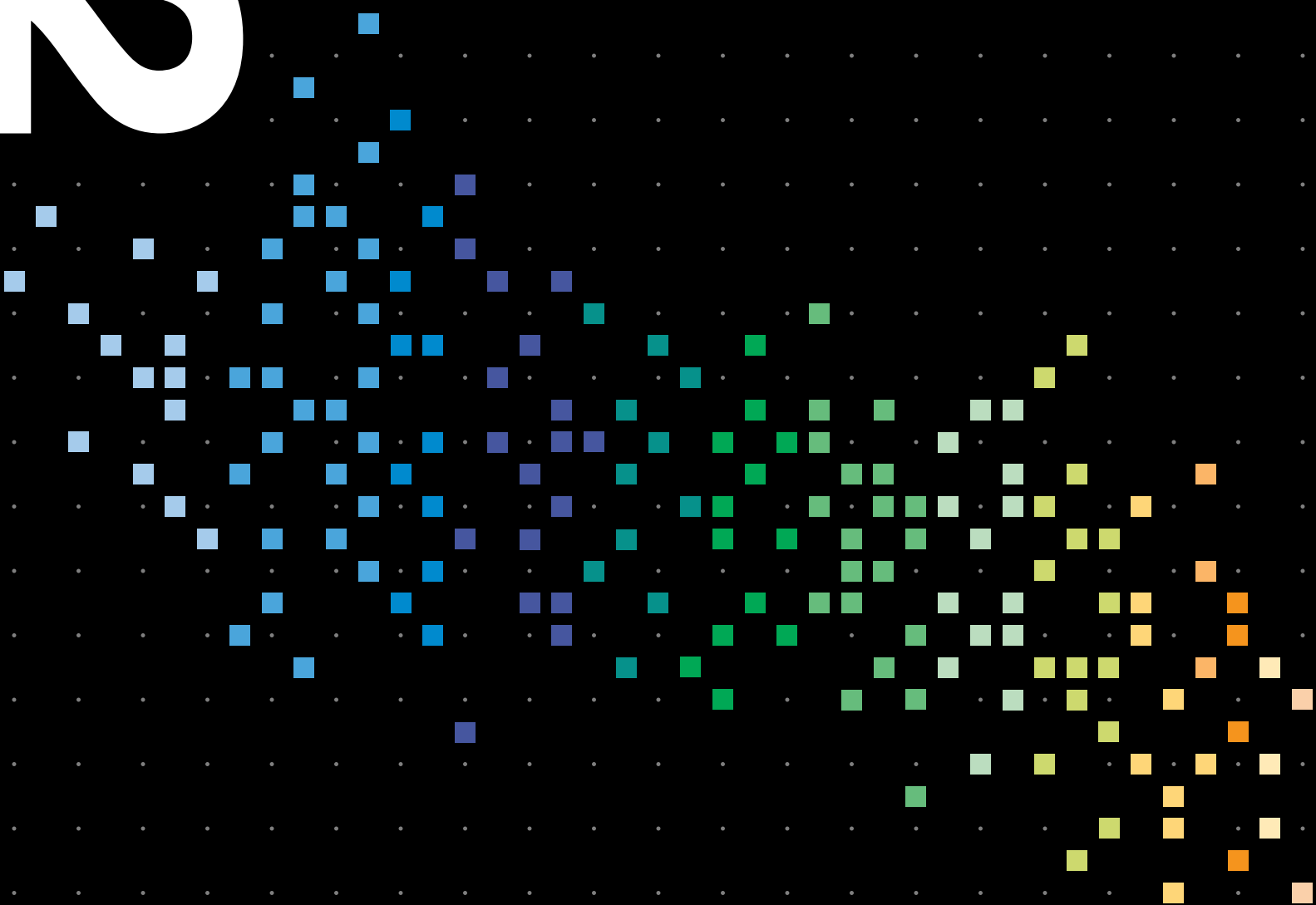
**Figure 4.** Who are the victims?



**Figure 5.** What are the other commonalities?



# 2



---

## Results and analysis



# Results and analysis

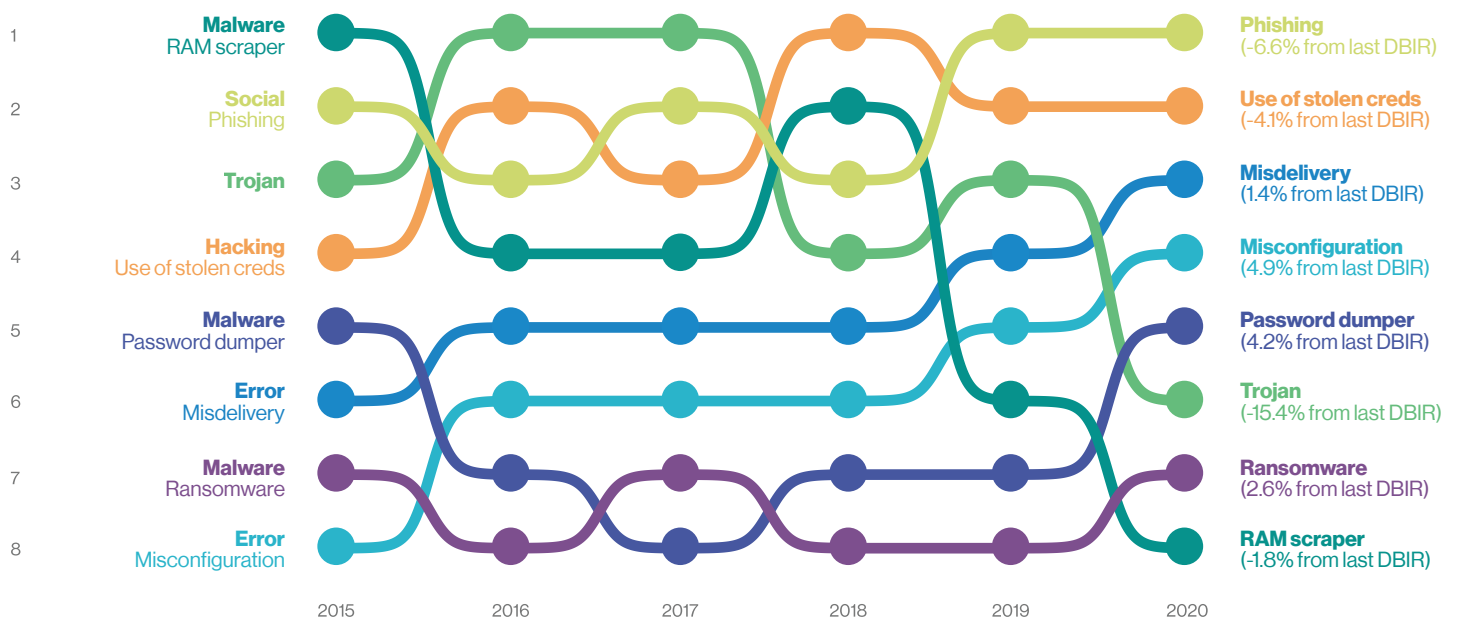
The results found in this and subsequent sections within the report are based on a dataset collected from a variety of sources, including cases provided by the Verizon Threat Research Advisory Center (VTRAC) investigators, cases provided by our external collaborators and publicly disclosed security incidents. The year-to-year data will have new incident and breach sources as we continue to strive to locate and engage with additional organizations that are willing to share information to improve the diversity and coverage of real-world events. This is a sample of convenience,<sup>6</sup> and changes in contributors—both additions and those who were not able to contribute this year—will influence the dataset. Moreover, potential changes in contributors’ areas of focus can shift bias in the sample over time. Still other potential factors, such as how we filter

and subset the data, can affect these results. All of this means that we are not always researching and analyzing the same population. However, they are all taken into consideration and acknowledged where necessary within the text to provide appropriate context to the reader. Having said that, the consistency and clarity we see in our data year-to-year gives us confidence that while the details may change, the major trends are sound.

Now that we have covered the relevant caveats, we can begin to examine some of the main trends you will see while reading through this report. When looking at Figure 6 below, let’s focus for a moment on the Trojan<sup>7</sup> line. When many people think of how hacking attacks play out, they may well envision the attacker dropping a Trojan on a system and then utilizing it as a

beachhead in the network from which to launch other attacks, or to expand the current one. However, our data shows that this type of malware peaked at just under 50% of all breaches in 2016, and has since dropped to only a sixth of what it was at that time (6.5%). Likewise, the trend of falling RAM-scraper malware that we first noticed last year continues. We will discuss that in more detail in the “Retail” section. As this type of malware decreases, we see a corresponding increase in other types of threats. As time goes on, it appears that attackers become increasingly efficient and lean more toward attacks such as phishing and credential theft. But more on those in the “Social” and “Hacking” subsections respectively. Other big players this year, such as Misconfiguration and Misdelivery, will be examined in the “Error” subsection.

**Figure 6.** Select action varieties in breaches over time



<sup>6</sup> Convenience sampling is a type of nonrandom sampling that involves the sample being drawn from that part of the population that is close to hand or available. More details can be found in our “Methodology” section.

<sup>7</sup> This year, we added a Trojan category to Malware. This is a combination of Malware RAT, Malware C2 and Backdoor, Hacking Use of backdoor or C2, and Malware Spyware/Keylogger.

# Actors

Let us begin by disabusing our readers of a couple of widely held, but (according to our data) inaccurate beliefs. As Figure 7 illustrates, in spite of what you may have heard through the grapevine, external attackers are considerably more common in our data than are internal attackers, and always have been. This is actually an intuitive finding, as regardless of how many people there may be in a given organization, there are always more people outside it. Nevertheless, it is a widely held opinion that insiders are the biggest threat to an organization's security, but one that we believe to be erroneous. Admittedly, there is a distinct rise in internal actors in the dataset these past few years, but that is more likely to be an artifact of increased reporting of internal errors rather than evidence of actual malice from internal actors. Additionally, in Figure 8, you'll see that Financially

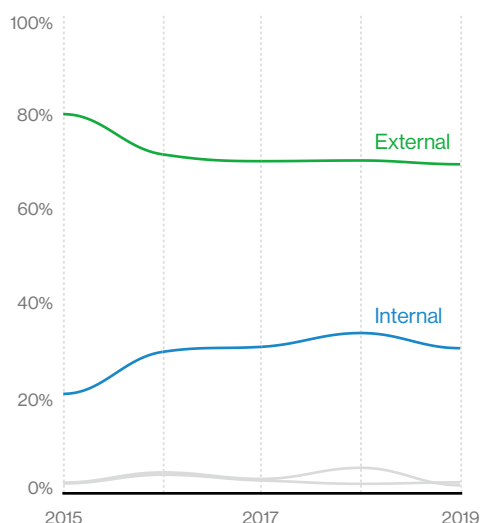
motivated breaches are more common than Espionage by a wide margin, which itself is more common than all other motives (including Fun, Ideology and Grudge, the traditional "go to" motives for movie hackers). There is little doubt that Cyber-Espionage is more interesting and intriguing to read about or watch on TV. However, our dataset indicates that it is involved in less than a fifth of breaches. But don't let that keep you away from the cinema, just make sure to save us some popcorn.

With regard to incidents, Figure 9 illustrates that Financial is still the primary motive, but it must be acknowledged that the Secondary motivation is not far behind. As a refresher (or fresher for our new readers), the compromised infrastructure in Secondary incidents is not the main target, but a means to an end as part of another attack.

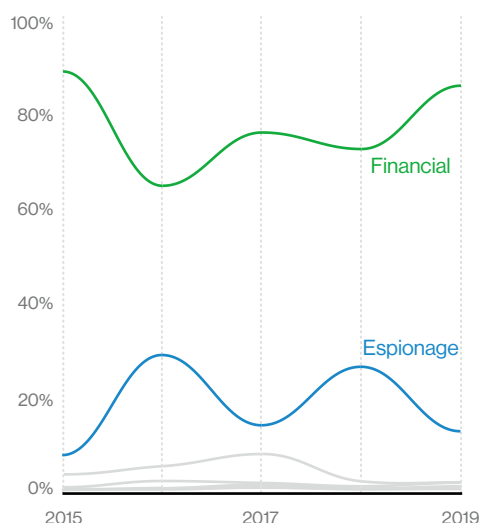
In fact, if we had included the Secondary Web application breaches (we removed this subset as mentioned in the "Incident classification patterns and subsets" section), the Secondary motive category would actually be higher than Financial.

When we look at criminal forums and underground data, 5% refer to a "service." That service could be any number of things including hacking, ransomware, Distributed Denial of Service (DDoS), spam, proxy, credit card crime-related or other illicit activities. Worse still, that "service" may just be hosted on your hardware. The simple fact is this: If you leave your internet-facing assets so unsecured that taking them over can be automated, the attackers will transform your infrastructure into a multi-tenant environment.

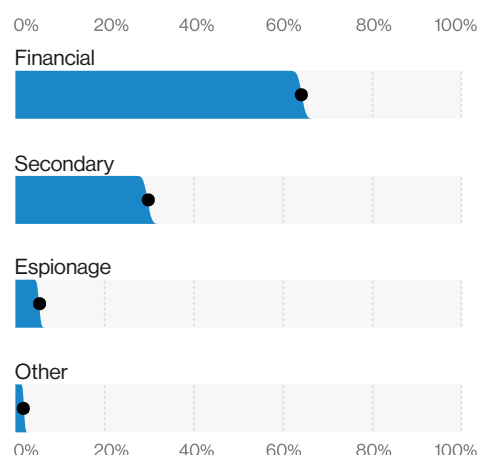
**Figure 7.** Actors over time in breaches



**Figure 8.** Actor motives over time in breaches



**Figure 9.** Top Actor motives in incidents (n = 3,828)





# Actions

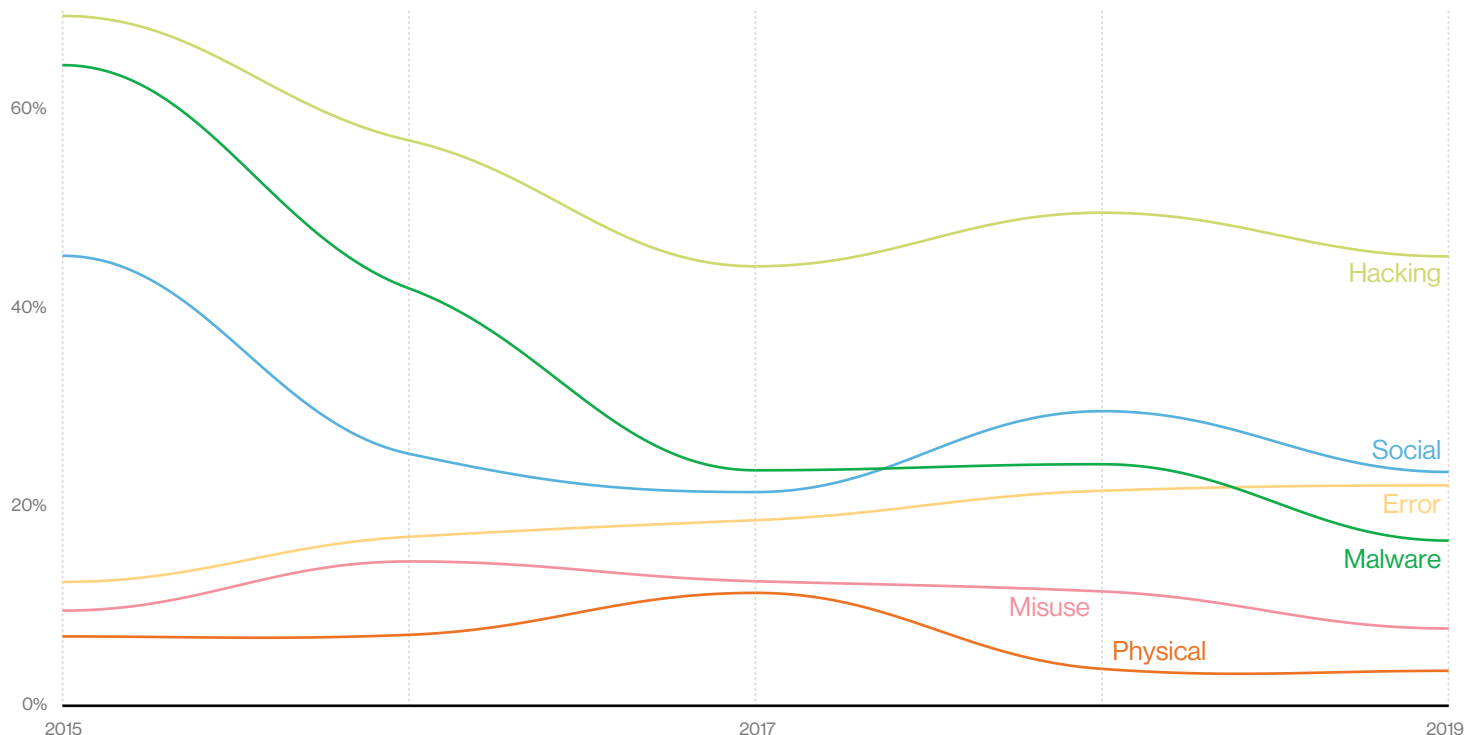
When we analyzed the high-level actions on Figure 11, we found that it mirrors Figure 6. The only action type that is consistently increasing year-to-year in frequency is Error. That isn't really a comforting thought, is it? Nevertheless, there is no getting away from the fact that people can, and frequently do, make mistakes and many of them probably work for you.

Physical breaches have stayed relatively level and infrequent, but Misuse, Hacking, Malware and Social have all decreased since last year's report. While Hacking and Social are down as a percent, they have remained close to the levels we have seen for the past few years. On the other hand, Malware has been on a consistent and steady decline as a percentage of breaches over the last five years.

Why is this? Has malware just gone out of fashion like poofy hair and common courtesy? No, we think that other attack types such as hacking and social breaches benefit from the theft of credentials, which makes it no longer necessary to add malware in order to maintain persistence. So, while we definitely cannot assert that malware has gone the way of the eight-track tape, it is a tool that sits idle in the attacker's toolbox in simpler attack scenarios.

It is important to keep in mind that the points made above are in reference to breaches and not incidents. The incidents tell us a somewhat different story. Ransomware—which in our dataset rarely results in a confirmed breach<sup>12</sup> unless paired with credential use—is on the rise. Still, as malware

tools continue to evolve and improve, there appears to be a sense that malware prevalence is decreasing somewhat, as this causes fewer instances that rise to the status of “incident” for our data contributors. This seems to have the effect on our dataset of a polarization: malware being either part of advanced attacks or the simpler (yet still effective) smash-and-grab compromises.



**Figure 11.** Actions over time in breaches

<sup>12</sup> We are aware of reports of ransomware families that are now capturing data before encrypting so the actors can threaten to also expose the data if the ransom is not paid. However, the cases logged were documented after October 31, 2019, the close date of the data scope for this issue.

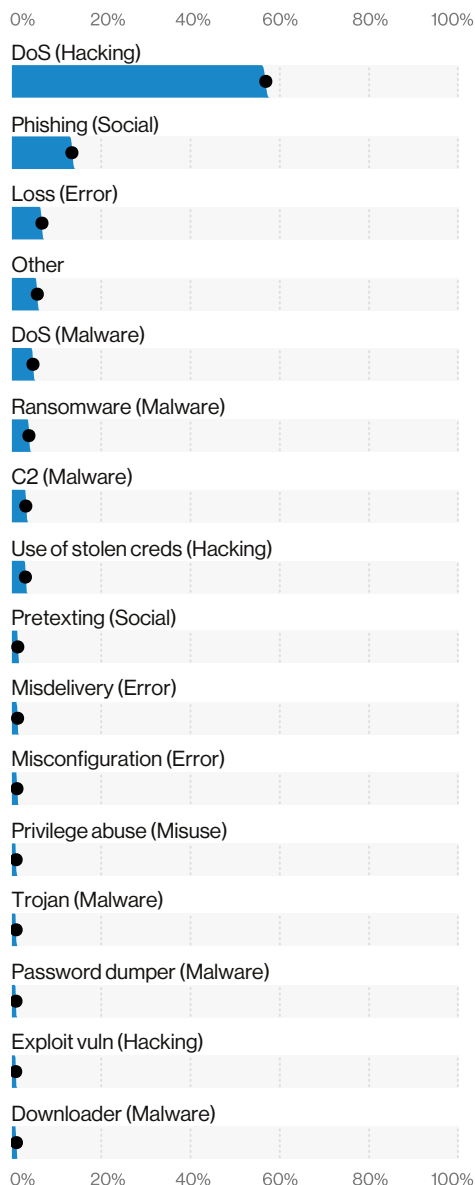
# Threat action varieties

Taking a peek at threat action varieties allows us to dig a bit deeper into the bad guy's toolbox. Figure 12 provides an idea of what action varieties drive incident numbers and, shocker, Denial of Service (DoS) plays a large part. We also see a good bit of phishing, but since data disclosure could not be confirmed, they remain incidents and do not graduate to breach status (but maybe they can if they take a couple of summer classes). In sixth overall, we see ransomware popping up like a poor relation demanding money—which, in many cases, they get.

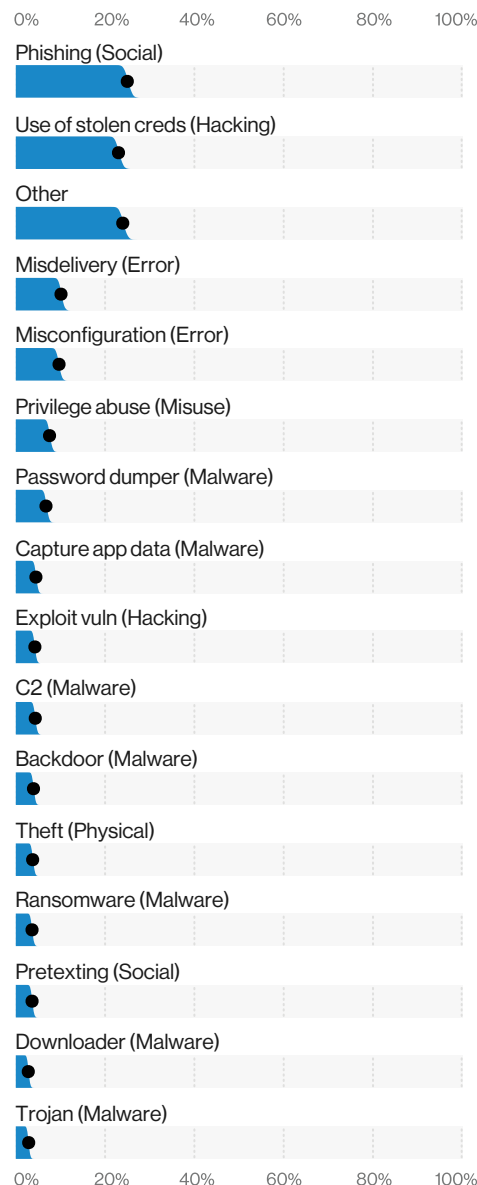
When we again switch back to looking at the top Action varieties for breaches in Figure 13, we see our old foes, Phishing, Use of stolen credentials and Misconfiguration in the top five. Misdelivery is making an impressive showing (mostly documents and email that ended up with the wrong recipients) this year. While we don't have data to prove it, we lean toward the belief that this is an artifact of breach disclosure becoming more normalized (and increasingly required by privacy laws around the world), especially for errors.

Finally, you'll notice "Other" in the mix. As we mentioned in the "DBIR Cheat sheet" section at the very beginning of this report, "Other" represents any enumeration not represented by one of the categories in the figure. It turns out there are a lot of breaches (675 to be specific) that didn't contain any of the top varieties. Breaches (like people and problems) come in many shapes and sizes and are never too far away from your front door.

**Figure 12.** Top threat Action varieties in incidents (n = 23,619)



**Figure 13.** Top threat Action varieties in breaches (n = 2,907)



# Error

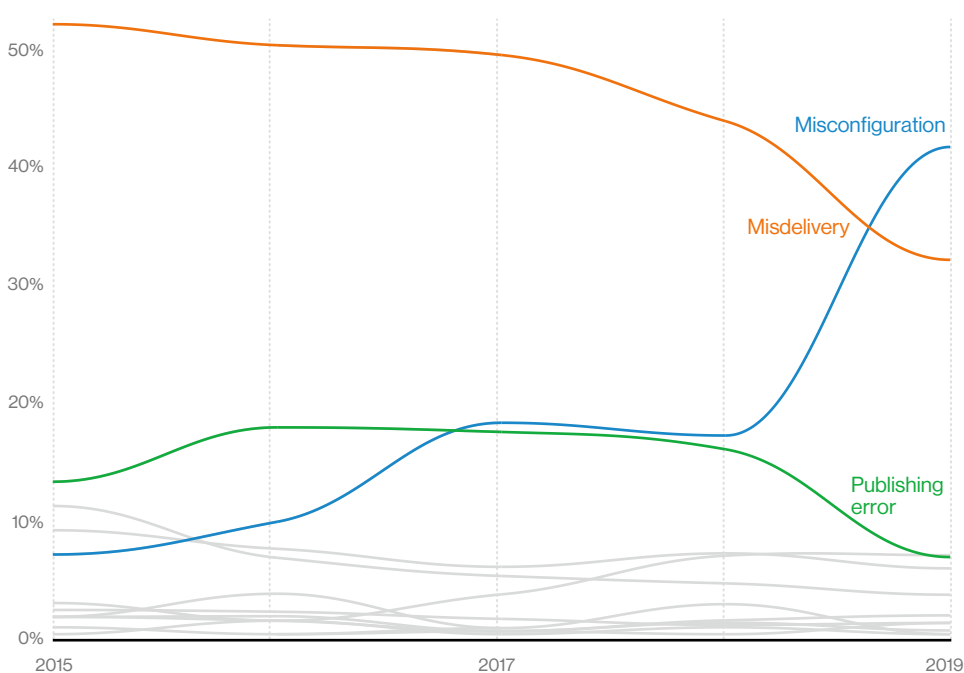
Errors definitely win the award for best supporting action this year. They are now equally as common as Social breaches and more common than Malware, and are truly ubiquitous across all industries. Only Hacking remains higher, and that is due to credential theft and use, which we have already touched upon. In Figure 14 you can see that since 2017, Misconfiguration errors have been increasing. This can be, in large part, associated with internet-exposed storage discovered by security researchers and unrelated third parties. While Publishing errors appear to be decreasing, we wouldn't be surprised if this simply means that errors

formerly attributed to publishing a private document on an organization's infrastructure accidentally now get labeled Misconfiguration because the system admin set the storage to public in the first place.

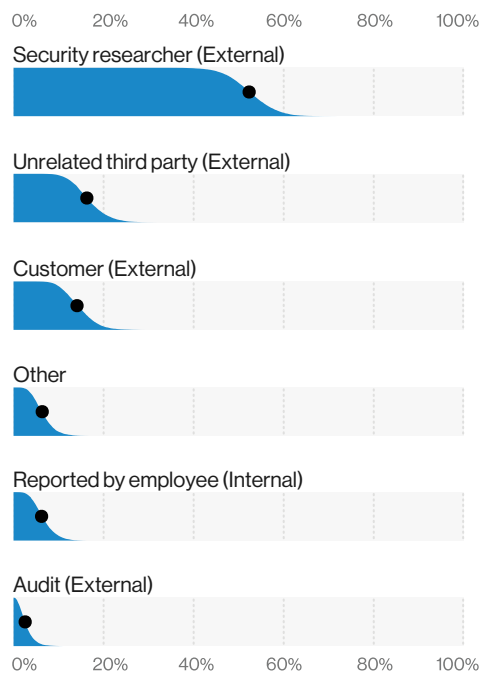
Finally, it is also worth noting what isn't making the list. Loss is down among the single digits this year. Disposal errors are also not really moving the needle. Errors have always been present in high-ish numbers in the DBIR in industries with mandatory reporting requirements, such as Public Administration and Healthcare. The fact that we now see Error becoming more apparent in other industries could mean

we are getting better at admitting our mistakes rather than trying to simply sweep them under the rug.

Of course, it could also mean that since so many of them are caught by security researchers and third parties, the victims have no choice but to utter "mea culpa." Security researcher has become the most likely Discovery method for an Error action breach by a significant amount (Figure 15), being over six times more likely than it was last year. However, we here on the DBIR team are of an optimistic nature, so we will go with the former conclusion.



**Figure 14.** Top Error varieties over time in breaches



**Figure 15.** Top discovery methods in Error breaches (n = 95)

# Malware

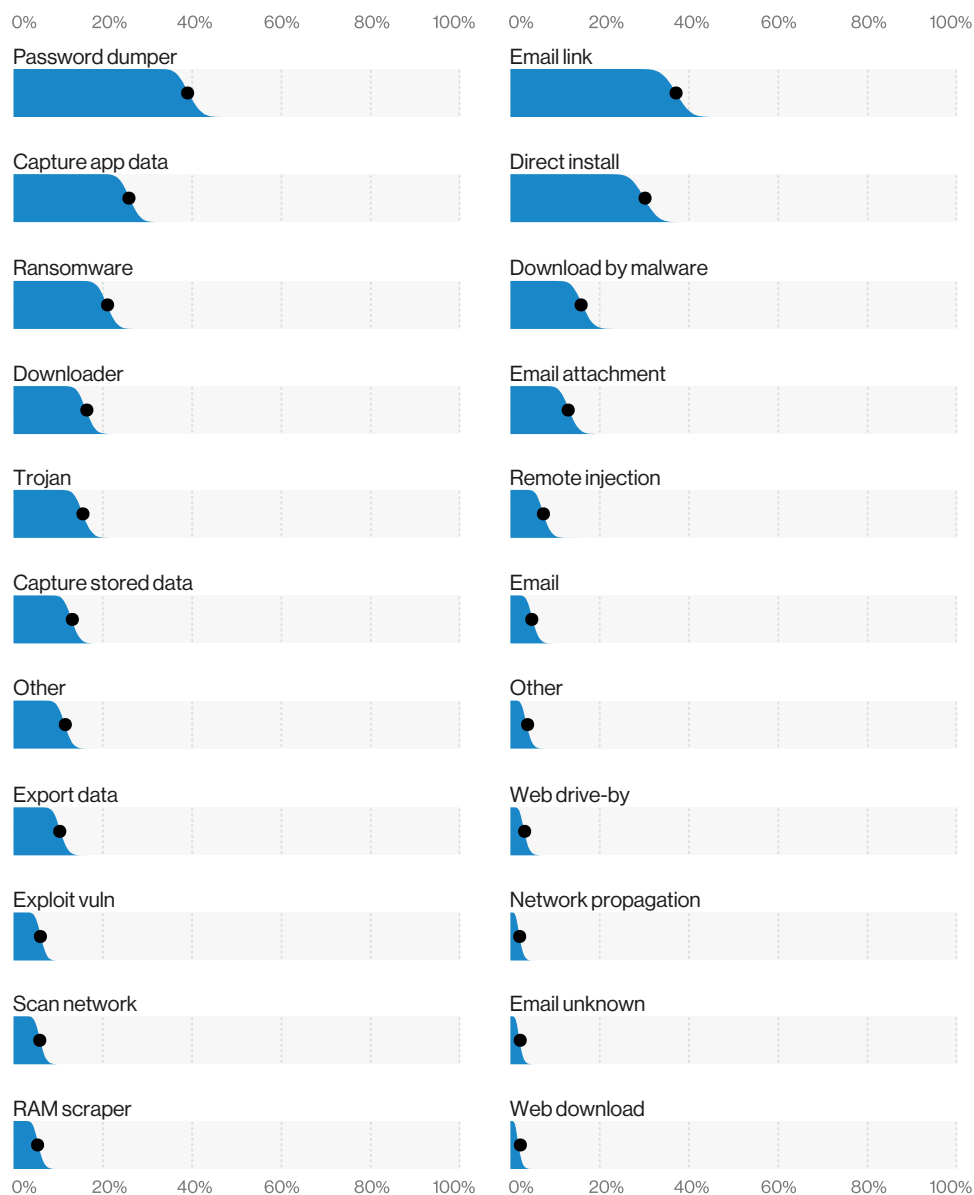
Our Malware findings further reinforce the trends of phishing and obtaining credentials with regard to breaches. As Figure 16 illustrates, Password dumper (used to get those sweet, sweet creds) has taken the top spot among breach Malware varieties. Email (usually associated with Phishing) and Direct install (an avenue generally—but not always—requiring credentials) are the top vectors.

Ransomware is the third most common Malware breach variety and the second most common Malware incident variety. Downloaders follow closely behind Ransomware, and they are clearly doing their jobs, not only moving Ransomware, but also Trojans.<sup>13</sup> It is perhaps worth noting that Cryptocurrency mining doesn't even make the top 10 list, which we know is sure to disappoint all our HODL readers.

However, it is important to acknowledge that the relative percentage of Malware that we see present in breaches and incidents may not correspond to your experiences fighting, cleaning and quarantining malware throughout your own organization. With that in mind, we would like to spend some time talking about bias, more precisely survivorship bias regarding those varieties.

---

**Password dumper (used to get those sweet, sweet creds) has taken the top spot among breach Malware varieties.**



**Figure 16.** Top Malware varieties in breaches (n = 506)

**Figure 17.** Top Malware vectors in breaches (n = 360)

<sup>13</sup> A combination of multiple malware varieties: RAT, Trojan, C2, Backdoor and Spyware/keylogger



## Survivorship bias

**We talk about survivorship bias (or more formally selection bias) in the “Methodology” section, but this is a good place for a call out. You, us, everyone looks at a lot of malware data. Our incident corpus suffers from the opposite of survivorship bias. Breaches and incidents are records of when the victim didn’t survive.**

**On the other hand, malware being blocked by your protective controls is an example of survivorship bias where the potential victim *didn’t* get the malware. Since we have both types of data at our disposal in the DBIR, it can highlight four possible situations:**

- 1. Large numbers in both blocks and incidents:** This is something big. It’s being blocked but also happening a lot
- 2. Large numbers in incidents but not blocks:** This is potentially happening more than it’s being caught
- 3. Large numbers in blocks but not incidents:** We’re doing well at this. It’s getting caught more than it’s getting through
- 4. Small numbers in both blocks and incidents:** This just ain’t happening much

## Ransomware

Traditionally, Ransomware is categorized as an incident in the DBIR and not as a breach, even though it is considered a breach in certain industries for reporting purposes (such as Healthcare) due to regulatory guidance. The reason we consider it only an incident is because the encryption of data does not necessarily result in a confidentiality disclosure. This year, however, ransomware figures more prominently in breaches due in large part to the confirmed compromise of credentials during ransomware attacks. In still other cases, the “breach” designation was due to the fact that personal information was known to have been accessed in addition to the installation of the malware.

Ransomware accounted for 3.5% of unique malware samples submitted for analysis, not such a big number overall. At least one piece of ransomware was blocked by 18% of organizations through the year,<sup>14</sup> even though it presented a fairly good detection rate of 82% in simulated incident data.

However, it shows up heavily in actual incidents and breaches, as discussed previously. This indicates that it falls into category #2 in the survivorship bias callout. It’s a big problem that is getting bigger, and the data indicates a lack of protection from this type of malware in organizations, but that can be stopped. Part of its continued growth can be explained by the ease with which attackers can kick off a ransomware attack. In 7% of the ransomware threads found in criminal forums and market places, “service” was mentioned, suggesting that attackers don’t even need to be able to do the work themselves. They can simply rent the service, kick back, watch cat videos and wait for the loot to roll in.

---

**It’s a big problem that’s continuing to get bigger.**

## Droppers and Trojans

As we pointed out earlier, Trojans, although still in the top five malware varieties, have been decreasing over time. However, their backdoor and remote-control capabilities are still a key functionality for more advanced attackers to operate and achieve their objectives in more intricate campaigns. Downloaders are a common way to get that type of malware on the network, and they made up 19% of malware samples. Nineteen percent were classified as backdoors and 12% were keyloggers.

Droppers and Trojans seem to fall into category #3 in the survivorship bias callout. We see them quite frequently in malware, but they do not necessarily appear in a large number of incidents and breaches. One possible explanation for this is that we might be simply getting better at blocking the cruder and more commoditized versions of this type of malware, thereby pushing unsophisticated attackers increasingly to smash-and-grab tactics. Additionally, the shift to web interfaces for most of our services may simply mean Trojans have a smaller attack surface to exploit.

<sup>14</sup> Please bear in mind that incidents that would result in a Ransomware attack can also be stopped before the malware even manifests itself, so this is maybe an underestimation.



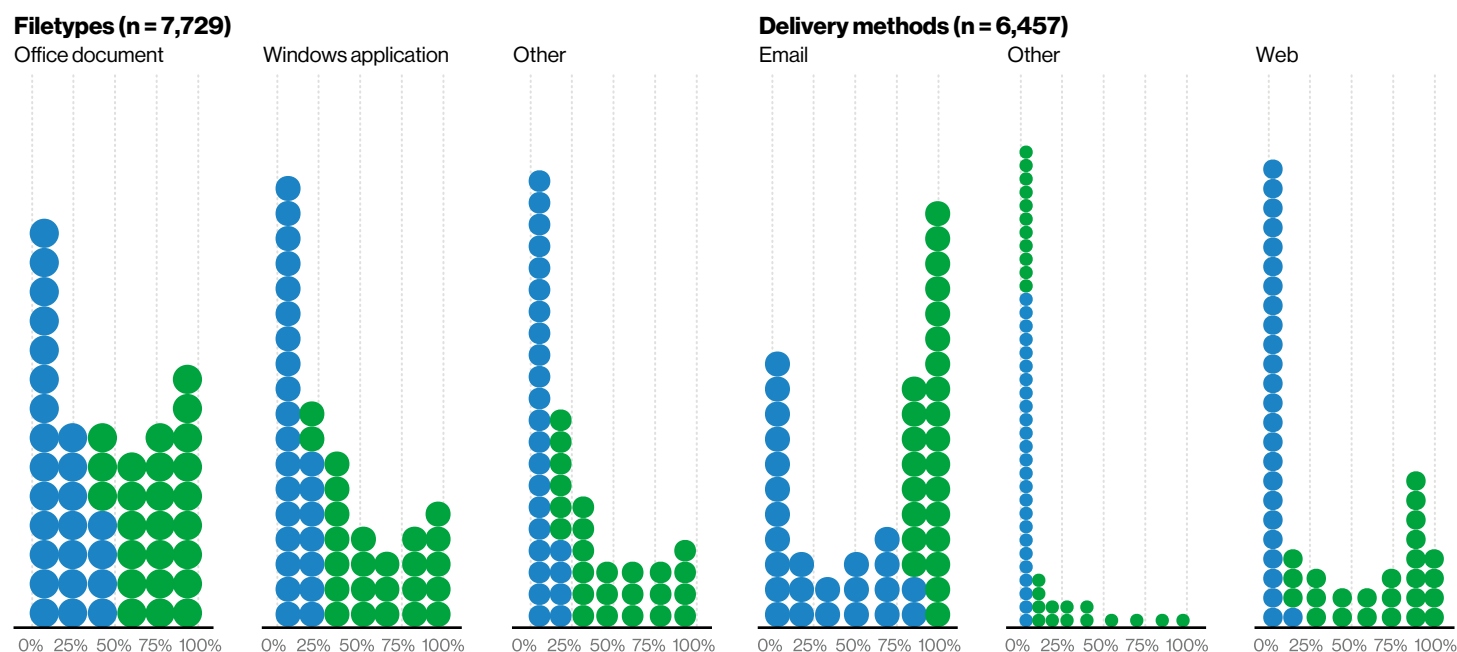
# Malware with vulnerability exploits

If Droppers and Trojans are examples of category #3, then Malware that exploits vulnerabilities falls under category #4. It ranks at the bottom of malware varieties in Figure 16. Figure 25 (ahead in the “Hacking” section) shows that exploiting vulnerabilities in Malware is even more rare than in Hacking (where it’s already relatively scarce). While successful exploitation of vulnerabilities does still occur (particularly for low-hanging fruit as in Figure 22—also in the “Hacking” section), if your organization has a reasonable patch process in place, and you do not have a state-aligned adversary targeting you, then your time might be better spent attending to other threat varieties.

## Cryptocurrency mining

The cryptocurrency mining malware variety falls squarely into category #4. It accounted for a mere 2.5% of malware among breaches and only 1.5% of malware for incidents. Around 10% of organizations received (and blocked) Cryptocurrency mining malware at some point throughout the course of the year.<sup>15</sup>

The breach simulation data clues us in on what might be happening, as it indicates that the median block rate for cryptocurrency mining malware was very high. Another valid theory is that cryptomining occurrences rarely rise to the level of “reported incident” unless we are talking about instances running on stolen cloud infrastructure. These cost your organization a lot of money while generating less loose change than the threat actor could have found in their couch cushions.



**Figure 18.** Top malware filetypes and delivery methods

<sup>15</sup> The potential underestimation from incidents being stopped before the malware manifests itself is also valid here.

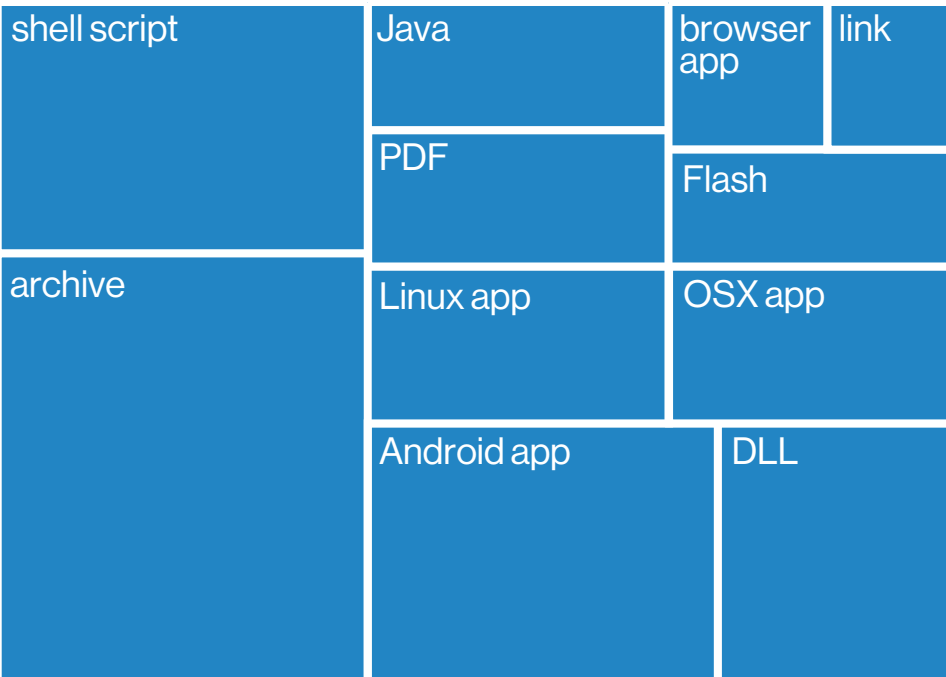
# Malware delivery

Finally, this year we’ve dug a bit deeper into the malware delivery methods. Office documents and Windows® apps still tend to be the malware filetype of choice; however, the “Other” category has also grown relatively large. Most malware is still delivered by email, with a smaller amount arriving via web services, and almost none by other services (at least when detected).

One takeaway from Figure 18 is that the “average” really doesn’t represent a great many companies. For example, approximately 22% of organizations

got almost none of their malware via email, while about 46% got almost all of theirs that way. If you look at the Office documents part of the malware filetypes chart, other than a spike of organizations near 0%, all the other dot piles are almost the same – meaning that type of delivery is almost uniformly distributed. When attempting to determine what percentage of malware your organization would receive as an Office document, you would be as likely to be correct by throwing a dart at that figure<sup>16</sup> as by basing it on data. This is not to indicate that it is low, just that it is simply all over the map.

Speaking of maps, Figure 19 provides a glimpse at the other filetypes of malware organizations typically see. It lacks the detail of Figure 18, but still serves as an adequate visual reminder that malware comes in a variety of types, most of which apparently look like lengths of hardwood flooring. Thankfully, as we stated previously, malware is not showing up as frequently in incidents and breaches. So, if you obtain a good tool to block it where possible you can focus your attention on more pressing matters.<sup>17</sup>



**Figure 19.** Other malware filetypes (n = 13.6 million)

<sup>16</sup> Other than zero obviously. And please exercise caution with sharp objects around coworkers, family members and pets if you attempt this.  
<sup>17</sup> Credential theft and use, Phishing and Errors.

# Hacking

At a high level, Hacking can be viewed as falling into three distinct groups:

1) those utilizing stolen or brute-forced credentials; 2) those exploiting vulnerabilities; and 3) attacks using backdoors and Command and Control (C2) functionality.

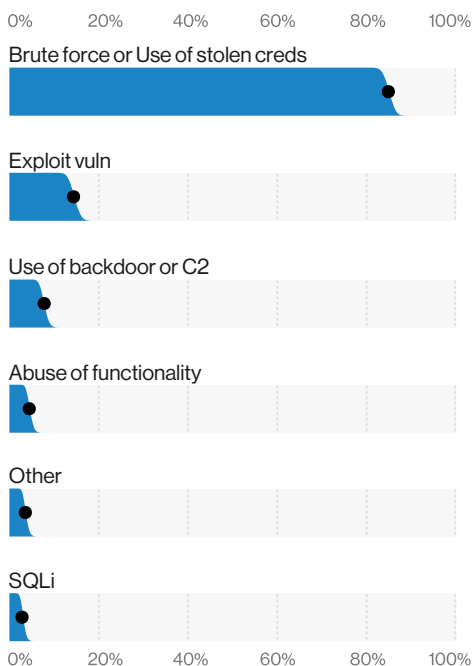
However, it must be said that Hacking and even breaches in general (at least in our dataset) are driven by credential theft. Over 80% of breaches within Hacking involve Brute force or the Use of lost or stolen credentials. These Hacking varieties (Figure 20 below), along with exploitation of a vulnerability (of which SQLi is a part), are associated in a major way with web applications as illustrated in Figure 21. We have spent

some time on this over the last year, and it is important to reassert that this trend of having web applications as the vector of these attacks is not going away. This is associated with the shift of valuable data to the cloud, including email accounts and business-related processes.

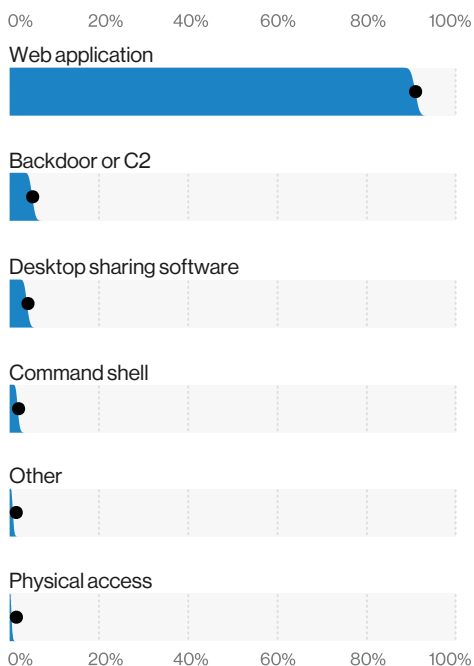
Use of backdoor or C2 (checking in at third place) are both associated with more advanced threats, since, for more intricate campaigns and data exfiltration missions, there is nothing quite like the human touch. For better or worse, the promise of fully autonomous Artificial Hacking Intelligence (AHI) is still at least 15 years away,<sup>18</sup> along with flying cars.

---

**Over 80% of breaches within Hacking involve Brute force or the Use of lost or stolen credentials.**

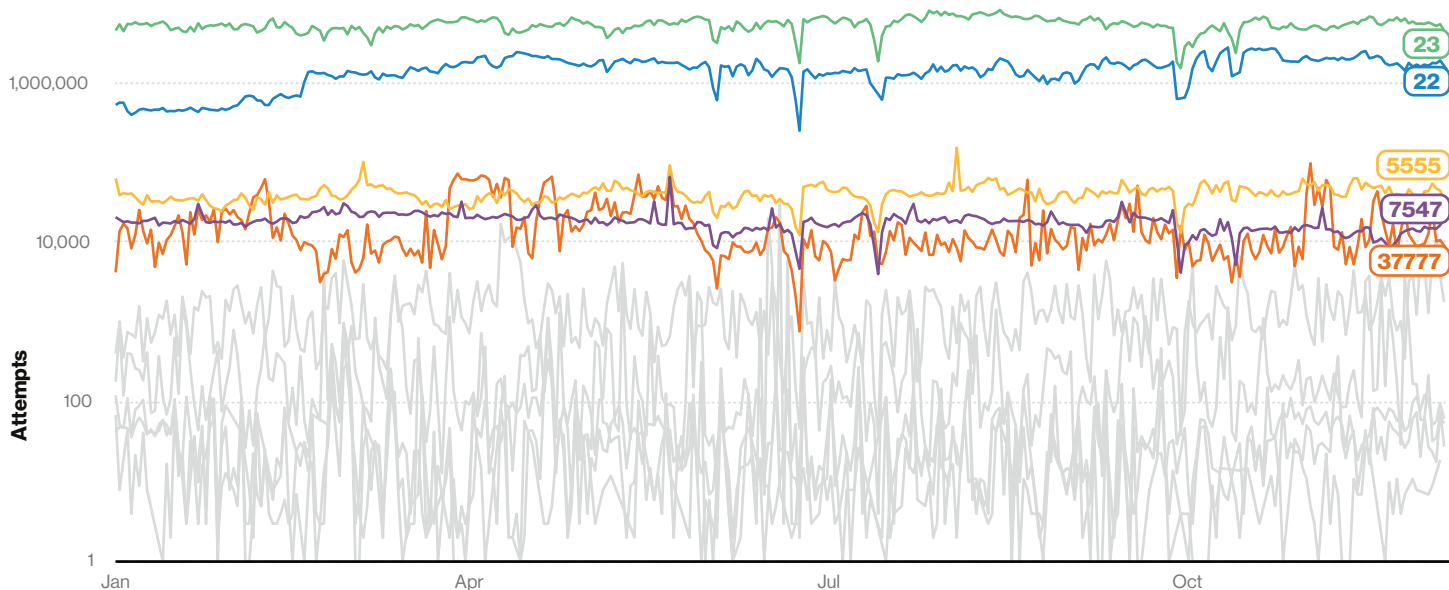


**Figure 20.** Top Hacking varieties in breaches (n = 868)



**Figure 21.** Top Hacking vectors in breaches (n = 1,361)

<sup>18</sup> [citation needed] I read this in some vendor marketing copy somewhere, I'm sure. OK, I didn't, but doesn't it sound like something I would?



**Figure 22.** Connection attempts by port over time in honeypot data (n = 2.55 billion)

## Using and abusing credentials

Criminals are clearly in love with credentials, and why not since they make their jobs much easier? If you refer back to Figure 6 at the very beginning of the Results and Analysis section, it is apparent that use of credentials has been on a meteoric rise. Figure 22 represents connection attempts by port over time based on contributor honeypot data, and provides another take on the topic. As it depicts, SSH (port 22) and Telnet (port 23) connection attempts are two orders of magnitude<sup>19</sup> above the next cluster of services. Let's explore credential stuffing and then move on to exploiting vulnerabilities.

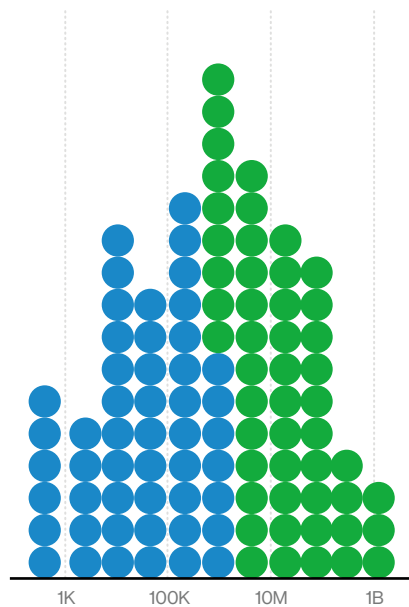
Additional contributor data sheds light onto the credential stuffing attacks criminals are attempting. Figure 23<sup>20</sup> shows the number of attempts orgs who had any credential stuffing attempts typically received. As you will notice, it is a relatively smooth bell curve with a median of 922,331. Granted, a good number of those login/password combos attempted will be as complex as "admin/admin" or "root/hunter2" but those sustained attacks over time are succeeding according to our incident dataset.

Something you might be wondering is "Do credential leaks lead to more credential stuffing?" We took a look at a dataset of credential leaks and compared it to the credential stuffing data we had. You can see in Figure 24 that the answer is no.<sup>21</sup> We found basically no relationship between a credential leak and the amount of credential stuffing that occurred the week after. Instead it appears to be a ubiquitous process that moves at a more or less consistent pace: Get a leak, append to your dictionary, continue brute forcing the internet. Rinse, repeat.

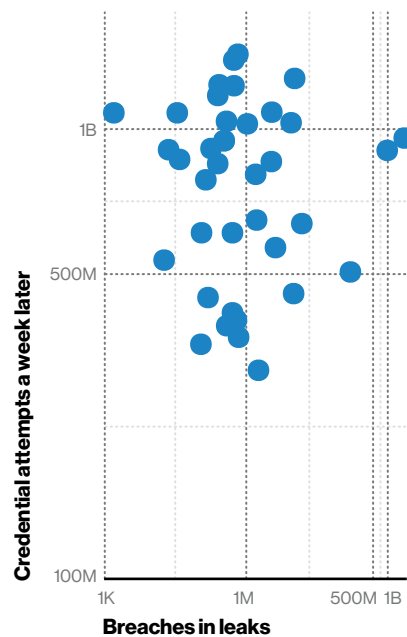
<sup>19</sup> They may seem close, but that is a log scale ([https://en.wikipedia.org/wiki/Logarithmic\\_scale](https://en.wikipedia.org/wiki/Logarithmic_scale)).

<sup>20</sup> If this figure is confusing, see the dot plot explanation in the "DBIR Cheat sheet" section.

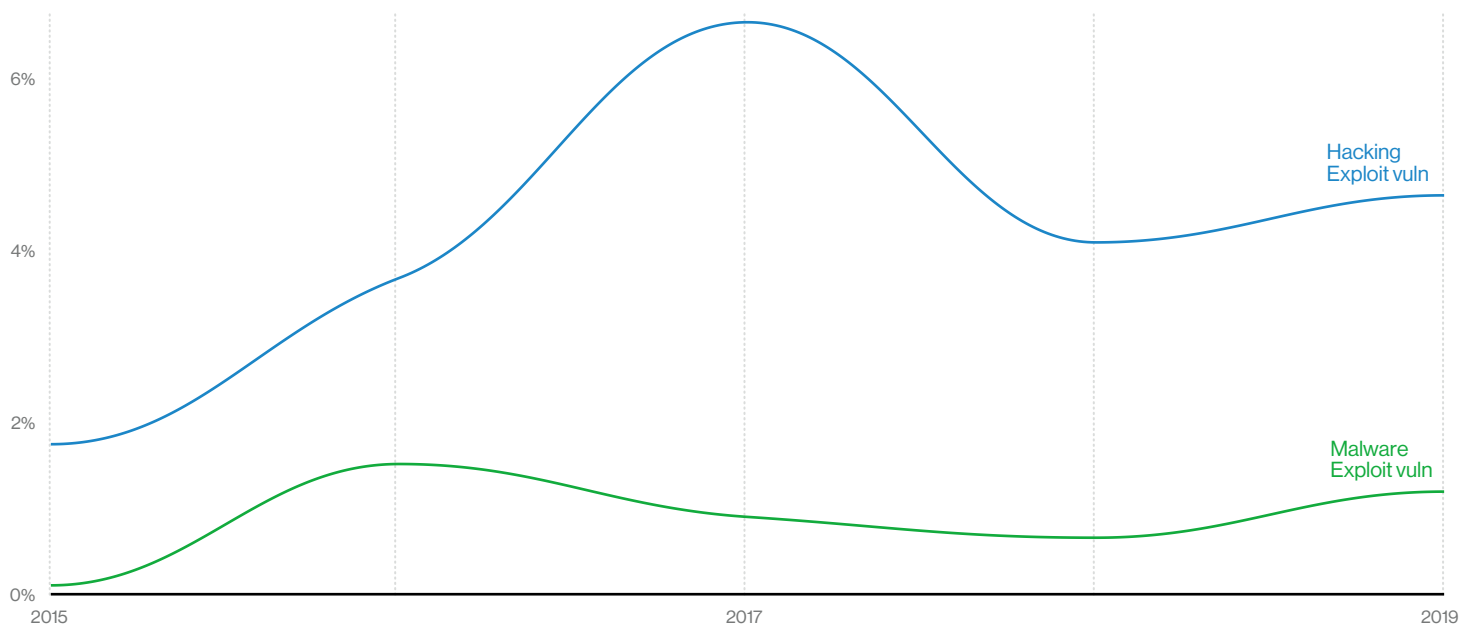
<sup>21</sup> Where are my negative result experiment fans? A toast to science, my colleagues!



**Figure 23.** Credential attempts per org per year (n = 631)



**Figure 24.** Relationship between credential leads and credential attempts one week later.  $R^2 = 0.006$  (n = 37)



**Figure 25.** Vulnerability exploitation over time in breaches

# Exploiting vulnerabilities

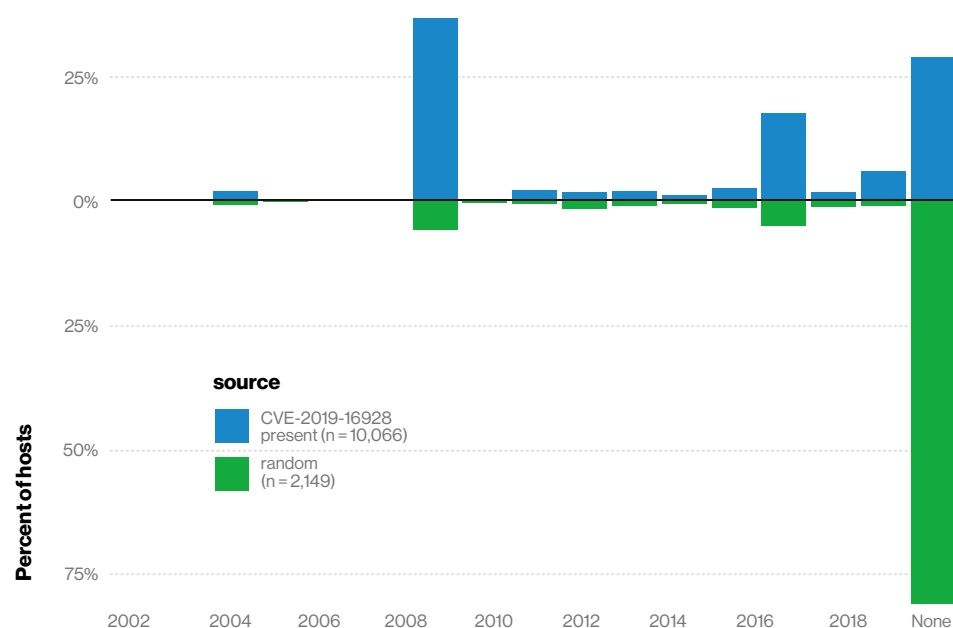
Vulnerabilities occupy a huge amount of mind-share in information security. Yet, harkening back to that bit about survivorship bias in the “Malware” section, it’s more of situation #3 than situation #1. There are lots of vulnerabilities discovered, and lots of vulnerabilities found by organizations scanning and patching, but a relatively small percentage of them are used in breaches, as you can see in Figure 25. Although exploiting vulnerabilities is in second place in breach Hacking varieties, it has not played a major role within incidents found in the DBIR over the last five years. In fact, it reached its peak at just over 5% as a Hacking variety in 2017. In our security information and event management (SIEM) dataset, most organizations had 2.5% or less of alerts involving exploitation of a vulnerability.<sup>22</sup>

But that doesn’t mean that the attackers don’t give it a try anyway. Clearly, the attackers are out there and if you leave unpatched stuff on the internet, they’ll find it and add it to their infrastructure.<sup>23</sup> We hear a lot about new vulnerabilities and their prevalence both on the internet and within organizations. Does the internet as a whole become more vulnerable with every new vulnerability that gets discovered?<sup>24</sup> And are those unpatched vulnerabilities that are adding to the problem likely to be present on *your* systems?

To test whether that<sup>25</sup> is true, we conducted a little investigation this summer. We looked at two sets of servers hosted on public IP addresses: ones vulnerable to an Exim vulnerability discovered in 2019<sup>26</sup> and randomly

chosen IPs. As we see in Figure 26, hosts that were vulnerable to the Exim vulnerability were also vulnerable to 10-year-old SSH vulnerabilities<sup>27</sup> much more frequently than the random sample.

The takeaway is that it wasn’t just the Exim vulnerability that wasn’t patched on those servers. NOTHING was patched. For the most part, no, the internet as a whole does not seem to be getting less secure with each new vulnerability, at least not after the short window before organizations that are on top of their patch management update their systems.<sup>28</sup> You can just as easily exploit those vulnerable servers with that I33t 10-year-old exploit you got from your h4x0r friend on Usenet.



**Figure 26.** Comparing oldest other vulnerability for internet-facing hosts with EXIM CVE-2019-16928 vs randomly selected hosts

22 Caveat emptor, to do this we used existing contributor mappings to MITRE ATT&CK and traced to our VCAF mapping as discussed in Appendix B.

23 Granted, I don’t have any studies that show that stealing CPU cycles is a lot cheaper than traditional infrastructure as a service (IaaS), but given my last cloud services bill, I don’t see how it couldn’t be.

24 TL;DR: Mostly no. Not for long anyway.

25 Does the internet as a whole get more vulnerable with each new vulnerability?

26 CVE-2019-16928

27 And basically, every vulnerability since then

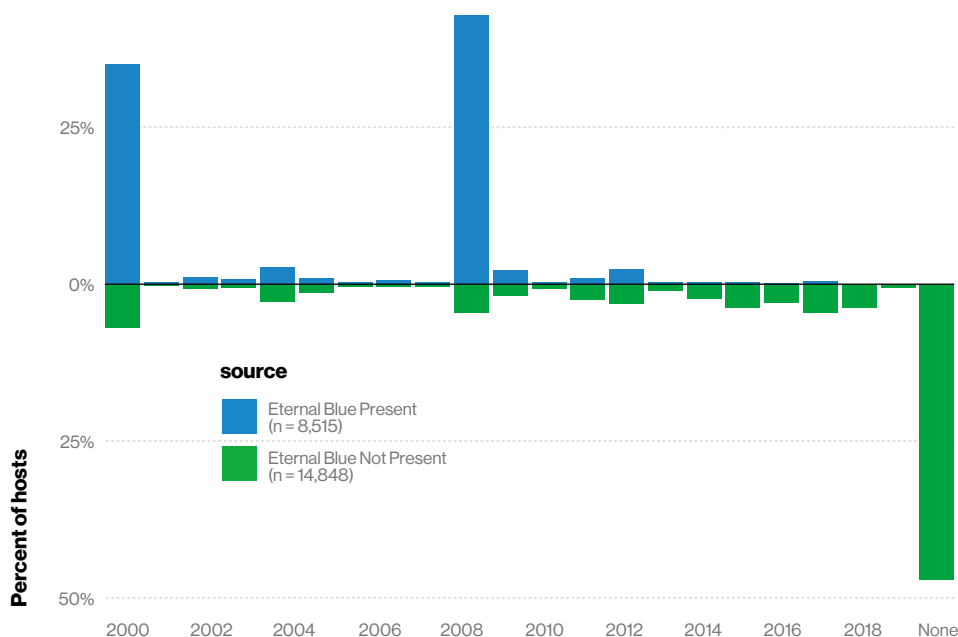
28 Shout-out to our summer intern Quinnan Gill who did this research for us. You’re awesome!

But what about the second question: Are those likely to be *your* systems that are vulnerable?<sup>29</sup> To test this, we took two samples from vulnerability scan data: organizations with the Eternal Blue vulnerability<sup>30</sup> present on their systems and those without. In Figure 27,<sup>31</sup> we see the same thing as in Figure 26. The systems that were vulnerable to Eternal Blue were also vulnerable to everything from the last decade or two. Once again, no, each new vulnerability is not making you that much more vulnerable. Organizations that patch seem to be able to maintain a good, prioritized patch management regime.

Still, we're not in the fourth survivorship bias situation here. Attackers *will* try easy-to-exploit vulnerabilities if they encounter them while driving around the internet. Since you just came from the "Credentials" section, you may remember that Figure 22, which illustrates that once you get below the SSH and Telnet lines on the chart, the next three services that we conveniently highlighted are port 5555 (Android Debug Bridge, or adb—really popular lately), port 7547 (common router RPC port) and port 37777 (popular with IP cameras and DVRs).

If you will allow us a mixed metaphor, there is no outrunning the bear in this case, because the bears are all being 3D-printed in bulk and automated to hunt you.

So, carry on my wayward son and keep doing what you're doing (you know, patching), and perhaps skip over to the "Assets" section to get an inkling of what you might be missing.



**Figure 27.** Comparing oldest other vulnerability for hosts with Eternal Blue vs hosts without

29 TL;DR: Again, probably not. If you are patching, of course.

30 CVE-2017-0144

31 We use Eternal Blue here and the Exim vulnerability in Figure 26 because the analysis for Figure 26 came from the summer while Figure 27 data is from last year, potentially before CVE-2019-16928.

# Social

If action types were people, you would probably give Hacking, Malware and Error a wide berth because they just sound like they would be less than friendly. But Social sounds as though it would be much more happy-go-lucky. More likely to house-sit for you, invite you to play bunko and include you in neighborhood barbecues. You'd be wrong though. Social comes with a devious attitude and a "take me to your manager" haircut. Figure 28 shows Social broken down into two types of incidents: Phishing and Pretexting.<sup>32</sup> When it comes to breaches, the ratio remains quite similar, only with slightly lower numbers.

Social actions arrived via email 96% of the time, while 3% arrived through a website. A little over 1% were associated with Phone or SMS, which is similar to the amount found in Documents. If you take a glance at Figure 29, you'll notice that while credentials are by far the most common attribute compromised in phishing breaches, many other data types are also well represented. Phishing has been (and still remains) a fruitful method for attackers. The good news is that click rates are as low as they ever have been (3.4%), and reporting rates are rising, albeit slowly (Figure 30).

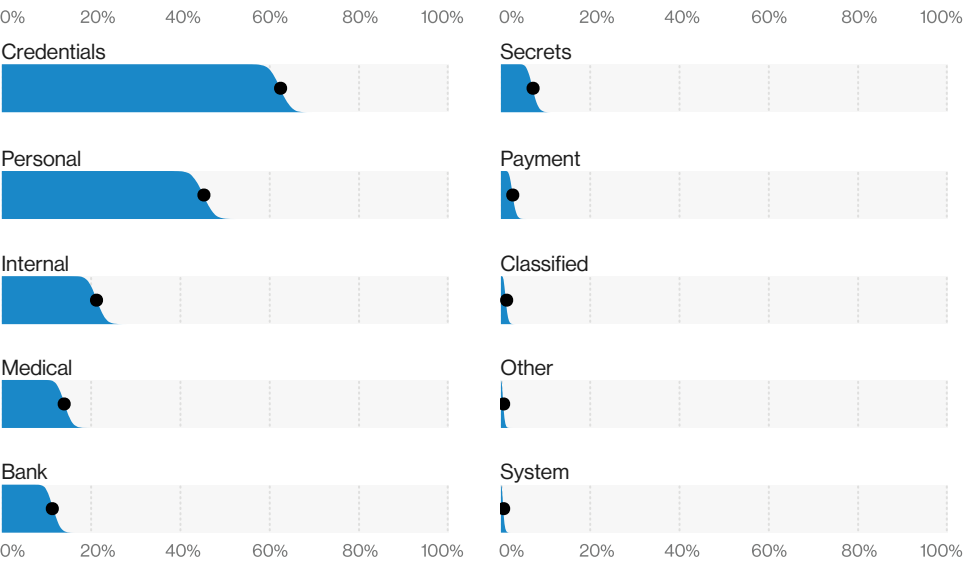


Figure 29. Top data varieties compromised in Phishing breaches (n = 619)

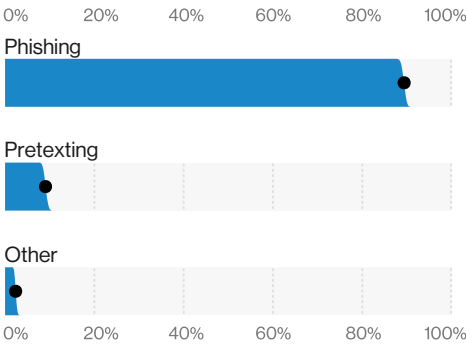


Figure 28. Top Social varieties in incidents (n = 3,594)

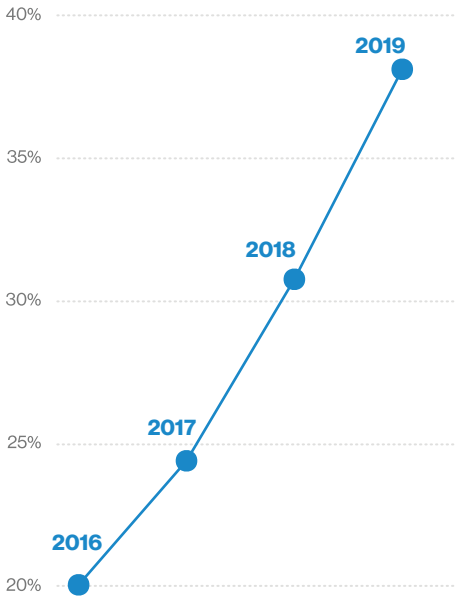


Figure 30. How many phishing test campaigns are reported at least once

32. Often business email compromises (BECs), but given that it works even if you don't compromise an email address, you might see us referring to Financially Motivated Social Engineering or FMSE.



# Financially Motivated Social Engineering

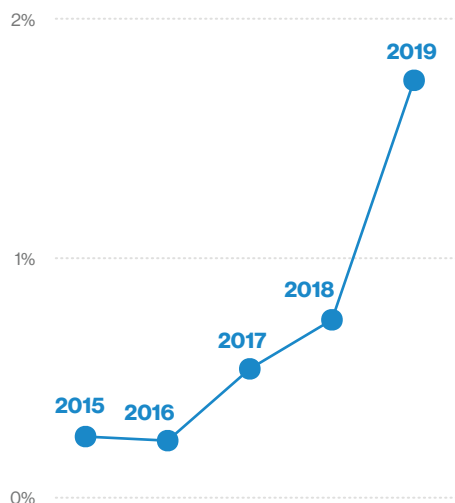
Financially Motivated Social Engineering (FMSE) keeps increasing year-over-year (Figure 31), and although it is a small percentage of incidents, in raw counts, there were over 500 in our dataset this year. These attacks typically end up in our Everything Else pattern, as they are purely social in nature. There is no malware component, as you would see in the more advanced nation-state scenario, nor is there any effort to gain a foothold and remain persistent in the victim's network. These are simply a “get what you can when you can” kind of attack.

This is not to say that they cannot be sophisticated in the lengths the adversary is willing to go to for success. In prior years, they would impersonate CEOs and other high-level executives and request W-2 data of employees. They have largely changed their tactics to just asking for the cash directly—why waste time with monetizing data? It's so inefficient. Their inventiveness in the pretext scenario to lend a level of believability to their attempt is a measure of how good these people are at their jobs.

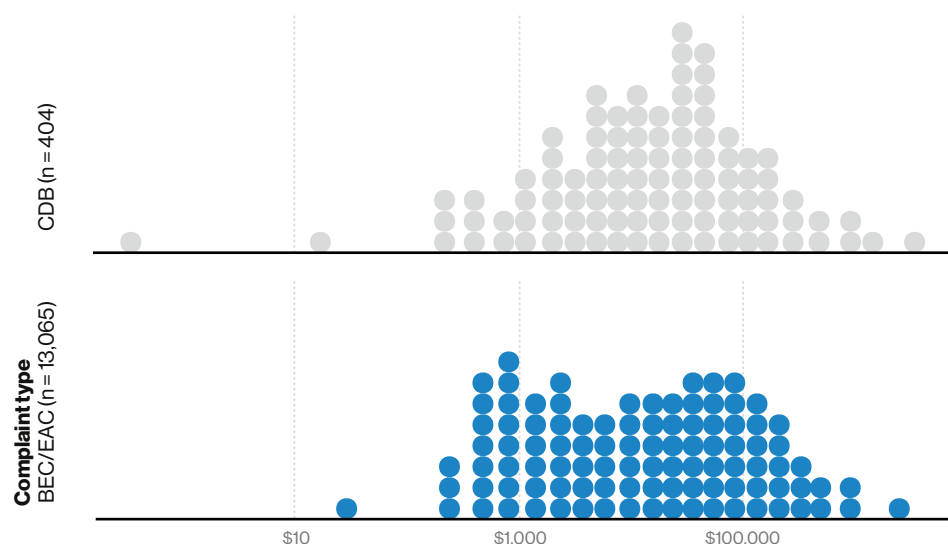
Last year, we looked at the median impact cost for incidents reported to the FBI IC3. With regard to business

email compromises (BEC), we noticed that most companies either lost \$1,240 or \$44,000 with the latter being slightly more frequent (Figure 32).

Also, last year we stated that when “the IC3 Recovery Asset Team acts upon BECs, and works with the destination bank, half of all U.S.-based business email compromise victims had 99% of the money recovered or frozen; and only 9% had nothing recovered.” They continued to record that metric and this year it improved slightly, indicating that 52% recovered 99% or more of the stolen funds and only 8% recovered nothing.



**Figure 31.** Financially Motivated Social Engineering (FMSE) over time in incidents

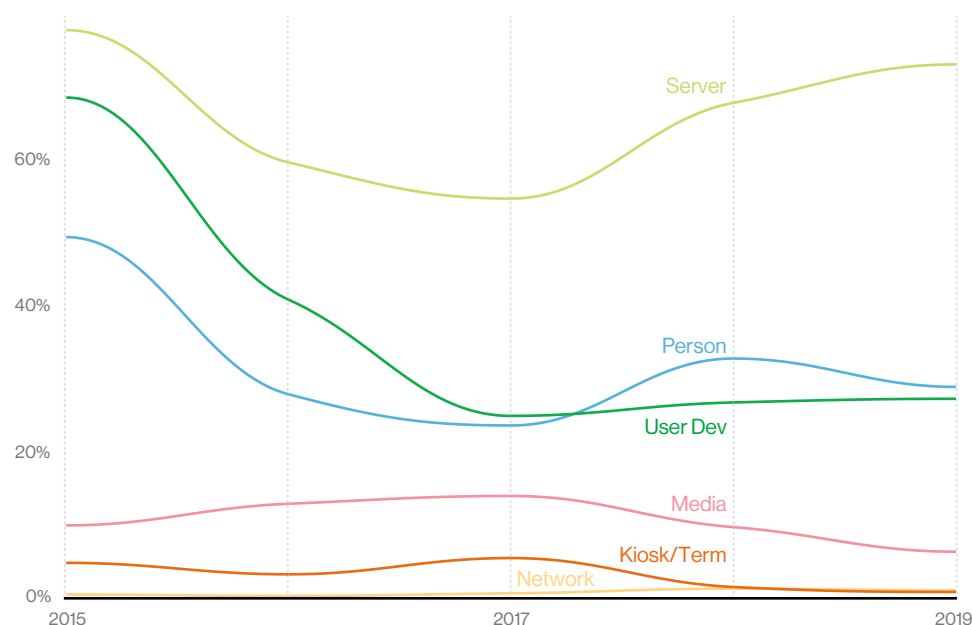


**Figure 32.** Loss amount in Corporate Data Breaches (CDB) and business email compromises/(individual) email account compromises (BEC/EAC) (Excludes complaints with zero loss amount)

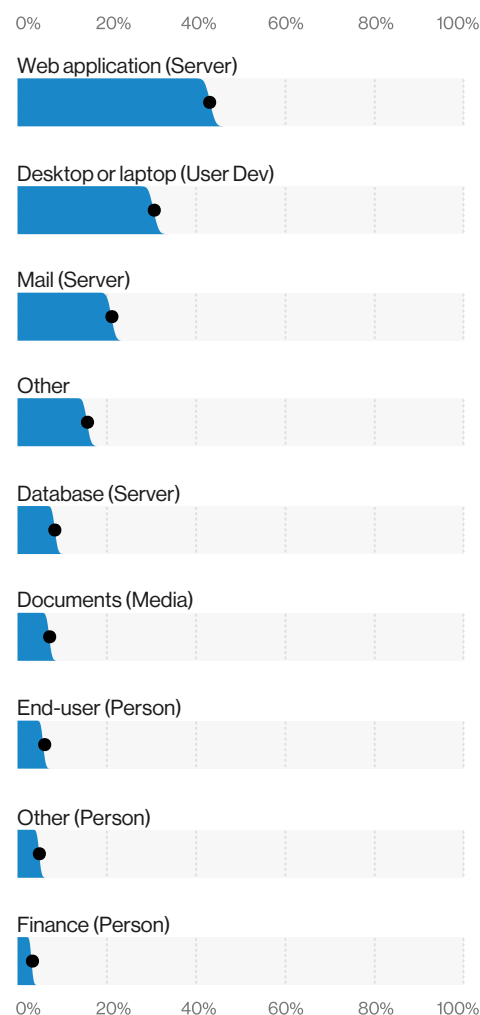
# Assets

Figure 33 provides an overview of the asset landscape. Servers are the clear leader and they continue to rise. This is mainly due to a shift in industry toward web applications (the most common asset variety in Figure 34) with system interfaces delivered as a software as a service (SaaS), moving away from that seven-year-old spreadsheet with those great macros that Bob from accounting put together. Person<sup>33</sup> holds second place for the second year in a row, which is not surprising given how Social actions have stayed relevant throughout this period.

Kiosks and Terminals continued to decline as they did last year. This is primarily due to attackers transitioning to “card not present” retail as the focus of their efforts, rather than brick-and-mortar establishments.



**Figure 33.** Assets over time in breaches



**Figure 34.** Top Asset varieties in breaches (n = 2,667)

<sup>33</sup> I know it is weird, maybe even dehumanizing, to think of a Person as an asset but this is meant to represent the affected party in an attack that has a social engineering component. People have security attributes too!

# Head in the clouds

Cloud assets were involved in about 24% of breaches this year, while on-premises assets are still 70%<sup>34</sup> in our reported breaches dataset. Cloud breaches involved an email or web application server 73% of the time. Additionally, 77% of those cloud breaches also involved breached credentials. This is not so much an indictment of cloud security as it is an illustration of the trend of cybercriminals finding the quickest and easiest route to their victims.

## Information Technology vs. Operational Technology

Last year we started tracking embedded assets, but that turned out to be less insightful than we anticipated. So, this year we began tracking Information Technology (IT) vs Operational Technology (OT) for assets involved in incidents instead. We hope to be able to do a more comprehensive analysis in the following years, but for now our findings were not particularly surprising: 96% of breaches involved IT, while 4% involved OT. Although 4% might not sound like a lot, if you happen to be in an industry that relies on OT equipment in your means of production, it's certainly adequate cause for concern.

## Mobile devices

This year we were minding our own business, eating some plums we found in the icebox, when over a thousand cases of Loss involving Mobile Devices showed up in our dataset. We would make this incredible spike in incidents one of our key findings, but we are pretty sure “forgetting your work mobile phone in a hipster coffee shop” is not a new technique invented in 2019. Turns out data collection is partially to blame here. We updated the collection protocols with a few of our contributors, and voilà, there they were. Those Error cases made up roughly 97% of the incidents we had on Mobile Devices.

The other 3% are very interesting, though. Those incidents are split almost evenly between Espionage and Financial motives, which is incredibly significant when our overall breakdown of motives is of 64% Financial and only 5% Espionage. And while the financially motivated ones vary from Theft to the use of the device as a vessel for Pretexting, the espionage-related cases are exclusively Malware-based compromises of mobile devices to further persistence and exfiltration of data by advanced State-affiliated actors.

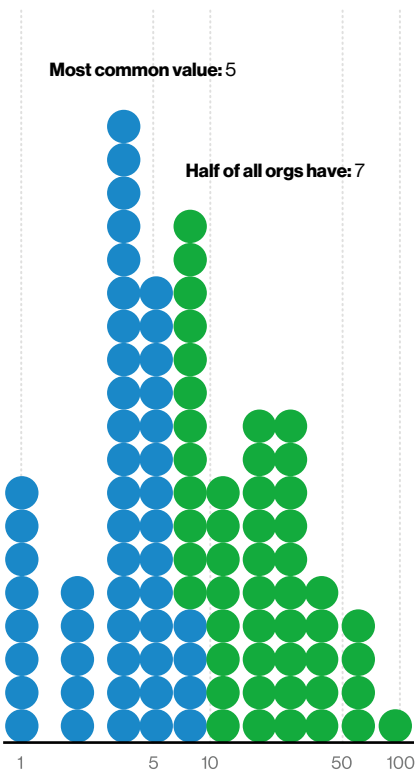
<sup>34</sup> The remainder were breaches where cloud was not applicable, such as where the asset is a Person.

# Asset management

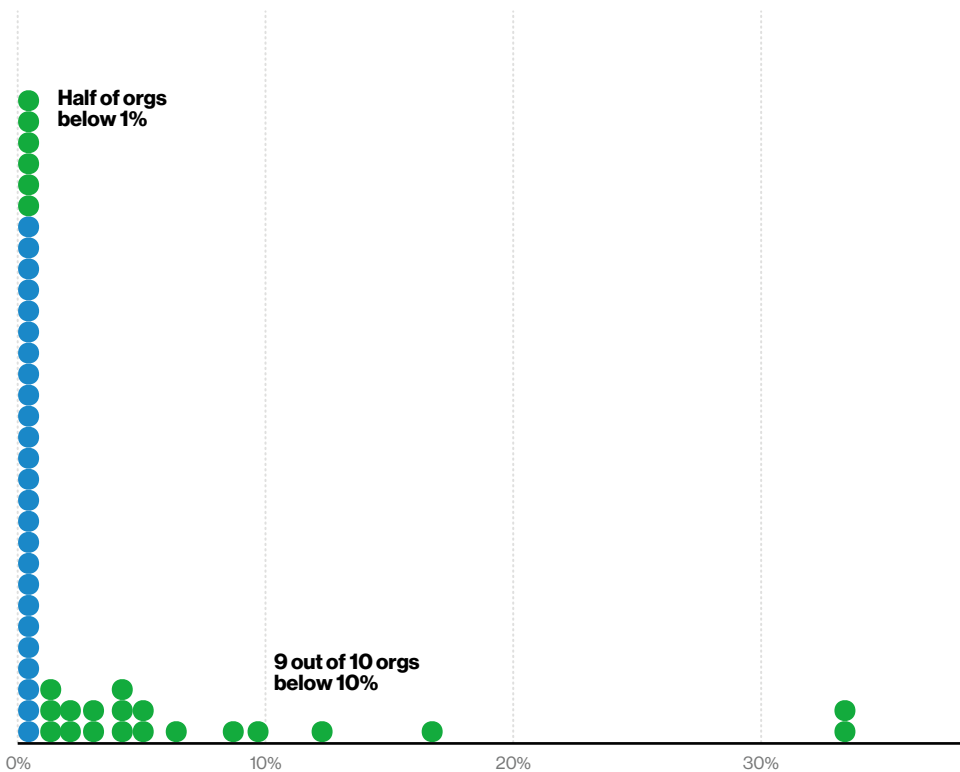
We mentioned back in the “Hacking” section that hosts susceptible to major new vulnerabilities tend to also still be defenseless against many older vulnerabilities. That finding is a bit of a double-edged sword in that, while it seems to suggest that patching is working, it also suggests that asset management may not be. We found that it was most often the case that organizations have approximately 43% of their internet-facing IPs in one network.<sup>35</sup> However, the most common number of networks that an organization occupies is five, and half of all organizations are present on seven or more (Figure 35). If you don't know what all those networks are, you might have an asset management problem. Therefore, it might not just be an asset management problem, but also a vulnerability management problem on the assets you did not realize were there.

In over 90% of organizations, less than 10% of their internet-facing hosts had any significant vulnerabilities. In half of all orgs, less than 1% of hosts had internet-facing vulnerabilities (Figure 36). That suggests that the vulnerabilities are likely not the result of consistent vulnerability management applied slowly, but a lack of asset management instead.

**Figure 35.** Number of additional networks per organization (n = 86)



**Figure 36.** Percent of organizations' public IPs with significant vulnerabilities (n = 110)



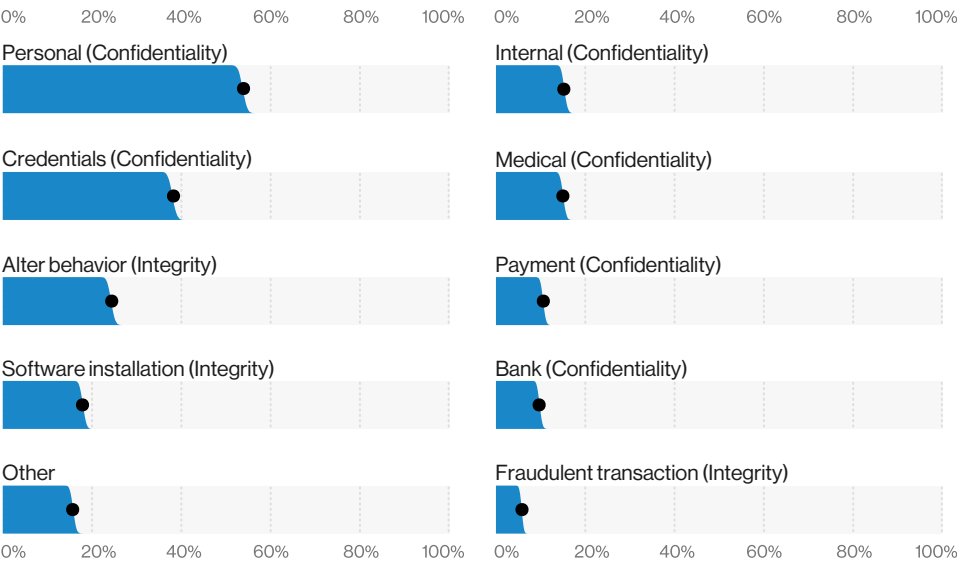
35 By “network,” we mean an autonomous system, represented by an autonomous system number (ASN): <https://www.apnic.net/get-ip/faqs/asn/>

# Attributes

The compromise of the Confidentiality of Personal data leads the pack among attributes affected in breaches, as shown in Figure 37. But keep in mind that this contains email addresses and is not just driven by malicious data exfiltration, but also by “benign” errors. The one-two punch of Hacking and Error puts email addresses (and by extension personal information) at the front of the pack. Certainly, Personal information goes way beyond just email addresses, but that is the designation where those reside.

In second place, we see Credentials, which should come as no surprise since we have covered that topic sufficiently already. Alter behavior appears next and is a result of Social breaches affecting the Integrity of our victims’ Person assets. Finally, we see Malware-related breaches causing the integrity violation of Software Installation.

One other notable observation from Figure 37 is that Bank and Payment data are almost equal. Five years ago, Payment information was far more common, but while compromise of bank information has stayed relatively level, Payment has continued to decline to an equivalent level.



**Figure 37.** Top compromised Attribute varieties in breaches (n = 3,667)

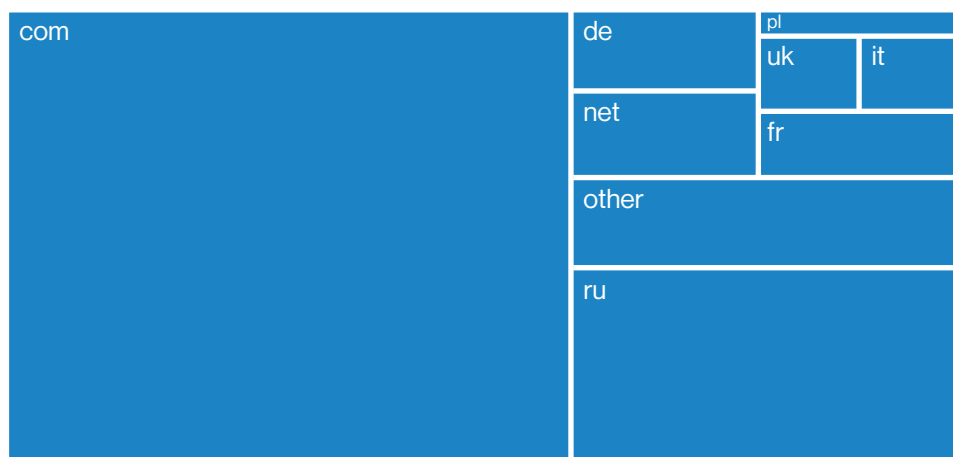
# Email address compromises

Given that email addresses are Personally Identifiable Information (PII) and that Personal is the most common variety of data to be breached in this year's report, we looked a bit more closely at some of the email leaks we have seen over the last 10 years. Figure 38 gives you a feel for what email top-level domains (TLDs) are being compromised the most. The "Other" category includes TLDs with less than 1% of emails, by the way.

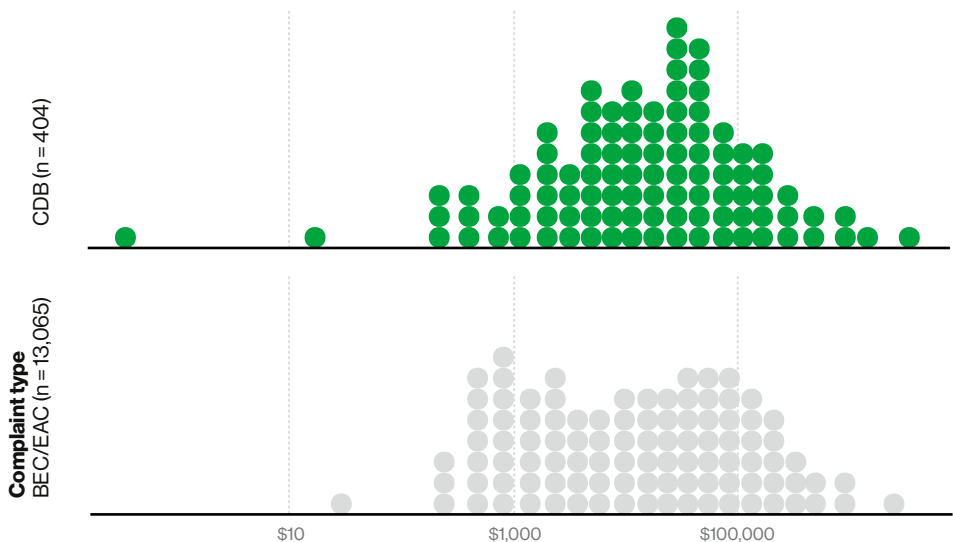
Since .com accounts for approximately 59% of leaked emails, we focused in on that a bit. The first 150 domains that we looked at showed that most were mail registration services. That accounted for about 97% of the breaches, and provides hope that most emails compromised aren't your employees' corporate addresses. However, the little matter of the remaining 3% was comprised of tens of millions of addresses.

# What's that attribute going to cost you?

As reported in FBI IC3 complaints, the most common loss was \$32,200 this year, up from about \$29.3k last year. That's still basically in the preowned car range, and while no one wants to lose that much money, it could certainly be much worse.



**Figure 38.** Prevalence of top-level domains (TLDs) in leaked emails (n = 3.94 billion)



**Figure 39.** Loss amount in Corporate Data Breaches (CDB) and business email compromises/(individual) email account compromises (BEC/EAC) (Excludes complaints with zero loss amount)

# How many paths must a breach walk down?

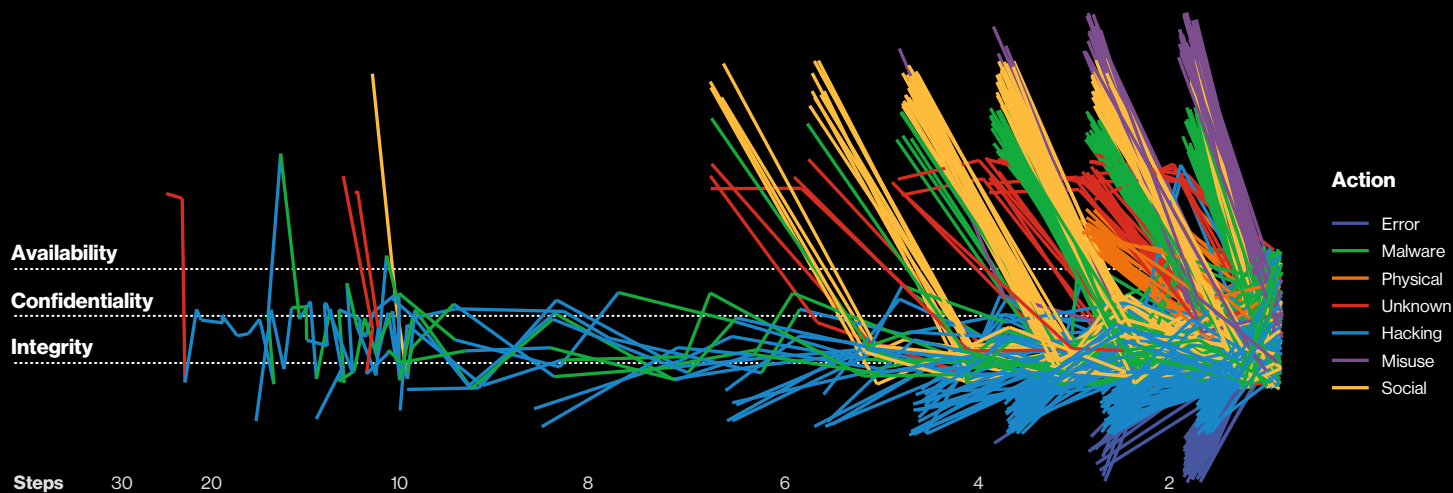
We tend to think about incidents and breaches as a point in time. You snap your fingers and all the attacker actions are complete, the stolen data is in the attacker's saddlebags and they are off down Old Town Road and away into the sunset. Still, we all know that is not quite what actually happens. Many of the attacks studied in this report fall somewhere between a stickup and the Great Train Robbery in terms of complexity. The good news is that defenders can use this to their advantage.

As you can see in Figure 40, attacks come in numerous forms and sizes, but most of them are short, having a small number of steps (you can notice that by how the volume of line segments thin out between the four and six steps markers). The long ones tend to be Hacking (blue) and Malware (green) breaches, compromising Confidentiality (the middle position) and Integrity (the lower position) as the attacker systematically works their way through the network and expands their persistence. The benefit in knowing

the “areas” (threat actions—colors/positions) attackers are more likely to pass through in their journey to a breach gives you first advantage, because you can choose where to intercept them. You may want to stop their initial action or their last. You may not want to go near them, so you don’t have to listen to “Old Town Road.” All of these options are understandable in accordance with your response strategy.<sup>36</sup>

36 Or to how susceptible you are to ubiquitous earworms.

**Figure 40.** Attack paths in incidents (n = 652. Two breaches, 77 and 391 steps respectively, not shown.)



OK, take a deep breath and look at Figure 40 on the previous page. No, a butterfly did not just vomit on your report. Don't worry about trying to understand all the graphic has to tell. Instead, let us convey the concept of what you are seeing here. This abstract work of art contains a line (a "path") for each of several hundred breaches. In the way a bar chart summarizes numbers, this graph summarizes paths taken by the attacker.

Each colored line segment (a "step") represents an action taken by the threat actor along with the associated attribute that was compromised. The color of each step represents the VERIS threat action of

the step, and the position where the step ends represents the attribute compromised. But the real trick to understanding this chart is that the paths start *from the left and move to the right*—the first step on a path will either come from the top of the chart or the bottom (because they have to come from somewhere) and "land" on the appropriate attribute.

So, if you pick any yellow step coming from the top of the chart starting at 4 on the horizontal axis and ending on the lower position of the chart, you just found yourself at the beginning of a four-step incident that started with a Social action that compromised the Integrity attribute. Also, notice how Error actions (the

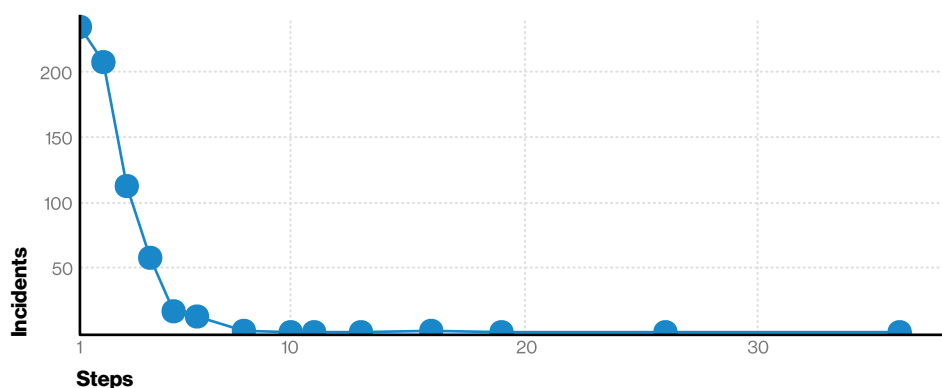
dark blue lines coming from the bottom of the chart) are usually part of very short paths and land on the Confidentiality attribute.

There's a small amount of noise put into the positions of the lines, since otherwise the same lines would be exactly on top of each other and we wouldn't be able to see a lot here. But mostly we did it for the art.

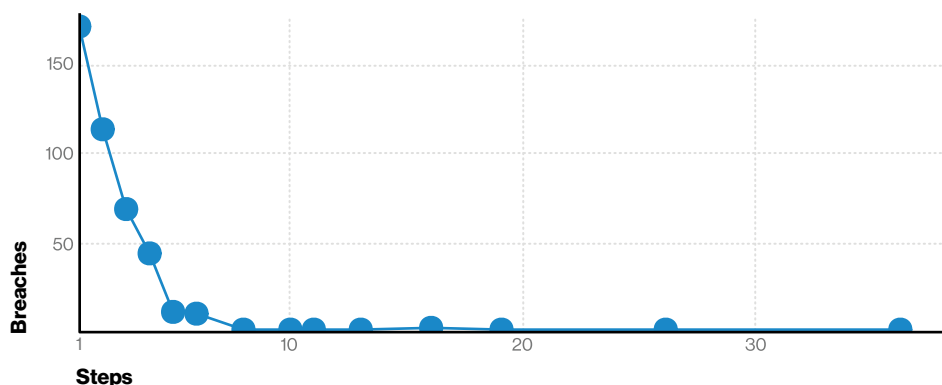
Figures 41 and 42 provide us with our next defensive advantage. Attackers prefer short paths and rarely attempt long paths. This means anything you can easily throw in their way to increase the number of actions they have to take is likely to significantly decrease their chance of absconding with the data. Hopefully by now we have driven home the significance and prevalence of credential theft and use. While we admit that two-factor authentication is imperfect, it does help by adding an additional step for the attacker. The difference between two steps (the Texas two-step) and three or four steps (the waltz) can be important in your defensive strategy.

**The difference between two steps (the Texas two-step) and three or four steps (the waltz) can be important in your defensive strategy.**

**Figure 41.** Number of steps per incident (n = 654. Two breaches, 77 and 391 steps respectively, not shown.)



**Figure 42.** Number of steps per breach (n = 429. Two breaches, 77 and 391 steps respectively, not shown.)





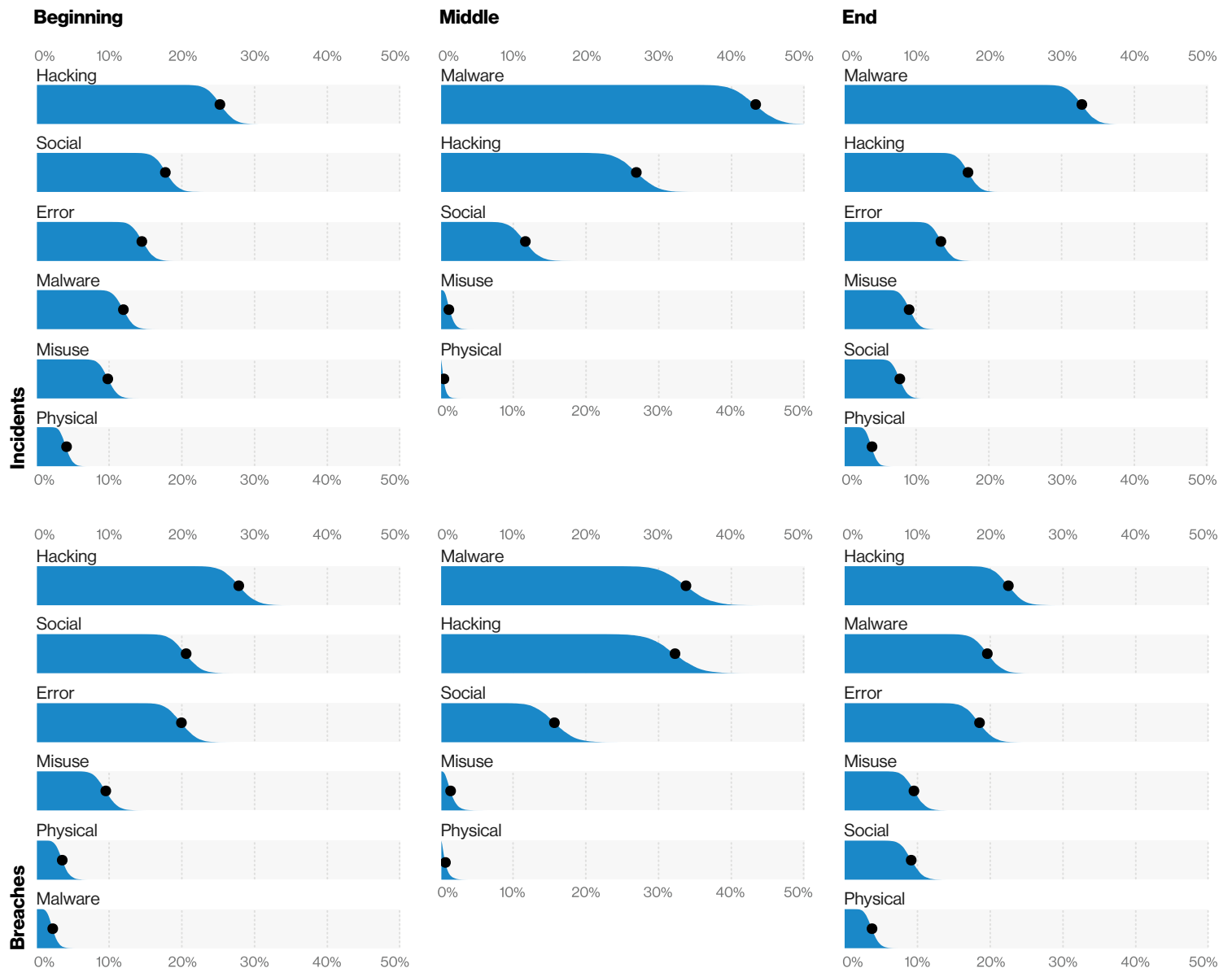
Finally, take a look at Figure 43. It shows what actions happen at the beginning, middle and end of both incidents and breaches. It is not what is on top that's interesting (we already know "Social – Phishing" and "Hacking – Use of stolen creds" are good ways to start a breach and "Errors" are so short that the beginning of the path is also the end). The interesting bit is what's near the bottom. Malware is rarely the

first action in a breach because it obviously has to come from somewhere. Conversely, Social actions almost never end an attack. In the middle, we can see Hacking and Malware providing the glue that holds the breach together. And so, our third defensive opportunity is to guess what you haven't seen based on what you have. For example, if you see malware, you need to look back in time for what

you may have missed, but if you see a social action, look for where the attacker is going, not where they are.

All in all, paths can be hard to wrap your head around, but once you do, they offer a valuable opportunity not just for understanding the attackers, but for planning your own defenses.

**Figure 43.** Actions at the beginning, middle and end of incidents and breaches

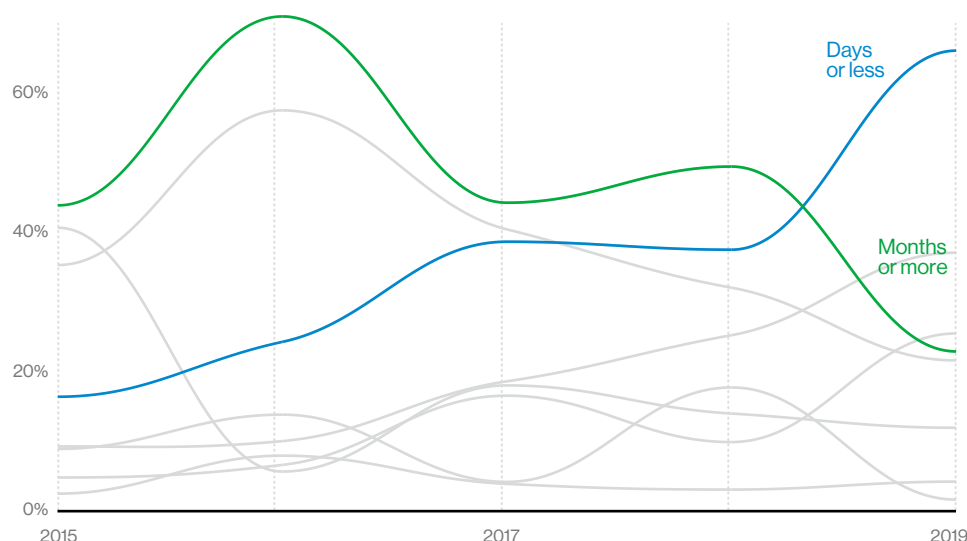


# Timeline

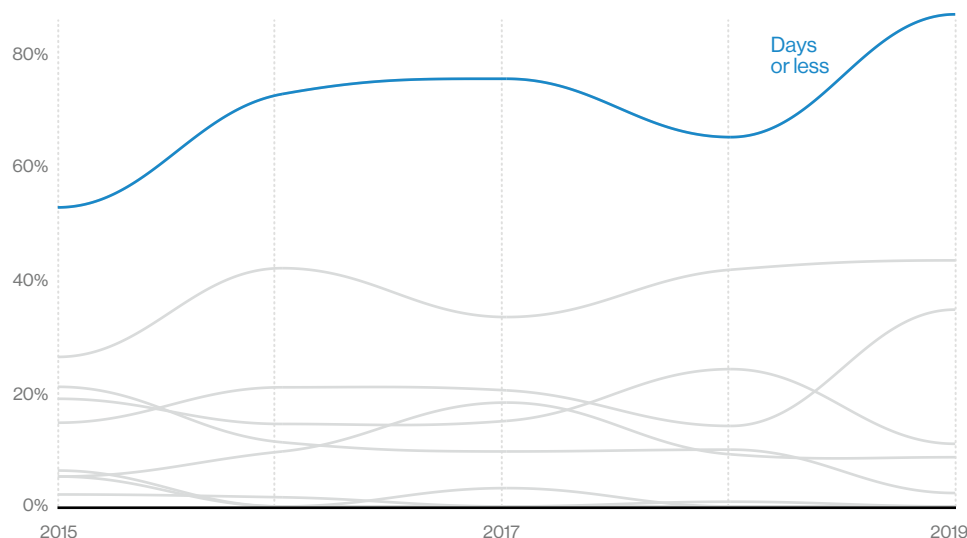
As we analyze how breach timelines have evolved over time, Discovery in days or less is up (Figure 44) and Containment in that same timeframe has surpassed its historic 2017 peak (Figure 45). However, before you break out the bubbly, keep in mind that this is most likely due to the inclusion of more breaches detected by managed security service providers (MSSPs) in our incident data contributors' sampling, and the relative growth of breaches with Ransomware as collateral damage, where Discovery is often close to immediate due to Actor disclosure.<sup>37</sup>

Discovery in Months or more still accounts for over a quarter of breaches. We are obligated to point out that since this is a yearly report, this is usually a trailing indicator of the actual number, as there are potentially a significant number of breaches that occurred in 2019 that just have not been discovered yet.

All in all, we do like to think that there has been an improvement in detection and response over the past year and that we are not wasting precious years of our life in a completely pointless battle against the encroaching void of hopelessness. Here, have a roast beef sandwich on us.



**Figure 44.** Discovery over time in breaches



**Figure 45.** Containment over time in breaches

<sup>37</sup> Nothing quite like a rotating flaming skull asking for cryptocurrency on your servers to help you "discover" a breach.

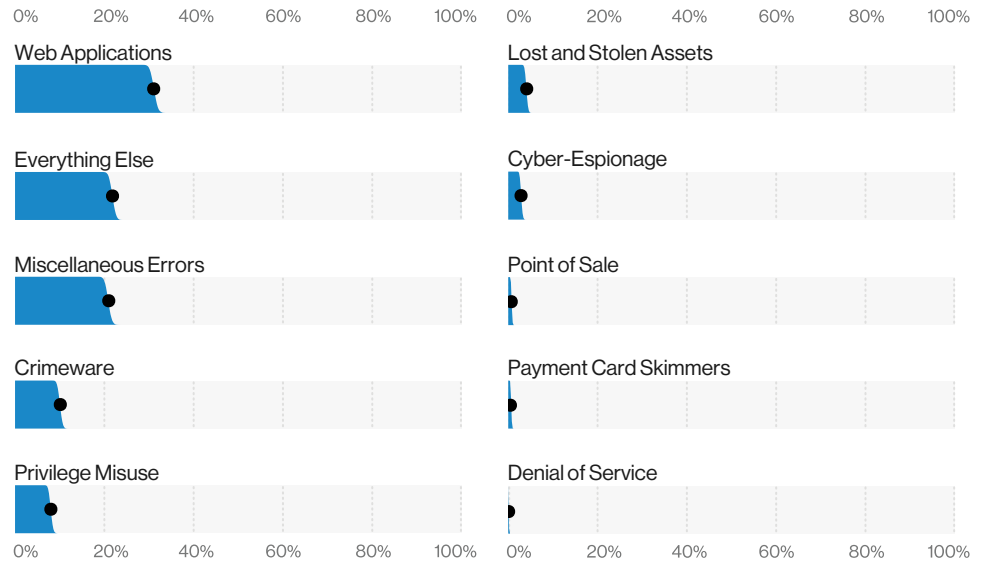
# Incident classification patterns and subsets

For the uninitiated, VERIS and the DBIR may seem overwhelming when you consider both the amount of data we possess (now over 755,000 incidents over the years) and the depth of that data (over 2,400 values we are able to track on each incident). To help us better understand and communicate this vast arsenal of information, we started to leverage what we call “Patterns” in 2014, which are essentially different clusters of “like” incidents. We won’t go too much into the data science-y aspect,<sup>38</sup> but the outcome was the identification of nine core clusters, our Incident Classification Patterns. This allows us to abstract upward and discuss the trends in the patterns rather than the trends in each of our different combinations: Actions, Assets, Actors and Attributes.

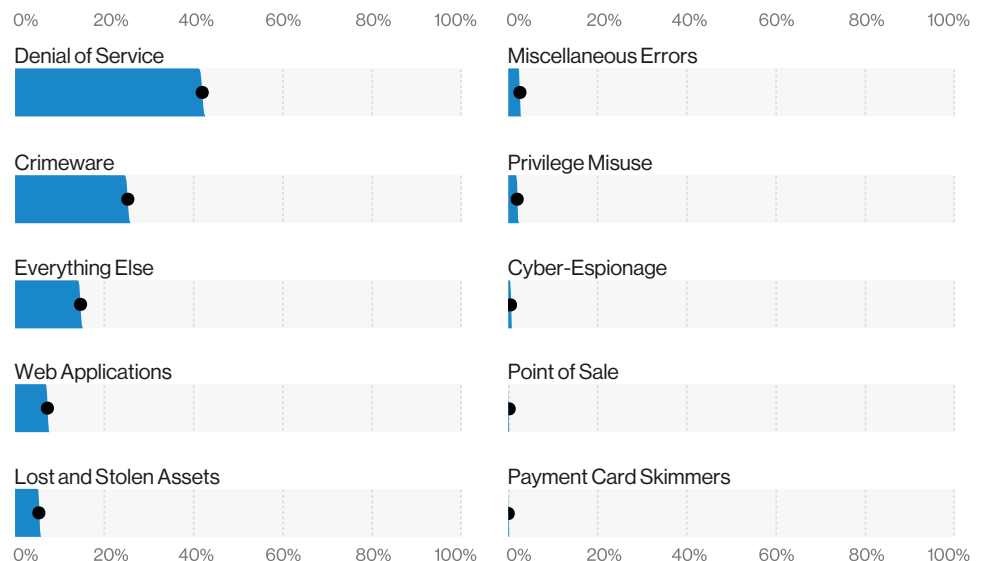
Looking over our 409,000 security incidents and almost 22,000 quality data breaches since the inception of the report, the numbers reveal that 94% of security incidents and 88% of data breaches fall neatly in one of the original nine patterns. However, when we focus our lenses on just this year’s data, the percentages drop to 85% of security incidents and 78% of data breaches.

Nothing better demonstrates this than our category of “Everything Else,” effectively designed to be our spare-USB-cable drawer of breaches, having risen to one of the top patterns due to the rise of Phishing, while some of the other patterns have drastically fallen since their initial inception. It seems that time waits for no pattern, and the only breach constant is breaches changing over time.

The patterns will be referenced more in the “Region” and “Industry” sections, but to get acquainted with them or to rekindle a prior relationship, they are defined here.



**Figure 46.** Patterns in breaches (n = 3,950)




**Figure 47.** Patterns in incidents (n = 32,002)

<sup>38</sup> We recommend taking a glance at the 2014 report if you are curious about the nerdy stuff.

# Patterns

## Crimeware


One of the oldest games in town, Crimeware includes all the malware that doesn't fall into the other patterns. Think of these as the common type of commodity malware that everyone has probably seen on some email claiming to be a fax or a missed delivery package. These incidents and breaches tend to be opportunistic and financially motivated.

 **Notable findings:** This year has continued the trend of modest increases in incidents and breaches involving Crimeware, now up to about 400, which is higher than last year and roughly matches the highest levels that were reached in 2015. Unsurprisingly, these types of attacks normally propagate through email, either as a link or as an attachment, dropping something nasty like a downloader, password dumper, Trojan or something that's got C2 functionality.

These types of attacks rely heavily on Social and Malware combined vectors, using Phishing in 81% of the incidents and some form of malware in 92%.

## Denial of Service

These attacks are very voluminous (see what we did there) in our dataset at over 13,000 incidents this year. Attacks within this pattern use differing tactics, but most commonly involve sending junk network traffic to overwhelm systems, thereby causing their services to be denied. The system can't handle both the incoming illegitimate traffic and the legitimate traffic.


 **Notable findings:** While the amount of this traffic is increasing as mentioned, in DDoS, we don't just look at the number of attacks that are conducted. We also look at the bits per second (BPS), which tells us the size of

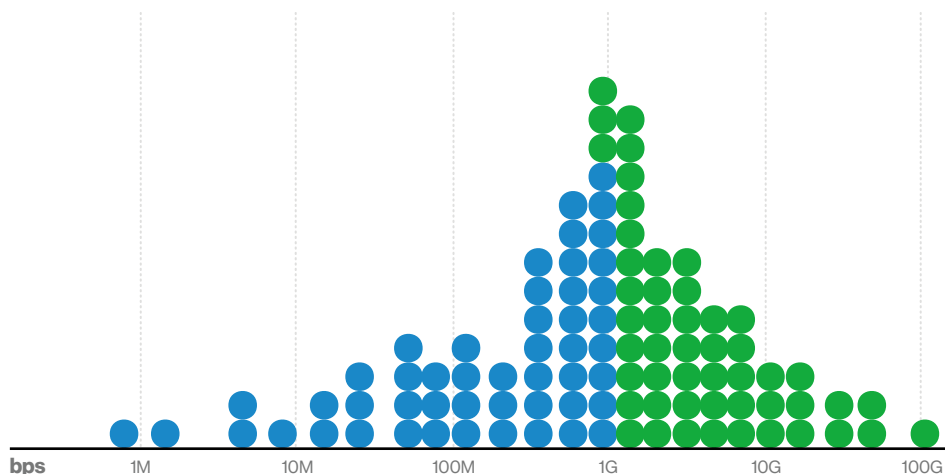
the attack, and the packets per second (PPS), which tells us the throughput of the attack. What we found is that, regardless of the service used to send the attacks, the packet-to-bit ratio stays within a relatively tight band and the PPS hasn't changed that much over time, sitting at 570 Mbps for the most common mode (Figure 48).

When it comes to defending against DDoS, a layered approach is best, with some of the attacks being mitigated at the network level by internet service providers and the others being handled at the endpoint or a content delivery network (CDN) provider. These attacks are prevalent because of their ease of use and the fact that internet-facing infrastructure can be targeted; however the impact to your organization and the decision of whether to mitigate will be based entirely on your business.

## Cyber-Espionage

This pattern consists of espionage, enabled via unauthorized network or system access, and largely constitutes nation-states or state-affiliated actors looking for those oh-so-juicy secrets.

 **Notable findings:** This is one of our patterns that has decreased this year, both in raw numbers and also as a percentage from 13.5% of breaches in 2018 to 3.2% of breaches in 2019. The drop in raw numbers could be due to either under-reporting or failure to detect these attacks, but the increase in volume of the other patterns is very much responsible for the reduction in percentage.




**Figure 48.** Most common distributed denial of service (DDoS) bits per second (BPS) (n = 195)

---

## Privilege Misuse


This pattern consists of “Misuse” actions, which are intentional actions undertaken by internal employees that result in some form of security incident.

 **Notable findings:** Misuse is down as a percentage of incidents, as the other patterns increase by association. However, that could be attributed to lower granularity data this year and may rise back to previous levels in 2021. On the other hand, breaches are showing a legitimate drop, which appears to be associated with less misuse of databases to access and compromise data.

---

## Miscellaneous Errors


Life is full of accidents and not to disappoint Bob Ross, but not all of them are happy little trees. This pattern captures exactly that, the unintentional (as far as we know) events that result in a cybersecurity incident or data breach.

 **Notable findings:** The majority of these errors are associated with either misconfigured storage or misdelivered emails, committed by either system admins or end users. We'll let you figure out which actor is associated with which action. In terms of discovery, these are often found by trawling security researchers and unrelated third parties who may have been on the receiving end of those stray emails. The Results and Analysis Error section goes into even more detail for those of you with this unique predilection.

---

## Payment Card Skimmers

This pattern is pretty self-explanatory: These are the incidents in which a skimmer was used to collect payment data from a terminal, such as an ATM or a gas pump.


 **Notable findings:** Our data has shown a continuous downward trend of incidents involving Point of Sale (PoS) Card Skimmers, which are now down to 0.7% of our breach data.

At approximately 30 incidents, it is showing a relatively marked decline from its peak of 206 back in 2013. This decrease could be attributed to a variety of different causes, such as less reporting to our federal contributors or shifts in the attacker methodology.

---

## Point of Sale (PoS)


This pattern includes the hacking and remote intrusions into PoS servers and PoS terminal environments for the purpose of stealing payment cards.

 **Notable findings:** Much like the Payment Card Skimmers, this pattern has received a notable decrease in the last few years, making up only 0.8% of total data breaches this year. The majority of these incidents include the use of RAM scrapers, which allow the adversaries to scrape the payment cards directly from the memory of the servers and endpoints that run our payment systems. However, the majority of payment card crime has moved to online retail.

---

## Lost and Stolen Assets

These incidents include any time where an asset and/or data might have mysteriously disappeared. Sometimes we will have confirmation of theft and other times it may be accidental.


 **Notable findings:** This pattern tends to be relatively consistent over the years, with approximately 4% of breaches this year (the previous two years fluctuating from 3% to 6% of breaches). These types of incidents occur in various different locations, but primarily occur from personal vehicles and victim-owned areas. Don't forget to lock your doors.

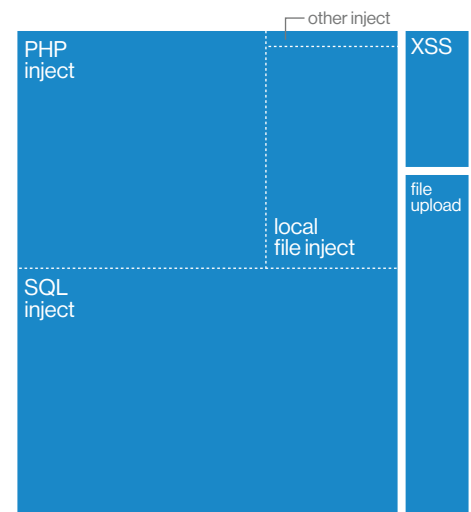
---

## Web Applications

Incidents in this pattern include anything that has a web application as the target. This includes attacks against the code of the actual web application, such as exploiting code-based vulnerabilities (Hacking—Exploit

Vuln) to attacks against authentication, such as Hacking—Use of Stolen Creds.

 **Notable findings:** In the data provided by contributors who monitor attacks against web applications (Figure 49), SQL injection vulnerabilities and PHP injection vulnerabilities are the most commonly exploited. This makes sense since these types of attacks provide a quick and easy way of turning an exposed system into a profit maker for the attacker. However, in vulnerability data, cross-site scripting (XSS), the infamous ding popup vulnerability, is the most commonly detected vulnerability and SQLi attacks are only half as common as XSS.




**Figure 49.** Web application attack blocks (n = 5.5 billion)

---

## Everything Else

This pattern is our graveyard of lost incident souls that don't fall into any of the previously mentioned patterns.


 **Notable findings:** The majority of these incidents are Phishing or Financially Motivated Social Engineering where attackers try to commit fraud via email. Rather than go into detail here, we'll point you to the Results and Analysis—Social section, which goes into great detail on Financially Motivated Social Engineering and Phishing.

# Subsets

In addition to the main nine Patterns, there is another level of patterns that we examine separately due to different factors that might skew our results and analysis, such as an extremely high volume of low-detailed incidents. This year, like the previous one, the subpatterns we examined separately are divided into the Botnet subset and Secondary motives.


## Botnet subset

This subset consists of 103,699 incidents from various occurrences of Trojans and malware being installed on desktops and servers. The majority of these incidents tend to be low quality and limited in detail, coming from multiple incident sources.

 **Notable findings:** In Figure 50, we see that botnets primarily affect the Financial, Information and Professional Services verticals. All these industries should focus on their customers' security as well as their own. The absolute numbers on this subset have more or less doubled from the previous year. Also, be mindful that these types of incidents impact everyone, with 41% of victims originating outside North America.

## Secondary webapp subset

This subset examines those security incidents in which the victim web application was a means to an end for a different attack. This is often seen in the form of servers being compromised and used as part of a botnet or to DDoS other systems.

 **Notable findings:** The Secondary subset represents a total of 5,831 incidents, with greater than 90% of them involving some form of hacking, malware and impacting servers. As we point out in the Actor section of Results and Analysis, if you give the bad guy the opportunity to add your infrastructure to theirs, they won't hesitate.

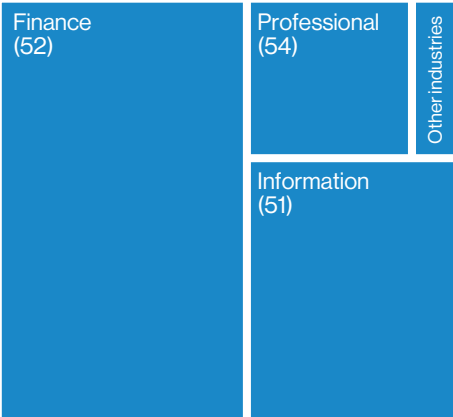
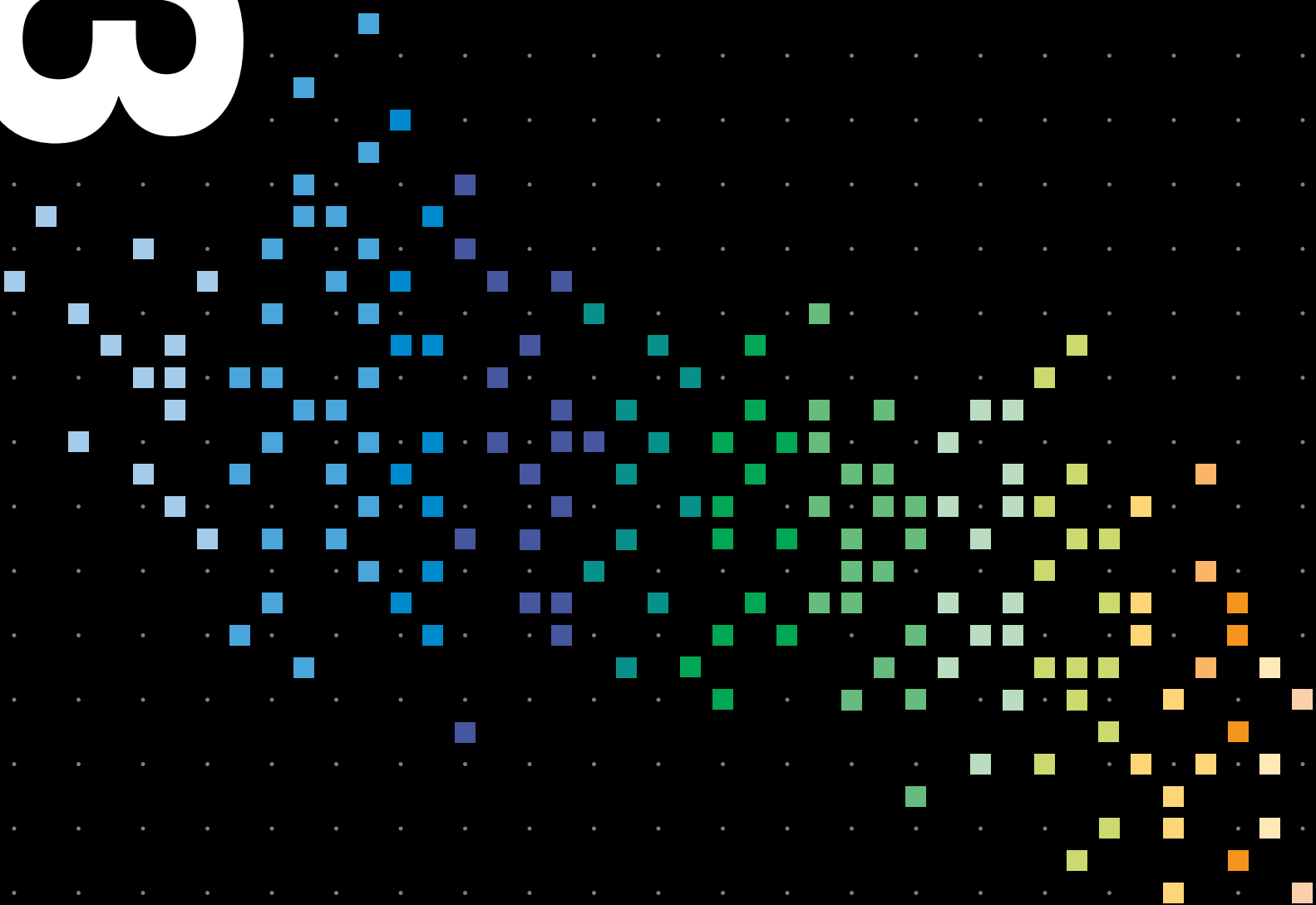
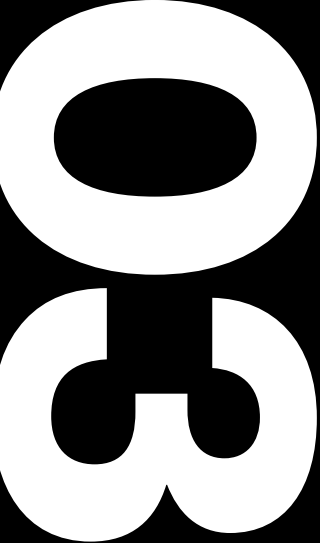


Figure 50. Botnet infections (n = 103,699)



---

# Industry analysis



# Introduction to industries

This year we collected 157,525 incidents and 108,069 breaches. That may sound impressive until you realize that 100,000+ of those breaches were credentials of individual users being compromised to target bank accounts, cloud services, etc. We break those out into the Secondary motive subset in the “Incident classification patterns and subsets” section. After filtering for quality and subsetting, we are left with the incidents and breaches in Table 1.

Our annual statement on what not to do with this breakout will now follow. Do not utilize this to judge one industry over another; a security staffer from an Administrative organization waving this in the face of their peer from the Financial sector and trash-talking is a big no-no. The number of breaches or incidents that we examine is heavily influenced by our contributors. These numbers simply serve to give you an idea of what we have to “work with,” and is part of our pledge to the

community to be transparent about the sourcing of the data we use in the report.

Figures 51 and 52 come with yet another warning. The numbers shown here are simply intended to help you to get your bearings with regard to industry. The smaller the numbers in a column, the less confidence we can provide in any statistic derived from that column.

Incidents:	Total	Small	Large	Unknown
Total	32,002	407	8,666	22,929
Accommodation (72)	125	7	11	107
Administrative (56)	27	6	15	6
Agriculture (11)	31	1	3	27
Construction (23)	37	1	16	20
Education (61)	819	23	92	704
Entertainment (71)	194	7	3	184
Finance (52)	1,509	45	50	1,414
Healthcare (62)	798	58	71	669
Information (51)	5,471	64	51	5,356
Management (55)	28	0	26	2
Manufacturing (31–33)	922	12	469	441
Mining (21)	46	1	7	38
Other Services (81)	107	8	1	98
Professional (54)	7,463	23	73	7,367
Public (92)	6,843	41	6,030	772
Real Estate (53)	37	5	4	28
Retail (44–45)	287	12	45	230
Trade (42)	25	2	9	14
Transportation (48–49)	112	3	16	93
Utilities (22)	148	5	15	128
Unknown	6,973	83	1,659	5,231
Total	32,002	407	8,666	22,929

Breaches:	Total	Small	Large	Unknown
Total	3,950	221	576	3,153
Accommodation (72)	92	6	7	79
Administrative (56)	20	6	10	4
Agriculture (11)	21	1	0	20
Construction (23)	25	1	10	14
Education (61)	228	15	22	191
Entertainment (71)	98	3	1	94
Finance (52)	448	32	28	388
Healthcare (62)	521	31	32	458
Information (51)	360	32	32	296
Management (55)	26	0	25	1
Manufacturing (31–33)	381	5	185	191
Mining (21)	17	0	5	12
Other Services (81)	66	6	1	59
Professional (54)	326	14	13	299
Public (92)	346	24	50	272
Real Estate (53)	33	3	3	27
Retail (44–45)	146	7	18	121
Trade (42)	15	1	6	8
Transportation (48–49)	67	3	6	58
Utilities (22)	26	2	4	20
Unknown	688	29	118	541
Total	3,950	221	576	3,153

Table 1. Number of security incidents by victim industry and organization size



## Breaches

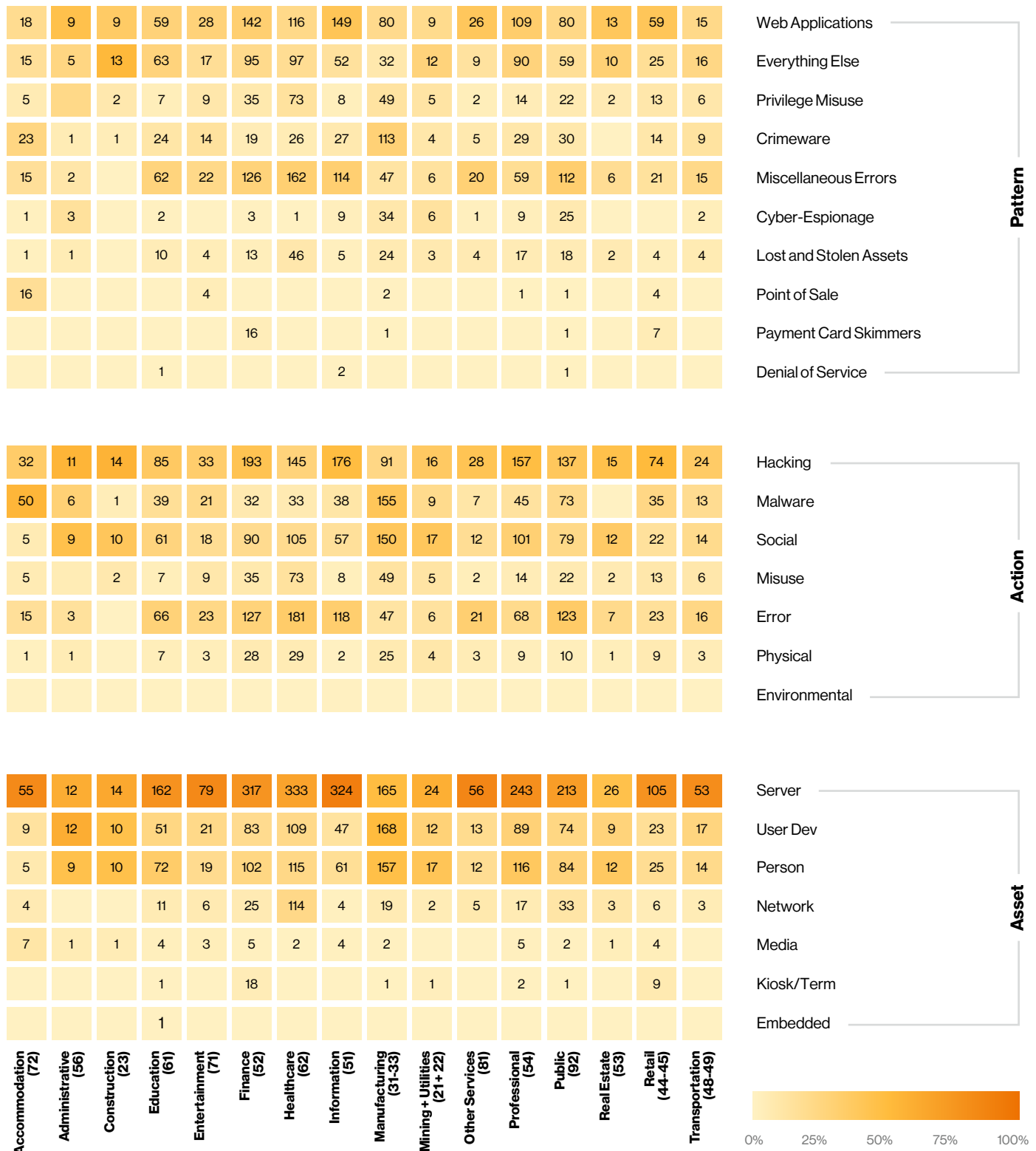


Figure 51. Breaches by Industry

## Incidents

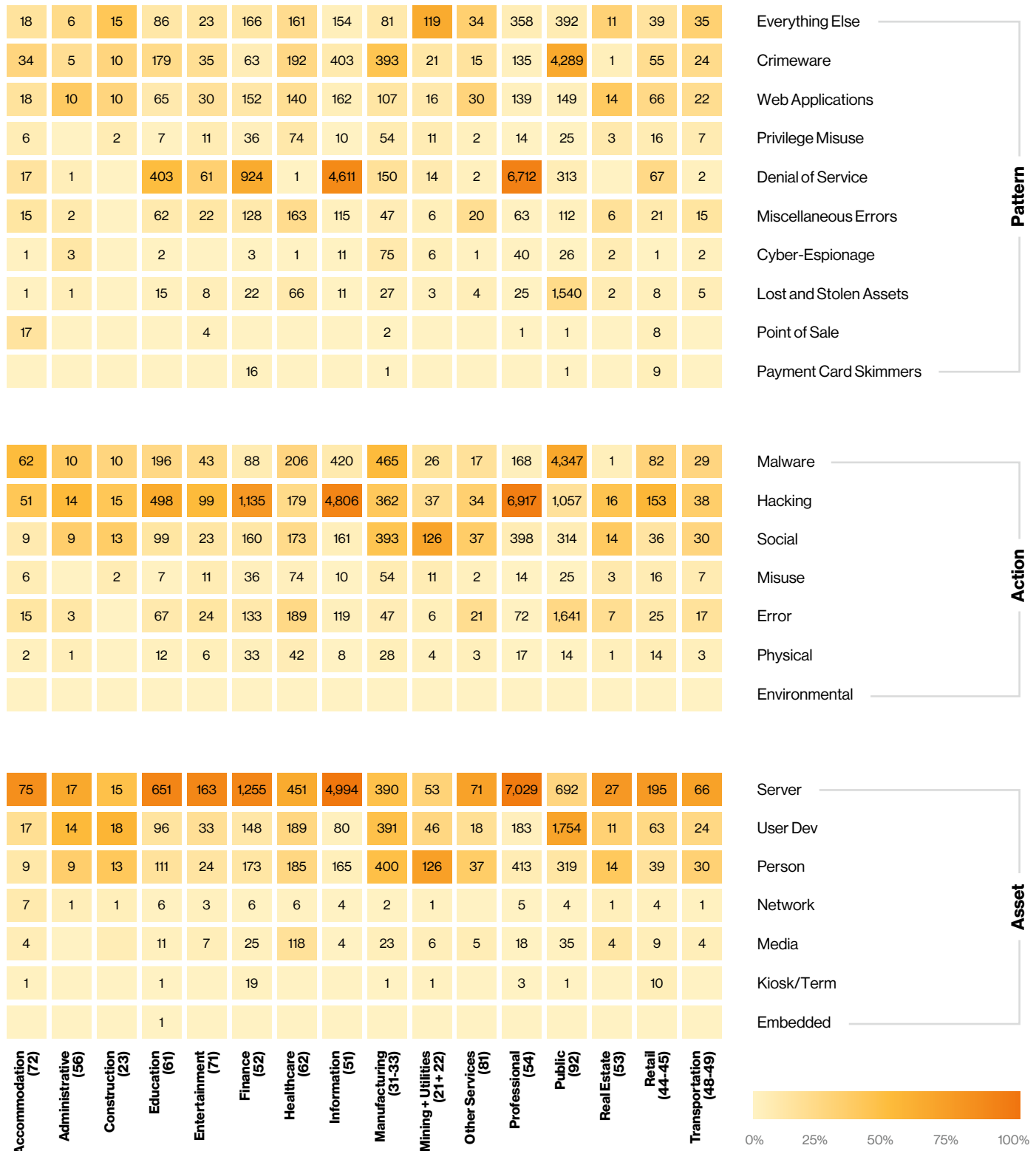


Figure 52. Incidents by Industry

For example, there are 35 total assets involved in Construction (NAICS 23) breaches. Of those, multiple assets may be contained in a single breach, meaning there are potentially fewer breaches (25) than our asset count. Considering how few breaches we have in this sector, our confidence in any statistic derived from them will be relatively low. However, in an attempt to bring our readers information on more industries, we have upped our statistical game. For example, instead of making a statement such as “64% of Construction breaches involved a server,” we would state “between 44% and 82% of breaches in Construction involved servers.” This is not an attempt to be coy,<sup>39</sup> we simply want to give you as much information as possible without being misleading and, in industries with such a small sample, that means using statistical ranges. You may notice something similar in bar charts where the black median dot is

removed. Please keep an eye out for the “Data Analysis Notes” at the bottom of the Summary table in each section. We will be pointing out things such as small sample sizes and other caveats there. Check out the “Methodology” section for more information on the statistical confidence background used throughout this report.

Another improvement on this year’s report is that we have standardized our control recommendations through a mapping between VERIS and the CIS Critical Security Controls. Each industry will have a “Top Controls” list on their Summary table. You can find more details about our mapping in our “CIS Control recommendations” section.

---

**Please note: Based on feedback from our readers, we know that while some study the report from cover to cover, others only skip to the section or industry vertical that is of direct interest to them. Therefore, you may notice that we repeat some of our definitions and explanations several times throughout the report, since the reader who only looks at a given section won’t know the definition or explanation that we might have already mentioned elsewhere. Please overlook this necessary (but possibly distracting) element.**

<sup>39</sup> Like a Gameboy.

# Accommodation and Food Services

NAICS  
72

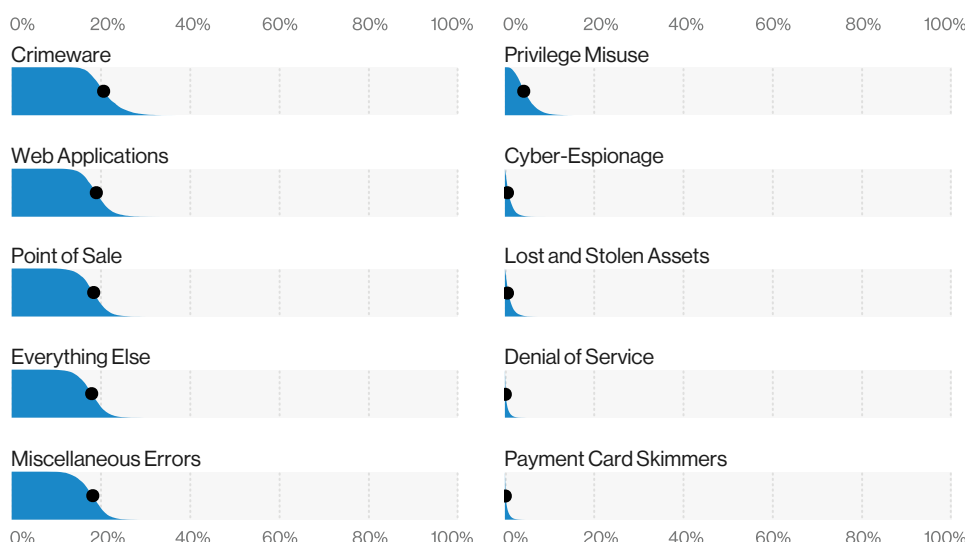
## Summary

**Point of Sale (PoS)-related attacks no longer dominate breaches in Accommodation and Food Services as they have in years past. Instead, responsibility is spread relatively evenly among several different action types such as malware, error and hacking via stolen credentials. Financially motivated attackers continue to target this industry for the payment card data it holds.**

<b>Frequency</b>	125 incidents, 92 with confirmed data disclosure
<b>Top Patterns</b>	Crimeware, Web Applications and Point of Sale represent 61% of data breaches.
<b>Threat Actors</b>	External (79%), Internal (22%), Multiple (2%), Partner (1%) (breaches)
<b>Actor Motives</b>	Financial (98%), Secondary (2%) (breaches)
<b>Data Compromised</b>	Payment (68%), Personal (44%), Credentials (14%), Other (10%) (breaches)
<b>Top Controls</b>	Limitation and Control of Network Ports, Protocols and Services (CSC 9), Boundary Defense (CSC 12), Data Protection (CSC 13)

## Breaches served with a smile

The Accommodation and Food Services industry is one that we have been tracking for quite a while. There's just something welcoming about it that keeps us coming back. One lesson that we learned from all our time spent here is that malware plays a relatively large role in this industry. Crimeware and PoS (both malware dependent) represent two of the top three patterns this year. These are joined by this year's darling of Web applications attacks, which covers both the Use of stolen credentials and the Exploitation of vulnerabilities, as seen in Figure 53.



**Figure 53.** Patterns in Accommodation and Food Services industry breaches (n = 92)

## 86 the PoS breaches.

We reported last year on the decrease in different attacks targeting the PoS, either the malware-based remote attacks or the skimmers, and this trend has continued this year as well (Figure 54). Even though PoS intrusions are still relatively common, accounting for 16% of breaches in this industry, they are nowhere near their high-water mark back in 2015. This may be (and probably is) indicative of the trend of adversaries to more quickly monetize their access in organizations by deploying ransomware rather than pivoting through the environment and spreading malware – a more time-costly endeavor.

## Do you want malware with that?

In spite of the decline in PoS intrusions, we're still seeing Crimeware being leveraged to capture payment card and other types of data at a higher rate than in

our overall dataset, accounting for a quarter of the breaches this year. The malware is found on desktops and servers alike. With regard to type, Figure 55 shows a decrease of RAM scrapers and an increase of malware that enables access to the environment, such as Trojans, Backdoors and C2. There is also a continued rise in Ransomware, which has been known to leverage existing infections to access the environment. While Ransomware is not the top malware variety in breaches, or showing up in scans, it should be on your radar.

More than just dollar bills, y'all

This is an industry rich in payment data, and that makes for an easy dollar for bad guys. But Payment data isn't the only type of data being compromised. Instead, we also see Personal data being compromised, often as a byproduct of attacks, so be sure to pay proper attention to your security program outside of your payment card environment.

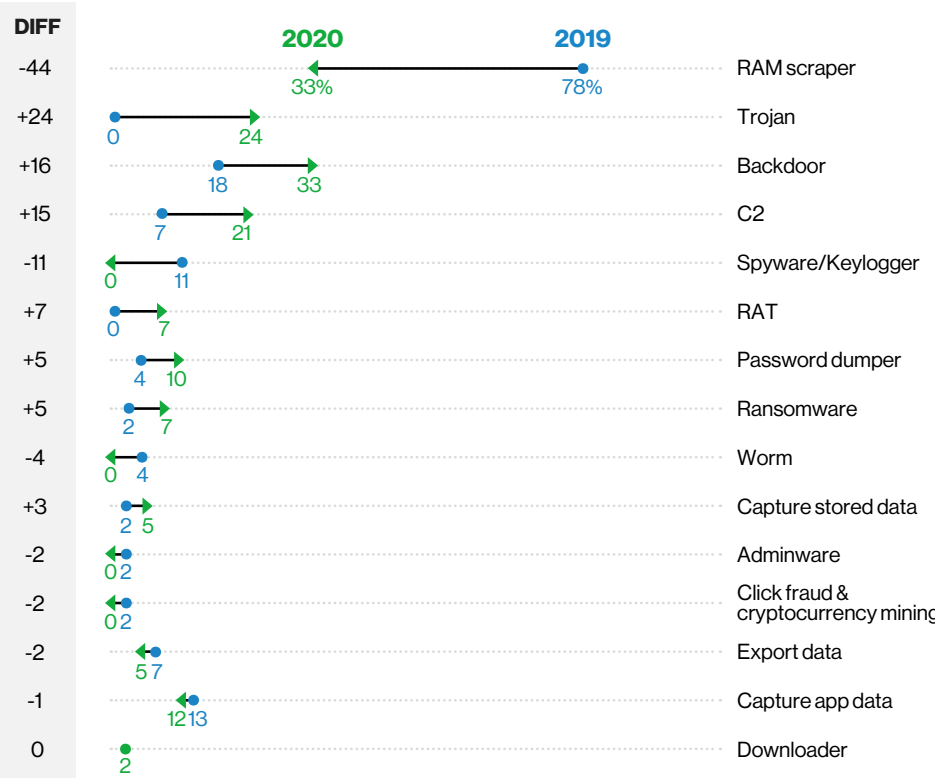


Figure 55. Top Malware over time in Accommodation and Food Services industry breaches; n = 45 (2019), n = 42 (2020)

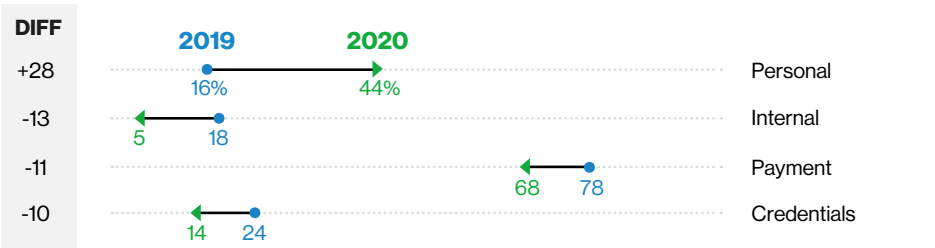


Figure 56. Top compromised data type over time in Accommodation and Food Services industry breaches; n = 51 (2019), n = 87 (2020)

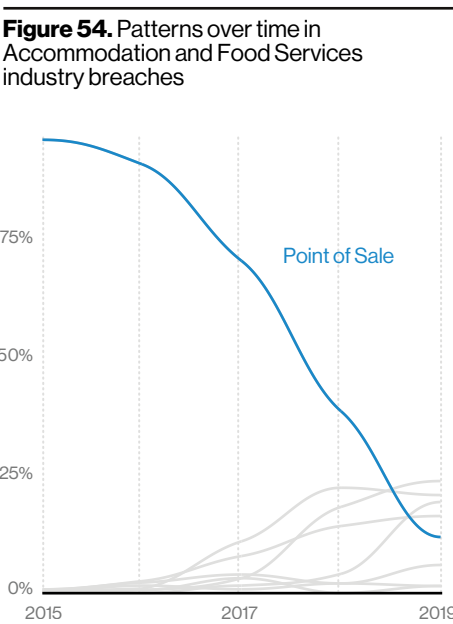


Figure 54. Patterns over time in Accommodation and Food Services industry breaches

# Arts, Entertainment and Recreation

NAICS  
71

## Summary

Web applications attacks led to many breaches in this sector. Denial of Service attacks had higher bits-per-second volume in this industry than in the overall dataset. Social engineering attacks and errors also figure prominently in this vertical.

Frequency	194 incidents, 98 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 68% of data breaches.
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (94%), Convenience (6%) (breaches)
Data Compromised	Personal (84%), Medical (31%), Other (26%), Payment (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17)

## Wake up in a good mood and start hacking.

While hackers were once described as being “like an artist,” organizations in this industry that have been on the receiving end of some of these artistic endeavors might have a slightly different opinion. Although creativity and novelty are the hallmarks of this industry, the majority of the breaches in this sector may suffer from artistic criticisms such as “derivative” or “this has been done before” given that the top breach patterns are Web Applications, Miscellaneous Errors and Everything Else (Figure 57).

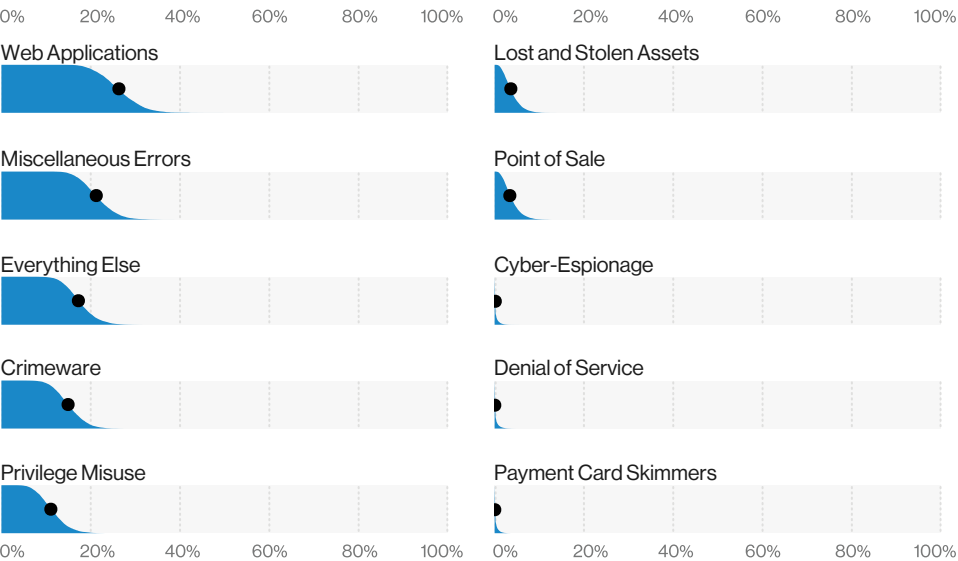


Figure 57. Patterns in Arts and Entertainment industry breaches (n = 98)

Fraudulent forgers fool frequently.

Much like how the authenticity of art can be difficult to establish, humans also struggle with determining the legitimacy of electronic communications. This accounts for the prevalence of the Everything Else pattern, where social engineering takes the wheel. In 2019, a Social action was found in approximately 18% of breaches. But to return to the topic of human nature, accidents and errors such as Misconfigurations and Misdeliveries remain a common issue for this sector. The growth in accidental breaches can be seen in Figure 58, where there has been a converging of Internal and External actors over the last few years. While this rise could be due to changes in breach reporting, it has remained consistent since 2016.

Untitled Work II

Companies want to be able to maintain their data’s integrity, and cybercriminals know that. This year, the top Malware varieties (Figure 59) included functionality, such as “Capture app data.” This and the others listed allow bad actors to steal quietly into your systems and siphon your data while leaving worms to spread across your environment and ransomware to lock away your key data. These are either introduced on web servers via a vulnerability, or on desktops through the tried and true method of email phishing.

The DDoS-er

One very interesting result from our research this year was that this industry experienced the highest rate of DDoS attacks (Figure 60), beating out even the Information sector—our usual winner—by a wide margin. This NAICS code contains the online gambling industry as a member, and they are likely the ones driving this trend. Apparently, DDoSing your business rival is a thing in that realm. Who knew?

Figure 59. Top Malware variety changes over time in Arts and Entertainment industry incidents; n = 14 (2015), n = 35 (2020)

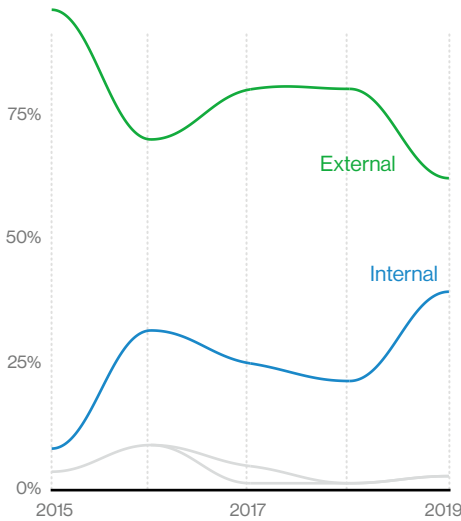
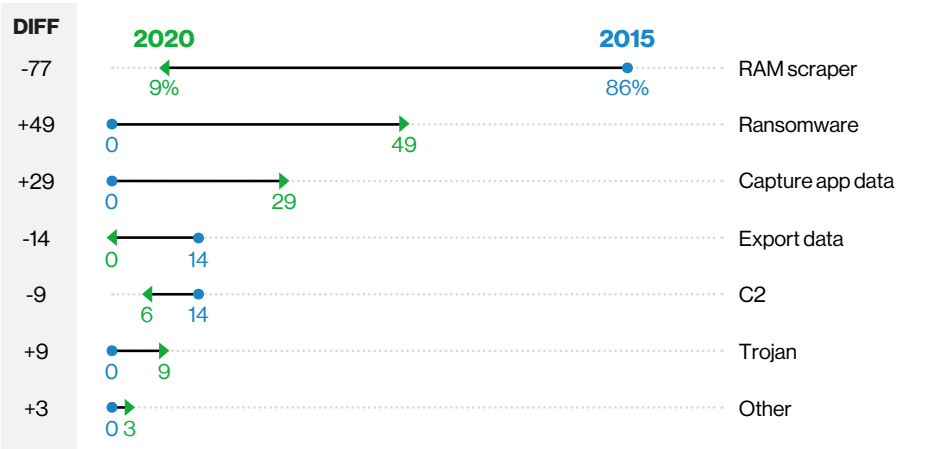
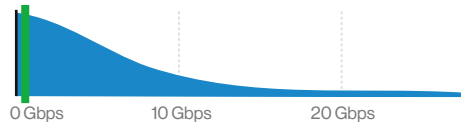


Figure 58. Actors over time in Arts and Entertainment industry breaches

Figure 60. Most common BPS in Arts and Entertainment industry DDoS (n = 5 organizations); all industries mode (green line): 565 Mbps



## Summary

**This vertical suffers from Web App attacks and social engineering, and the use of stolen credentials remains a problem. However, it boasts a low submit rate for phishing and exhibits a surprisingly low number of employee errors.**

<b>Frequency</b>	37 incidents, 25 with confirmed data disclosure
<b>Top Patterns</b>	Everything Else, Web Applications and Crimeware represent 95% of all incidents.
<b>Threat Actors</b>	External (95%), Internal (5%) (incidents)
<b>Actor Motives</b>	Financial (84%–100%), Grudge (0%–16%) (incidents)
<b>Data Compromised</b>	Personal and Credentials
<b>Top Controls</b>	Secure Configurations (CSC 5, CSC 11), Boundary Defense (CSC 12), Account Monitoring and Control (CSC 16)
<b>Data Analysis Notes</b>	Actor Motives are represented by percentage ranges, as only 10 breaches had a known motive. We are also unable to provide percentages for Data Compromised.

## Rob the builder

Having delved a bit deeper into our data, we were able to build sections on several new industries this year, and Construction is among them. Although the Construction industry may not be the first thing that comes to mind when you think of data breaches, it is a critical industry that generates a great deal of economic growth and helps to sustain the nation's infrastructure. When viewed from that perspective, one question that may come to mind is, "What motivates the attacks in this industry?" Most cases were financially motivated and were typically carried out by organized criminal groups. The majority of these attacks were opportunistic in nature, which means that the actors who perpetrated them had a very well-calibrated hammer they knew how to make work, and were just looking for some unprotected nails.

Since this is the first time we've all sat down together at the Construction industry table, we should take a moment to talk about the top attack patterns from the Summary table on the left. The Everything Else pattern is basically our bucket for attacks that do not fit within the other patterns. There are quite a bit of social engineering attacks in it, and they frequently come in the form of either a pretext attack (invented scenarios to support the attacker's hope that the victim will do what they are asking them to do) or general phishing, for the less industrious criminal who doesn't want to expend all that effort. Web Applications attacks are what they sound like: people hacking into websites to get to the data. Crimeware is your basic malware attack; ransomware falls in here and is increasingly popular. While a ransomware attack usually doesn't result in a data breach, threat actors have been moving toward taking a copy of the data before triggering the encryption, and then threatening a breach to try to pressure the victims into paying up.

## How they do that voodoo they do

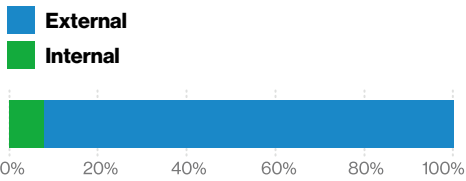
We mentioned social engineering as a common approach in this industry (and in the dataset as a whole). The bad guys use this approach simply because it works. Whether the adversary is trying to convince the victims to enter credentials into a web page, download some variety of malware or simply wire them some cash, a certain percentage of your employees will do just that (Figure 61). What is a proactive security person to do? We've talked about how important it is to know you're a target—and while the click rate shows that people in this industry fall for the bait slightly more often than the average Joe, it is important for them to report that they've been targeted. While the submission rate after clicking is quite low for the sector, so is the reporting rate. You can tell by all the stacked companies at 0% in the Figure 62 dot plot.



**Figure 61.** Median click rate in Construction industry phishing tests (n = 532); all industries median (green line): 3.6%



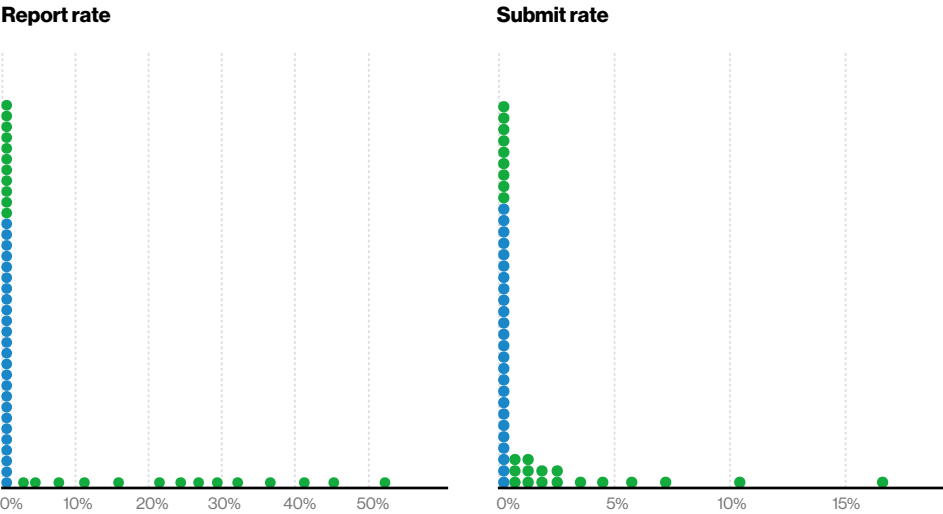
For the Web Applications attacks, the most common hacking variety was the use of stolen credentials. Sometimes these were obtained from a phishing attack, and sometimes they were just part of the debris field from other breaches. Employees reusing their credentials for multiple accounts (both professional and personal) increases risk for organizations when there are breaches and the stolen credentials are then used for credential stuffing. The key to reducing this risk is to ensure that the stolen credentials are worthless against your infrastructure by implementing multifactor authentication methods.



**Figure 63.** Actors in Construction industry breaches (n = 25)

**We love our employees.**

One thing that really stood out when we looked at this sector was how low the Internal actor breaches were. Internal actor breaches come in two flavors: Misuse (malicious intent) and Error (accidental). This sector had very few breaches involving either, as shown in Figure 63.



**Figure 62.** Median rates in Construction industry phishing tests (n = 532)

# Educational Services

NAICS  
61

## Summary

This industry saw phishing attacks in 28% of breaches and hacking via stolen credentials in 23% of breaches. In incident data, Ransomware accounts for approximately 80% of Malware infections in this vertical. Educational Services performed poorly in terms of reporting phishing attacks, thus losing critical response time for the victim organizations.

Frequency	819 incidents, 228 with confirmed data disclosure
Top Patterns	Everything Else, Miscellaneous Errors and Web Applications represent 81% of breaches.
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (92%), Fun (5%), Convenience (3%), Espionage (3%), Secondary (2%) (breaches)
Data Compromised	Personal (75%), Credentials (30%), Other (23%), Internal (13%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configuration (CSC 5, CSC 11)

## An island of misfit breaches

You may be wondering, “What is this Everything Else pattern that is top of the class in this sector?” It sounds like the kitchen drawer where all the odds and ends wind up, and in a way, it is. If an attack doesn’t meet the criteria of one of the other attack patterns, it ends up here, with that olive pit remover you got from your Secret Santa.

Phishing dominates the Everything Else pattern by a comfortable margin, not unlike many other industries. However, the Educational Services sector stands out by also getting a failing grade in phishing reporting practices. Of all industries, according to our non-incident data, only 24% of organizations had any phishing reporting at all, and none of them had at least 50% of the emails reported in phishing awareness campaigns. It is exceedingly important to encourage your user base to let you know when your organization is being targeted. If they don’t report it, you miss out on your early warning system.

Similarly, the prevalence of the Web Applications pattern is mostly because of the use of stolen creds on cloud email accounts. Although we cannot say this is the organizations’ fault, according to our non-incident data analysis, Educational Services have the longest<sup>40</sup> number of days in a year—28—where they had credential dumps run against them. The global median here is eight days. The overall number of credentials attempted is also one of the highest of all industries we analyzed for this year’s report (Figure 64).

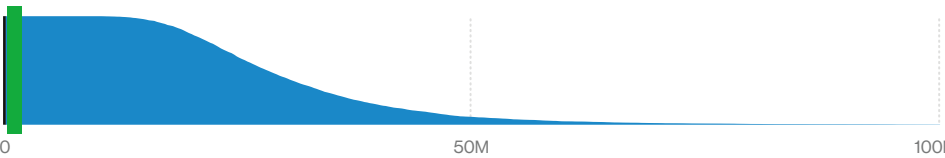
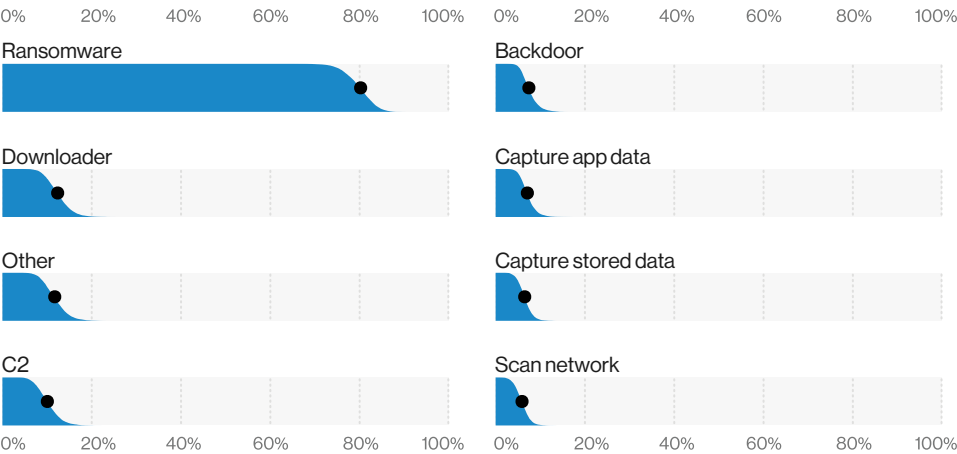


Figure 64. Credential stuffing attempts in Education industry web blocks (n = 8); all industries mode (green line): 1.11 M

40 Mode of industry

Outside of those two patterns, sadly, the news is still not great. Ransomware is really taking hold of Education vertical incidents, and has been responsible for 80% of the Malware-related incidents, up from 48% last year (Figure 65). All of those Ransomware cases have also played a role in the increase we have seen in financially motivated incidents for the past two years.

One additional concern in this sector is the fact that, according to our analysis, this is the only industry where malware distribution to victims was more common via websites than email. This information doesn't really seem to make sense until you consider malware being distributed via unmonitored email (such as personal mail accounts from students on bring-your-own devices connected to shared networks), and all of those infections obviously endanger the larger organization.



**Figure 65.** Top Malware varieties in Education industry incidents (n = 129)

# Financial and Insurance

NAICS  
52

## Summary

The attacks in this sector are perpetrated by external actors who are financially motivated to get easily monetized data (63%), internal financially motivated actors (18%) and internal actors committing errors (9%). Web Applications attacks that leverage the Use of stolen credentials also continue to affect this industry. Internal-actor-caused breaches have shifted from malicious actions to benign errors, although both are still damaging.

Frequency	1,509 incidents, 448 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 81% of breaches.
Threat Actors	External (64%), Internal (35%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (91%), Espionage (3%), Grudge (3%) (breaches)
Data Compromised	Personal (77%), Other (35%), Credentials (35%), Bank (32%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

## Why is everybody always picking on me?

The Financial and Insurance sector has always had a target on its back due to the kinds of data it collects from its customers. The data shows that the sector remains a favorite playground for the financially motivated organized criminal element again this year. Web Applications attacks are in competition with the Miscellaneous Errors pattern for the top cause of most breaches, as shown in Figure 66. It is a bit disturbing when you realize that your employees' mistakes account for roughly the same number of breaches as external parties who are actively attacking you. Apparently, it really is hard to get good help these days, and you can take that to the bank.

The Misuse action was among the top three causes of breaches for this vertical in last year's report, but it dropped from 21.7% in the 2019 report to only 8% this year. While this pattern saw a decline in our overall dataset, we are not of the opinion that all employees have suddenly become virtuous with regard to abusing their access. It is more likely that this is simply reflective of a change in contributor visibility rather than a sign of extreme moral rectitude in the workforce.

We switch our focus from malicious actions to those that were unintentional in Figure 67. The most common Error was Misdelivery, which is pretty much exactly what it sounds like: sending information to the wrong person. This can be with electronic data, such as an email sent to the incorrect recipient by an autofill in the "To:" field. Or it can be paper documents, such as a mass mailing that is incorrectly addressed. Both can result in a large breach, depending on what file(s) were attached to the email, or how large the mass mailing was.

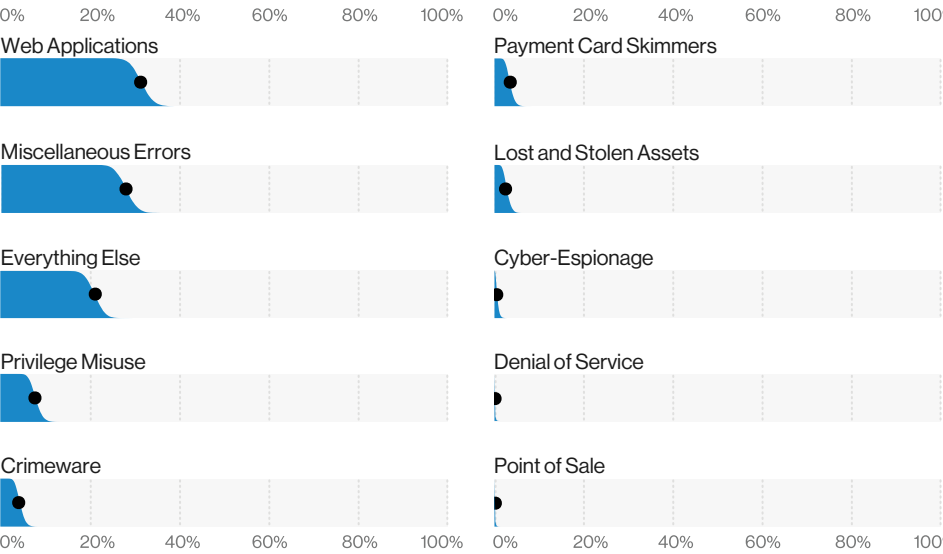
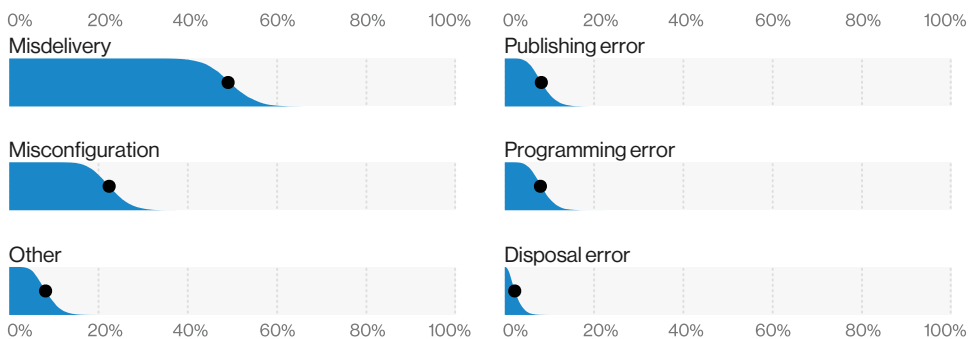


Figure 66. Patterns in Finance and Insurance industry breaches (n = 448)

**Figure 67.** Top Error varieties in Finance and Insurance industry breaches (n = 109)



The second most common Error is one that has been experiencing a surge in popularity—the Misconfiguration. This occurs when someone (often a system administrator) fails to secure a cloud storage bucket or misconfigures firewall settings. In the case of both Misdelivery and Misconfiguration, the motivation was overwhelmingly carelessness. Good security practices? Ain't nobody got time for that.

## The wallflowers of the breach world

Like the shy creatures that line the walls of the middle school dance, those attacks that are shy in providing sufficient detail end up in the Everything Else pattern. Here languish the average, yet successful, phishing attacks, and the increasingly common business email compromise in its various forms. Among its many incarnations is the phishing email masquerading as coming from someone in the executive level of the company asking for something of monetary value.

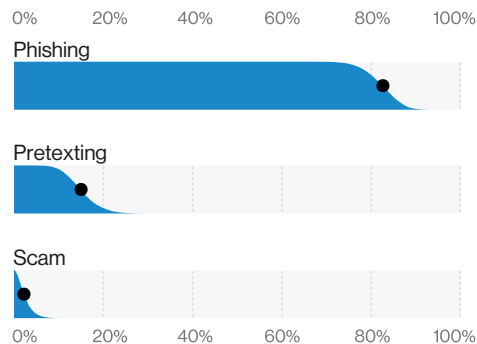
## Keep on playing those mind games together.

We also see invented scenarios (Pretexting) manufactured in order to plausibly convince the target to transfer money to the attacker's bank account. Figures 68 and 69 illustrate the popularity of these common social attacks. One key takeaway is that the weakest link in many organizations is their staff. Is it likely that the average user (who was targeted based on their access to data) will challenge a request that appears to be coming from someone who has the authority to fire them? Our *Magie 8-Ball* data indicates that signs point to no.

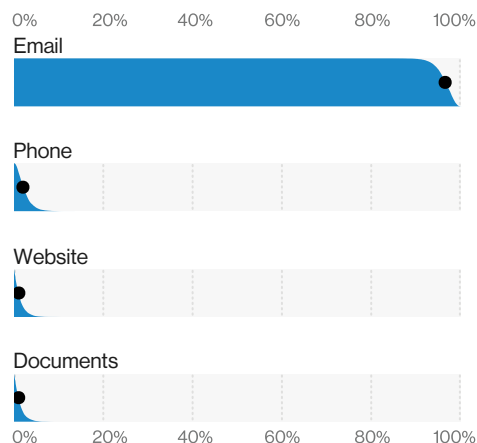
The majority of attacks in this sector are perpetrated by external actors who are financially motivated to access easily monetized data stored by the victim organizations. While there remains a small amount of Cyber-Espionage by nation-state actors in this industry, most attacks are perpetrated by someone who is all about the shekels.

## #somefilter

As stated in past versions of this report, we utilize filters in our data analysis for a variety of things, including focusing on a given industry, threat actor type, etc. We also use them to exclude certain subsets of data in order to reduce skew and to help us find trends that might otherwise be missed. However, we do not ignore this data; we analyze it separately in other sections of this report. You can read more about it in our “Incident classification patterns and subsets” section. Specifically, for Finance, there were tens of thousands of incidents on the Botnet subset analyzed separately.



**Figure 68.** Social varieties in Finance and Insurance industry breaches (n = 86)



**Figure 69.** Social vectors in Finance and Insurance industry breaches (n = 86)

# Healthcare

NAICS  
62

## Summary

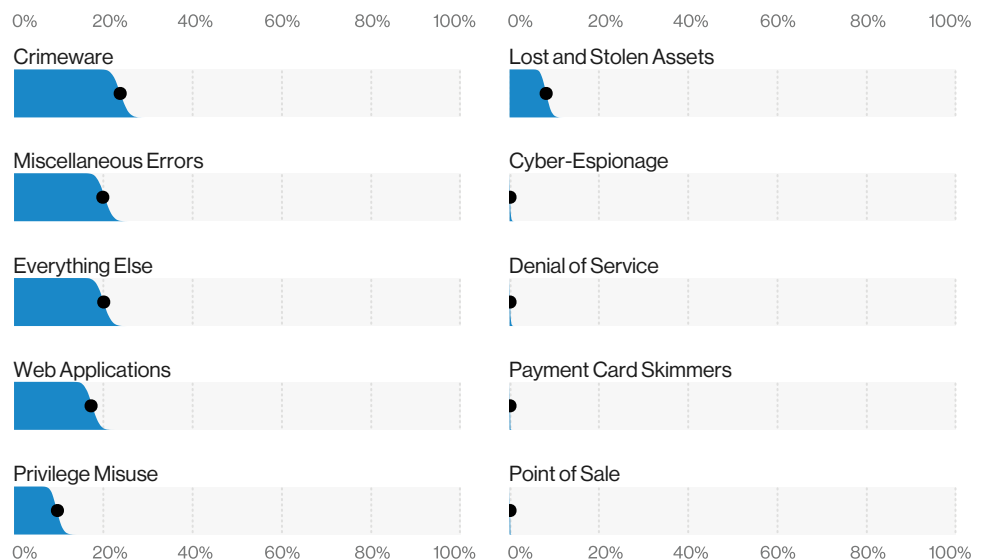
Financially motivated criminal groups continue to target this industry via ransomware attacks. Lost and stolen assets also remain a problem in our incident dataset. Basic human error is alive and well in this vertical. Misdelivery grabbed the top spot among Error action types, while internal Misuse has decreased.

<b>Frequency</b>	798 incidents, 521 with confirmed data disclosure
<b>Top Patterns</b>	Miscellaneous Errors, Web Applications and Everything Else represent 72% of breaches.
<b>Threat Actors</b>	External (51%), Internal (48%), Partner (2%), Multiple (1%) (breaches)
<b>Actor Motives</b>	Financial (88%), Fun (4%), Convenience (3%) (breaches)
<b>Data Compromised</b>	Personal (77%), Medical (67%), Other (18%), Credentials (18%) (breaches)
<b>Top Controls</b>	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Data Protection (CSC 13)

**As contributors come and go, our dataset will change, and that change will be visible in both the types of attacks and the overall number of breaches we include in this report.**

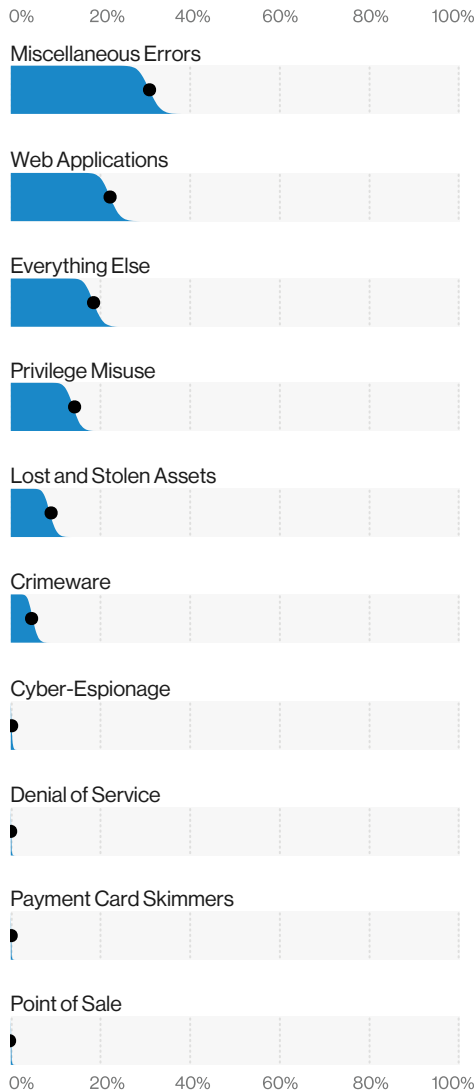
This year, we saw a substantial increase in the number of breaches and incidents reported in our overall dataset, and that rise is reflected within the Healthcare vertical. In fact, the number of confirmed data breaches in this sector came in at 521 versus the 304 in last year's report. Since this is the *Data Breach Investigations Report*, we tend to put more focus on actual confirmed breaches. But in Healthcare, given the Department of Health and Human Services' (HHS) guidance on ransomware cases for example,<sup>41</sup> the incidents hold higher relevance than they might in a different vertical despite the data being simply "at-risk" rather than a confirmed compromise.

Figure 70 shows the breakdown of the patterns for incidents in Healthcare. The Crimeware pattern includes Ransomware incidents, and as one might expect, that pattern accounts for a large portion of the incidents in this sector. If we drop further down the list in this chart, we see that one pattern that tends to get lost in the shuffle is Lost and Stolen Assets. Because the asset is not available, proving whether the data was accessed or not is no simple matter. Therefore, we code these as incidents with data being "at-risk" rather than as a confirmed compromise. Our caution to the reader is not to assume that because the attacks aren't showing up as confirmed breaches in our dataset, you won't have to declare a breach according to the rules that govern your industry.



**Figure 70.** Patterns in Healthcare industry incidents (n = 798)

<sup>41</sup> "The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule." <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>



**Figure 71.** Patterns in Healthcare industry breaches (n = 521)

## Take three patterns and call me in the morning.

If you've been following the "Healthcare" section for some time, you may notice a big change in the breach pattern rankings on Figure 71. This is the first year that the Privilege Misuse pattern is not in the top three. However, this pattern saw a significant proportional drop in our dataset overall—not just in the Healthcare vertical. In the 2019 report, we showed Privilege Misuse at 23% of attacks, while in 2020, it has dropped to just 8.7%. Does that indicate that insiders are no longer committing malicious actions with the access granted to them to accomplish their jobs? Well, we wouldn't go quite that far. However, it will be interesting to see if this continues as a trend when next year's data comes in.

Another change that goes along with decreased insider misuse breaches is the corresponding drop in multiple actor breaches. The Healthcare sector has typically been the leader in this type of breach—which usually occurs when External and Internal actors combine forces to abscond with data that is then used for financial fraud. The multiple actor breaches last year were at 4% and this year we see a drop to 1%. The 2019 DBIR reported a first in that the Healthcare vertical had Internal actor breaches (59%) exceeding those perpetrated by External actors (42%). This year, External actor breaches are slightly more common at 51%, while breaches perpetrated by Internal actors fall to 48%. However, this is a small percentage and Healthcare remains the industry with the highest amount of internal bad actors.

As with many things in life, as one attack grows more prevalent, others begin to decrease. So the story goes with the Miscellaneous Errors pattern. While it has frequently graced the top three patterns in this sector, it took the gold this year. In case you are curious, the top mistake within Healthcare is our old friend, Misdelivery.

This Error tends to fall into two major categories:

- Someone is sending an email and addresses it to the wrong (and frequently wider) distribution—it's an added bonus if a file containing sensitive data was attached
- An organization is sending out a mass mailing (paper documents) and the envelopes with the addresses become out of sync with the contents of the envelope. If sampling is not done periodically throughout the mailing process to ensure that they remain \*NSYNC, then it's bye, bye, bye to your patients' sensitive information

When thinking of the Healthcare vertical, one naturally thinks of Medical data. And, unsurprisingly, this is the industry in which that type of data is the most commonly breached. However, we also see quite a lot of both Personal data (which can be anything from basic demographic information to other covered data elements) and Credentials stolen in these attacks. The second most common pattern for Healthcare is the Web Applications attack. As more and more organizations open patient portals and create new and innovative ways of interacting with their patients, they create additional lucrative attack surfaces.

Finally, we see a good deal of the Everything Else pattern, which is not unlike a lost and found for attacks that do not fit the criteria of any other attack pattern. It is within this pattern that the business email compromise resides. If you're not familiar with this attack, it is typically a phishing attack with the aim of leveraging a pretext (an invented scenario to give a reason for the victim to do what the attacker wants) to successfully transfer money (by wire transfer, gift cards or any other means). Although these are common attack types across the dataset, it is a good reminder to Healthcare organizations that it isn't only patient medical data that is being targeted.

---

### **When did you first notice these symptoms?**

The time required to compromise and exfiltrate data has been getting smaller in our overall dataset. Unfortunately, the time required for an organization to notice that they have been breached is not keeping pace. There is a discrepancy there somewhat akin to how long it takes you to earn your wages vs how long it takes for them to be taxed. Some attacks, by their very nature, will both happen quickly and be detected quickly. A good example is a stolen laptop—how long does it take someone to smash a car window and make off with the loot? (That is a rhetorical question, so don't mail in answers, there is no prize for getting it right.) Likewise, it also doesn't take much time for the owner to come back to their car and see the break-in.

Both of these will have a short duration due to the nature of the crime. In contrast, an insider who has decided to abuse their access to copy a small amount of data each week and sell it to their buddy, who in turn utilizes it for financial fraud, may not be caught for a very long time.



## Summary

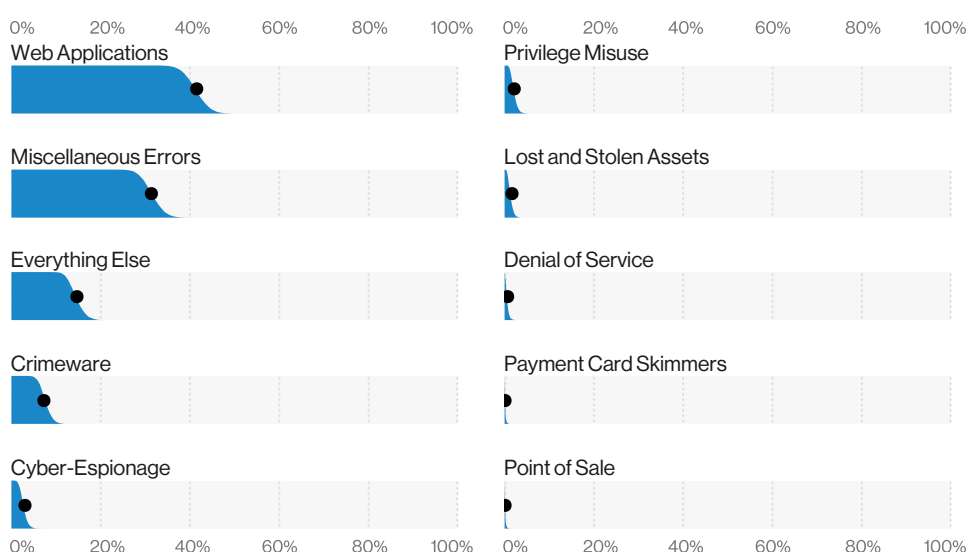
**Web App attacks via vulnerability exploits and the Use of stolen credentials are prevalent in this industry. Errors continue to be a significant factor and are primarily made up of the Misconfiguration of cloud databases. Growth in Denial of Service attacks also remains a problem for the Information sector.**

<b>Frequency</b>	5,741 incidents, 360 with confirmed data disclosure
<b>Top Patterns</b>	Web Applications, Miscellaneous Errors and Everything Else represent 88% of data breaches.
<b>Threat Actors</b>	External (67%), Internal (34%), Multiple (2%), Partner (1%) (breaches)
<b>Actor Motives</b>	Financial (88%), Espionage (7%), Fun (2%), Grudge (2%), Other (1%) (breaches)
<b>Data Compromised</b>	Personal (69%), Credentials (41%), Other (34%), Internal (16%) (breaches)
<b>Top Controls</b>	Secure Configurations (CSC 5, CSC 11), Continuous Vulnerability Management (CSC 3), Implement a Security Awareness and Training Program (CSC 17)

## Come one, come all!

Welcome to the Information industry portion of the DBIR, and boy are you in for a treat! This section has it all: web applications attacks, errors, phishing and even some malware. The main three patterns witnessed in the NAICS 51 sector for 2019 were Web Applications with over 40% of breaches, followed by Miscellaneous Errors and, at a distant third, Everything Else (Figure 72).

**Figure 72.** Patterns in Information industry breaches (n = 360)



Since 2019, Web Applications attacks have increased significantly, both in terms of percentage and in raw number of breaches.. This is one that organizations in this industry should keep an eye out for, as adversaries are dividing their effort equally between utilizing web exploits and stolen credentials to gain access to your web applications. Considering this vertical has a high dependence on external services and the internet, one shouldn't be too shocked to learn that this industry has a higher percentage of web application exploitations than other industries. However, based on our non-incident data, Information also has one of the highest percentages of vulnerability patching completed on time (Figure 73).

## An anthem to errors

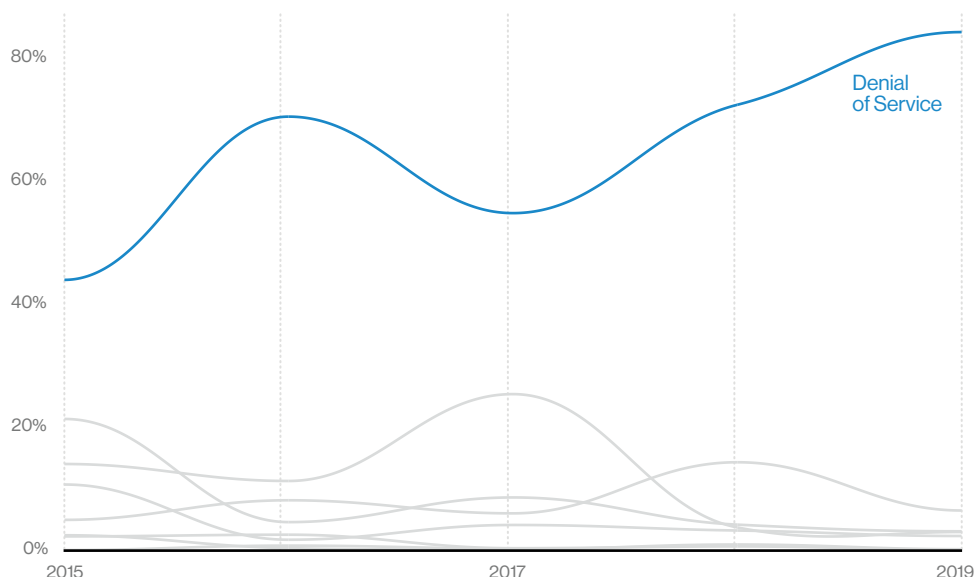
Errors are everywhere and the technical wizards that run our information infrastructure are not immune. This is why Errors are the second most common type of breach, maintaining relatively similar levels to previous years (this is not an area where consistency is a good thing). Misconfigurations are by far the most common type of errors, and largely relate to databases or file storages not being secured and directly exposed on a cloud service. These are the types of incidents that you hear security researchers discovering through simple trawling of the internet to see what's exposed. The optimist in us hopes that as these new technologies become more commonly used, people will stop (or at least slow down) making these types of mistakes. On the other hand, the realist in us wouldn't put any money on it.

## You, sir, are a phish.

Technical issues are not the only thing impacting this technology-based sector. Organizations in this vertical have fallen prey to the same type of social engineering attacks that affect everyone else. Most of these attacks fall into our Everything Else pattern and account for 16% of the breaches we saw in 2019. In terms of social attacks, there is a relatively even split between phishing and pretexting (the bad guy just asks for information via email or uses some existing conversation in order to make a more convincing request). One of the common techniques we've seen is the use of typo-squatted domains of partners that are used to send existing email threads or request an update to a bank account.

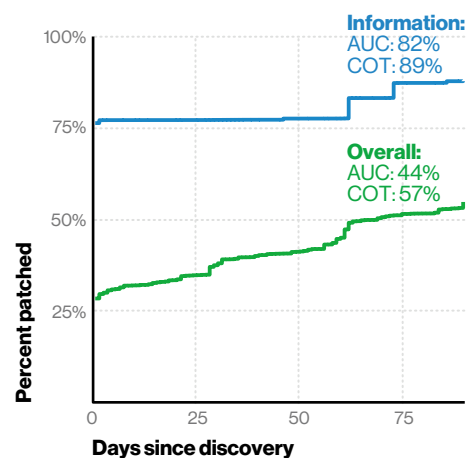
## Fast speeds and full bandwidths

Big interweb pipes are a key part of this industry since consumers demand that videos load fast and website content gets updated at the speed of an unladen European swallow. Unfortunately, cybercriminals know how important that is, and have been persistently targeting this industry with DoS attacks to disrupt their services and capabilities. The 2019 data showed continued growth in terms of the percentage of DDoS incidents (Figure 74). Not only does this industry get targeted more than a red barrel in a first-person shooter, they're also facing attacks with the second highest median BPS—meaning these attacks tend to pack a punch. Unfortunately for many companies, these attacks often need a helping hand to mitigate, so it helps to have a Player 2 in your corner.



**Figure 74.** Patterns over time in Information industry incidents

**Figure 73.** Patching in Information industry vulnerabilities (n = 36,255)



# Manufacturing

NAICS  
31-33

## Summary

**Manufacturing is beset by external actors using password dumper malware and stolen credentials to hack into systems and steal data. While the majority of attacks are financially motivated, there was a respectable showing of Cyber-Espionage-motivated attacks in this industry as well. Internal employees misusing their access to abscond with data also remains a concern for this vertical.**

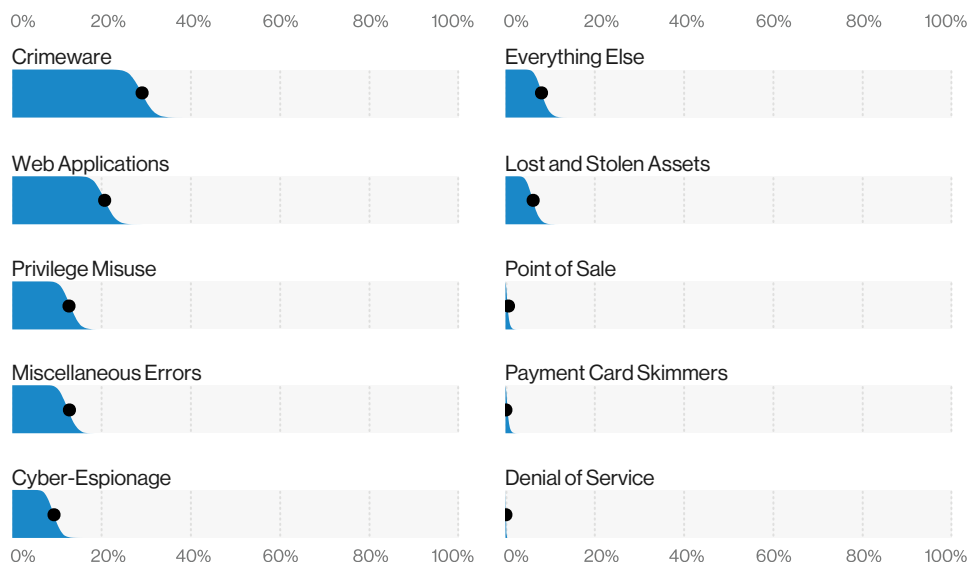
<b>Frequency</b>	922 incidents, 381 with confirmed data disclosure.
<b>Top Patterns</b>	Crimeware, Web Applications and Privilege Misuse represent 64% of breaches.
<b>Threat Actors</b>	External (75%), Internal (25%), Partner (1%) (breaches)
<b>Actor Motives</b>	Financial (73%), Espionage (27%) (breaches)
<b>Data Compromised</b>	Credentials (55%), Personal (49%), Other (25%), Payment (20%) (breaches)
<b>Top Controls</b>	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Data Protection (CSC 13)

## Bad actors, bad actions, bad puns

It has been said that the proper study of mankind is Man(ufacturing), or at least we are pretty sure that is how the adage goes. We hope so at least, because we have been giving a lot of thought to that topic. The Manufacturing vertical is very well represented this year with regard to both incidents and breaches. As always when we see a large increase, it could be indicative of a trend or simply a reflection of our caseload. In this instance, it is certainly the latter.

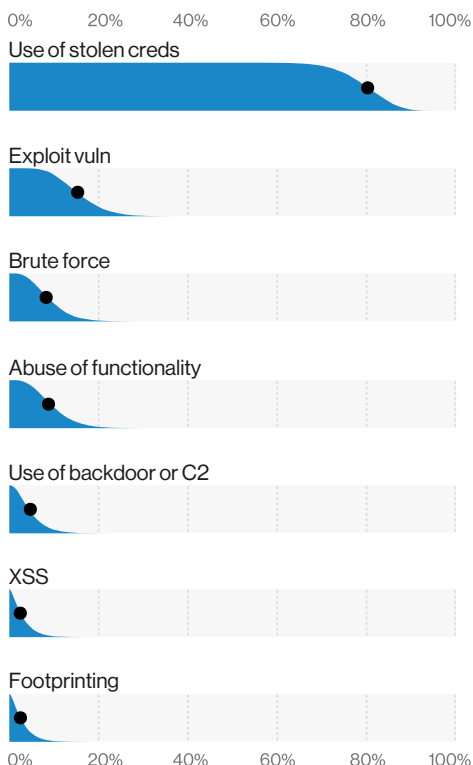
However, NAICS 31-33 has long been a much-coveted target of cybercrime and this year is no exception. Whether it is a nation-state trying to determine what its adversary is doing (and then replicate it) or just a member of a startup who wants to get a leg up on the competition, there is a great deal of valuable data for attackers to steal in this industry. And steal it they do. The predominant means they employ for this theft falls under the Crimeware pattern, as shown in Figure 75. Namely, the Password dumper, Capture app data and Downloader varieties.

This combination of obtain password, infiltrate network, download software and then capture data paints a very clear picture of what's going on in this vertical, but it may not be a picture you want hanging on your wall if you do business in this area. But while we are on the topic of malware in general, keep in mind that ransomware (while not considered a breach in this report) is still a very present danger for this industry at 23% of all malware found in incidents.



**Figure 75.** Patterns in Manufacturing industry breaches (n = 381)

**Figure 76.** Hacking varieties in Manufacturing industry breaches (n = 44)



Web Applications attacks took the number-two place this year and are dominated by the Use of the stolen credentials to compromise a variety of web apps used in enterprises. Sometimes these credentials are obtained via malicious links served up in successful phishing attacks, sometimes they are obtained via desktop sharing and sometimes it is unclear how the victim is infected. Regardless of how they are compromised, these credentials, often of the cloud-based email variety, are very successful as a means to an end in this vertical, as you can see in Figure 76.

There are several patterns that are closely grouped around the third-place position for Manufacturing: Misuse (13%), which by definition involves insiders, and is mostly Privilege abuse—the actor has legitimate access but they use those privileges to do something nefarious—and Data mishandling, of which prime examples are sending company data via personal email or placing it on cloud drives in order to work from home (Figure 77).

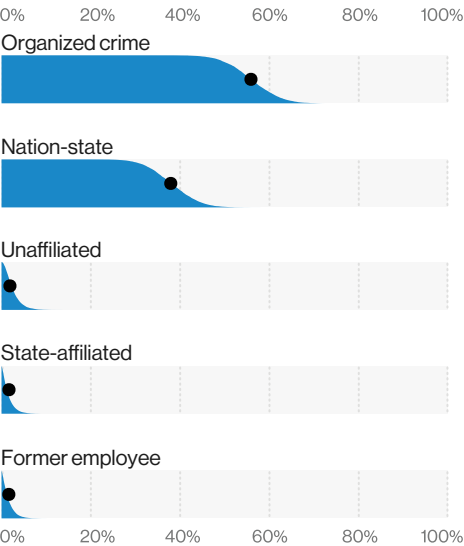
Error is ubiquitous in all of the verticals this year, and in Manufacturing it is in keeping with the trend of Misdelivery and Misconfiguration that we see in other industries. Finally, we would be remiss to not say a word or two regarding cyber-espionage-related attacks.

**Figure 77.** Misuse varieties in Manufacturing industry breaches (n = 49)

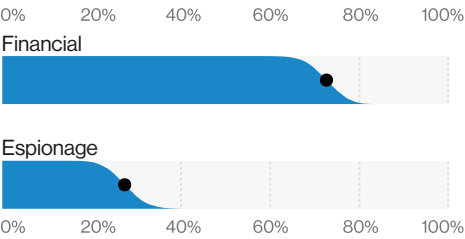


As a glance at Figures 78 and 79 reveals, 38% of actors were of the Nation-state variety, and 28% of breaches were motivated by Espionage. As we have mentioned in previous reports, it is cheaper and simpler to steal something than to design it yourself. And while large organizations are often willing to outsource their help-desk functions, they are, as a rule, not as eager to ship off their intellectual property and research-and-design generation to foreign locales.

**Figure 78.** External actor varieties in Manufacturing industry breaches (n = 83)



**Figure 79.** External actor motives in Manufacturing industry breaches (n = 121)



# Mining, Quarrying, and Oil & Gas Extraction + Utilities

NAICS  
21+22

## Summary

Breaches are composed of a variety of actions, but Social attacks such as Phishing and Pretexting dominate incident data (no confirmation of data disclosure). Cyber-Espionage-motivated attacks and incidents involving OT assets are also concerns for these industries.

Frequency	194 incidents, 43 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Cyber-Espionage represent 74% of breaches.
Threat Actors	External (75%), Internal (28%), Multiple (2%) (breaches)
Actor Motives	Financial (63%–95%), Espionage (8%–43%), Convenience/Other/Secondary (0%–17% each), Fear/Fun/Grudge/Ideology (0%–9% each) (breaches)
Data Compromised	Credentials (41%), Personal (41%), Other (35%), Internal (19%) (breaches)
Top Controls	Secure Configurations (CSC 5, CSC 11), Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17)
Data Analysis Notes	Actor motives are represented by percentage ranges, as only 21 breaches had a known motive.

## It's an NAICS mashup!

This new section combines the Mining, Quarrying, and Oil and Gas Extraction (NAICS 21) with the Utilities (NAICS 22) industries for a joint view of the incidents and breaches that affected them. We really dug deep, but we were unable to strike oil for an exclusive section for NAICS 21 on this year's report. (There must be a minimum number of incidents for the statistics to be valid.) However, we believe that this blended section with NAICS 22 will be an electrifying read and hopefully not too dry.

If you review Figure 80, you can see that while Everything Else, Web Applications and Cyber-Espionage seem to be the top three patterns in breaches, it is statistically impossible to tell which one is more prevalent—they simply overlap too much. It's exciting to have such a diversity of breaches in a brand-new industry section, but it also makes it difficult to focus on precise recommendations beyond "Note to all CISOs: Secure all the things!"

Even so, it is important to point out that the Everything Else pattern, both in incidents and breaches, is dominated by Phishing with mostly financial gain as a motive, including pretexting attacks that were clearly FMSEs.

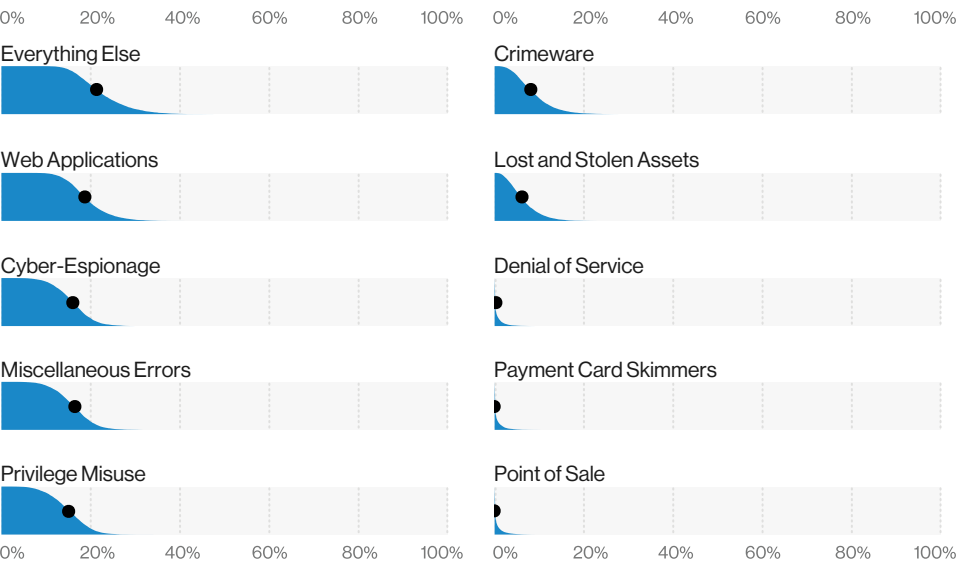


Figure 80. Patterns in Mining and Utilities industry breaches (n = 43)

## If I closed my eyes, was it still a breach?

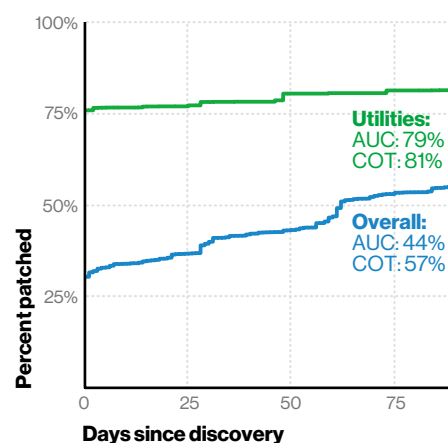
Since the Everything Else pattern is the largest for incidents (cases in which there was potential data disclosure but it was not confirmed), special attention is needed here. There were about as many incidents with potential data disclosure as there were confirmed breaches in these industries. This is especially concerning for a vertical with a broad range of possible percentages for Espionage-motivated breaches (between 8% and 43%), while in all incidents it accounts for 10% of the motives.

Wrapping up the top patterns, Web Applications is filled with the Use of stolen creds that were gathered by Phishing. Meanwhile, Miscellaneous Errors favors Misconfiguration and Publishing Errors, both action varieties that can be mitigated with stronger processes and personnel training.

Unpatched vulnerabilities in your web application infrastructure may lead to them being found by someone with a set of tools to exploit them in an automated fashion. Keeping your infrastructure patches up to date is certainly a security best practice. In looking at our non-incident data surrounding time to patch (Figure 81), we found the Utilities sector had a better-than-average score. This is good news because our research has found that the patches that do not get applied within the first quarter of being released frequently don't get applied at all. This gives the adversaries time to build tools that will make it easy even for a novice to attack the infrastructure that remains vulnerable.

Also, as these industries have become a focus of our reporting, we have added OT-specific fields to track incidents involving OT equipment in the latest version of VERIS. The total number of cases we have for this year are few, but they are mainly concerned with this sector along with Manufacturing (NAICS 31–33).

**Figure 81.** Patching in Mining and Utilities industry vulnerabilities (n = 151,658)



# Other Services NAICS 81

## Summary

**Financial gain is the highest motive for External actors, with Web Applications being 39% of breaches. Error among employees is another issue for this sector, particularly with regard to Misconfiguration and Misdelivery. While Credentials are a desirable target, it is Personal data that is most frequently stolen here.**

<b>Frequency</b>	107 incidents, 66 with confirmed data disclosure
<b>Top Patterns</b>	Web Applications, Miscellaneous Errors and Everything Else represent 83% of breaches.
<b>Threat Actors</b>	External (68%), Internal (33%), Multiple (2%) (breaches)
<b>Actor Motives</b>	Financial (60%–98%), Espionage (0%–28%), Convenience/Fear/Fun/Grudge/Other/Secondary (0%–15% each) (breaches)
<b>Data Compromised</b>	Personal (81%), Other (42%), Credentials (36%), Internal (25%) (breaches)
<b>Top Controls</b>	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Secure Configurations (CSC 5, CSC 11)
<b>Data Analysis Notes</b>	Actor Motives are represented by percentage ranges, as only 12 breaches had a known motive. Some charts also do not have enough observations to have their expected value shown.

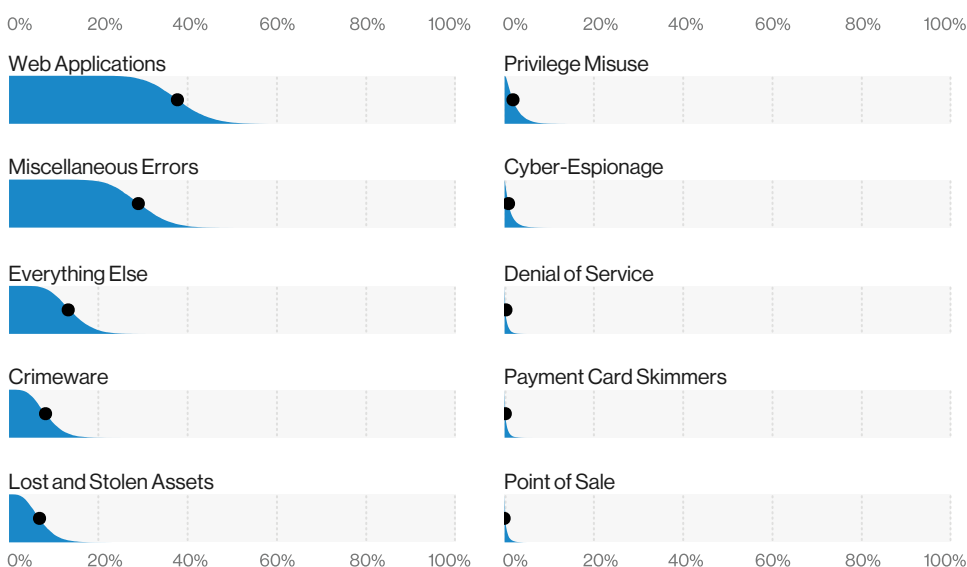
## Break on through to the other side.

The Other Services (NAICS 81) industry is also new to the report this year. This NAICS code is one of several that are surprisingly broad, covering everything from various personal and repair services to non-profit religious and social benefit organizations. Oddly enough, it even includes a subcode (814) for private households, but those are not represented in this dataset. For an incident to be eligible for inclusion in the DBIR, there must be a victim organization, since that is where the laws focus, and where the controls are most likely to have good effect. As we have mentioned in the other new sections, while this is the first year we are including this industry in the report, we have data going back a few years on this sector.

## Jockeying for that top spot

The top breach patterns in this industry were Web Applications attacks, Miscellaneous Errors and Everything Else. When looking at the incident patterns (not confirmed data breaches), the patterns remain the same, albeit in a different order.

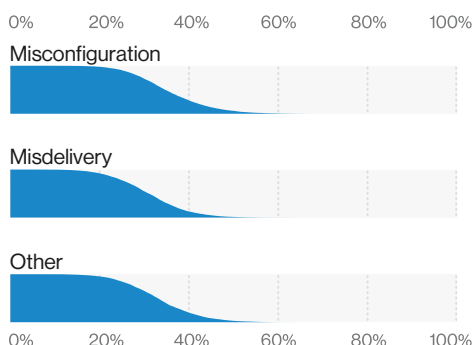
The main change from last year's data for this vertical is the drop in the Cyber-Espionage pattern. Last year it held the first place slot in the footrace, and you can see from Figure 82 that it has since told the other patterns "go on ahead, I'll catch up" as it struggles to catch its breath. Consistent with this change, we've seen the variety and motivation of the External actor breaches transform from State-affiliated/Espionage into Organized crime/Financial. It seems the people who like to go after data for the sheer joy of monetizing it have found a friend in this sector.



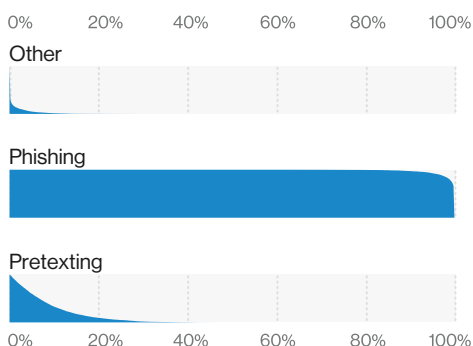
**Figure 82.** Patterns in Other Services industry breaches (n = 66)



**Figure 83.** Top Error varieties in Other Services industry breaches (n = 21)



**Figure 84.** Top Social varieties in Other Services industry breaches (n = 12)



The Web Applications attack pattern includes the Hacking actions, and the favored action variety tends to be the Use of stolen credentials. It makes sense—who wouldn't like credentials when trying to break into some else's computer? What burglar would say no to a set of free keys? And while the use of a backdoor or Command and Control (C2) infrastructure is always nice, if you can just waltz in the front door, why exert yourself? Do you enjoy being asked questions?

### What can go wrong will happen to me.

The Miscellaneous Errors pattern is all about the mistakes your employees make. Two stand out from the rest in the field of errors for Other Services: Misconfiguration and Misdelivery (Figure 83). Misconfiguration errors are the frenemies of Information Security. These breaches are caused by Internal actors (frequently a system admin or DBA, as they have access to large amounts of data) doing things such as standing up an instance of the data on a cloud platform, but neglecting to put in any security controls to limit access. Once that happens, it is a matter of time before the intrepid security researchers out there find it via their search tools and someone gets a call.

Misdelivery—when sensitive data goes to the wrong recipient(s)—is the other most common Error in this sector. A good example is when the autocomplete in an email “To:” or “Cc:” field occurs and directs to the incorrect party. In other instances, it is the mass-mailing misstep where the addresses are no longer paired with the correct contents. It is never good to have your customer open a letter only to find someone else's Personally Identifiable Information (PII) inside.

Finally, we have the Everything Else pattern, which is our version of potpourri. This is where the attacks that do not meet the criteria of the other patterns end up. Not exactly the fragrant flowers of the security breach world, these attacks are frequently made up of phishing attacks in which not a great deal of detail was provided.

The business email compromises also live within this pattern. They typically come in two main flavors: the pretext and the C-level impersonation. For the pretext, there is an invented scenario and usually an attempt to get either an invoice paid or a direct wire transfer to an adversary-controlled bank account. They may compromise the mail account of the executive and wait until the person is traveling to elevate the sense of urgency, and to minimize the ability to contact the person in order to verify the legitimacy of the request. The latter type is when the actor pretends to be a member of the executive suite, but they ask for data rather than a wire transfer. Figure 84 illustrates that phishing and pretexting are still thriving in this vertical. Both of these social engineering actions typically arrive via email.

# Professional, Scientific and Technical Services

NAICS  
54

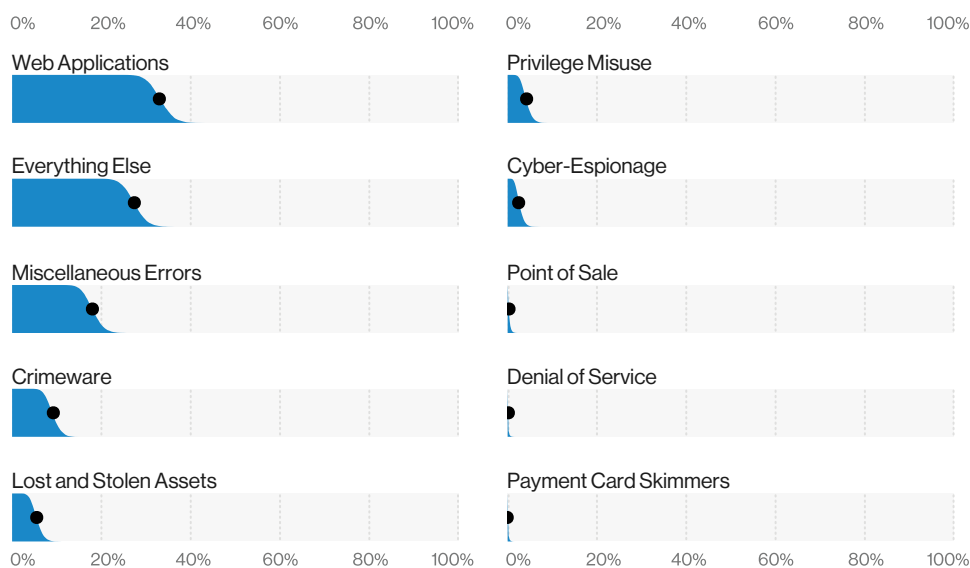
## Summary

**Financially motivated attackers continue to steal credentials and leverage them against web application infrastructure. Social engineering in the form of Phishing and Pretexting is a common tactic used to gain access. This industry also suffers from Denial of Service attacks regularly.**

<b>Frequency</b>	7,463 incidents, 326 with confirmed data disclosure
<b>Top Patterns</b>	Web Applications, Everything Else and Miscellaneous Errors represent 79% of breaches.
<b>Threat Actors</b>	External (75%), Internal (22%), Partner (3%), Multiple (1%) (breaches)
<b>Actor Motives</b>	Financial (93%), Espionage (8%), Ideology (1%) (breaches)
<b>Data Compromised</b>	Personal (75%), Credentials (45%), Other (32%), Internal (27%) (breaches)
<b>Top Controls</b>	Secure Configuration (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12)

This industry is made up of a wide range of companies primarily offering service directly to customers. They range from lawyers, accountants and architects to research labs and consulting firms. They share some common traits: Their internet presence is very important to the livelihood of the organization, and their employees are human and make mistakes.

We mentioned the importance of their internet presence to the members of this industry. This is why the Web Applications attack pattern was seen so frequently this year (Figure 85). These attacks are driven by the use of stolen credentials (frequently obtained in phishing attacks, but also may be laying around on the web from another company's breach, just waiting for some enterprising hacker to find). These attacks drive the theft of personal data in the sector, and given that there are always people willing to try their luck at using stolen credentials against whatever web infrastructure they encounter, are unlikely to end anytime in the near future.



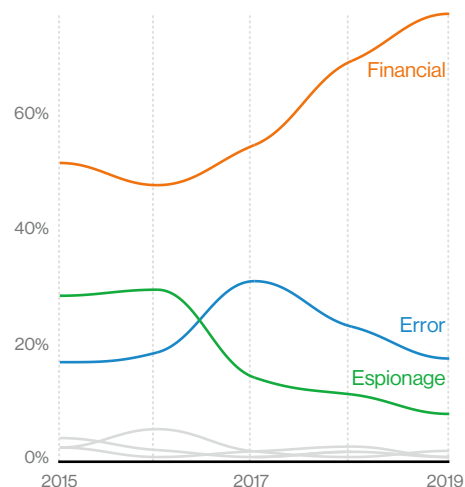
**Figure 85.** Patterns in Professional Services industry breaches (n = 326)

## I feel attacked.

Why would organizations in this sector be targets of attacks? You have heard the expression “Location, location, location”? This sector is the location of lots of useful personal data (in fact, apart from Credentials, Personal information is the most targeted data type in these breaches). This isn’t necessarily an industry full of financial information or payment card records, but personal information can be quite lucrative for a number of different kinds of financial fraud, hence the attraction. Figure 86 shows the continued growth of Financially motivated breaches at the expense of Espionage (and even Errors).

The Everything Else pattern is our scrap bin of unwanted attacks—if they do not fit the criteria of the other patterns, they end up here. They are largely low-detail phishing attacks, but sometimes the social engineering perpetrator puts a bit of actual effort into their work and invents a likely scenario to entice their prey. If you’re familiar with the business email compromise, this is where that lives. Professional Services is middle of the road when it comes to being on the receiving end of phishing attacks. But this attack isn’t just about receiving the attack—it is about whether the victim clicks, and if they submit their data. It is also about whether they raise a flag with their internal security people to let them know “what they done did.”

The news about phishing in this sector is a bit of a mixed bag. In Figure 87, we see that click rate is right on the overall median. You can also see in Figure 88 that submit rates are low (notice the large stack of companies on the 0% of the right chart—Submit rate), which is the good news—you want the number of people giving out their credentials to be low. Sadly, the bad news is that the reporting rate is low as well (there is also a large stack of companies on the 0% of Report rate), meaning that your people are not telling you they’ve fallen victim to a phish. That second measure—the Report rate—is critical so that the organization’s security response team can mitigate the effects of the breach.

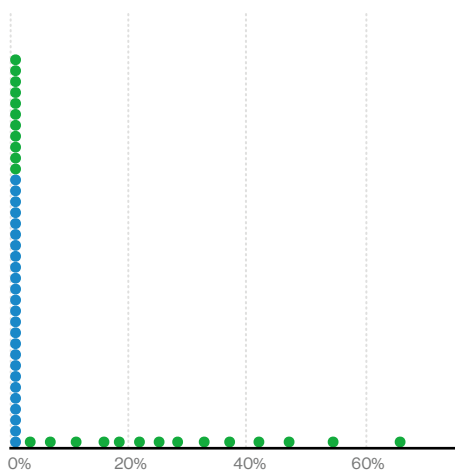


**Figure 86.** Motives over time in Professional Services industry breaches

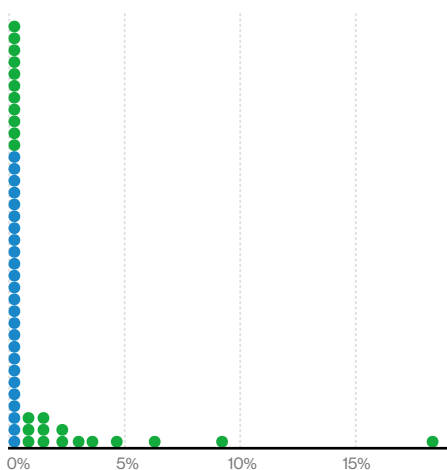


**Figure 87.** Median click rate in Professional Services industry phishing tests; all industries median (green line): 3.6%

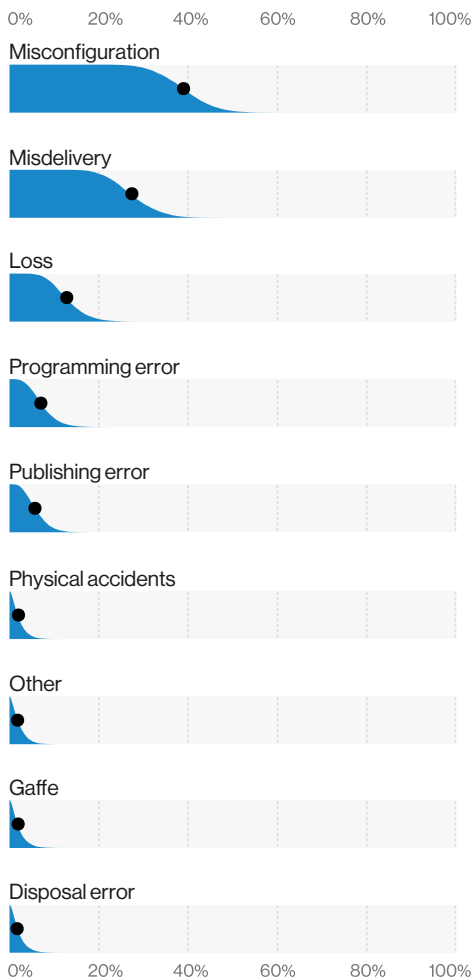
### Report rate



### Submit rate



**Figure 88.** Median rates in Professional Services industry phishing tests (n = 2,583)



**Figure 89.** Error varieties in Professional Services industry breaches (n = 67)

## I should not have done that.

Miscellaneous Errors figure prominently in this industry, but really any industry is susceptible to their employees' mishaps causing a breach. Figure 89 shows the errors that are on top in this industry—namely Misconfiguration, Misdelivery and Loss. Misconfiguration has become increasingly reported, primarily because there are people out there actively looking for this type of breach. This happens when someone drops some of their data into a cloud database instance but fails to put any protective measures in place. We mentioned people are actively searching for this, right? Yeah, then hilarity ensues—not really.

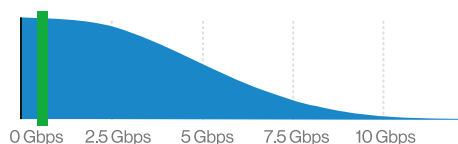
Misdelivery is frequently via paper documents in the mail, when person A gets person B's paperwork, but it can also happen via email when people are careless about addressing emails and what they attach. Loss is a bit of a different animal. When the item lost is electronic, like a laptop, this would not be counted as a breach in our dataset. For it to be counted, there must be a confirmed compromise of the confidentiality aspect of the data—and confirming access is difficult when you don't have the asset anymore. While the Loss error appears in our dataset, it is most frequently an incident, not a breach. However, here it is a breach, so what gives? Well, it would have to be an asset that is in human-readable format, like paper documents. We count them as a breach since there are no protections at all on printed matter. This is why people put caution signs on printers to give people an extra heads-up that, once printed, documents need to be treated carefully if they contain sensitive information.

## Final deliverables

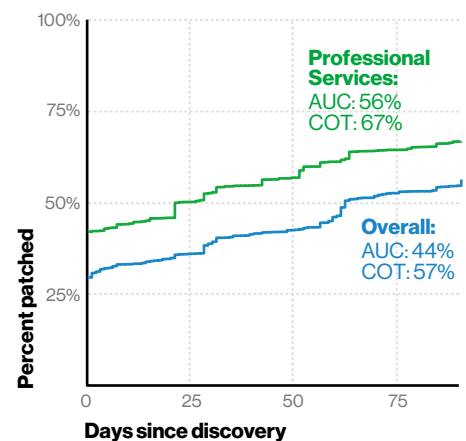
Left out of the breach patterns is Denial of Service, since it also does not typically result in an actual confidentiality breach. DDoS was over 90% of incidents in Professional Services and Figure 90 shows us that this sector has slightly above average DDoS bits per second.

To wrap up with some good news, Figure 91 shows that Professional Services has a better-than-average patch rate, completing 67% of patches in the first quarter from those being first made available from the manufacturer. If you've read the Results and Analysis—Action—Hacking section, you know that it's not the slow patching that's the problem; it's the systems in the remaining third that never get patched that are likely to come back to haunt you.

**Figure 90.** Most common BPS in Professional Services industry DDoS (n = 30 organizations); all industries mode (green line): 565 Mbps



**Figure 91.** Patching in Professional Services industry vulnerabilities (n = 87,857)



# Public Administration NAICS 92

## Summary

**Ransomware is a large problem for this sector, with financially motivated attackers utilizing it to target a wide array of government entities. Misdelivery and Misconfiguration errors also persist in this sector.**

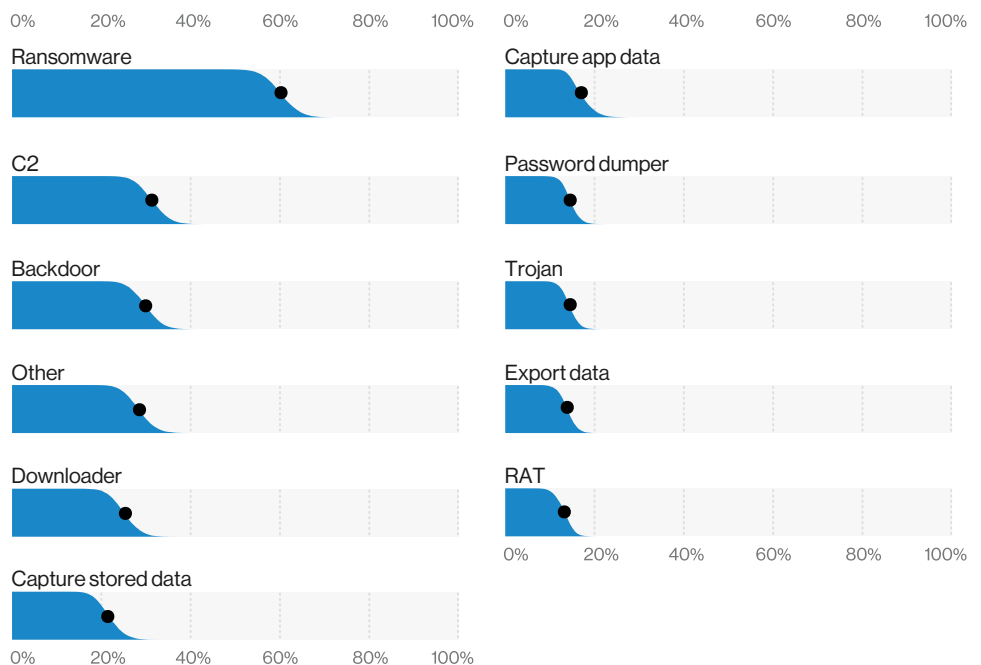
<b>Frequency</b>	6,843 incidents, 346 with confirmed data disclosure
<b>Top Patterns</b>	Miscellaneous Errors, Web Applications and Everything Else represent 73% of breaches.
<b>Threat Actors</b>	External (59%), Internal (43%), Multiple (2%), Partner (1%) (breaches)
<b>Actor Motives</b>	Financial (75%), Espionage (19%), Fun (3%) (breaches)
<b>Data Compromised</b>	Personal (51%), Other (34%), Credentials (33%), Internal (14%) (breaches)
<b>Top Controls</b>	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

## I can see clearly now.

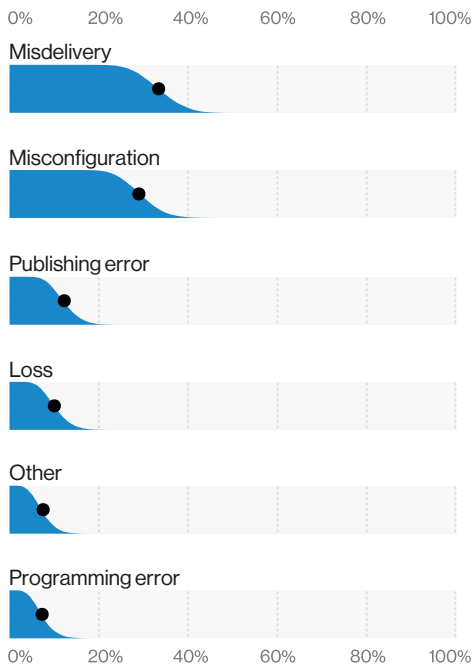
The Public Administration sector is an illustration of what good partner visibility into an industry looks like. The bulk of our data in this vertical comes from partners inside the United States federal government who have a finger on the pulse of data breaches inside Public Administration. As we have stated elsewhere in this report, in order to meet the threshold for our definition of a data breach, the compromise of the confidentiality aspect of data must be confirmed. However, reporting requirements for government are such that run-of-the-mill malware infections or simple policy violations still must be disclosed. Therefore, we see an inordinately large number of incidents and a correspondingly small number of breaches.

When we look at the difference in the attack patterns in this sector, for example, the top three for breaches are Miscellaneous Errors, Web Applications attacks and Everything Else. When we look at the same data for incidents, the top three patterns are Crimeware (malware attacks), Lost and Stolen Assets, and Everything Else.

With regard to malware in the incident dataset, Figure 92 indicates that Ransomware is by far the most common, with 61% of the malware cases. This malware is most commonly downloaded by other malware, or directly installed by the actor after system access has been gained. However, ransomware isn't typically an attack that results in a confidentiality breach. Rather, it is an integrity breach due to installation of the software, and an availability breach once the victim's system is encrypted. Thus, these attacks do not typically appear when we discuss data breaches.



**Figure 92.** Top Malware varieties in Public Administration incidents (n = 198)



**Figure 93.** Top Error varieties in Public Administration breaches (n = 92)

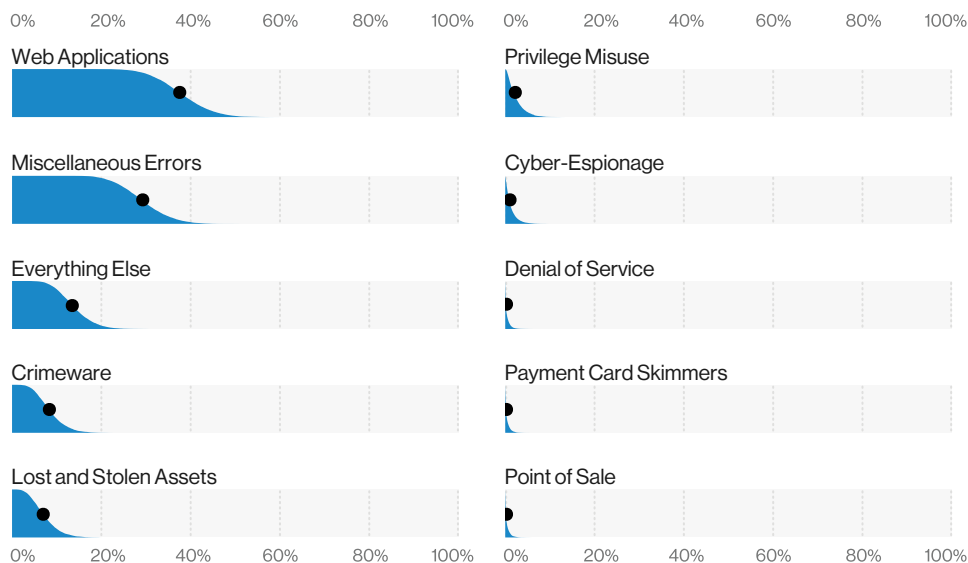
The same is true of Lost and Stolen Assets. These are unencrypted devices or they wouldn't be considered even at risk of a data breach. Unless, of course, the decryption key is also lost at the same time in human-readable format (before you jeer, keep in mind that we have actually seen this). The data on these devices is most likely protected only by a password, and is therefore considered at-risk in our dataset, and not a confirmed data breach.

## No Regrets<sup>42</sup>

In the red corner, Miscellaneous Errors is the most prominent pattern in this industry when looking at confirmed data breaches. Figure 93 shows us that Misdelivery remains a big problem for the public sector. This is when sensitive information goes to the wrong recipient. It may be via electronic means, such as emails that are misaddressed, or it may be old-fashioned paper documents. Those mass mailings (and nobody can hold a candle to the volume of paper sent out by government entities) where the envelopes and their contents become out of sync can be a serious problem.

In the blue corner, weighing in at 30% of breaches, we have Misconfiguration, the other contender for the top variety of Error. A Misconfiguration data breach is when someone (usually a system administrator or someone in another privileged technical role) spins up a datastore in the cloud without the security measures in place to protect the data from unauthorized access. There are security researchers out there who spend their time looking for just this kind of opportunity. If you build it, they will come.

Looking back at changes from last year to this, the top three patterns have altered composition quite a lot. The 2019 report showed the top three breach patterns as Cyber-Espionage, Miscellaneous Errors and Privilege Misuse. You can see the difference in the rankings in Figure 94. Both Cyber-Espionage and Privilege Misuse declined in our dataset overall this year, and have dropped into the single digit percentages in this sector.



**Figure 94.** Patterns in Public Administration breaches (n = 346)

<sup>42</sup> Well, except for these ugly tattoos we got on a dare last year.

# Real Estate and Rental and Leasing

NAICS  
53

## Summary

Web Applications attacks utilizing stolen credentials are rife in this vertical. Social engineering attacks in which adversaries insert themselves into the property transfer process and attempt to direct fund transfers to attacker-owned bank accounts are also prevalent. Like many other industries, Misconfigurations are impacting this sector.

Frequency	37 incidents, 33 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 88% of data breaches.
Threat Actors	External (73%), Internal (27%) (breaches)
Actor Motives	Financial (45%–97%), Convenience/Espionage (0%–40% each), Fear/Fun/Grudge/Ideology/Other/Secondary (0%–21% each) (breaches)
Data Compromised	Personal (83%), Internal (43%), Other (43%), Credentials (40%) (breaches)
Top Controls	Top Controls: Secure Configuration (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12)
Data Analysis Notes	Actor motives are represented by percentage ranges, as only eight breaches had a known motive. Some charts also do not have enough observations to have their expected value shown.

## SOLD!

There is nothing quite like that feeling of owning your first home. Moving in, enjoying the smell of fresh paint and reflecting on all the memories you'll make. Our data for this vertical indicates that cybercriminals are also being allowed to move right in and make themselves at home. Whether they are attending a showing of your data via Web Applications attacks, utilizing social engineering in the Everything Else pattern or simply being asked to drop in by your employees through an assortment of Miscellaneous Errors, they are certainly being made welcome. As you can see in Figure 95, it is difficult to state conclusively which of these three patterns is the statistical leader but we can assert that they are all in the running.

## Don't leave the key under the welcome mat.

Although we saw a rather small number of breaches in this sector over the last year, there are some interesting high-level findings to discuss. As in many other sectors, criminals have been actively leveraging stolen credentials to access users' inboxes and conduct nefarious activities. In fact, across all industries, credential theft is so ubiquitous that perhaps it would be more accurate to consider them time-shares rather than owned. Meanwhile, other external actors are relying on social engineering to get the job done. Some of these activities are simply aimed at stealing your data, but in other cases these attacks can be used to tee up a separate assault, as seen in many of the attacks that leverage pretexting.

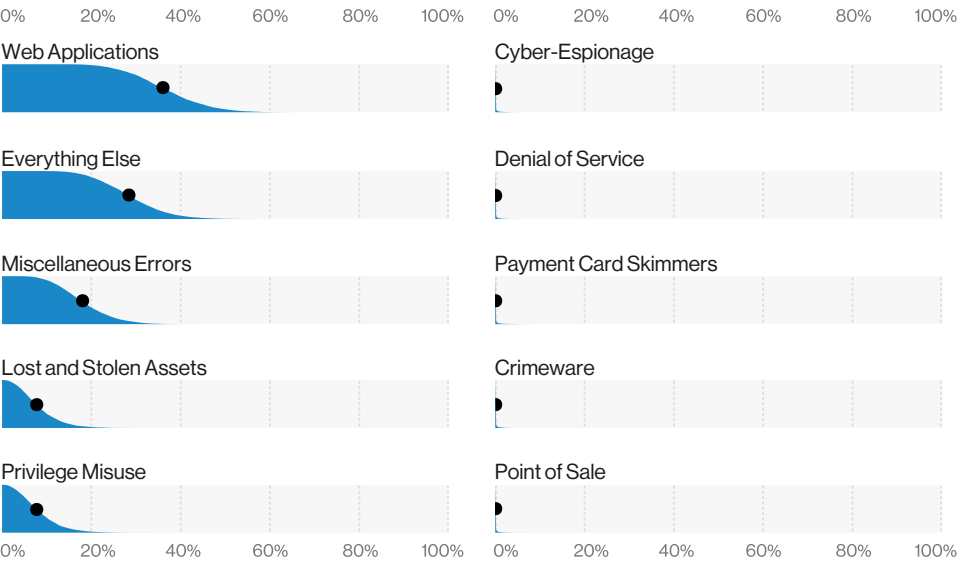
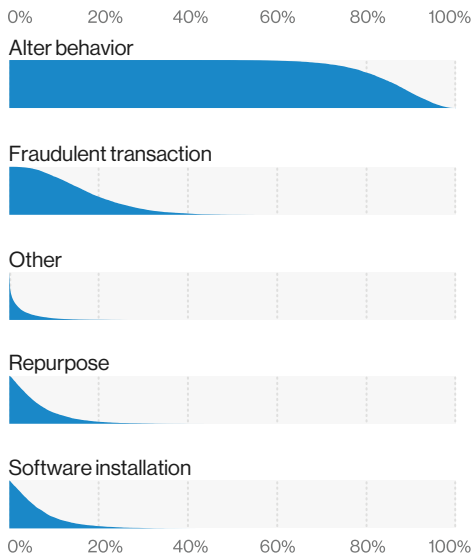


Figure 95. Patterns in Real Estate industry breaches (n = 33)



**Figure 96.** Top integrity impacts in Real Estate industry incidents (n = 16)



**Figure 97.** Top Error varieties in Real Estate industry incidents (n = 7)

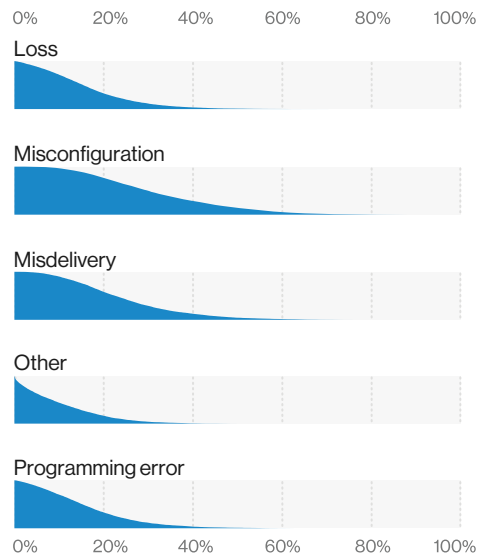


Figure 96 shows how Bad Guys<sup>TM43</sup> exploit the milk of human kindness to dupe well-meaning employees into assisting them to achieve their objectives. They use pretexts to alter someone's behavior in such a manner that the employee divulges sensitive information, or otherwise unwittingly helps them to commit fraud. One example of this type of social engineering is when the attacker inserts themselves into an email thread regarding the sale or purchase of a new home and convinces the victim organization to transfer funds to attacker-owned bank accounts. It's worthwhile to make a phone call to confirm details before making this type of significant transaction.

## You sent that to who?!

Even though this is the first time we have written an industry section for "Real Estate," we have been collecting data on this industry for a number of years. This enables us to analyze how the patterns have evolved over time in this vertical. This year, one of the more interesting findings was the continuity in volume of Errors. These Error-related breaches involve Misconfigurations (forgetting to turn those restrictive permissions on), Misdeliveries (email and/or paper documents sent to the incorrect recipient) and Programming errors (mistakes in code) as seen in Figure 97. These Error actions accounted for 18% of data breaches in the Real Estate vertical. If you do business in this industry, we urge you to take time for security awareness training and the implementation of sound policies and procedures.

43 Surely someone has trademarked this, right?



## Summary

**Attacks against e-commerce applications are by far the leading cause of breaches in this industry. As organizations continue to move their primary operations to the web, the criminals migrate along with them. Consequently, Point of Sale (PoS)-related breaches, which were for many years the dominant concern for this vertical, continue the low levels of 2019's DBIR. While Payment data is a commonly lost data type, Personal and Credentials also continue to be highly sought after in this sector.**

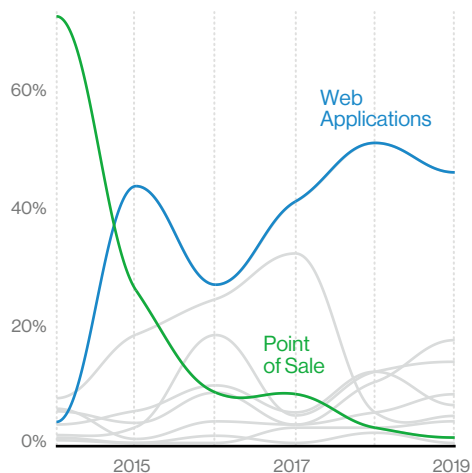
<b>Frequency</b>	287 incidents, 146 with confirmed data disclosure
<b>Top Patterns</b>	Web Applications, Everything Else and Miscellaneous Errors represent 72% of breaches.
<b>Threat Actors</b>	External (75%), Internal (25%), Partner (1%), Multiple (1%) (breaches)
<b>Actor Motives</b>	Financial (99%), Espionage (1%) (breaches)
<b>Data Compromised</b>	Personal (49%), Payment (47%), Credentials (27%), Other (25%) (breaches)
<b>Top Controls</b>	Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11), Continuous Vulnerability Management (CSC3)

## I'll buy that for \$1.

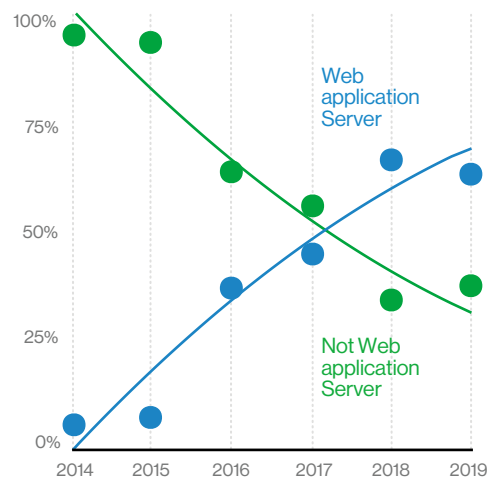
We are sure it comes as no surprise to anyone in this sector, but the Retail industry is a frequent target for financially motivated actors. Retail as an industry is almost exclusively financially motivated too, so it is only fair. This sector is targeted by criminal groups who are trying to gain access to the wealth of payment card data held by these organizations. Last year's trend of transitioning from card-present to card-not-present crime continued, which drove a similar decrease since 2016 in the use of RAM-scraper malware. Personal data figures prominently in Retail breaches and is more or less tied with Payment for the top data type compromised. Certainly, if the attacker cannot gain access to Payment data, but stumbles across Personal data that is lucrative for other types of financial fraud, they will not file a complaint.

## To the web with you!

Figure 98 provides us with a good view through the display case as it were in the "Retail" section. Over the last few years (2014 to 2019), attacks have made the swing away from Point of Sale devices and controllers, and toward Web Applications. This largely follows the trend in the industry of moving transactions primarily to a more web-focused infrastructure. Thus, as the infrastructure changes, the adversaries change along with it to take the easiest path to data.<sup>44</sup> Attacks against the latter have been gaining ground. In the 2019 DBIR, we stated that we anticipated Retail breaches were about to lose their majority to web-server-related breaches, and in Figure 99, we can see that has in fact occurred. Be sure to play the lucky lotto numbers printed on the back cover. Winner, winner! Chicken dinner!



**Figure 98.** Patterns over time in Retail industry breaches



**Figure 99.** Web application Server vs Not Web application Server assets in Retail Payment data breaches over time

<sup>44</sup> Of course, if you haven't made this transition, your PoS infrastructure remains at risk.

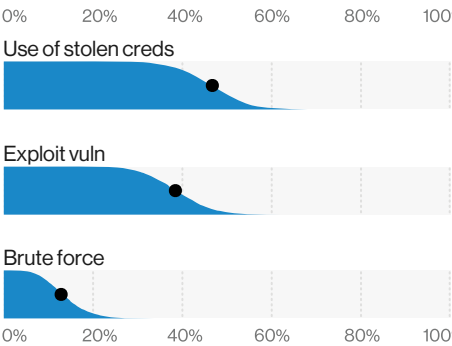
The Web Applications pattern is composed of two main action varieties: the use of stolen credentials and the exploitation of vulnerable web app infrastructure. Figure 100 shows that Exploit vuln and Use of stolen creds are close competitors for first place in the Hacking varieties category and there is not a great deal to distinguish between them from a percentage point of view. In a perfect world, someone else's data breach would not raise the risk to your own. However, that is increasingly not the case, with the adversaries amassing datastores of credentials from other people's misfortune and trying them out against new victims.

**You hold the key to my heart.**

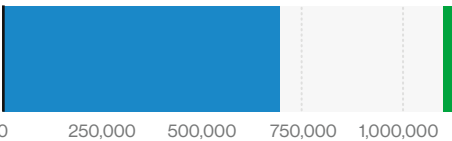
Our non-incident data tells us that in this vertical (Figure 101), credential stuffing is a significant problem. While it is slightly below the most common value for all industries this year, it is not likely that people who have so many keys (credentials) will stop trying them on whatever locks they can find.

When the bad actors are not using other people's keys against your infrastructure, they are using unpatched vulnerabilities in your web apps to gain access. Based on the vulnerability data in Figure 102, only about half of all vulnerabilities are getting patched within the first quarter after discovery. It is best not to put those patches on layaway but go ahead and handle them as soon as possible. We know from past research that those unpatched vulnerabilities tend to linger for quite a while if they aren't patched in a timely manner—people just never get around to addressing them. Our analysis found that SQL, PHP and local file injection are the most common attacks that are attempted in this industry (Figure 103).

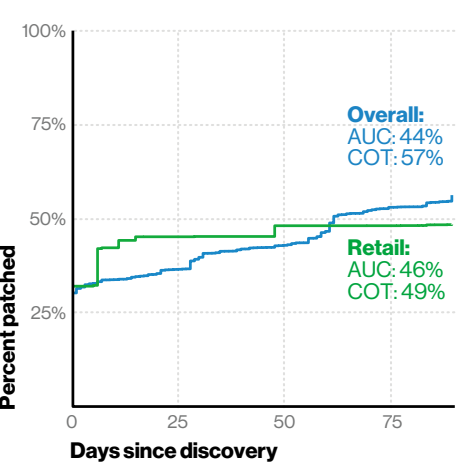
**Figure 100.** Top Hacking varieties in Retail industry breaches (n = 48)



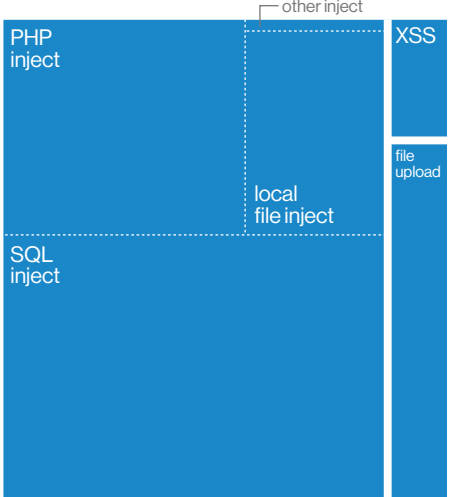
**Figure 101.** Credential stuffing attempts in Retail industry web blocks (n = 284); all industries mode (green line): 1.11M



**Figure 102.** Patching in Retail industry vulnerabilities (n = 35,098)



**Figure 103.** Varieties in Retail industry web application attack blocks (n = 2.22 billion)

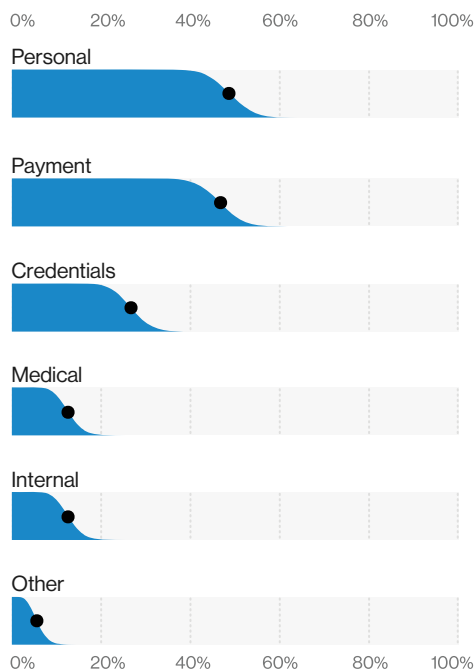


## Data types

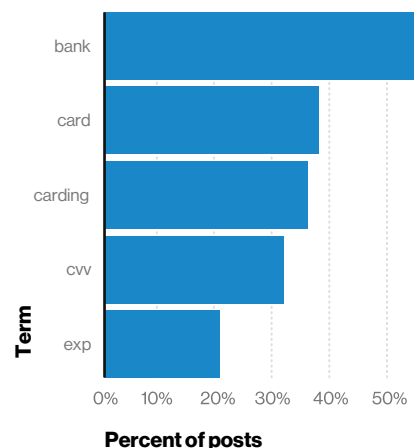
If we were to create a ranking of the most easily monetizable data types, surely Payment card data would be at the top. After all, who doesn't have the urge to try out that brand new credit card and "break it in" when it first arrives? Figure 104 shows us that the attackers feel the same way, and likely want to build upon their sweet gaming rig with someone else's money. However, Personal data is tied with Payment data as the reigning champion. It's easy to forget that as web apps increasingly become the target of choice, the victims' Personal data is sometimes boxed up and shipped off right along with the Payment data as a *lagniappe*.

Figure 105 lists the top terms in hacking data from criminal forum and marketplace posts. It stands to reason that they would (like any good SEO effort) tailor their terms to what is most in demand. Clearly banking and payment card data is high on everybody's wish list, although those who are doing this type of trade do not need to go to the lengths of finding a dusty lamp to have those wishes granted.

**Figure 104.** Top data varieties in Retail industry breaches (n = 135)



**Figure 105.** Top terms in hacking-related criminal forum posts (n = 3.35 million)



# Transportation and Warehousing

NAICS  
48-49

## Summary

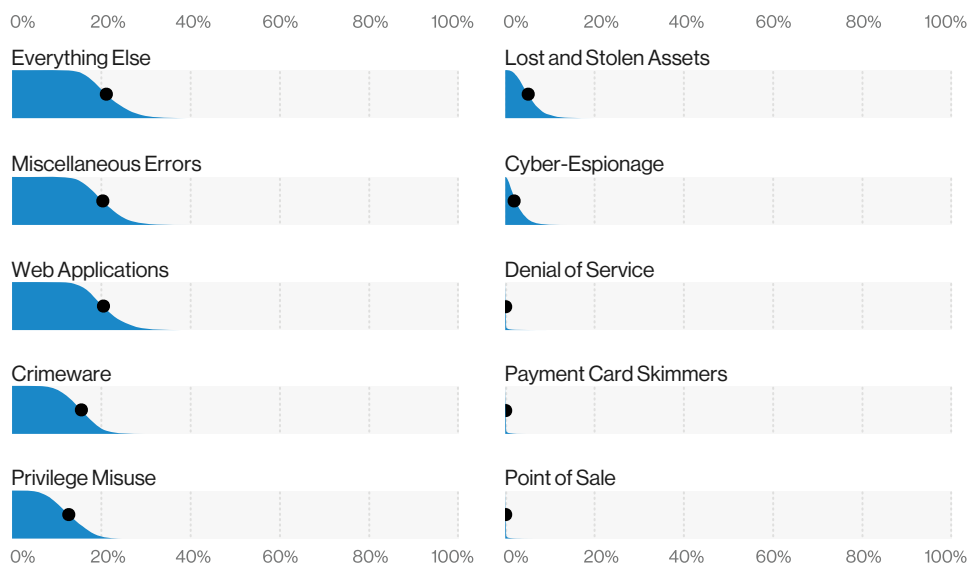
Financially motivated organized criminals utilizing attacks against web applications have their sights set on this industry. But employee errors such as standing up large databases without controls are also a recurring problem. These, combined with social engineering in the forms of phishing and pretexting attacks, are responsible for the majority of breaches in this industry.

<b>Frequency</b>	112 incidents, 67 with confirmed data disclosure
<b>Top Patterns</b>	Everything Else, Web Applications and Miscellaneous Errors represent 69% of breaches.
<b>Threat Actors</b>	External (68%), Internal (32%) (breaches)
<b>Actor Motives</b>	Financial (74%–98%), Espionage (1%–21%), Convenience (0%–15%) (breaches)
<b>Data Compromised</b>	Personal (64%), Credentials (34%), Other (23%) (breaches)
<b>Top Controls</b>	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Secure Configurations (CSC 5, CSC 11)
<b>Data Analysis Notes</b>	Actor motives are represented by percentage ranges, as only 26 breaches had a known motive. Some charts also do not have enough observations to have their expected value shown.

The Transportation and Warehousing industry is a new one for our report. If you're reading this report for the first time for just this reason, pull up a chair, we're glad to have you! As you know, this industry is all about getting people and goods from point A to point B, and about storing those goods until they're needed. Once transported, the people are usually good enough to find their own places to stay, but that's another industry entirely.

## All roads lead to pwnd.

What is causing breaches in this sector? Our data shows us that Web Applications attacks and Miscellaneous Errors are quite common, and the Everything Else pattern is also prevalent, but more on that later (Figure 106). Web applications are a common attack across the dataset, and a fact of life in this era is that if you have an internet-facing application, someone out there will eventually get around to testing your controls for you. The Hacking, Social and Malware actions were the most common in this industry, which supports the Web Applications pattern's prominence.



**Figure 106.** Patterns in Transportation industry breaches (n = 67)

Keep your eyes on the road.

Miscellaneous Errors are simply a byproduct of being human—we make mistakes. The most common error in this industry was Misconfiguration, as shown in Figure 107. A typical misconfiguration error scenario is this: An internal actor (frequently a system admin or DBA) stands up a database on a cloud service without any of those inconvenient access controls one would expect to see on sensitive data. Then, an enterprising security researcher finds this instance using a search engine that is made to spot these unprotected datastores and poof, you have a breach.

That Everything Else pattern mentioned earlier—it is a place we store odds and ends for attacks that don't fit into the other attack patterns, and within this pattern lives the business email compromise (BEC). These usually come in as a phishing email, although they can also be done over the phone. The goal of the attacker is either to get data or facilitate a wire transfer to their conveniently provided bank account. These attacks are perpetrated largely by organized criminal actors with a financial motive.

You can see in Figure 108 the most common motive of the external actors in this sector. While there are some espionage-motivated actors, they are few and far between when compared to financially motivated attackers. The data type of choice in this vertical appears to be Personal, which is being closely tailgated by Credentials.

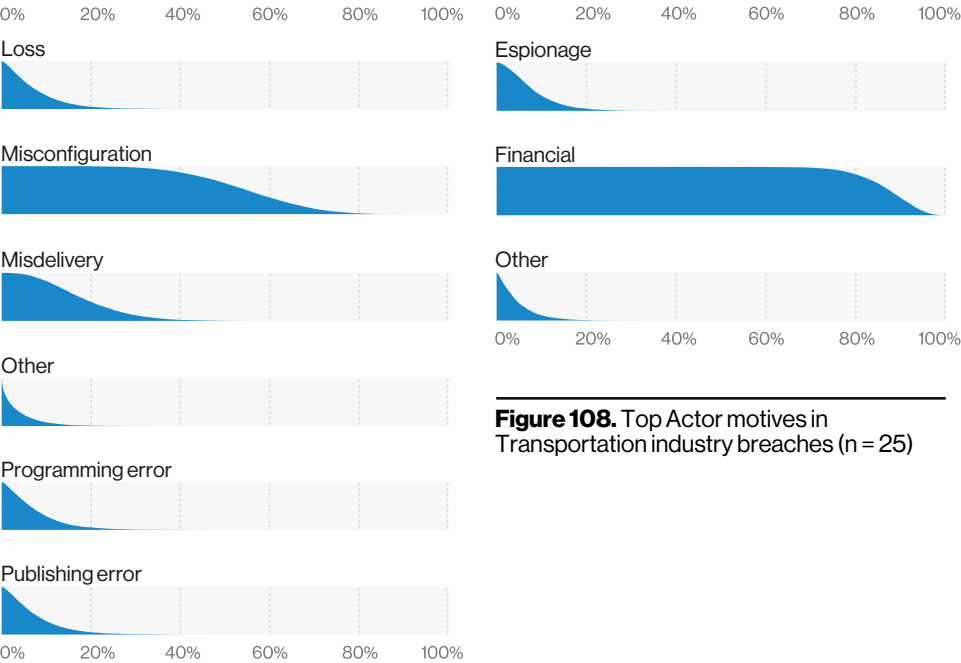


Figure 107. Top Error varieties in Transportation industry breaches (n = 15)

# 04



---

## Does size matter? A deep dive into SMB breaches

# Does size matter?

## A deep dive into SMB breaches

### Summary

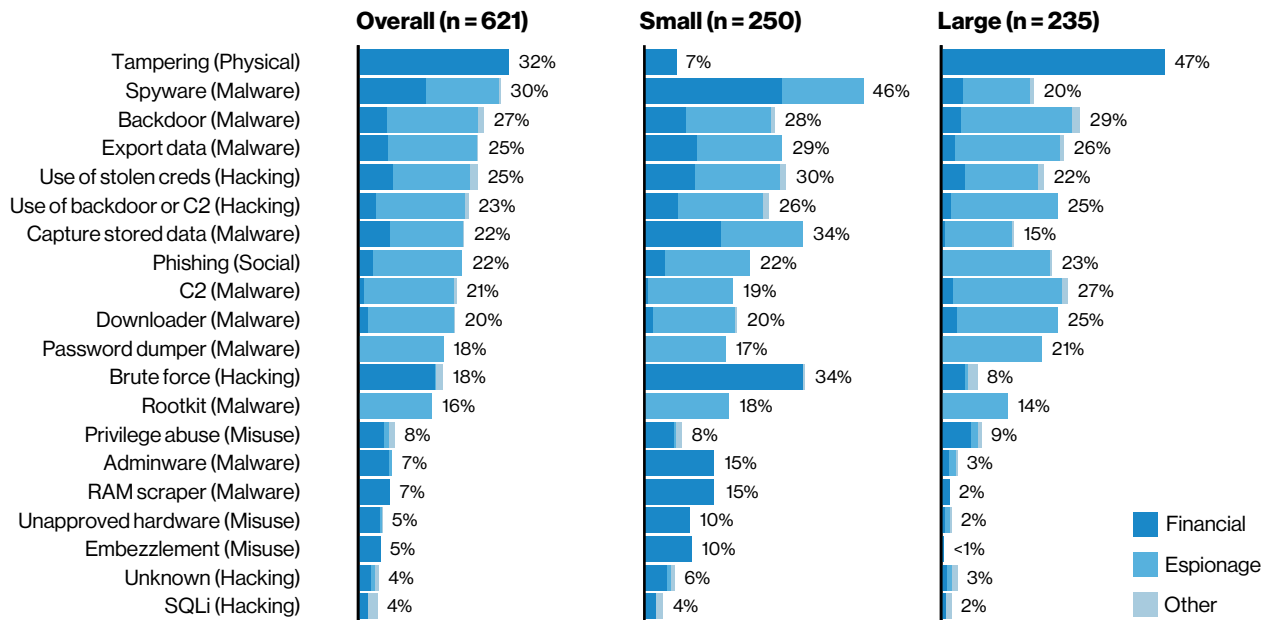
**While differences between small and medium-sized businesses (SMBs) and large organizations remain, the movement toward the cloud and its myriad web-based tools, along with the continued rise of social attacks, has narrowed the dividing line between the two. As SMBs have adjusted their business models, the criminals have adapted their actions in order to keep in step and select the quickest and easiest path to their victims.**

Frequency	Small (less than 1,000 employees) 407 incidents, 221 with confirmed data disclosure	Large (more than 1,000 employees) 8,666 incidents, 576 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 70% of breaches.	Everything Else, Crimeware and Privilege Misuse represent 70% of breaches.
Threat Actors	External (74%), Internal (26%), Partner (1%), Multiple (1%) (breaches)	External (79%), Internal (21%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (83%), Espionage (8%), Fun (3%), Grudge (3%) (breaches)	Financial (79%), Espionage (14%), Fun (2%), Grudge (2%) (breaches)
Data Compromised	Credentials (52%), Personal (30%), Other (20%), Internal (14%), Medical (14%) (breaches)	Credentials (64%), Other (26%), Personal (19%), Internal (12%) (breaches)

### A trip down memory lane

Several years ago (the 2013 edition of the report to be precise), we took a look at some of the differences and similarities between small businesses (under 1,000 employees) and large businesses (1,000+ employees). Since a lot can change in seven years, we thought we would once again compare and contrast the two and see what story the data tells us. After all, now more than ever due to the proliferation of services available as commodities in the cloud, including platform as a service (PaaS), software as a service (SaaS) and any other \*aaS of which you can conceive, a small business can behave more like a large one than ever before. Therefore, we asked ourselves the question, “Have the differences in capabilities evened the playing field out a bit between the two with regard to the detection of and response to security incidents?” Since you’re reading this section, you’ve probably already guessed that the answer is “Yes!” Let’s dive in and examine how much has changed, and in what ways the song remains the same.

The first thing we noticed when populating the Summary table is the wide chasm between the two when it comes to numbers of incidents and breaches. Breaches are more than twice as common in the larger companies than in the small ones. Does this mean the small organizations are flying under the radar, or are they simply not aware they’ve received visitors of the uninvited variety? And the inequality between the two when it comes to number of incidents is staggering. Is it an obvious case of “mo’ money, mo’ problems” for large



**Figure 109.** Top 20 threat actions (referencing the 2013 DBIR)

enterprises? Is it due to increased visibility or perhaps a much wider attack surface? We find ourselves in the same position that some professional sports referees have been in recently as we realize it's hard (maybe more so in the Big Easy) to make the right call.

We call out the beginning attack patterns in the table at the beginning of this section, but the pattern concept wasn't born yet the last time we focused on organization size. In looking back, we can tell you there have been some changes in the most frequent causes (or as we like to call them in VERIS, action varieties) since 2013. The top 20 threat actions figure from the 2013 DBIR (Figure 109) lists the top 20 threat action varieties of the year, broken out into small and large organizations.

You can see that for large organizations, the top action was Physical tampering (wait, what?). For small organizations, in contrast, it was Spyware, although Brute-force hacking

and Capturing stored data was not far behind. Skipping ahead seven years to our current dataset, we see that both large (Figure 110) and small (Figure 111) organizations have a top threat action of Phishing, with the Use of stolen credentials and Password dumpers in the top three for both (only in reverse order). Regardless, the same three contestants are leading the pack in both and that is an interesting finding. Phishing was considerably further down the list in 2013, as compared to the prime position it holds now.

### Give me your keys and your wallet.

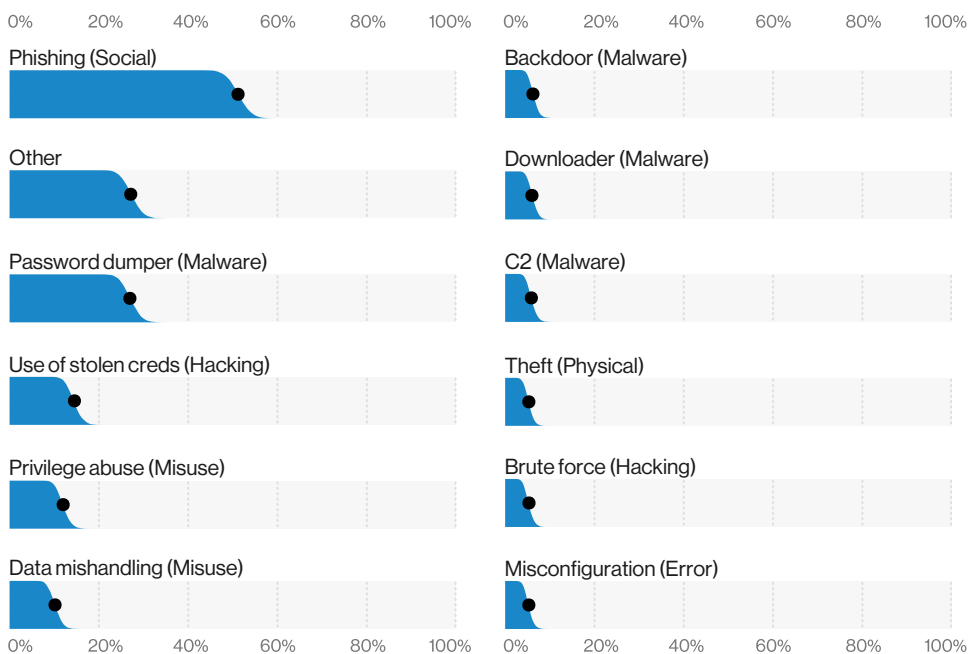
In 2013, far and away the favorite data type to steal was Payment card information. Back in those days, criminals would walk a long way (barefoot, in the snow, uphill both ways) to obtain this type of data (and they were thankful for the opportunity!). Following that, Credentials were a fan favorite, and Internal and

Secret data were also very much in vogue. Examining the types of data stolen today, in both small and large organizations, we see that Payment card data is so last year. Today's criminal (lacking the work ethic of 2013) is primarily concerned with obtaining Credentials, regardless of the target victims' size. Personal data also seems to be highly sought after, irrespective of the size of an organization. After those two heavy hitters, it becomes too close to call between Medical, Internal or Payment data.

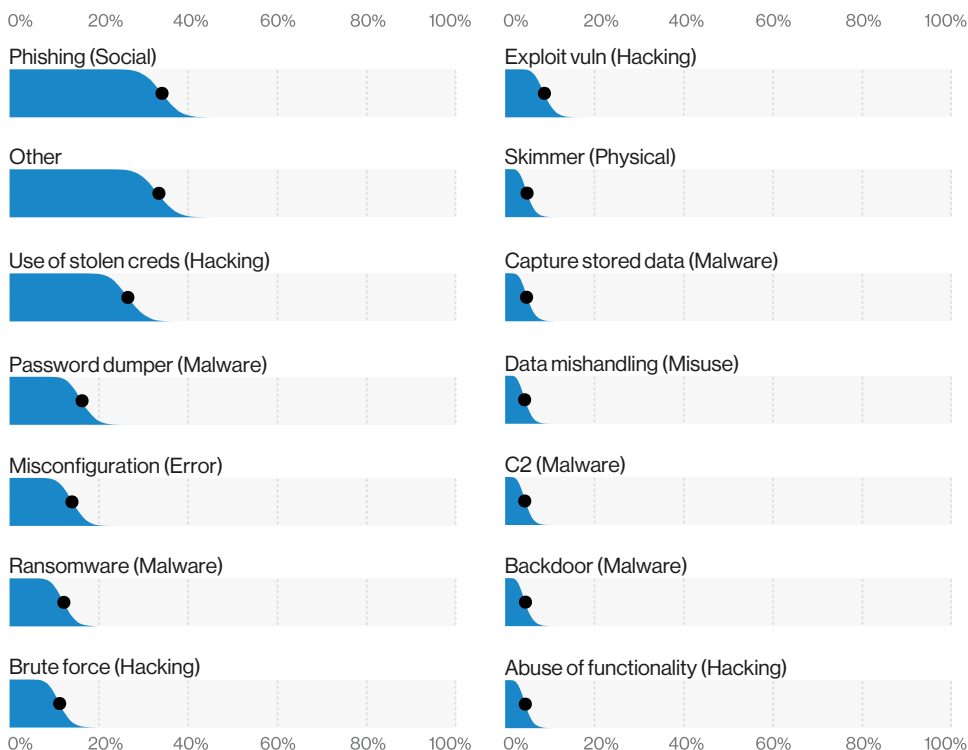
Another change from 2013 is the types of assets commonly attacked (Figure 112). The top asset for large companies (47%) was an ATM, while Point of Sale (PoS) controllers (34%) (followed closely at 29% by the Point of Sale terminal) were the top assets for small organizations. All of those assets have now fallen entirely off the list for both org types. Nowadays, organizations regardless of size are troubled with attacks on User devices, Mail servers and People (social attacks).



**Figure 110.** Top action varieties in large organization breaches (n = 448)



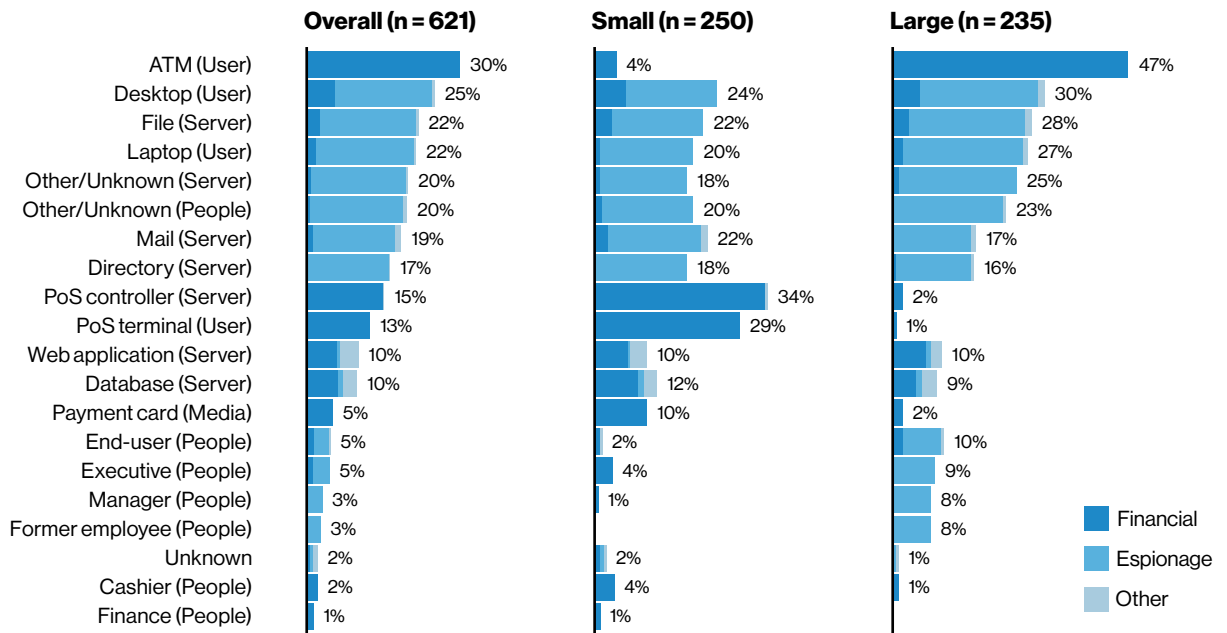
**Figure 111.** Top action varieties in small organization breaches (n = 194)



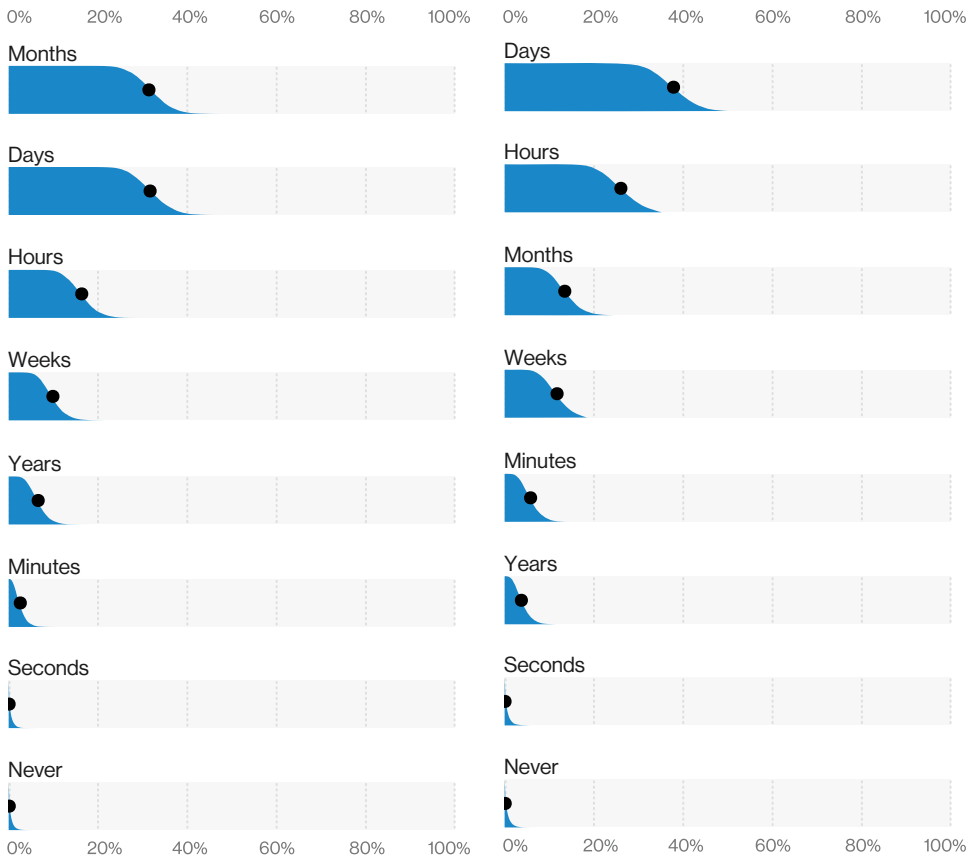
## No time like the present

Moving on to the differences in the dataset for this year alone (otherwise we can't talk about patterns), the top attack patterns for small organizations were Web Applications, Everything Else and Miscellaneous Errors, with none of them emerging as the obvious winner. Meanwhile, large organizations are contending with Everything Else, Crimeware and Privilege Misuse as their main issues. Web Applications attacks are self-explanatory, while the Everything Else pattern is a pantechicon stuffed with bits and bobs that do not fit anywhere else. Packed away in here you will find attacks such as the business email compromise—a social attack in the form of phishing, purporting to be from a company executive who is requesting data or a wire transfer. Miscellaneous Errors is a wide-ranging pattern that encompasses the many means (and they are legion) by which someone you employ can hurt your organization without malicious intent. The Crimeware pattern is your garden-variety malware and tends to be deployed by criminals who are financially motivated. Finally, Privilege Misuse is an act (usually malicious in nature) in which an Internal actor can ruin both your day and your brand.

When examining Timeline data, we noticed that the number of breaches that take months or years to discover is greater in large organizations (Figure 113) than in small organizations (Figure 114). This seems a bit counterintuitive. On the one hand, large organizations have a much larger footprint and could possibly be more likely to miss an intrusion on an internet-facing asset that they forgot they owned, but small orgs have a reduced attack surface so it might be easier to spot a problem. On the other hand, large orgs typically have dedicated security staff and are able to afford greater security measures, whereas small businesses often do not. Whatever the reason, there is a rather marked disparity between them with regard to Discovery.

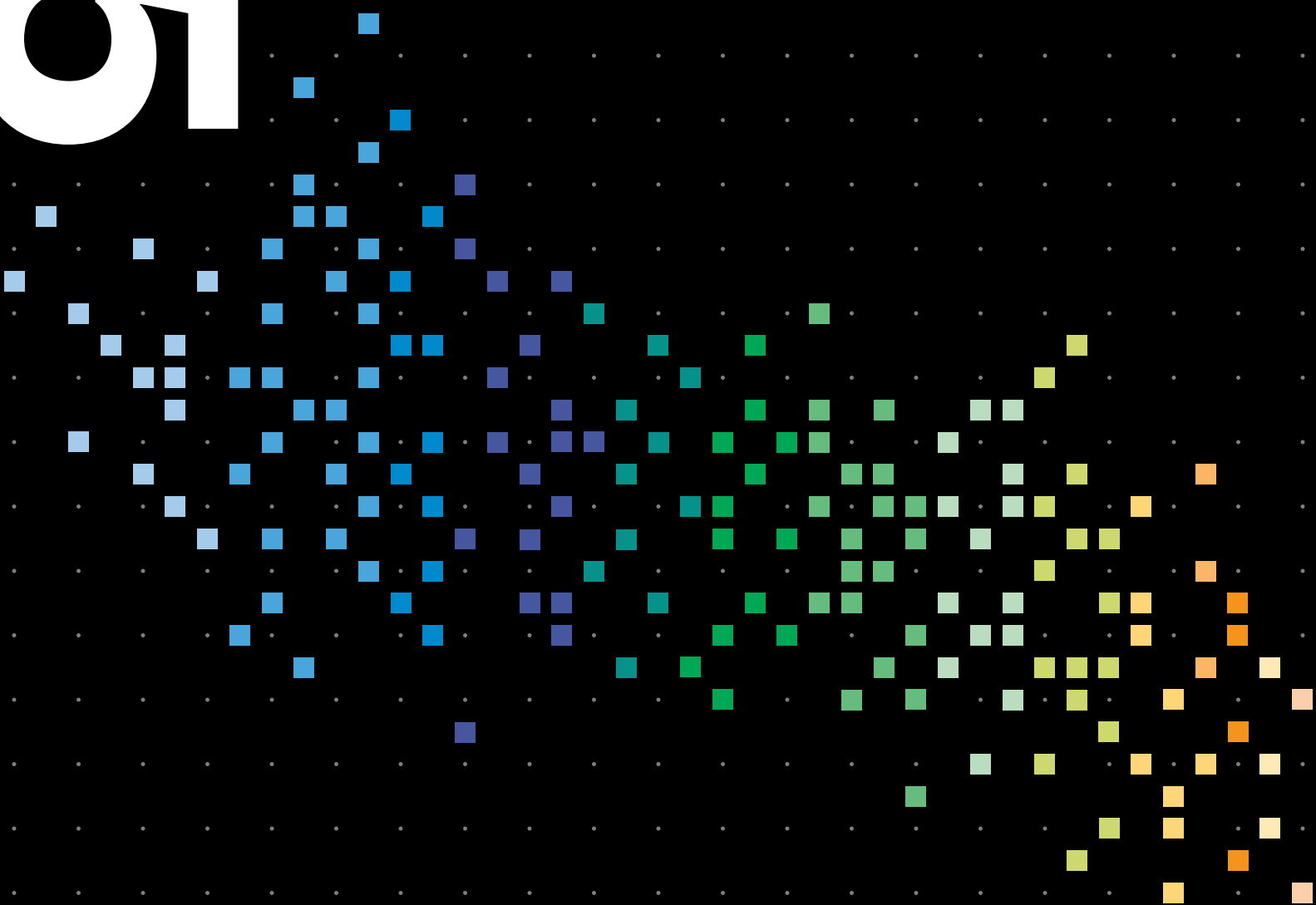
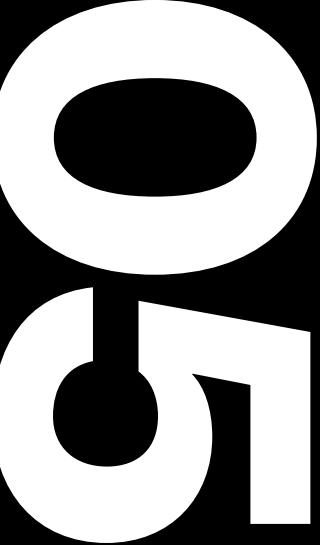


**Figure 112.** Varieties of compromised assets (referencing the 2013 DBIR)



**Figure 113.** Discovery time in large organization breaches (n = 121)

**Figure 114.** Discovery time in small organization breaches (n = 102)



---

**Regional  
analysis**

# Introduction to regions

Incidents	Total	Small (1–1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	32,002	407	8,666	22,929	Total	3,950	221	576	3,153
APAC	4,055	27	33	3,995	APAC	560	22	24	514
EMEA	4,209	57	88	4,064	EMEA	185	41	53	91
LAC	87	14	10	63	LAC	14	5	5	4
NA	18,648	231	6,409	12,008	NA	920	130	209	581
Unknown	5,003	78	2,126	2,799	Unknown	2,271	23	285	1,963
Total	32,002	407	8,666	22,929	Total	3,950	221	576	3,153

**Table 2.** Number of security incidents by victim Region and organization size

**We present for the first time a focused analysis on macro-regions of the world, thanks to the diligent work of the team this year to increase the diversity of our data contributors and the more precise statistical machinery we have put in place.**

After the filtering and subset creation described in the “Introduction to industries” section, we are left with a similar result on Table 2. We define regions of the world in accordance with the United Nations M49<sup>45</sup> standard, joining the respective super-region and subregion of a country together. By combining them even further, the subjects of our global focus are:

- **APAC** – Asia and the Pacific, including Southern Asia (034), South-eastern Asia (035), Central Asia (143), Eastern Asia (030) and Oceania (009)
- **EMEA** – Europe, Middle East and Africa, including Africa (002), Europe including Northern Asia (150) and Western Asia (145)
- **LAC** – Latin America and the Caribbean (419), also including for

redundancy due to potential different encodings South America (005), Central America (013) and Caribbean (029)

- **NA** – Northern America (021), mainly consisting of breaches in the U.S. and Canada, as well as Bermuda, which has also been busy lately for some reason

As the table clearly shows, we have better coverage in some regions than in others. However, we did not want to leave anyone out of our around-the-world tour, and this is where a lot of our estimative language and percentage ranges will come in handy.

This is also a great opportunity for us to ask for our readers to help us by sharing your data so we have more data breaches to report on. Please don't take this as an invitation to create data breaches by either malicious intent or by accident! However, by suggesting new potential data contributors from the regions where you, our readers, would like more detailed analysis, and by encouraging organizations in those areas to contribute data to the report, we can continue expanding our coverage and providing better analysis each new year.

The same caution with small sample numbers we discussed in the “Introduction to industries” section applies to Figure 115 – some of them are so small that you can easily step on them like the Lego pieces your kid leaves lying around. Believe us when we tell you that a biased statement that does not take into consideration the small sample size (n value) is just as painful. Be on the lookout for “Data Analysis Notes” in the “Latin America and the Caribbean” section where we will be calling out those “small samples” and check out the “Methodology” section for more information on the statistical confidence background used throughout this report.

**Please note: Based on feedback from our readers, we know that while some study the report from cover to cover, others only skip to the section or region that is of direct interest to them. Therefore, you may notice that we repeat some of our definitions and explanations several times, since the reader who only looks at a given section won't know the definition or explanation that we might have already mentioned elsewhere. Please overlook this necessary (but possibly distracting) element.**

<sup>45</sup> [https://en.wikipedia.org/wiki/UN\\_M49](https://en.wikipedia.org/wiki/UN_M49)

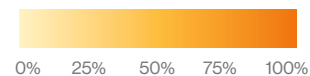
## Breaches

18	8	2	74
30	26	1	19
162	35	2	305
2	1		35
86	21	4	165
			15
			5
8	11	2	122
255	88	4	189
87	22	4	184
423	133	8	363
56	38	5	165
8	11	2	122
2	2	1	36
45	40	4	340
			1
2			22
4	7		71
	1	1	17
45	40	4	408
326	137	11	563
36	32	4	289
APAC	EMEA	LAC	NA

## Incidents

1,170	136	13	4,638
30	29	2	22
743	1,293	54	11,279
798	2,602	6	504
5	6		1,601
86	22	4	171
			17
1	2		7
9	12	3	194
1,214	113	6	228
89	26	4	1,717
2,586	2,585	68	12,257
1,215	1,306	20	4,768
9	12	3	194
3	4	1	80
685	1,483	8	445
			1
2			27
4	10		117
1	1	2	25
688	1,483	8	514
2,610	2,598	75	12,066
228	71	9	2,215
APAC	EMEA	LAC	NA

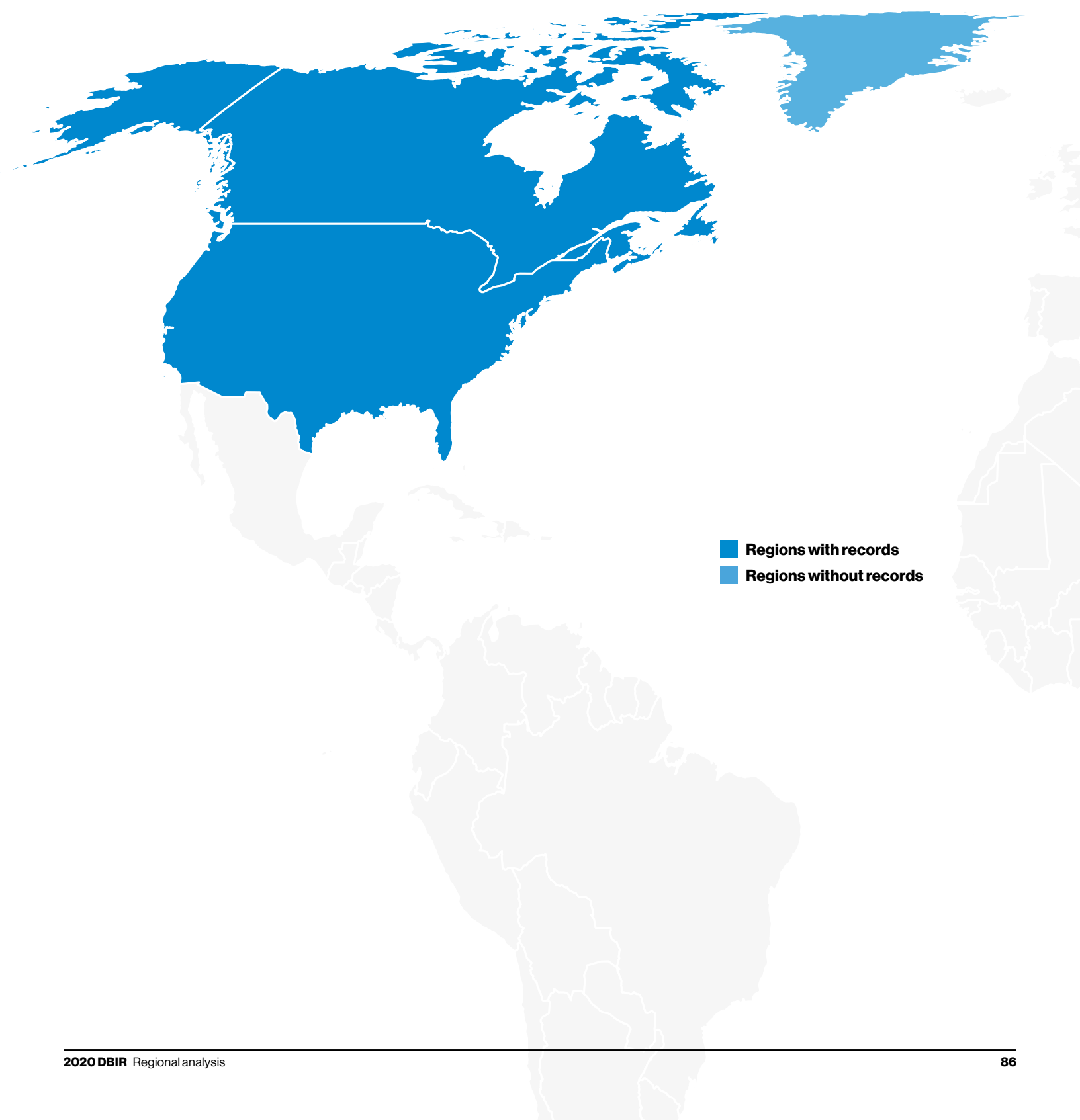
Crimeware	Pattern
Cyber-Espionage	
Denial of Service	
Everything Else	
Lost and Stolen Assets	
Miscellaneous Errors	
Payment Card Skimmers	
Point of Sale	
Privilege Misuse	
Web Applications	
Environmental	Action
Error	
Hacking	
Malware	
Misuse	
Physical	
Social	
Embedded	Asset
Kiosk/Term	
Media	
Network	
Person	
Server	
User Dev	



**Figure 115.** Breaches and incidents by region

# Northern America (NA)

**Figure 116.** Northern America (NA) region



The region designated as Northern America consists of the United States and Canada, as well as some outlying islands such as Bermuda.

There are a couple of factors that need to be kept in mind when looking at the findings below. First of all, this region accounts for 69% of all incidents and 55% of all breaches in our dataset this year. That does not mean that good security practice has disappeared into the Bermuda Triangle, though. Northern America has arguably some of the most robust data reporting standards<sup>46</sup> in existence, particularly in Healthcare and Public administration. Therefore, the number of incidents and breaches are likely to be higher than in areas with less stringent disclosure requirements. Also, it must be admitted that while this report is becomingly increasingly global in scope, many of our contributors are located in and are primarily concerned with Northern American organizations. As a result of these factors, outcomes for this region are not too dissimilar from the findings for the overall dataset. Nevertheless, there are a few interesting differences and highlights worthy of discussion.

Phish and whistle, whistle and phish<sup>47</sup>

Everything Else is the top pattern for this region (Figure 117). That is due in large part to the number of financially motivated phishing attacks that we see across so many industries (Figure 118). In the past, we have observed that security awareness training can help limit the frequency and/or impact of phishing attacks. However, in some instances, this training appears to be either not carried out at all or delivered in an insufficient or inadequate manner. Whatever the reason, telling employees not to click phishing emails can be as effective as yelling “ear muffs” when you don’t want your child to hear something unpleasant.

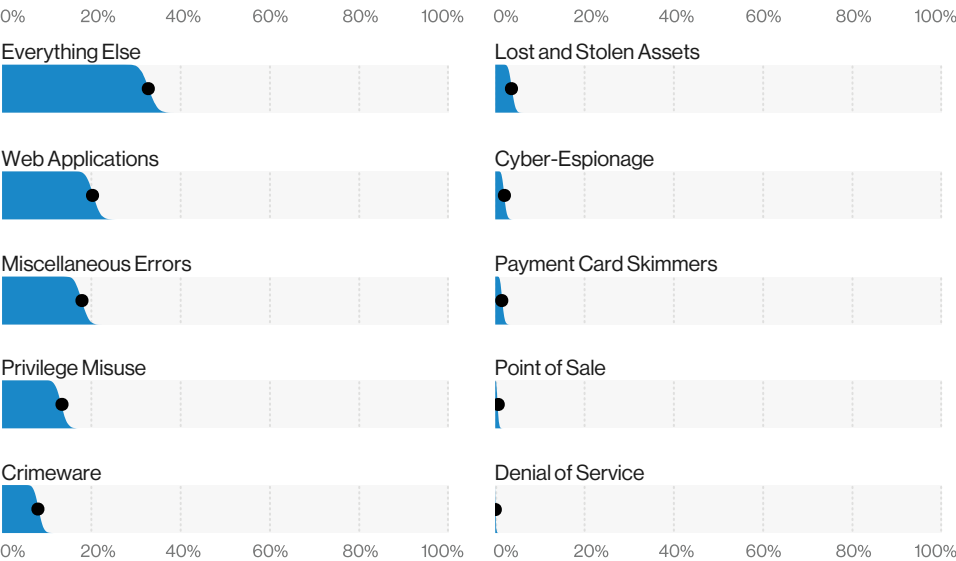


Figure 117. Patterns in Northern American breaches (n = 920)

Summary

Northern American organizations suffered greatly from financially motivated attacks against their web application infrastructure this year. Hacking via the Use of stolen credentials was most commonly seen, with social engineering attacks that encourage the sharing of those credentials following suit. Employee error was also routinely observed in our dataset.

Frequency	18,648 incidents, 920 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Miscellaneous Errors represent 72% of all data breaches in Northern America.
Threat Actors	External (66%), Internal (31%) Partner (5%), Multiple (1%) (breaches)
Actor Motives	Financial (91%), Espionage (5%), Grudge (3%) (breaches)
Data Compromised	Personal (43%), Credentials (43%), Other (35%), Internal (21%) (breaches)

46 This is largely due to the robust data breach notification laws passed over the years, such as California S.B. 1386 passed in 2002, which served as a blueprint for other states in the U.S. and has now been augmented by the California Consumer Privacy Act (CCPA) in the Golden State.

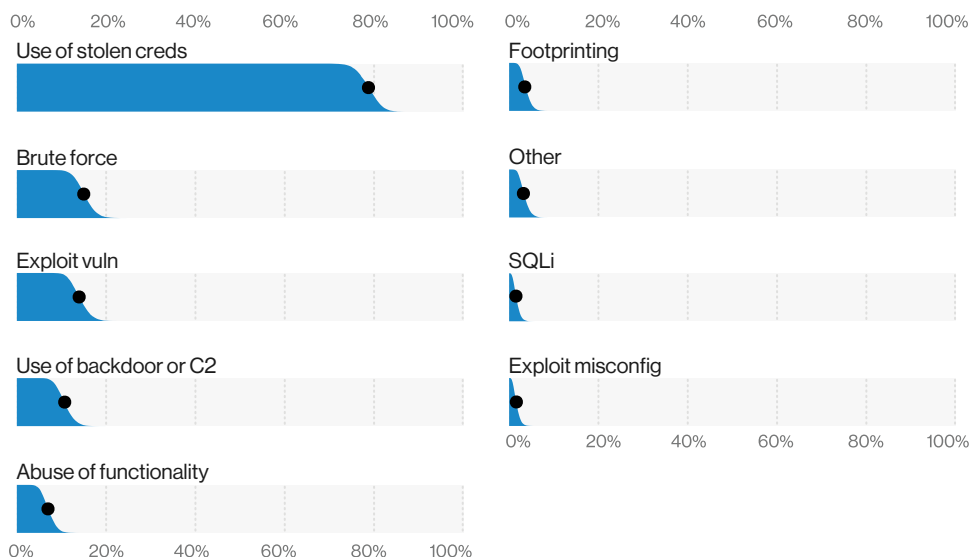
47 We hope you will allow us a paraphrase of the words of the great John Prine. He will be sorely missed.

**Figure 118.** Social varieties in Northern American breaches (n = 322)

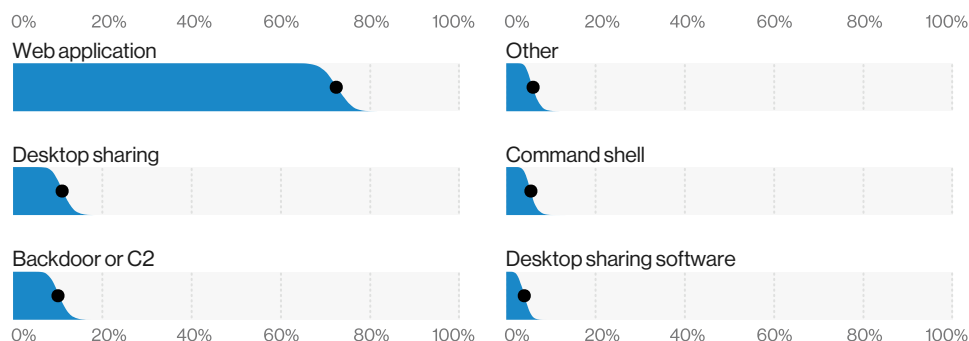


## Get your head out of your ... cloud.

Web app attacks also loom large in Northern America. The majority of these attacks are carried out via the Use of stolen credentials (Figure 119), which are then used to hack into web-based email and other web applications utilized by the enterprise (Figure 120). We have mentioned in past reports that, with the growing trend of businesses moving toward cloud-based solutions, we could expect the Use of stolen credentials to increase proportionally. This does seem to be the case.



**Figure 119.** Top Hacking varieties in Northern American breaches (n = 268)



**Figure 120.** Top Hacking vectors in Northern American breaches (n = 260)

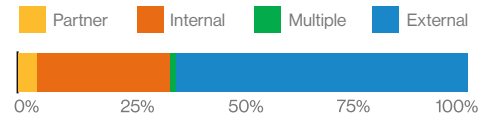


## See! This is why we can't have anything nice.

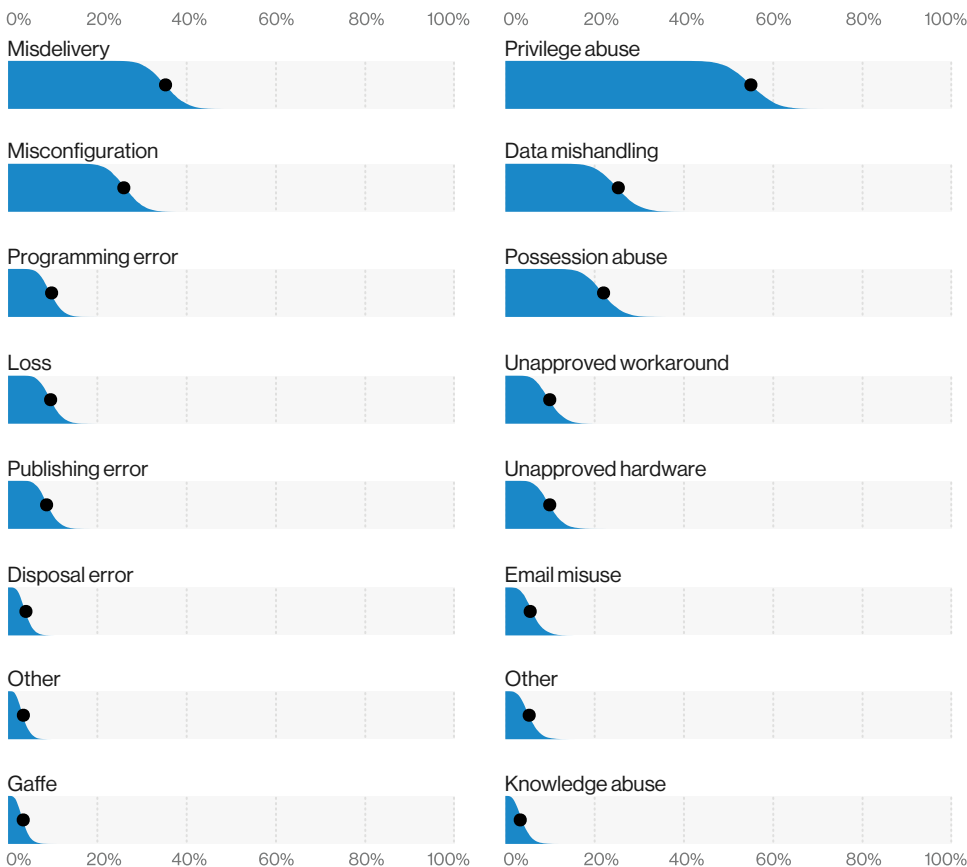
You don't need External actors to harm your organization as long as your employees are willing to do their work for them. The number of Internal actors is somewhat high (30%) this year for this region and for the dataset as a whole (Figure 121). This is explained by the prevalence of Error and Privilege Misuse actions. Both are caused by Internal actors and both can be very damaging to an organization, but while Error is unintentional, Misuse can be (and often is) malicious in nature.

Let's take a quick look at the Error actions. As you can see in Figure 122, the vast majority of all error-related breaches are caused by Misdelivery (sending data to the incorrect recipient) and Misconfiguration (i.e, forgetting to secure to a storage bucket). For whatever reason, these Error types seem to be the peanut-butter-and-jelly sandwich of the breach world this year. Perhaps Internal actors are simply too busy trying to perfect their Renegade dance on TikTok these days; we do not know for sure. Whatever the reason, these errors are found in every industry and region, and in alarmingly large percentages. As mentioned elsewhere in this report, the vector for these errors is almost entirely carelessness on the part of the employee.

Turning our attention to Misuse, we see a proliferation of Privilege abuse (56%). This is using legitimate access for an illegitimate purpose. Somewhat farther down the ladder, we see approximately equal percentages of Data mishandling and Possession abuse (Figure 123). No matter how you view it, this region would benefit from increased controls for Internal actors.



**Figure 121.** Actors in Northern American breaches (n = 908)

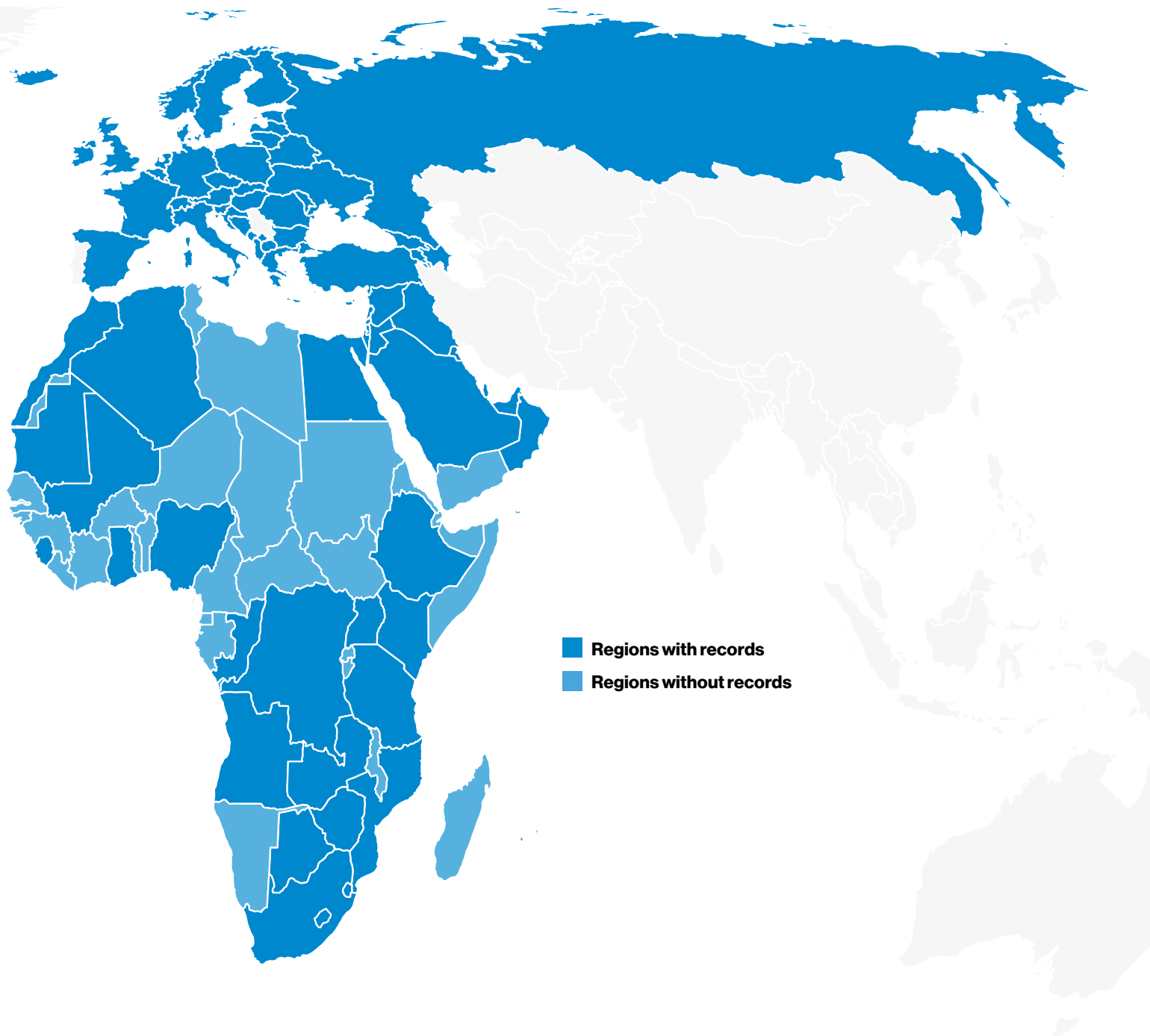


**Figure 122.** Top Error varieties in Northern American breaches (n = 166)

**Figure 123.** Top Misuse varieties in Northern American breaches (n = 121)

# Europe, Middle East and Africa (EMEA)

**Figure 124.** Europe, Middle East and Africa (EMEA) region



As our world has become increasingly smaller over the years, it seems that the scope of our report has done the opposite.

In that spirit of growth and exploration, we will examine data from Europe, the Middle East and Africa (EMEA) in this section. While some readers may consider it “over there,” the types of attacks and cybersecurity incidents experienced by those in EMEA are quite similar to what we observe elsewhere. In this region, Web Applications, Everything Else and Cyber-Espionage are the top patterns associated with the 185 breaches that we tracked this year (Figure 125).

The Web Applications pattern encompasses two major attacks that greatly affect this region. The first is Hacking via the Use of stolen credentials, which accounts for approximately 42% of data breaches. This scenario usually plays out in the following manner: An attacker uses credentials, typically gathered either through phishing or malware, to access a web application platform owned by the organization and commit wickedness of one type or another. This year, we’ve seen adversaries target assets such as outward-facing email servers, but also other platforms such as business-related applications. The second type of attack associated with this pattern is the use of exploits against web-facing applications to either gain access to the system data itself, or to repurpose the server for something more nefarious. These attacks account for close to 20% of our breaches in EMEA this year. If you haven’t checked your external-facing websites recently for unpatched vulnerabilities or missing multifactor logins, you might want to get on that.

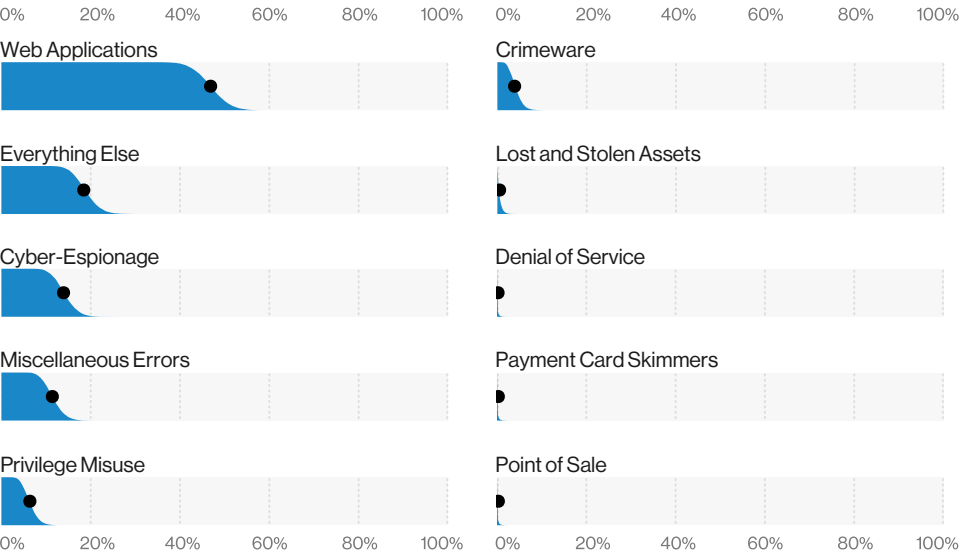
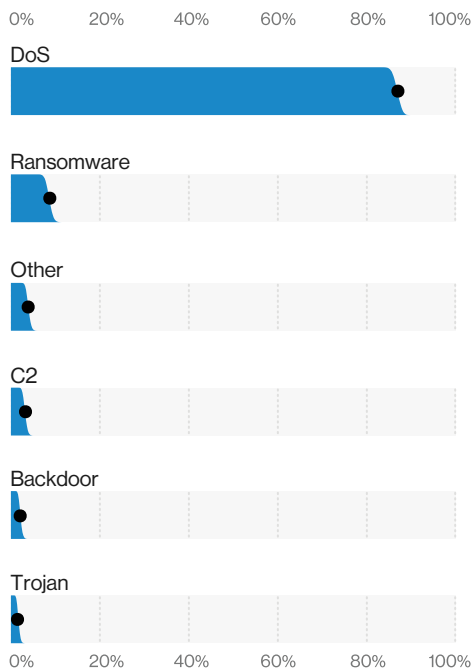


Figure 125. Patterns in EMEA breaches (n = 185)

Summary

Attackers are targeting web applications in EMEA with a combination of hacking techniques that leverage either stolen credentials or known vulnerabilities. Cyber-Espionage attacks leveraging these tactics were common in this region. Denial of Service attacks continue to cause availability impacts on infrastructure as well.

Frequency	4,209 incidents, 185 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Cyber-Espionage represent 78% of data breaches in EMEA.
Threat Actors	External (87%), Internal (13%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (70%), Espionage (22%), Ideology (3%), Fun (3%), Grudge (3%), Convenience (1%) (breaches)
Data Compromised	Credentials (56%), Internal (44%), Other (28%), Personal (20%) (breaches)



**Figure 126.** Top Malware varieties in EMEA incidents (n = 1,298)

The next pattern, Everything Else, is a catch-all category for breaches and incidents that do not readily fit into one of the other patterns. In this instance, it mostly consists of typical business email compromises (BEC) and represents 19% of the data breaches within this region. In this type of incident, fraudsters will mimic a business partner, client, executive, etc., in order to get an organization to transfer a payment over to an attacker-owned bank account. These attacks vary in degree of sophistication between spear-phishing and pretexting (where a bad actor hijacks an existing thread and inserts themselves into the conversation, thereby making it much harder to catch the fraudulent action).

### I spy.

In third place was the Cyber-Espionage pattern, accounting for 14% of the region's breaches, which is substantially higher than the average of 3% for the overall dataset. This is an interesting finding, and there is not a clear-cut reason for it. The most likely explanation is that it may be an artifact of our data contributors and the cases they happen to encounter in these locales. But then again, James Bond is British after all. In this sort of incident, one should expect to see the hallmarks of the Advanced Persistent Threat (APT) attack—combinations of social attacks (phishing) to gain access, along with malware being dropped and deployed in the environment in order to maintain persistence and remain unobserved.

### Zooming out

If we take a step back and look at the larger class of incidents, we see that Denial of Service (DoS) attacks topped the regional charts for malware varieties (Figure 126). An interesting point is that while DoS attacks accounted for a very high percentage of incidents in this area's overall corpus, they actually had one of the lowest rates of bits per second (BPS) of any region. The second most common malware for the region was ransomware, which continues to be ubiquitous globally. In fact, if we remove DoS attacks, ransomware accounts for 6% percent of all incidents here, and is commonly associated with C2/backdoors, Brute forcing and Password dumpers. All the more reason we should keep our endpoints malware free and our servers locked down.

# Asia-Pacific (APAC)

**Figure 127.** Asia-Pacific (APAC) region



Summary

The APAC region is being targeted by financially motivated actors deploying ransomware to monetize their access. This region is also beset by phishing (often business email compromises), internal errors and has a higher-than-average rate of Cyber-Espionage-related breaches. Web application infrastructure is being targeted both by Denial of Service attacks affecting the availability of the assets, and by hacking attacks leveraging stolen credentials.

Frequency	4,055 incidents, 560 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 90% of breaches.
Threat Actors	External (83%), Internal (17%), Partner (0%) (breaches)
Actor Motives	Financial (63%), Espionage (39%), Fun (4%) (breaches)
Data Compromised	Credentials (88%), Internal (14%), Other (9%), Personal (6%) (breaches)

The Asia-Pacific (APAC) region includes a vast amount of territory, including most of Asia, what many refer to as Oceania (e.g., Australia and New Zealand), and numerous island nations in and around the Pacific.

An incident does not a breach make ... or does it?

In Figure 128, we can see the patterns that account for the majority of incidents in this region. It is important to note that some of those patterns, while prevalent, do not usually result in a confirmed breach. For instance, in the Crimeware pattern, the second most common Malware variety is Ransomware incidents. These are both an Integrity violation (Software Installation) and an Availability violation (Obscuration) as they encrypt the data, but instances where the data is known to be viewed and stolen (Confidentiality) remain relatively rare. However, in our data collection for next year's report,<sup>48</sup> cases are surfacing in which certain groups of actors are using the tactic of "naming and shaming" their victims in an attempt to exert additional pressure on them to pay the ransom. In other cases, the actors will copy some or all of the data prior to encrypting it, and then post excerpts on their websites<sup>49</sup> in order to further incentivize their victims to pay up.

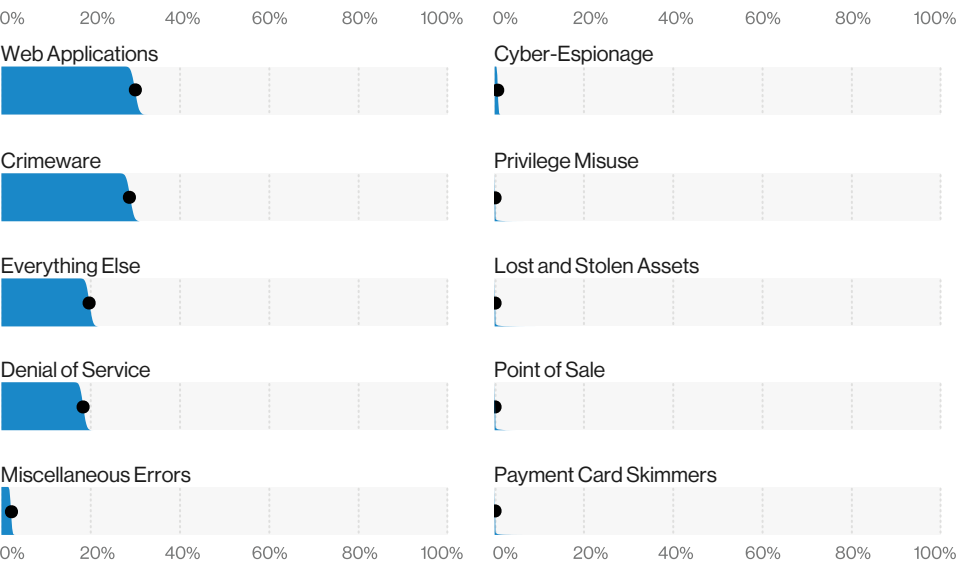


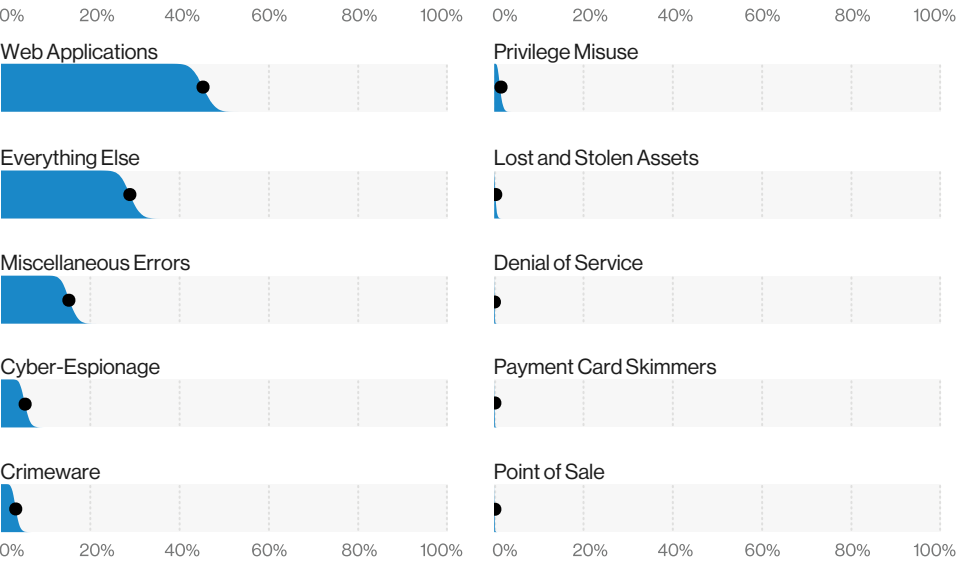
Figure 128. Patterns in APAC incidents (n = 4,055)

48 Sisyphus has nothing on us!  
49 Some examples from publicly disclosed incidents: <https://github.com/vz-risk/VCDB/issues?q=is%3Aopen+is%3Aissue+label%3ARansomware-N%26S>

Web Applications attacks were the top pattern for both incidents and confirmed breaches in APAC. These attacks are most frequently someone testing their trusty store of stolen credentials against your web-facing infrastructure and crossing their fingers they will see success. Not surprisingly, with the problem of credential reuse and the vast treasure trove of resulting credential dumps, there are a fair number of hackers laughing all the way to the bank. If that strategy does not work for our hoodie-clad friends, the use of social engineering will frequently gain them the keys to the kingdom. Clearly, something is working, since Credentials were the top stolen data type in the region's breaches.

The second most common pattern was Everything Else (Figure 129). This serves as a category for breaches that do not fit the criteria for the other attack patterns. There are a couple of common attacks that live within this pattern. One of them, the business email compromise (BEC), is an attack that starts with a phishing email. The attacker is frequently masquerading as someone in the executive suite of the company and is trying to influence the actions of someone who would not normally be comfortable challenging a request from them. For example, a payroll clerk believes they are being told to reroute deposits to a different account by the CEO of the organization and so they do as instructed – only to find later that the request did not actually come from that executive.

Sometimes this comes in the form of a pretext (an invented scenario). One common example is asking for money via a wire transfer to a specific (never before used) account. In either case, unless there is a process in place to handle these kinds of unusual requests from someone in high authority, the organization will likely see an incident.



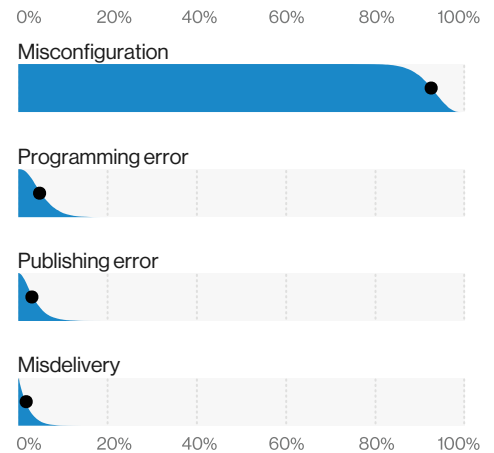
**Figure 129.** Patterns in APAC breaches (n = 560)

---

## Oops, did I do that?

A word of warning: What you are about to hear may shock you, but people are not perfect. Yes, we know, we didn't believe it at first either. But our dataset certainly indicates that it is the case, and neither organization type nor region seems to make much difference. In fact, the Miscellaneous Errors pattern comes in third in the APAC regional data. What are these errors? Why are they happening to me? Hop in and we will take you on a tour of the many ways the people who make up an organization can cause a breach without actually meaning to.

Figure 130 shows the bulk of these are Misconfiguration errors, and are due to Carelessness. Misconfiguration errors have long been a boon companion of this report. They occur when an employee—typically a system administrator or some other person with significant access to scads (yes that is a technical term) of data—stands up a database in the cloud without the usual security controls. “This will be fine. Surely nobody will locate this here,” they think to themselves. Or perhaps the lunch special ends at two and they leave with the intention of putting those controls in place at the very next convenient moment. But often that moment only arrives after a security researcher, or much worse an attacker, has already found them. Yes, believe it or not there are truly a sizeable number of people who are employed (and some who are freelance) to find these nuggets of data strewn about on the internet just waiting to be unearthed. What comes next depends on the motives of the person who found the data. Most security researchers will notify the organization (if they can figure out who it belongs to). However, sometimes it isn't a person with motivations of notification, but rather an intention to monetize this tasty find on the dark web.



**Figure 130.** Error varieties in APAC breaches (n = 55)



# Latin America and the Caribbean (LAC)

**Figure 131.** Latin America and the Caribbean (LAC) region



## Summary

**Even though there are a relatively small number of incidents and breaches recorded in the region, the results clearly show consistency with the global dataset. Denial of Service attacks are seen with a higher intensity than expected, and ransomware incidents are a serious problem.**

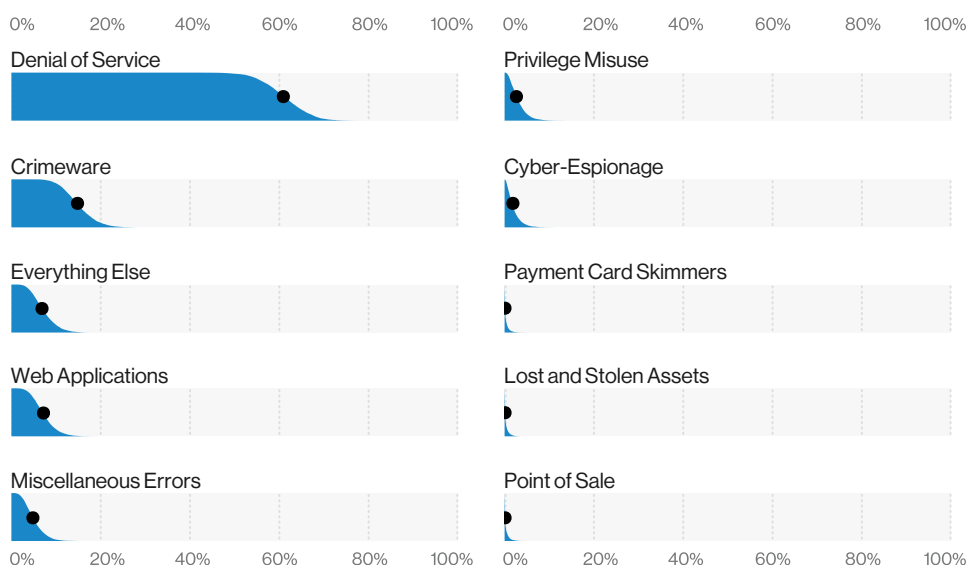
<b>Frequency</b>	87 incidents, 14 with confirmed data disclosure
<b>Top Patterns</b>	Denial of Service, Crimeware and Web Applications represent 91% of incidents.
<b>Threat Actors</b>	External (93%), Internal (7%), Partner (1%), Multiple (1%) (incidents)
<b>Actor Motives</b>	Financial (52%–87%), Espionage/Ideology (2%–27% each), Fun/Grudge (0%–15% each), Convenience/Fear/Other/Secondary (0%–8% each) (incidents)
<b>Data Compromised</b>	Credentials, Personal, Internal, Secrets and System (incidents)
<b>Data Analysis Notes</b>	Actor motives are represented by percentage ranges, as only 24 incidents had a known motive.

## It's the law—or not.

Before we begin, it is important to point out that not all of the countries in this region have a legal requirement to notify of a data breach either to the government or to those affected, with the notable exceptions of Mexico and Colombia (where only the government is required to be notified). As such, we can surely expect a significant under-reporting of incidents and breaches here. It should be interesting to see if, as in other areas of the world where new disclosure laws are passed, the reporting ramps up and we find that it was just the tip of the iceberg being reported before. Hopefully, we can entice new contributors in LAC to increase the quality of our data. (Is this you? Let's talk.)

All things considered, we see a clear mirroring of the data we have available for this region in the global dataset. The majority of actors in all incidents are External, with the 93% in the region being very similar to the 92% of the entire dataset. Likewise, 52% to 87% of incidents were Financially motivated in LAC, while 64% were so motivated in the global data.

The top patterns for incidents are also consistent with the larger dataset, with Denial of Service representing between 50% to 70%, while Crimeware, Web Applications and Everything Else are tightly grouped (Figure 132). Crimeware is largely made up of incidents involving Ransomware, which have a very strong showing in this region in relation to other action varieties.



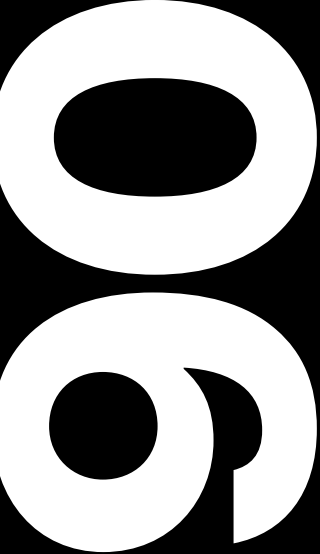
**Figure 132.** Patterns in LAC incidents (n = 87)

For all those similarities, this region had the largest median bits per second (BPS) by far—with 9 Gbps—where the global median was just a little over 500 Mbps (Figure 133). This higher intensity is in line with what one would expect from Denial of Service attacks against Financial organizations, which were over-represented in our regional DDoS data.

One of the things that has been reinforced in analyzing the data across the different locales is that, regardless of whether a specific country is represented in the dataset from year to year, all countries are seeing similar types of attacks. Time and again, we see that the adversaries are not adjusting their tactics based on the geographic location of their victims. They adjust their attacks based on what they need to do to gain access. So, while we have seen some differences across the regions, we are consistently finding that the kinds of attacks are common to all.



**Figure 133.** Most common BPS in LAC region DDoS (n = 52 DDoS); all regions mode (green line): 565 Mbps



# Wrap-up

---

**Well, that's it, folks! Thank you for joining us again. We hope you enjoyed reading the report and found the contents informative. As always, we send our most sincere thanks to our readers, supporters and contributors. This job can be a bit of a heavy lift at times, but it is also a labor of love. We feel very fortunate to be able to create this report and share the findings with you. We are grateful to all of you who have supported this endeavor with your time and resources. We hope to meet you all back here again next year, and in the meantime, be well, be prosperous and be prepared for anything.**

# CIS Control recommendations

---

## CIS Critical Security Controls (CSCs)

---

**CSC 1** Inventory and Control of Hardware Assets

---

**CSC 2** Inventory and Control of Software Assets

---

**CSC 3** Continuous Vulnerability Management

---

**CSC 4** Controlled Use of Administrative Privileges

---

**CSC 5** Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

---

**CSC 6** Maintenance, Monitoring and Analysis of Audit Logs

---

**CSC 7** Email and Web Browser Protections

---

**CSC 8** Malware Defenses

---

**CSC 9** Limitation and Control of Network Ports, Protocol and Services

---

**CSC 10** Data Recovery Capabilities

---

**CSC 11** Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

---

**CSC 12** Boundary Defense

---

**CSC 13** Data Protection

---

**CSC 14** Controlled Access Based on the Need to Know

---

**CSC 15** Wireless Access Control

---

**CSC 16** Account Monitoring and Control

---

**CSC 17** Implement a Security Awareness and Training Program

---

**CSC 18** Application Software Security

---

**CSC 19** Incident Response and Management

---

**CSC 20** Penetration Tests and Red Team Exercises

**For all the years of hard work, the DBIR can finally have some standardized controls, as a treat.**

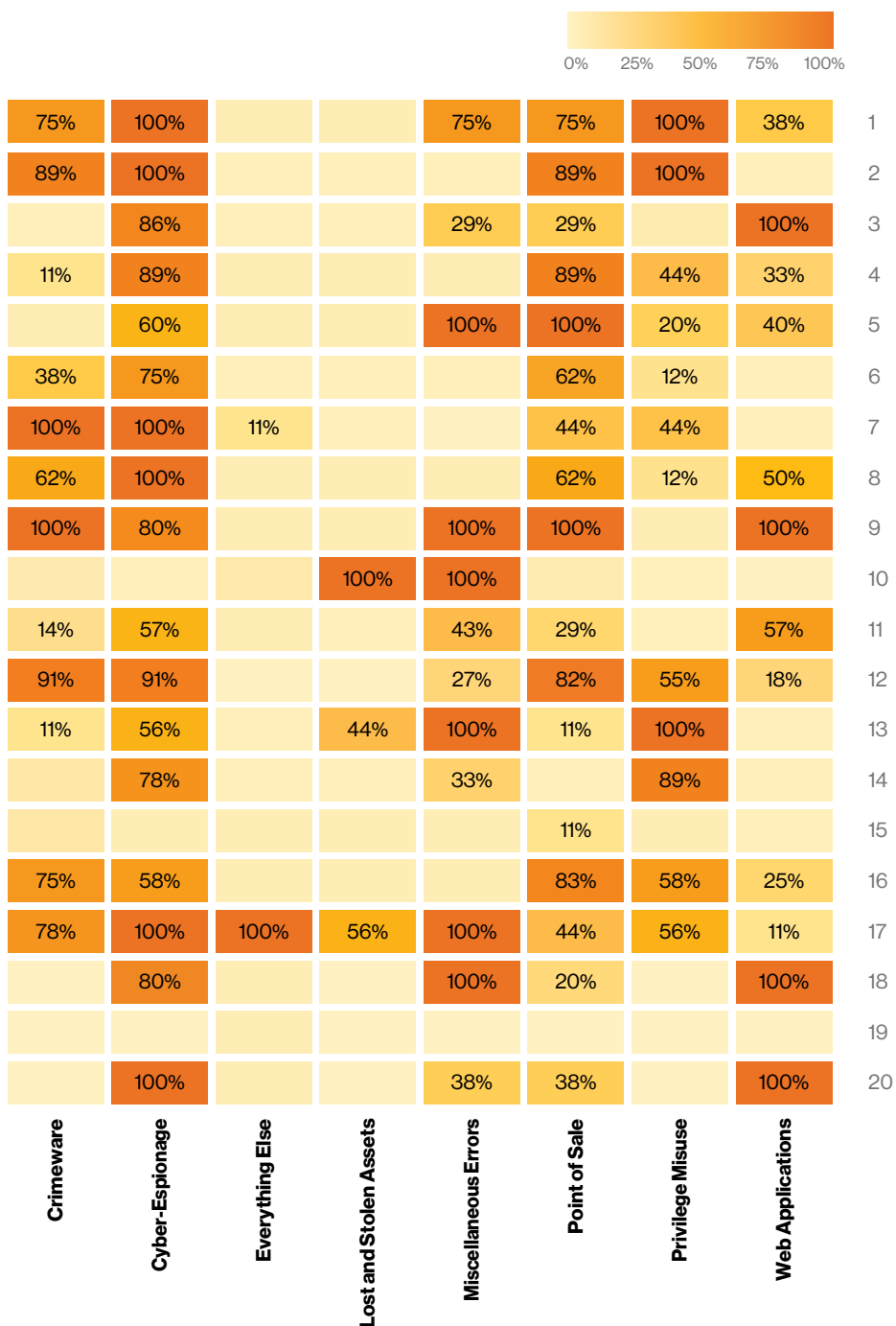
To be fair, this is simply a new take on an old approach. If you were to take out the 2014 version of the DBIR, blow the dust off of the cover and glance through the findings, you'll see an effort that we undertook to help standardize our approach to talking about defense and controls.

In this effort, we aligned our findings with the Center for Internet Security (CIS) Critical Security Controls (version 6 at the time) to provide you, our most devoted and loyal readers, with a way to match our findings to your security efforts. You may (or may not) be happy to hear that we've revisited our earlier attempt to help provide you with the same types of integration and assist you with tying your security program prioritization to our data.

---

## Why CIS?

Most of us probably have our own preferences regarding security frameworks and guidance, and the authors of this report are certainly not without theirs (hint: one of us may have contributed to the CIS Critical Security Controls [CSCs] at one point or another), but there are several empirical reasons why we chose this specific collection of controls. In brief, they provide sufficient levels of detail to meaningfully tie back between our Actions and Vectors, and there's a multitude of different mappings between the CIS CSCs and other standards freely available online. Also, it helps that we jibe with their non-profit community approach.



For those who are unacquainted with the CIS CSCs, they are a community-built, attacker-informed prioritized set of cybersecurity guidelines that consist of 171 safeguards organized into 20 higher-level controls. One of the unique elements of the CIS CSCs is their focus on helping organizations understand where to start their security program. This prioritization is represented in two ways:

- Through the ordering of the Critical Security Controls so that they allow a loose prioritization (Critical Security Control 1: Inventory of Hardware is probably a better place to start than Critical Security Control 20: Penetration Testing)
- Introduced in version 7.1<sup>50</sup> is the concept of Implementation Groups, in which the 171 safeguards are grouped based on the resources and risks the organizations are facing. This means that a smaller organization with fewer resources (Implementation Group 1) shouldn't be expected to implement resource- and process-intensive controls such as Passive Asset Discovery even if it is within Critical Security Control 1, while an organization with more resources and/or a higher risk level may want to consider that control.

**Figure 134.** Percentage of Safeguards mapped to Patterns by Critical Security Control

50 <https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/>

---

## How we used it

The more observant among you may notice that we included a new item on our Summary tables in our industry sections that identify the Top Controls for the breaches found in that specific industry. To get those Top Controls, we developed a mapping between the VERIS Actions and the safeguards and then aggregated them at the Critical Security Control level. This allows you to get a rough approximation of some of the controls that you should consider prioritizing for your security program.

Figure 134 is based on the initial mapping we did and captures the percentage of safeguards per Critical Security Control that play a role in mitigating the patterns identified.<sup>51</sup> Below is also a quick description of some of the top controls identified across all the industries analyzed. Additional information on the actual Critical Security Controls can be found on the CIS website.<sup>52</sup>

---

## Continuous Vulnerability Management (CSC 3)

A great way of finding and remediating things like code-based vulnerabilities, such as the ones found in web applications that are being exploited and also handy for finding misconfigurations.

---

## Secure Configuration (CSC 5, CSC 11)<sup>53</sup>

Ensure and verify that systems are configured with only the services and access needed to achieve their function. That open, world-readable database facing the internet is probably not following these controls.

---

## Email and Web Browser Protection (CSC 7)

Since browsers and email clients are the main way that users interact with the Wild West that we call the internet, it is critical that you lock these down to give your users a fighting chance.

---

## Limitation and Control of Network Ports, Protocols and Services (CSC 9)

Much like how Control 12 is about knowing your exposures between trust zones, this control is about understanding what services and ports should be exposed on a system, and limiting access to them.

---

## Boundary Defense (CSC 12)

Not just firewalls, this Control includes things like network monitoring, proxies and multifactor authentication, which is why it creeps up into a lot of different actions.

---

## Data Protection (CSC 13)

One of the best ways of limiting the leakage of information is to control access to that sensitive information. Controls in this list include maintaining an inventory of sensitive information, encrypting sensitive data and limiting access to authorized cloud and email providers.

---

## Account Monitoring (CSC 16)

Locking down user accounts across the organization is key to keeping bad guys from using stolen credentials, especially by the use of practices like multifactor authentication, which also shows up here.

---

## Implement a Security Awareness and Training Program (CSC 17)

Educate your users, both on malicious attacks and the accidental breaches.

---

## The future is under control.

To aid us both in our continuous improvement and transparency, we'll be adding our mapping of Critical Security Controls to our VERIS GitHub page at <https://github.com/vz-risk/veris>. We encourage you to use it as well and provide feedback on how you think we can improve. This is really our first step toward making this more accessible and easier for others to leverage, and while we acknowledge that this first version may have room for improvement, we plan to iterate rapidly on it. The more we share a common language, the easier it will be for us to work together toward more secure environments and organizations.

<sup>51</sup> One thing of note is that the CIS Controls are focused on cybersecurity best practices and don't touch upon things like physical security (Payment Card Skimmers pattern) or availability practices (Denial of Service pattern), so we did not include them in our diagram.

<sup>52</sup> <https://www.cisecurity.org/controls/cis-controls-list/>

<sup>53</sup> We combined both Secure Configuration for Desktops, Servers and Workstations (CSC 5) AND Secure Configuration for Networking Devices (CSC 11), for two reasons. For one, it's difficult to know if it's a networking issue or a system issue that is the ultimate cause of the breach and for another, it's become increasingly more difficult to separate the network from the device in certain environments.

# Year in review<sup>54</sup>

---

## January

The first intelligence collection in 2019 was an FBI Liaison Alert System on APT10 intrusion activities targeting cloud-based managed service providers. Throughout the month, the Verizon Threat Research Advisory Center (VTRAC) intelligence collections reflected a continuation of some of 2018's trends and emerging developments that would occupy us throughout the new year. New intelligence linked two Russian APT-grade actors, GreyEnergy and APT28 (Sofacy). Two months since we began tracking "the DNSpionage campaign," new collections revealed its global span and complexity. GandCrab and Ryuk ransomware surged in January, in part to occupy the vacuum left after the SamSam operators were indicted and ceased operations. The VTRAC continued to track and report Magecart payment card scripting skimmer attacks on e-retailers, a threat that would resurface several more times in 2019. The Indian subsidiary of Milan-based Tecnimont SpA, fell prey to a fraud after US\$18.6 million (₹130 crore) was stolen by Chinese hackers. The attackers breached the email system of the Mumbai branch to learn the "rhythm" of the business, identifying key players, vocabulary and customs. A series of staged conference calls with executives in Italy and a Swiss lawyer convinced the head of the Indian office to transfer funds to Hong Kong banks.

---

## February

Australia's parliament revealed that its computer network had been compromised by an unspecified "security incident." Norwegian cloud computing company Visma attributed a breach to the menuPass threat actor. A whaling campaign was observed that was probably aiming for Office 365 credentials to be used for a business email compromise operation. The Bank of Valetta in Malta was the victim of a €13 million fraud. Analysis of weaponized documents used by APT-grade actors in APAC sought to determine if a shared "digital quartermaster" was supplying multiple actors, including multiple state-aligned ones. It found links among some Chinese actors but that "the current exchange of offensive cyber tools remains opaque," and requires more research.

---

## March

The successful exploitation of new vulnerabilities was a recurring problem in March, including vulnerabilities in Cisco Adaptive Security Appliances, Cold Fusion, Drupal, Microsoft Exchange Server and the Windows kernel. Attacks on two "zero-day" vulnerabilities were mitigated among 36 patches on "Patch Tuesday." "Operation ShadowHammer" by the Chinese Winnti threat actor tampered with software updates from PC maker ASUSTeK Computer to install malware on victims' computers. Aluminum manufacturer Norsk Hydro was attacked with LockerGoga ransomware. Citrix disclosed a data breach after the FBI warned them the attackers probably used a password spraying attack to gain a foothold. We collected intelligence about three separate campaigns targeting point-of-sale systems.

54 Thanks to David M. Kennedy from the VTRAC for this contribution.



---

## April

Pharmaceutical company Bayer announced it had prevented an attack by the Winnti threat actors targeting sensitive intellectual property. The Indian IT services giant Wipro was breached in order to attack its customers. The ultimate aim of the group behind the attack appeared to be gift-card fraud. The Vietnam-aligned APT32 (Ocean Lotus) actor targeted foreign automotive companies to acquire IP. The U.S. Department of Energy reported grid operators in Los Angeles County, California, and Salt Lake County, Utah, suffered a DDoS attack that disrupted their operations, but did not cause any outages. The US-CERT warned that multiple VPN applications store the authentication and/or session cookies insecurely in memory and/or log files. Cisco, Palo Alto Networks, F5 Networks and Pulse Secure products were affected. A new DNS hijacking campaign, "Sea Turtle," was discovered targeting private and public organizations primarily located in the Middle East and North Africa.

---

## May

Patch Tuesday in May included patches for CVE-2019-0708, a vulnerability in Remote Desktop Protocol that was nicknamed "BlueKeep." A hue and cry to patch so as to avoid an imminent WannaCry-like worm went hyperbolic. The City of Baltimore, Maryland, was paralyzed by RobbinHood ransomware. A new ransomware, "Sodinokibi" appeared to be spreading from unpatched Oracle WebLogic servers. Magecart groups continued to deploy payment card scraping scripts. They expanded their targeted platforms beyond Magento to the PrismWeb and OpenCart e-commerce platforms. A vulnerability in Magento patched in March became the target of mass scanning and SQLinjection attacks.

---

## June

LabCorp disclosed that a breach at a third-party billing collections firm exposed the personal information of 7.7 million Americans. Chinese intelligence services hacked into the Australian National University to collect data they could use to groom students as informants before they were hired into the civil service. U.S. grid regulator NERC issued a warning that Xenotime, a major hacking group with suspected Russian ties, was conducting reconnaissance into the networks of electrical utilities. "Operation Soft Cell" ran over the course of seven years by the APT10 Chinese espionage actor. They hacked into 10 international mobile phone providers operating across 30 countries to track dissidents, officials and suspected spies. The operators behind GandCrab ransomware announced they were shutting down. Most analysts assessed they were simply shifting from GandCrab to Sodinokibi.

---

## July

Capital One revealed a hacker accessed data on 100 million credit card applications, including Social Security and bank account numbers. Improperly secured Amazon cloud storage was at the heart of the theft of 30 GB of credit application data by a single subject. Microsoft revealed that it had detected almost 800 cyberattacks over the past year targeting think tanks, non-governmental organizations and other political organizations around the world, with the majority of attacks originating in Iran, North Korea and Russia. Several major German industrial firms, including BASF, Siemens and Henkel, announced that they had been the victim of a state-sponsored hacking campaign by the Chinese Winnti group.

---

## August

On Friday, August 16, 22 Texas towns were infected with Trickbot followed by Sodinokibi ransomware after attackers breached their managed service provider (MSP), TSM Consulting, and employed the MSP's ConnectWise Control remote management tool to distribute the malware. The following week, malware researchers observed revived activity in Emotet distribution networks. In June, the Emotet crew seemed to suspend operations. By mid-September, Emotet seemed to be fully operational. Emotet had been linked to multiple Russian threat actors, including Mummy Spider, TA542 and TA505. Emotet mal-spam had been delivering other malware payloads, including Dridex, Ursnif, Trickbot and Ryuk.

---

## September

At the end of August and early in September, multiple sources began reporting strategic web compromises targeting Tibetan rights activists and ethnic minority Uyghurs using iOS and Android Trojans. Operation Soft Cell reported in June was probably part of this campaign. Another new Chinese APT-grade actor, APT5, emerged and was discovered attacking vulnerable VPN servers. Two zero-day Windows vulnerabilities were included in September's Patch Tuesday and before the end of the month, Microsoft released an out-of-cycle patch for a third zero-day. A breach at social video-game developer Zynga affected over 175 million players.

---

## October

In October, the VTRAC was swamped by intelligence covering APT-grade actors, including TA505, FIN6, FIN7 and RTM cybercrime actors. FIN4, FIN6 and Carbanak were linked to different Magecart groups. Intelligence was received on cyber-espionage and cyber-conflict actors included Charming Kitten, Turla, Winnti and APT29 actors. We learned of a September attack on India's Kudankulam Nuclear Power Plant (KNPP) by the Lazarus group. The attack did not affect either the nuclear power plant control system or the electricity-generating power plant control system. A new spin on business email compromises emerged and was dubbed "Vendor Email Compromises."

---

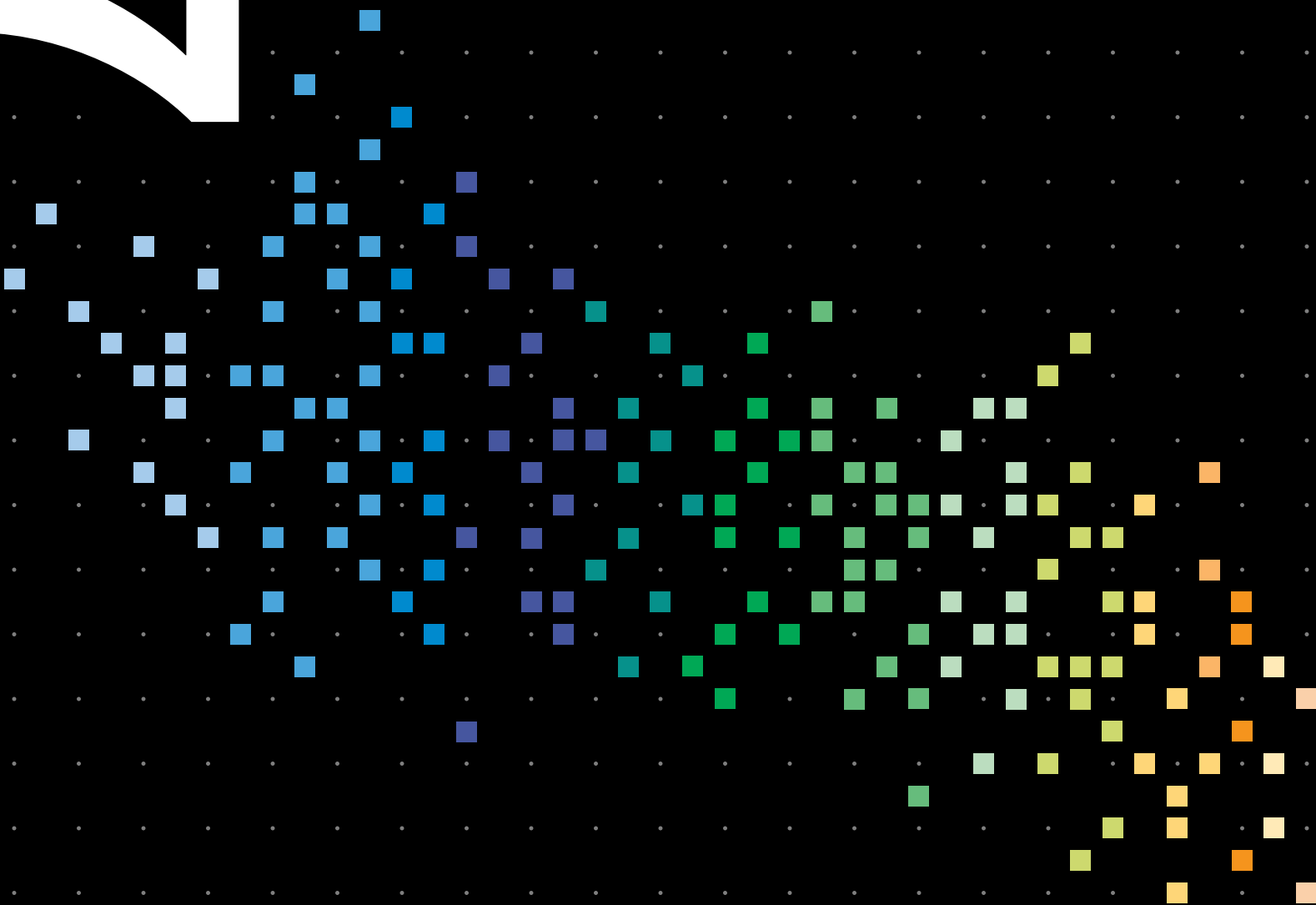
## November

Facility services company Allied Universal suffered a Maze ransomware infection. The miscreants demanded about US\$2 million in bitcoin and threatened to release 5 GB of stolen internal files if they weren't paid. They did release at least 700 MB. Before the end of the year, criminals behind at least four ransomware families had begun to exfiltrate internal files before triggering file encryption. They threatened to make the data public to add leverage on the victims to pay. The Iranian APT33 had been targeting industrial control system (ICS) equipment that is used in oil refineries, electrical utilities and manufacturing.

---

## December

The U.S. government warned of malicious spam-spreading Dridex banking Trojans that were used to gain a foothold to infect networks with BitPaymer ransomware. Petróleos Mexicanos (Pemex) was the victim of DoppelPaymer, a variant of Dridex and BitPaymer. One of 36 vulnerabilities Microsoft patched was being exploited in watering-hole attacks before December's Patch Tuesday. Microsoft released another out-of-cycle security bulletin and patch for a SharePoint vulnerability that was being exploited in the wild. The Gallium threat actor was linked to Operation Soft Cell and the watering-hole attacks on Tibetans and Uyghurs.



---

# Appendices

# Appendix A: Methodology

## One of the things readers value most about this report is the level of rigor and integrity we employ when collecting, analyzing and presenting data.

Knowing that our readership cares about such things and consumes this information with a keen eye helps keep us honest. Detailing our methods is an important part of that honesty. In order to continue to increase the transparency of our work, we introduced a couple of new features we are including in the report this year.

First, we make mistakes. A column transposed here, a number not updated there. We're likely to discover a few things to fix. When we do, we'll list them on our corrections page: <https://enterprise.verizon.com/resources/reports/dbir/2020/report-corrections/>

Second, we check our work. The same way the data behind the DBIR figures can be found in our GitHub repository,<sup>55</sup> for the first time we're also publishing our fact-check report there as well. It's highly technical, but for those interested, we've attempted to test every fact in the report.<sup>56</sup>

---

## Non-committal disclaimer

We would like to reiterate that we make no claim that the findings of this report are representative of all data breaches in all organizations at all times. Even though the combined records from all our contributors more closely reflect reality than any of them in isolation, it is still a sample. And although we believe many of the findings presented in this report to be appropriate for generalization (and our confidence in this grows as we gather more data and compare it to that of others), bias undoubtedly exists.

While we may not be perfect, we believe we provide the best obtainable version of the truth and a useful one at that. Please review the "Acknowledgement and analysis of bias" section below for more details on how we do that.

---

## The DBIR process

Our overall process remains intact and largely unchanged from previous years. All incidents included in this report were individually reviewed and converted (if necessary) into the VERIS framework to create a common, anonymous aggregate dataset. If you are unfamiliar with the VERIS framework, it is short for Vocabulary for Event Recording and Incident Sharing; it is free to use and links to VERIS resources that are at the beginning of this report.

The collection method and conversion techniques differed between contributors. In general, three basic methods (expounded below) were used to accomplish this:

- 
- 1 Direct recording of paid external forensic investigations and related intelligence operations conducted by Verizon using the VERIS WebApp

---

  - 2 Direct recording by contributors using VERIS

---

  - 3 Converting contributors' existing schema into VERIS

All contributors received instruction to omit any information that might identify organizations or individuals involved.

Reviewed spreadsheets and VERIS WebApp JavaScript Object Notation (JSON) are ingested by an automated workflow that converts the incidents and breaches into the VERIS JSON format as necessary, adds missing enumerations and then validates the record against business logic and the VERIS schema. The automated workflow subsets the data and analyzes the results. Based on the results of this exploratory analysis, the validation logs from the workflow and discussions with the contributors providing the data, the data is cleaned and reanalyzed. This process runs nightly for roughly three months as data is collected and analyzed.

<sup>55</sup> <https://github.com/vz-risk/dbir/tree/gh-pages/2020>

<sup>56</sup> Interested in how we test them? Check out Chapter 9, Hypothesis Testing, of ModernDive: <https://moderndive.com/9-hypothesis-testing.html>

---

## Incident data

Our data is non-exclusively multinomial, meaning a single feature, such as “Action,” can have multiple values (i.e., “Social,” “Malware” and “Hacking”). This means that percentages do not necessarily add up to 100%. For example, if there are five botnet breaches, the sample size is five. However, since each botnet used Phishing, installed Keyloggers and Used stolen credentials, there would be five Social actions, five Hacking actions and five Malware actions, adding up to 300%. This is normal, expected and handled correctly in our analysis and tooling.

Another important point is that when looking at the findings, “Unknown” is equivalent to “unmeasured.” Which is to say that if a record (or collection of records) contain elements that have been marked as “unknown” (whether it is something as basic as the number of records involved in the incident or as complex as what specific capabilities a piece of malware contained), it means that we cannot make statements about that particular element as it stands in the record—we cannot measure where we have no information. Because they are “unmeasured,” they are not counted in sample sizes. The enumeration “Other” is, however, counted as it means the value was known but not part of VERIS or not included, as is the case with “top” figures. Finally, “Not Applicable,” (normally “NA”), may be counted or not counted depending on the hypothesis.

This year, we have made liberal use of confidence intervals to allow us to analyze smaller sample sizes. We have adopted a few rules to help minimize bias in reading such data. Here we define “small sample” as less than 30 samples.

- 
- 1 Sample sizes smaller than five are too small to analyze
  - 2 We won’t talk about count or percentage for small samples. This goes for figures too and is why some figures lack the dot for the median frequency
  - 3 For small samples, we may talk about the value being in some range, or values being greater/less than each other. These all follow the hypothesis testing and confidence interval approaches listed above
- 

## Incident eligibility

For a potential entry to be eligible for the incident/breach corpus, a couple of requirements must be met. The entry must be a confirmed security incident, defined as a loss of confidentiality, integrity or availability. In addition to meeting the baseline definition of “security incident,” the entry is assessed for quality. We create a subset of incidents (more on subsets later) that pass our “quality” filter.

The details of what is a “quality” incident are:

- 
- 1 The incident must have at least seven enumerations (e.g., threat actor variety, threat action category, variety of integrity loss, et al.) across 34 fields OR be a DDoS attack. Exceptions are given to confirmed data breaches with less than seven enumerations
  - 2 The incident must have at least one known VERIS threat action category (hacking, malware, etc.)
- 

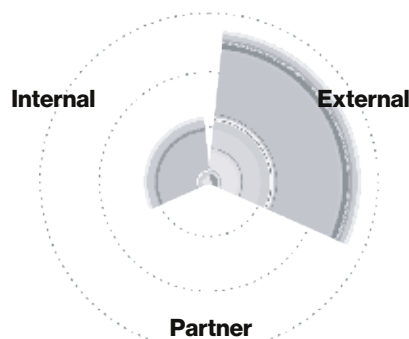
In addition to having the level of details necessary to pass the quality filter, the incident must be within the time frame of analysis (November 1, 2018, to October 31, 2019, for this report). The 2019 caseload is the primary analytical focus of the report, but the entire range of data is referenced throughout, notably in trending graphs.<sup>57</sup> We also exclude incidents and breaches affecting individuals that cannot be tied to an organizational attribute loss. If your friend’s laptop was hit with Trickbot, it would not be included in this report.

Lastly, for something to be eligible for inclusion into the DBIR, we have to know about it, which brings us to several potential biases we will discuss below.

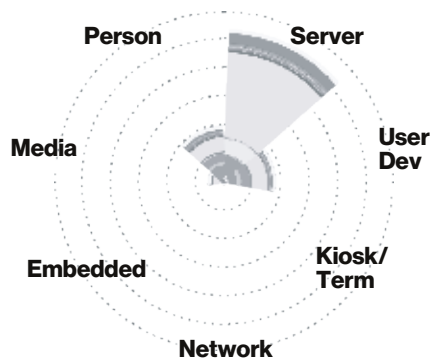
57 Our line figures use the calendar year the incident occurred in as they are continuous, while our dumbbell charts use the year of the DBIR report, as they are ordinal.



**Figure 135.** Individual contributions per Action



**Figure 136.** Individual contributions per Actor



**Figure 137.** Individual contributions per Asset



**Figure 138.** Individual contributions per Attribute

## Acknowledgement and analysis of bias

Many breaches go unreported (though not in our sample). Many more are as yet unknown by the victim (and thereby unknown to us). Therefore, until we (or someone) can conduct an exhaustive census of every breach that happens in the entire world each year (our study population), we must use sampling.<sup>58</sup> Unfortunately, this process introduces bias.

The first type of bias is random bias introduced by sampling. This year, our maximum confidence is  $\pm 1.5\%$ <sup>59</sup> for breaches and  $\pm 0.5\%$  for incidents, which is related to our sample size. Any subset with a smaller sample size is going to have a wider confidence margin. We've expressed this confidence in the conditional probability bar charts (the "slanted" bar charts) that we have been using since the 2019 report.

The second source of bias is sampling bias. We strive for "the best obtainable version of the truth"<sup>60</sup> by collecting breaches from a wide variety of contributors. Still, it is clear that we conduct biased sampling. For instance, some breaches, such as those publicly disclosed, are more likely to enter our corpus, while others, such as classified breaches, are less likely.

<sup>58</sup> Interested in sampling? Check out Chapter 7, Sampling, of ModernDive: <https://moderndive.com/7-sampling.html>

<sup>59</sup> This and all confidence intervals are 95% confidence intervals determined through bootstrap simulation. Read more in Chapter 8, Bootstrapping and Confidence Intervals, of ModernDive: <https://moderndive.com/8-confidence-intervals.html>

<sup>60</sup> Eric Black, "Carl Bernstein Makes the Case for 'the Best Obtainable Version of the Truth,'" by way of Alberto Cairo, "How Charts Lie" (a good book you should probably read regardless)

The four figures at left are an attempt to visualize potential sampling bias. Each radial axis is a VERIS enumeration and we have stacked bar charts representing our data contributors. Ideally, we want the distribution of breaches to be roughly equally divided between contributors in the stacked bar charts along all axes. Axes only represented by a single source are more likely to be biased. However, contributions are inherently thick tailed, with a few contributors providing a lot of data and many contributors providing a few records within a certain area. Still, we mostly see that most axes have multiple large contributors with small contributors adding appreciably to the total incidents along that axes.

You'll notice a rather large single contribution on many of the axes. While we'd generally be concerned about this, it represents a contribution aggregating several other sources, so not an actual single contribution. It also occurs along most axes, limiting the bias introduced by that grouping of indirect contributors.

The third source of bias is confirmation bias. Because we use our entire dataset for both exploratory analysis as well as hypothesis testing, we inherently test our hypotheses on the same data we used to make them. Until we develop a good collection method for data breaches or incidents from Earth-2 or any of the other Earths in the multiverse,<sup>61</sup> this is probably the best that can be done.

As stated above, we attempt to mitigate these biases by collecting data from diverse contributors. We follow a consistent multiple-review process and when we hear hooves, we think horse, not zebra.<sup>62</sup> We also try to review findings with subject matter experts in the specific areas ahead of release.

---

## Data subsets

We already mentioned the subset of incidents that passed our quality requirements, but as part of our analysis, there are other instances where we define subsets of data. These subsets consist of legitimate incidents that would eclipse smaller trends if left in. These are removed and analyzed separately (as called out in the relevant sections). This year, we have two subsets of legitimate incidents that are not analyzed as part of the overall corpus:

- 1 We separately analyzed a subset of web servers that were identified as secondary targets (such as taking over a website to spread malware)
- 2 We separately analyzed botnet-related incidents

Both subsets were separately analyzed the last three years as well.

Finally, we create some subsets to help further our analysis. In particular, a single subset is used for all analysis within the DBIR unless otherwise stated. It includes only quality incidents as described earlier and excludes the aforementioned two subsets.

---

## Non-incident data

Since the 2015 issue, the DBIR includes data that requires the analysis that did not fit into our usual categories of "incident" or "breach." Examples of non-incident data include malware, patching, phishing, DDoS and other types of data. The sample sizes for non-incident data tend to be much larger than the incident data, but from fewer sources. We make every effort to normalize the data (for example, weighting records by the number contributed from the organization so all organizations are represented equally). We also attempt to combine multiple partners with similar data to conduct the analysis wherever possible. Once analysis is complete, we try to discuss our findings with the relevant partner or partners so as to validate it against their knowledge of the data.

<sup>61</sup> The DBIR is a pre-Crisis on Infinite Earths work environment.

<sup>62</sup> A unique finding is more likely to be something mundane (such as a data collection issue) than an unexpected result.

# Appendix B: VERIS Common Attack Framework (VCAF)

## **VERIS was developed as a solution to the need for consistent definitions of incident and breach data for analysis.**

With its close ties to the DBIR and data analysis, it was created to remove the ambiguity inherent in terms surrounding breaches and provide a data-driven structure capable of quantifying the majority of breaches. While VERIS covers a lot of different detailed information about an incident, including things such as Victim demographics and Timeline, the core of VERIS is captured in what we call the four “A’s” of an incident: Actor, Action, Asset, Attribute.

However, VERIS was not designed to represent precise and detailed tactical and technical minutiae around attackers’ techniques, chosen methods of persistence or methodology for executing malicious code on a compromised asset. Thankfully, it doesn’t need to because there is something else that has come along to help address that need.

## **Massive (adoption of) ATT&CK**

MITRE privately developed the original Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework starting in 2013 as a means of codifying adversarial behavior and released it publicly in 2015.<sup>63</sup> ATT&CK has become a well-established way for describing the tactical actions used by attackers (including a heavy focus on

advanced threats). Much like VERIS, ATT&CK is subdivided into a handful of key components, but the core of the framework are the “Techniques,” which describe the atomic means of how an attacker achieves an objective called a “Tactic.” The 260+ Techniques in ATT&CK for Enterprise are logically grouped with their corresponding 11 Tactics, which describe the different objectives an adversary might take as part of their intrusion.

---

### **We’re better when we’re together.**

While both VERIS and ATT&CK grew out of different needs and different objectives, VERIS to codify incidents and ATT&CK to codify adversary technique, there is without a doubt an overlap between the two that could be leveraged to improve the value of both standards. To get a better understanding of the relationships between these two frameworks, the team spent some time researching to see if they could map the VERIS framework to the ATT&CK techniques and vice-versa, the results of which you can see in Figure 139.

---

### **What is this, a crossover episode?**

Our solution to bridge the gap and help operationally connect the relationships between ATT&CK and VERIS is through the creation of an extension that we call the VERIS Common Attack Framework (VCAF).

VCAF serves as a bridge to ATT&CK, covering the portions of VERIS not in ATT&CK with the aim of creating a holistic framework. At its very core, VCAF is made of two components: one is the conceptual mapping between VERIS and ATT&CK, and another is the extension of ATT&CK with techniques that cover all possible Threat Actions present in VERIS. As much as we would have liked to leverage a default “meteor falling from the sky” technique in ATT&CK, those events are definitely quite rare.<sup>64</sup>

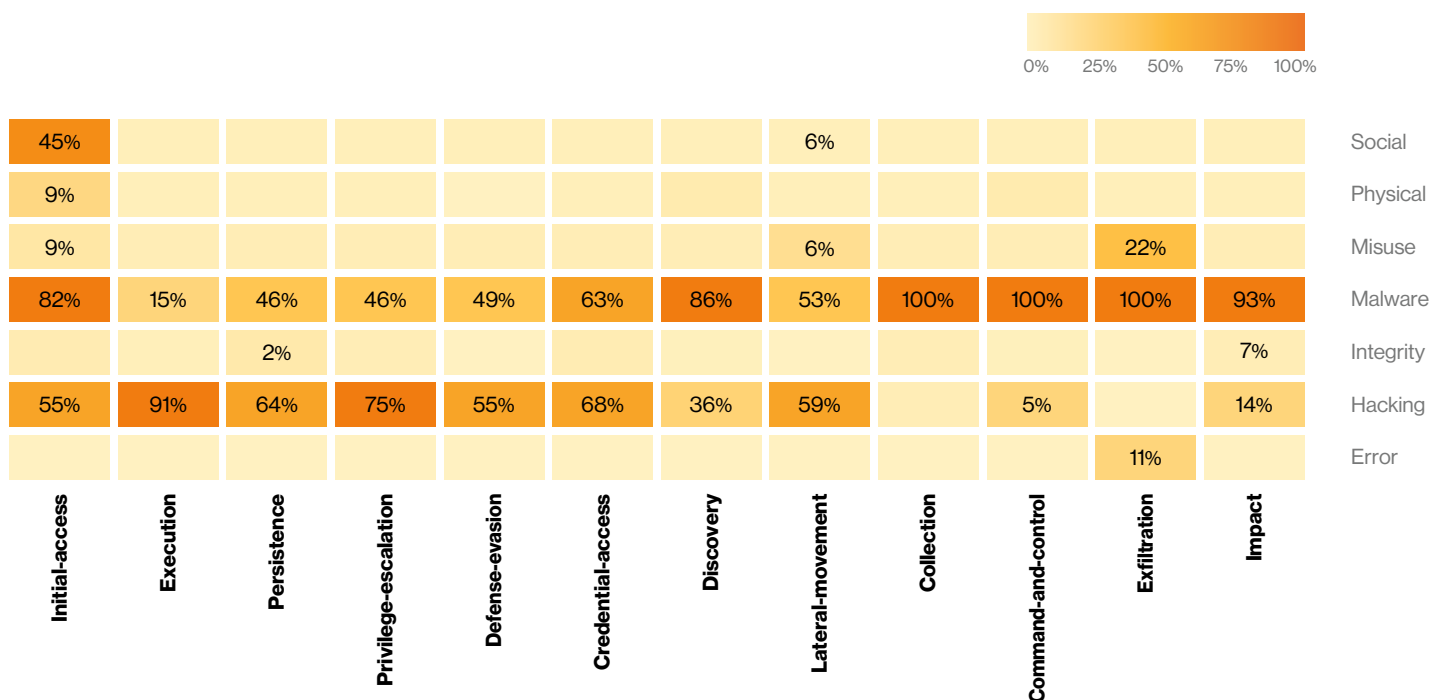
This approach should be flexible enough to accommodate both general categories found in VERIS (such as Ransomware) and some of the more specific attack types found either in VERIS or ATT&CK. Aside from expanding the scope of what is covered and can be tracked, using VCAF can help provide essential context to these incidents. Below is a list that includes a variety of the different benefits of leveraging this powerful combination:

- Understand the technical details associated with an incident
- Prioritize mitigations based on previous all incident types (not just the malware or hacking kind)
- Better understand the junction of targeting and capabilities
- Capture incident context that goes beyond technical artifacts
- Ease communication of cybersecurity concepts with non-cybersecurity experts

<sup>63</sup> <https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf>

<sup>64</sup> But they sure have a large impact!





**Figure 139.** Percentage of MITRE Techniques covered by VERIS

In this issue of the DBIR, we used VCAF to map simulated breach data, SIEM data and malware features to VERIS action categories to compare and draw conclusions in conjunction with our incident corpus.

## The beginning of something great

Clearly, VCAF is not the end-all be-all of cybersecurity frameworks. It is a modest step toward having an

integrated way for the community to discuss security incidents and attackers. As the number of cybersecurity frameworks grows and the field of knowledge surrounding cybersecurity topics deepens, there is a need for us as a community to integrate our own languages and understanding in an effort to help us communicate to the larger community of non-cybersecurity experts. Keep your eyes peeled for future developments and information on VCAF by visiting<sup>65</sup> our VERIS GitHub page at <https://github.com/vz-risk/veris>.

<sup>65</sup> And don't forget to smash that like and subscribe button!

# Appendix C

---

**Michael D'Ambrosio**  
Assistant Director  
U.S. Secret Service

---

**Jonah Force Hill**  
Senior Cyber Policy Advisor  
U.S. Secret Service

## Following the money—the key to nabbing the cybercriminal

This year's DBIR has once again highlighted the principal motive for the vast majority of malicious data breaches: the pursuit of profit. This is surprising to some, given the extensive media coverage of national security-related breaches. However, it should not be. Most malicious cyber actors are not motivated by national security or geopolitical objectives, but rather by simple greed. Cybercriminals primarily profit through fraud and extortion. They target financial and payment systems, steal information to use in various fraud schemes, and hold IT systems hostage through ransomware and other means. Whatever their criminal scheme, they then depend upon a money movement and laundering apparatus to transfer and liquidate their proceeds.

That is why the U.S. Secret Service was first assigned responsibility for investigating cybercrimes in the early 1980s, before it was even called “cyber,” and why we continue to do so today. Secret Service agents are financial crimes investigators, skilled not only at “following the money,” but at preventing criminals from profiting from their activities and at recovering the stolen assets of victims. When investigating any criminal cyber incident, a data breach, an “unlimited ATM cash-out” conspiracy, a ransomware attack or any other diverse, financially motivated crime committed via the internet, the heart of the Secret Service's approach is following the money.

We have learned over the decades that it is through the movement of funds—from the victim to the criminal, between and among criminals, and through the process of money laundering—that investigators are able to generate the greatest insights and criminal leads. Malware samples and indicator sharing are useful, no doubt, but it is the money and where it moves that leads to arrests, asset seizures and the recovery of assets stolen from victims of fraud.

For example, in a typical business email compromise (BEC) scheme, a victim is lured into sending a payment, usually via a wire transfer, to a bank account maintained under a criminal's control. The methods used in the deception part of the crime can range from highly sophisticated (such as deploying tailor-made malware) to shockingly simple (such as impersonating a vendor on the phone). How the fraudsters fool the victim is often insignificant; what is important is how they move and liquidate their proceeds.

Smart criminals understand this. They know that the accounts, shell companies and processes they use to move their stolen funds contain a wealth of location data and other information that can lead to their arrest. As a result, criminals try to distance themselves and their identities from all accounts and institutions that might be associated with their crimes.

There are number of ways criminals do this, but one of the principal mechanisms is the use of “mules,” outside individuals recruited to participate in the scheme. Mules can be either witting or unwitting participants. Some mules join the scheme with full knowledge of the criminal nature of their involvement; others are recruited through what appear to be legitimate job postings. Still others are victims themselves of ancillary frauds, often romance scams, in which they are conned into believing that they are sending money to a romantic partner, when in fact they are just moving money for crooks.

A similar dynamic exists in cases of ransomware and in other crimes in which cryptocurrencies play a role. When an organization pays a ransom to unlock its IT systems, for instance, the criminal generally instructs the victim to send a bitcoin payment to a cryptocurrency wallet.

These wallets are hosted either on a cryptocurrency exchange, which can be either legitimate or illegitimate, or on a device operated by the criminal or an associate. Here too, the criminals seek to obscure the location of the wallets and to limit access to any other information that might tie their activities to a specific wallet or account.

Criminals engaged in ransomware attacks employ many of the same techniques as BEC scammers to cover their tracks. They may pay mules to set up crypto wallets, or con unwitting mules into thinking they have landed a legitimate job in the cryptocurrency industry. They may use cryptocurrency tumblers and mixers to swap funds from one form of cryptocurrency to another (for instance, from bitcoin to ether), to keep law enforcement from tracking their movements on the blockchain. They may set up shell companies, open overseas bank accounts and move money repeatedly from one country to the next, all with the aim of making their financial movements as difficult as possible to trace.

Yet there is always a chokepoint. If cybercriminals want to enjoy the fruit of their criminal labor, they must convert their profits into a form of money they can actually use, without being tracked by law enforcement. These chokepoints

create the greatest opportunities to counter cybercriminal activity.

The Secret Service focuses on these chokepoints to disrupt these financial flows, whether they are explicitly illicit services or legitimate businesses that are exploited by criminals. Through undercover operations, confidential informants and partnerships with industry and the broader law enforcement community, the Secret Service excels at identifying and interdicting these illicit financial flows. In 2019, the Secret Service prevented \$7.1 billion of cybercrime losses and returned over \$31 million in stolen assets to victims of fraud.

The lessons for industry are simple: Invest in the defense of your networks and, in the event of a breach, collect as much evidence as you can. When shared with law enforcement partners, that evidence can lead not only to the arrest of the criminal, but also to the seizure of their assets. In many cases, the recovered money can be returned to the victim. This is how we prevent cybercriminals from operating with impunity. It is a collective struggle. Let's work together.

# Appendix D

---

## Diego Curt

Chief Compliance Officer  
State of Idaho, Office of the Governor—  
Information Technology Services

## State of Idaho enhances incident response program with VERIS.

We hear it all the time. We need to share incident and breach information for improved decision-making. The State of Idaho was facing the same issue, trying to get different agencies to share incident and breach information for improved decision-making and better cyber-defense investment. In order to address this, the State of Idaho designed a program that gained approval from various stakeholders, including the legal department. The program consists of two fundamental components and three core components.

---

### The two fundamental components are:

- 1 **Cyber Kill Chain<sup>66</sup> developed by Lockheed Martin, Inc.**—used to promote actionable intelligence-process thinking and serves as a blueprint for building an effective cybersecurity program
- 2 **National Institute of Standards and Technology (NIST) Cybersecurity Framework<sup>67</sup>**—a risk reporting framework used to assess the readiness and maturity of cybersecurity controls throughout the enterprise

---

### The three core components of the program are:

- 1 **NIST SP 800-53<sup>68</sup> Incident Response Control Family**—used to govern and ensure all control processes are addressed and matured on a continuous basis
- 2 **Vocabulary for Event Recording and Incident Sharing (VERIS)**—an easy-to-use, systematically structured language/taxonomy used to gather intelligence from incidents and breaches for better decision-making and information sharing
- 3 A commercial web-based application that brings together first responders, emergency management, National Guard, cyber-incident response handlers, etc., into one platform that houses the VERIS language/taxonomy

<sup>66</sup> <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

<sup>67</sup> <https://www.nist.gov/cyberframework>

<sup>68</sup> <https://nvd.nist.gov/800-53>

At the heart of the program is the VERIS taxonomy. VERIS is a language/taxonomy designed to help an organization hurdle over the issues many organizations are concerned about—sharing confidential data with outsiders. Without the capability to incorporate a common language (VERIS) designed to share incident information, the State of Idaho would never have been able to gain approval from various stakeholders (including the legal department) to share incident and breach information both internally (other agencies) and externally (DHS, FEMA, etc.).

Some of the areas in which VERIS has helped improve the State of Idaho's ability to share information are:

- It has created awareness and interest that there is a better way to gather and use intelligence information from adverse events that we respond to from time to time
- It is an open source framework that works well with other incident response frameworks
- It is an easy-to-use full-schema taxonomy/language designed to be incorporated and implemented within a short period of time

- It provides a way for business executives to get involved with their organization's cybersecurity efforts and simplifies intelligence gathering by repetitively asking four basic questions: Whose actions affected the asset? What actions affected the asset? Which asset was affected? How was the asset affected?

VERIS provides a solid language foundation that can be used to build a strong intelligence-driven incident response program. Couple that with other open source frameworks and you have one heck of an incident response program.

# Appendix E: Contributing organizations

---

## A

Akamai Technologies  
Apura Cyber Intelligence  
AttackIQ  
Australian Federal Police

---

## B

BeyondTrust  
Bit Discovery  
Bit-x-bit  
BitSight

---

## C

Center for Internet Security  
CERT European Union  
CERT Insider Threat Center  
CERT Polska  
Check Point Software Technologies Ltd.  
Chubb  
Cisco Talos Incident Response  
Coalition (formerly BinaryEdge)  
Computer Incident Response Center  
Luxembourg (CIRCL)  
CrowdStrike  
Cybercrime Central Unit of the Guardia  
Civil (Spain)  
CyberSecurity Malaysia, an agency  
under the Ministry of Science,  
Technology and Innovation (MOSTI)

---

## D

Defense Counterintelligence and  
Security Agency (DCSA)  
Dell (formerly EMC-CIRC)  
DFDR Forensics  
Digital Shadows  
Dragos, Inc.

---

## E

Edgescan  
Elevate Security  
Emergence Insurance

---

## F

F-Secure (formerly MWR InfoSecurity)  
Federal Bureau of Investigation—  
Internet Crime Complaint Center (FBI IC3)  
Financial Services Information  
Sharing and Analysis Center (FS-ISAC)

---

## G

Government of Telangana, ITE&C  
Dept., Secretariat  
Government of Victoria, Australia—  
Department of Premier and Cabinet (VIC)  
GreyNoise

---

## H

Hasso-Plattner Institut  
Hyderabad Security Cluster

---

## I

ICSA Labs  
Irish Reporting and Information  
Security Service (IRISS-CERT)

---

## J

JPCERT/CC

---

## K

Kaspersky  
KnowBe4

---

## L

Lares Consulting  
LMG Security

---

## M

Malicious Streams  
Micro Focus (formerly Intersect)  
Mishcon de Reya  
mnemonic  
Moss Adams (previously AsTech Consulting)

---

## N

National Cybersecurity and  
Communications Integration Center (NCCIC)  
NetDiligence  
NETSCOUT

---

## P

Paladion Networks Pvt Ltd.  
Palo Alto Networks  
ParaFlare Pty Ltd  
Proofpoint (formerly Wombat Security)

---

## Q

Qualys

---

## R

Rapid7  
Recorded Future

---

## S

S21sec  
SecurityTrails  
Shadowserver Foundation  
Shodan  
SISAP—Sistemas Aplicativos  
SwissCom

---

## T

Tetra Defense (formerly Gillware  
Digital Forensics)  
Tripwire

---

## U

United States Computer Emergency  
Readiness Team (US-CERT)  
U.S. Secret Service

---

## V

VERIS Community Database  
Verizon Cyber Risk Programs  
Verizon DDoS Shield  
Verizon Digital Media Services  
Verizon Managed Security Services—  
Analytics (MSS-A)  
Verizon Network Operations and Engineering  
Verizon Professional Services  
Verizon Threat Research Advisory  
Center (VTRAC)  
Vestige, Ltd.  
VMRay

---

## W

Wandera  
WatchGuard Technologies

---

## Z

Zscaler

