NATIONAL ASSOCIATION OF Community Health Centers®

Cybersecurity: Know the Basics and Ask the Right Questions

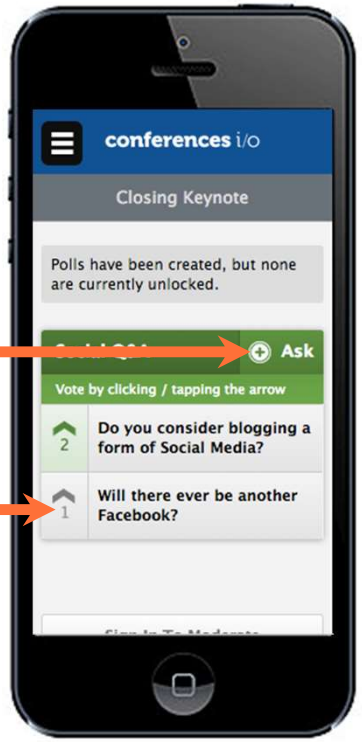
Monday October 31

Virtual Participants

Chat
(use to talk with peers)

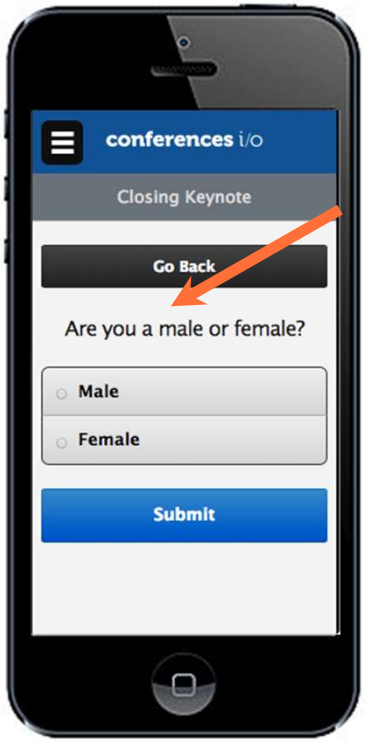
Polling/Q&A
(participate in polls, ask questions to faculty)

In-Person Participants



Give us Feedback

Up-Vote a Comment



Click on question and then Respond to Polls when they appear

Vote / Give Feedback/ Respond to Polls

THE NACHC MISSION

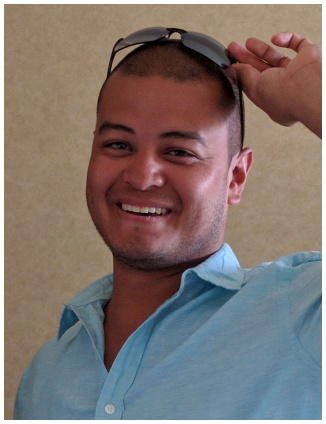
America's Voice for Community Health Care

The National Association of Community Health Centers (NACHC) was founded in 1971 to promote efficient, high quality, comprehensive health care that is accessible, culturally and linguistically competent, community directed, and patient centered for all.

NATIONAL ASSOCIATION OF Community Health Centers®

Meet Your Speakers

Arnel Mendoza
Director of Information Systems
QueensCare Health Centers



Nick Rosario
Independent Security Researcher
Chenb0x Development

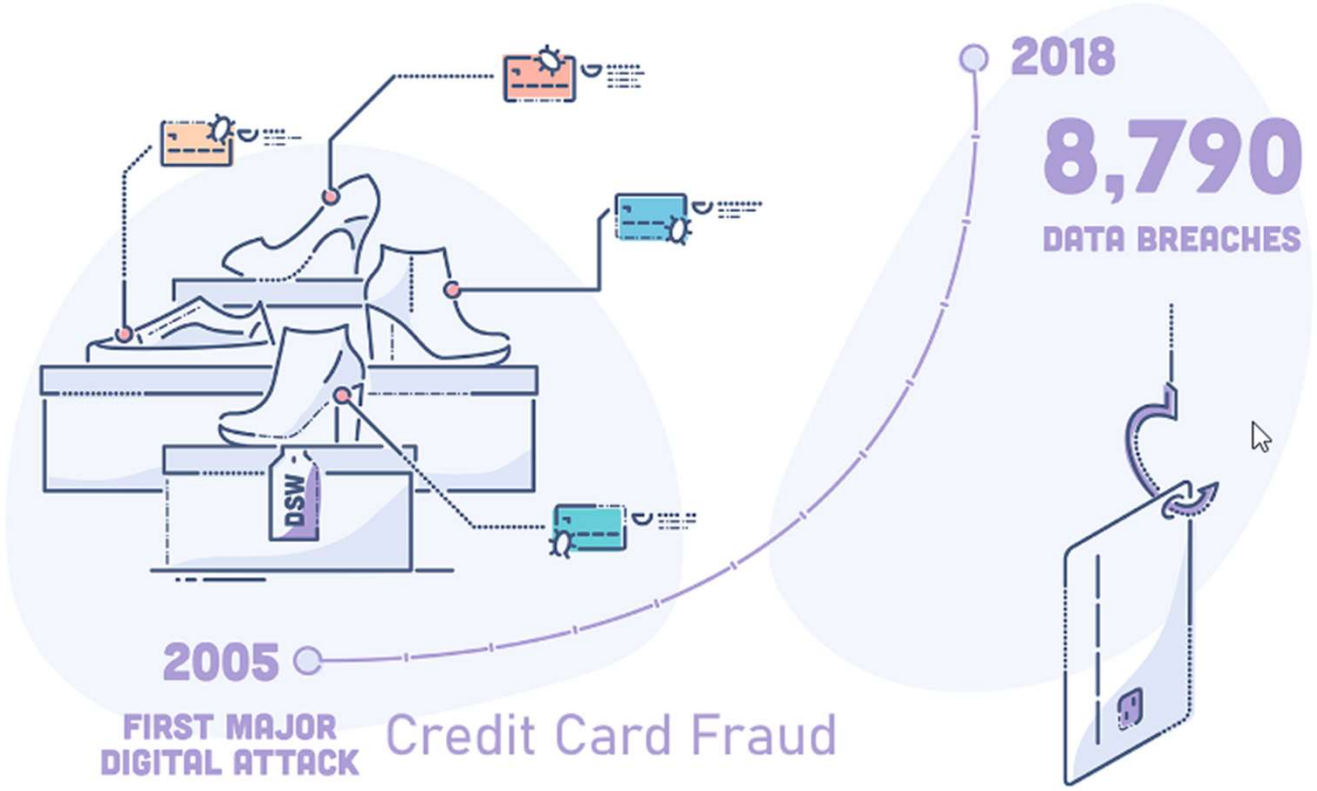
Understanding Cybersecurity

1. What's The Big Deal?
2. Could It Happen to My Organization
3. How Do I Know Where I Am Most Vulnerable
4. What Do I Do If I Get Breached
5. How Much Should You Be Spending On Cybersecurity
6. Cultivating A Culture of Cybersecurity Awareness

The Basics

A Basic Infrastructure protects.
A Good Infrastructure enables.
A Great Infrastructure innovates.

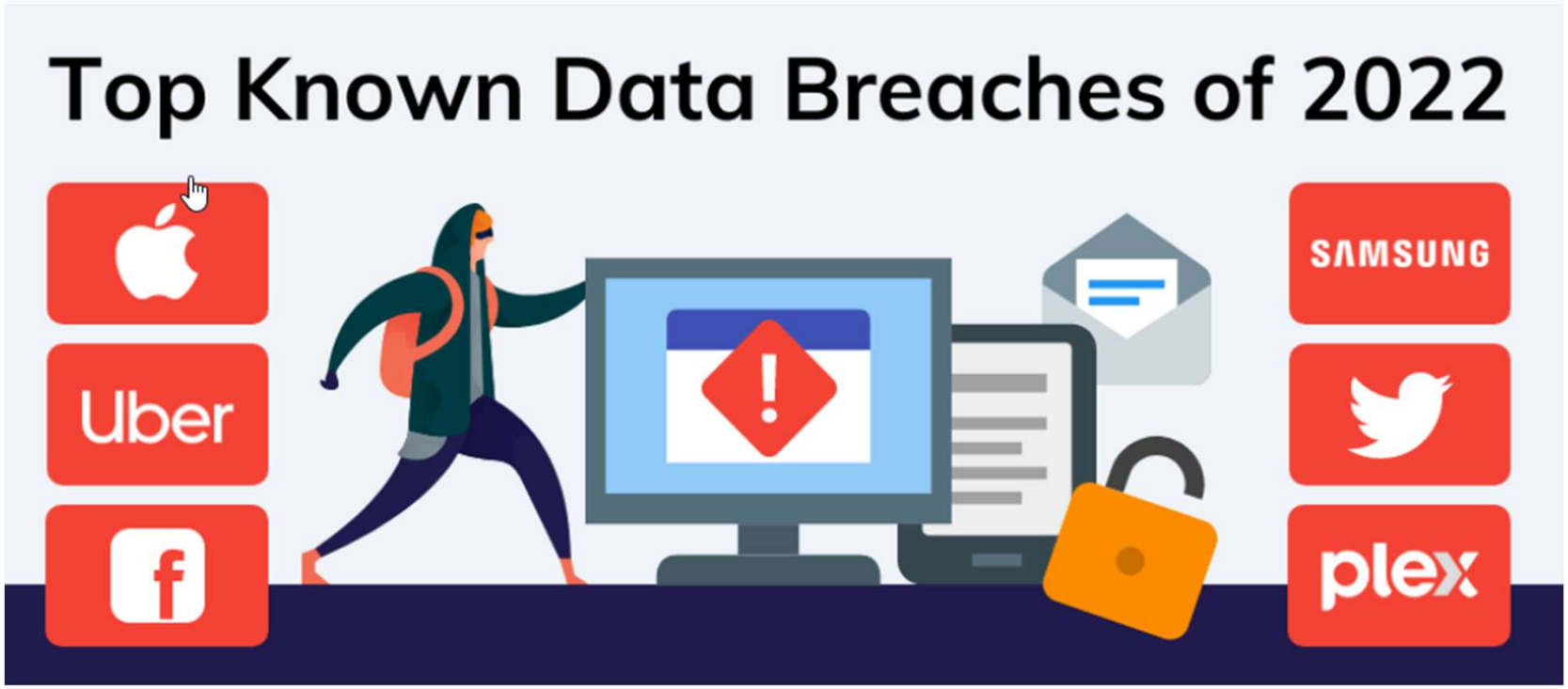
Evolution of Data Breaches



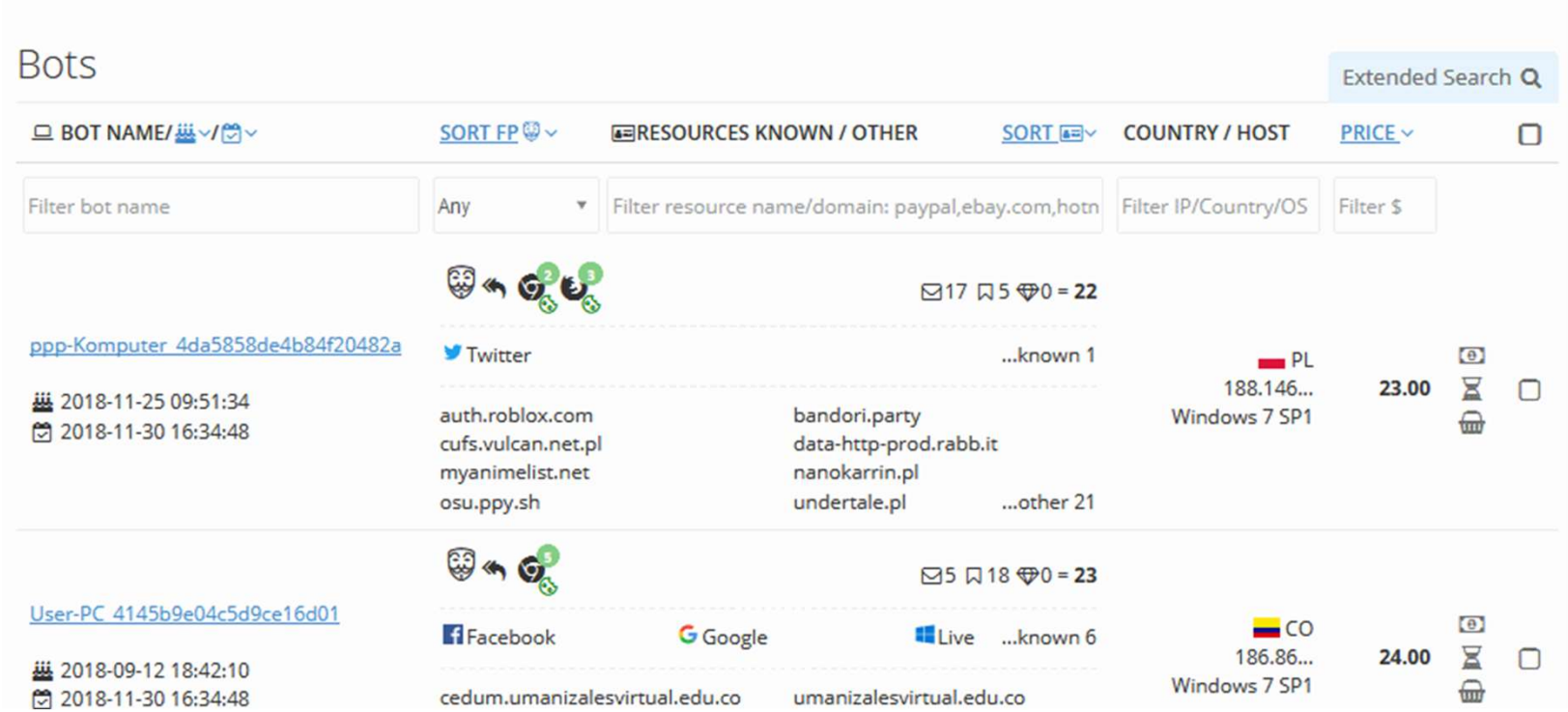
Global Cost of Cybercrime 2022

- The bad guys got better at being badder, FASTER.
- Cybercrime is now more profitable than the Global Drug Trade!

Top Breaches: 2022

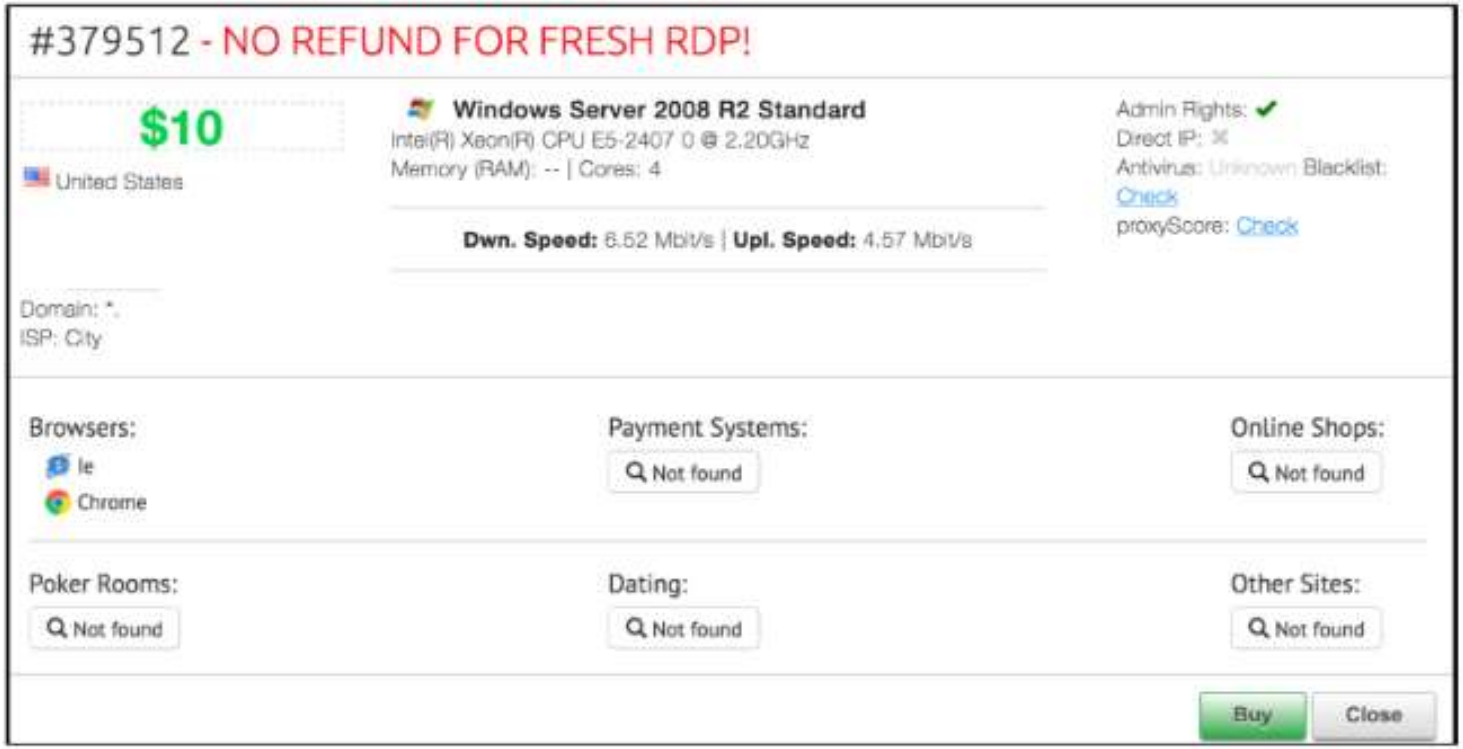


Malware Bots Are Easily Bought



Source: Genesis Marketplace Help Page (Dark web)

Corporate Credentials Are Easily Purchased



Source: HelpNetSecurity

Dark Web Price Index 2022

Category		Price
Credit Card Data	Credit Card details, account balance to $5000	$120
	Credit Card details, account balance up to $1000	$80
Payment Processing Svcs	Paypal transfer from stolen account $1,000 - $5000 balances	$45
Crypto Accounts	Kraken verified account	$250
	Hacked Coinbase verified account	$120
Social Media	Hacked Facebook account	$45
	Hacked Instagram account	$40
Hacked Services	Netflix account 1-yr subscription	$15
Malware	USA, Can, UK, AU med quality 70% success rate per 1,000 installs	$1200
	Europe low-quality slow-speed low success rate	$120

Source: Privacy Affairs

5 Most Common Ways Credentials Are Stolen

- Phishing
- Use of Malware/Bots
- Bad Websites
- Brute Force (Weak Passwords)
- Public WiFi

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Do you know any community health center that has been affected by a data breach?

Industry Impact: XXX Community Health Center (REAL)

- A community Health Center in Los Angeles, CA was hit by ransomware on Feb 2021

- Zeppelin ransomware was triggered by a phishing attack
- 26,000+ patient records were exfiltrated
- All systems were encrypted at block level, including backups
- Forensics determined threat actors had access to the system as early as a week earlier
- Ransom was paid
- Thousands of man-hours were spent on immediate remediation (15-17 hour days)
- Full access to systems were not recovered for at least 5 days

NATIONAL ASSOCIATION OF Community Health Centers®

Live Content Slide

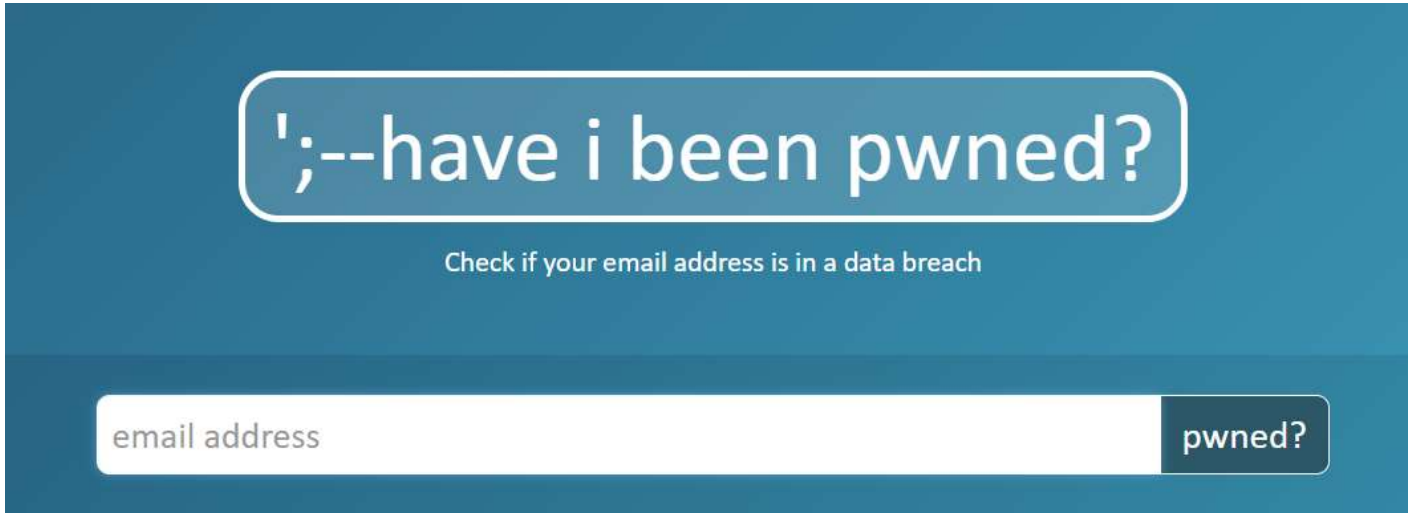
When playing as a slideshow, this slide will display live content

Poll: If your organization is hit by ransomware, should you pay to get your data back?

Cost of A Data Breach

The Healthcare Industry had the highest cost of data breach of all industries
Source: IBM Cost of A Data Breach Report 2022

Exercise: Have Your Credentials Been Stolen?



https://haveibeenpwned.com

Could It Happen To My Organization?

Data Breach Response Times

Healthcare Industry Statistics:

- Average Number of Days to Detect a Data Breach: 277
- Average Number of Days to Contain a Breach: 103
- Combined, that is an ENTIRE YEAR

Source: ©IBM Security Cost of a Data Breach Report 2021

From the California Attorney General's Website

Organization Name	Date(s) of Breach	Reported Date
Keck Medicine of USC	01/20/2022	09/30/2022
County of Los Angeles Department of Public Health	07/01/2020	08/23/2022
Anthem Blue Cross	05/07/2022	09/28/2022
San Diego American Indian Health Center	05/05/2022	08/15/2022
Northern California Fertility Medical Center	07/24/2022	09/28/2022
Kaiser Foundation Health Plan, Inc., Southern California	05/20/2022	07/15/2022
Humana	05/07/2022	09/21/2022
Radiology Associates of Albuquerque and Advanced Imaging, LLC.	12/22/2020, 08/03/2021	09/09/2022
Covenant Care California, LLC	02/24/2022, 05/03/2022	09/01/2022
AllOne Health	09/01/2021, 03/24/2022	07/20/2022
Pandemic Response Lab	09/06/2021	06/24/2022

How Do You Know You Haven't Been Breached Already?

Don’t Be The Low Hanging Fruit For Hackers

You have to make your infrastructure hardened and secure enough so the bad guys move on to an easier target.

What To Do First: Quantify Your Risk

If you want to know what to spend on for cybersecurity, you must first determine where you are most vulnerable.

Basic Assessment Tools

https://www.flex-protection.com/#self

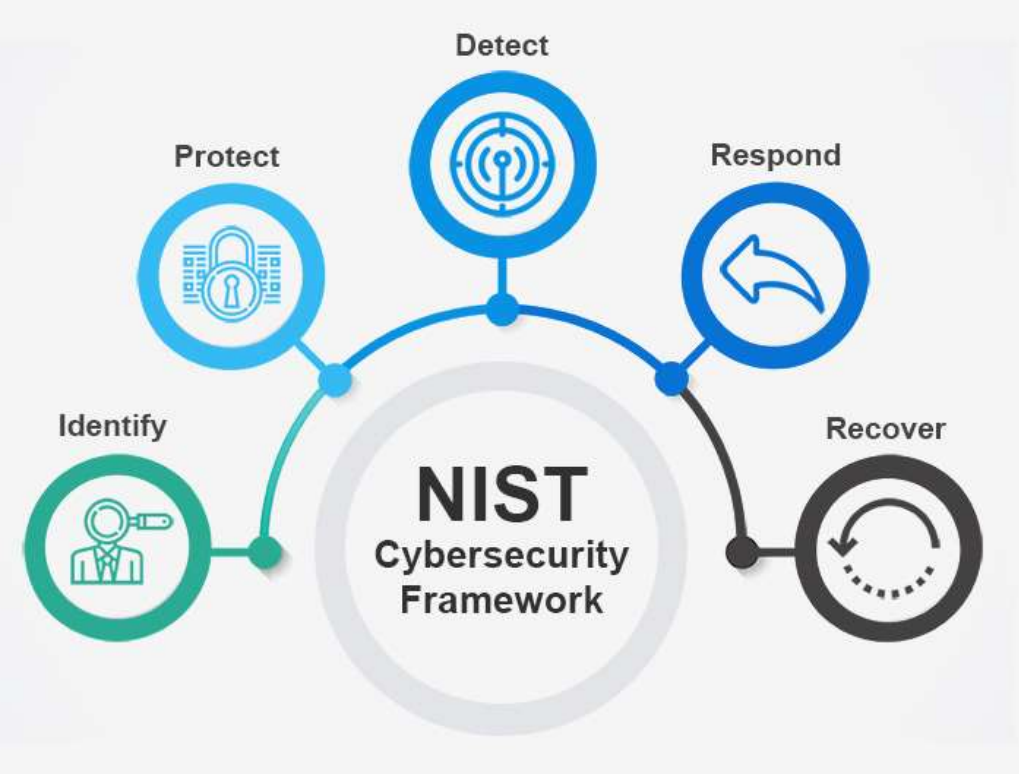
Security Self-Assessment

Please select the response that best represents your company or organization for each risk factor.

Flex-Protection Security+ CERTIFIED

Do you have a written Information Security Policy that is endorsed and supported by top management?	Yes
How often are employees and management given Security Awareness Training (SAT)?	At least annually
Do you have a documented Data Inventory - a list of key data stores, where they are located, and how they are protected?	Yes, and it's current
Is there a convenient list of Security Best Practices that all computer users are familiar with?	Yes, everyone is familiar
Is critical data backed up automatically every day, onto separate computers used for this purpose?	Yes, automated and verified
Does your company have remote or traveling employees who need network access?	No, everyone works on site
Have you had a network vulnerability scan or professional security assessment from a third party consultant or advisor?	Yes, on a regular basis
Does your company or organization have a public-facing web site?	No web site
Are you covered by a Data Defender subscription to insure best practices and basic documentation?	Enterprise Data Defender in place
First Name / Last Name / Phone Number / Work E-mail	DISPLAY RESULT

NIST Cybersecurity Framework



Identify	This function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
Protect	This function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
Detect	This function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.
Respond	This function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
Recover	This function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

NIST Cybersecurity Framework

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Funtion	Category	Sub Category
Identify	6	29
Protect	6	39
Detect	3	18
Respond	5	16
Recover	3	6

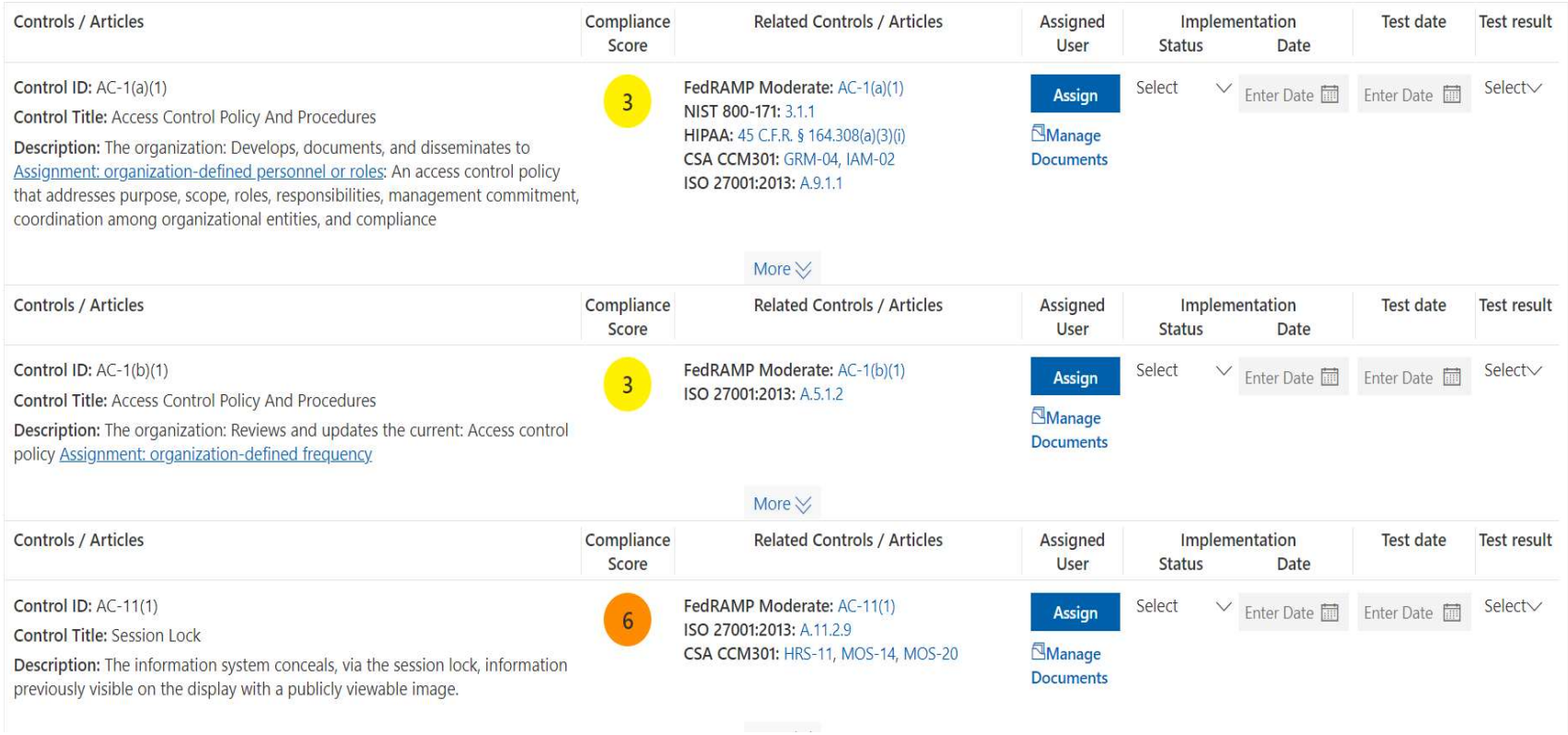
108 Total Questions

NIST Assessment Tools Are Available Online For Free

https://info.cipher.com/information-security-maturity-self-assessment-survey?hsCtaTracking=74bb7494-7d0f-4858-a7f3-c3fcf5bd62e3%7C3d2dffce-c1b0-46bd-9b4e-83d081ef2f0b

https://info.expel.io/NIST-CSF-Tool-Thank-you.html?aliId=eyJpIjoiTmdZY250bVJ5UTVFelEwciIsInQiOiIzRW85SXlqXC9UUGptN0thTkRNNUhTQT09In0%253D

Office 365 Has an NIST Governance Tool



Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-1(a)(1) **Control Title:** Access Control Policy And Procedures **Description:** The organization: Develops, documents, and disseminates to Assignment: organization-defined personnel or roles: An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	3	**FedRAMP Moderate:** AC-1(a)(1) **NIST 800-171:** 3.1.1 **HIPAA:** 45 C.F.R. § 164.308(a)(3)(i) **CSA CCM301:** GRM-04, IAM-02 **ISO 27001:2013:** A.9.1.1	Assign Manage Documents	Select	Enter Date	Enter Date	Select
More							

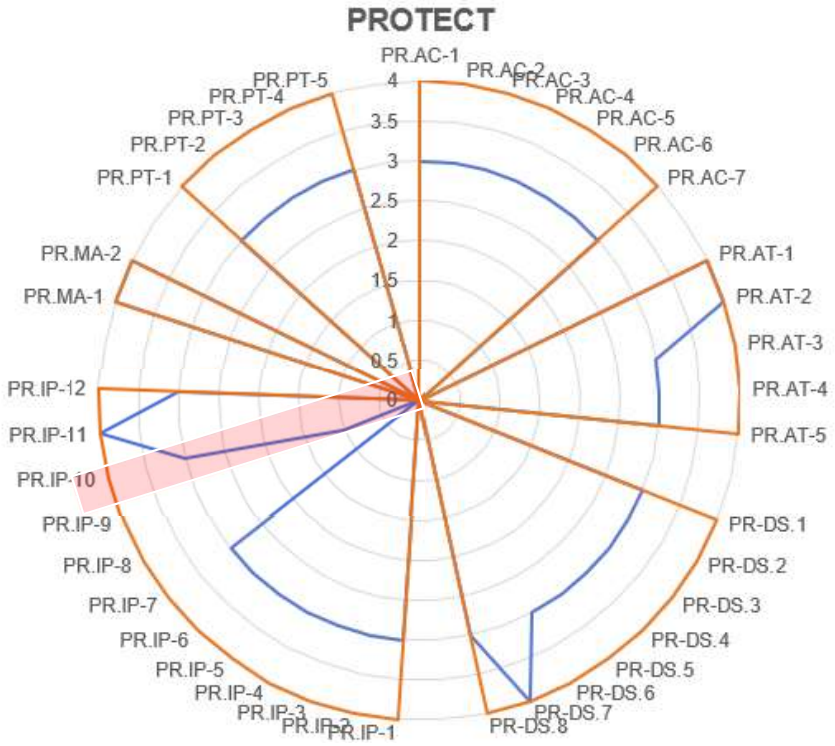
Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-1(b)(1) **Control Title:** Access Control Policy And Procedures **Description:** The organization: Reviews and updates the current: Access control policy Assignment: organization-defined frequency	3	**FedRAMP Moderate:** AC-1(b)(1) **ISO 27001:2013:** A.5.1.2	Assign Manage Documents	Select	Enter Date	Enter Date	Select
More							

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-11(1) **Control Title:** Session Lock **Description:** The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	6	**FedRAMP Moderate:** AC-11(1) **ISO 27001:2013:** A.11.2.9 **CSA CCM301:** HRS-11, MOS-14, MOS-20	Assign Manage Documents	Select	Enter Date	Enter Date	Select

Fill Out The Spreadsheet Assessment

Protect: Self-scoring worksheet (note: enter an "as is" and "to be" score, from 0 to 5, in column D and E .
Identity Management
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-2: Physical access to assets is managed and protected
PR.AC-3: Remote access is managed
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate
PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security an
Awareness and Training
PR.AT-1: All users are informed and trained
PR.AT-2: Privileged users understand roles and responsibilities
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities
PR.AT-4: Senior executives understand roles and responsibilities
PR.AT-5: Physical and information security personnel understand roles and responsibilities
Data Security
PR.DS-1: Data-at-rest is protected
PR.DS-2: Data-in-transit is protected
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
PR.DS-4: Adequate capacity to ensure availability is maintained
PR.DS-5: Protections against data leaks are implemented

A Heatmap of Your Biggest Vulnerabilities



Example Weakness:
PR.IP-10: Response and recovery plans are tested

Know Your Risks/Vulnerabilities

- 3rd Party Internal and External Network Penetration Testing.
- You don't know what you don't know.

Test Your Organization– Penetration Testing

- Assessing the true security of your Organization
- Mimic what a true malicious actor would due when targeting your network
- Ensure Compliance
- Create an Action Plan to prioritize your vulnerabilities as part of your security program
- Test all aspects of your security posture – Network, Applications, and Physical
- Best

NATIONAL ASSOCIATION OF Community Health Centers®

Health Choice Network
a Family of Health Centers
25+ Years of Service

Cybersecurity Best Practices

PEOPLE

- Password/User M
- Security Awarene
- Organizational Cu
- Compliance
- Security Awarene
- HIPAA & Cyber Ed staff
- Security Officer/L
- Role-Based Acces

PROCESS

- ngoing Risk Management
- ata Backup
- yber-insurance in place
- ompliance
- cident Response
- usiness Continuity Processes
- etwork Pen Testing
- ngoing Audits

- Intrusion Protection Systems
- Device Encrypsion
- Segmented Networks
- MFA (Multi-Factor Auth

Cybersecurity Basics: GCA Cybersecurity Toolkit

1. Know What You Have
2. Update Your Defenses
3. Beyond Simple Passwords
4. Prevent Phishing and Malware
5. Backup and Recover
6. Protect Your Email and Reputation

Adapted from https://gcatoolkit.org/

Free Tools from CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Free Cybersecurity Services and Tools | CISA
https://www.cisa.gov/free-cybersecurity-servies-and-tools

A Word About Free/Low Cost Tools

When talking to vendors, always use the magic words: **NON-PROFIT PRICING**
Always look for **FREE** or **SIGNIFICANTLY DISCOUNTED** resources

monday.com for nonprofits

SALESFORCE FOR NONPROFIT

Microsoft 365 resources for nonprofits

Google for Nonprofits.

Mobile Beacon for Nonprofits

Nessus Essentials free vulnerability assessment solution

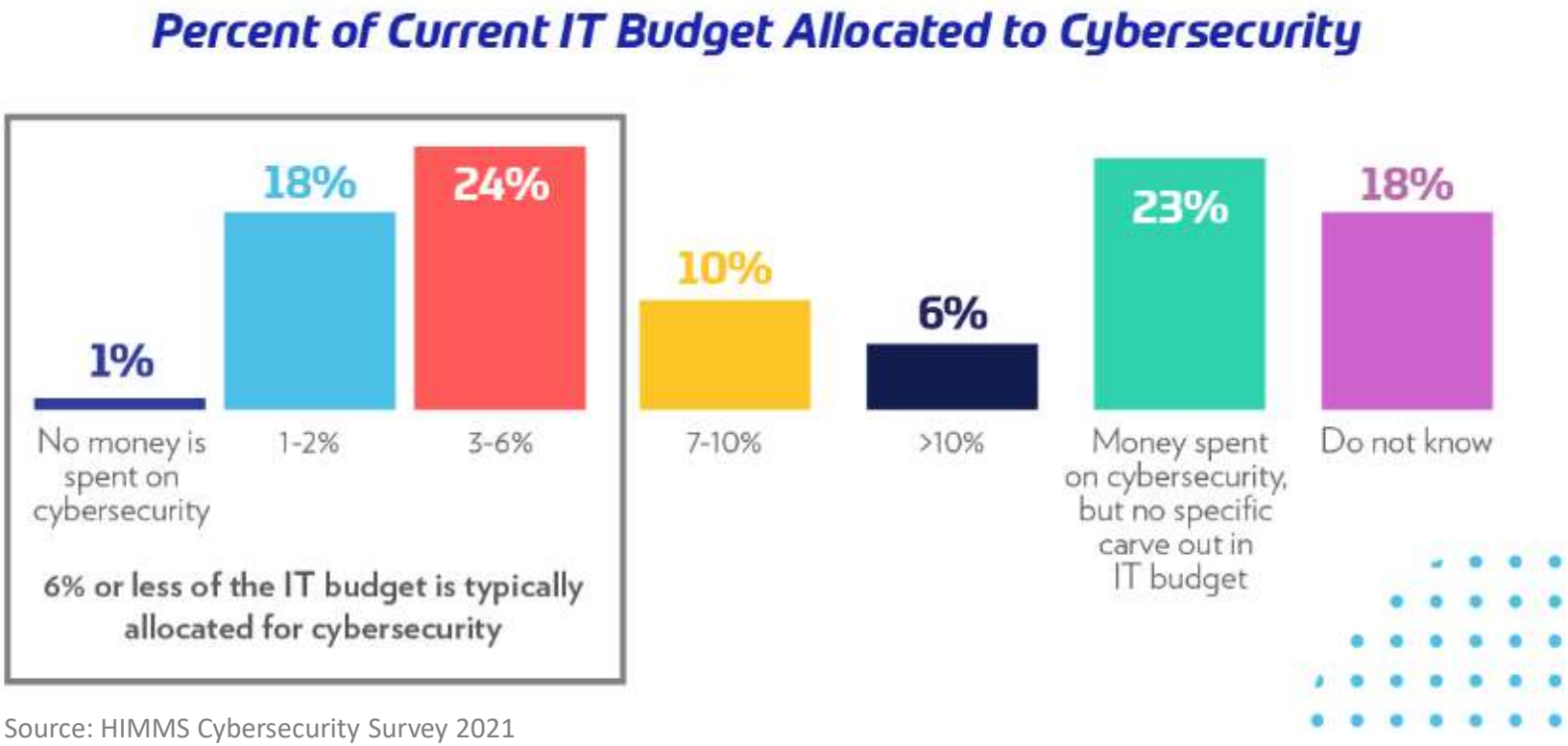
CISA's Cyber Hygiene Vulnerability Scanning email vulnerability@cisa.dhs.gov

prey **DEVICE TRACKING & PROTECTION**

Cloudflare Universal SSL certificate FREE

GRR RAPID RESPONSE Incident Response Framework

How Much Are You Spending For Cybersecurity?



Source: HIMMS Cybersecurity Survey 2021

Why Is This That Important?

Technology Leaders Must Learn to Speak the Language of the C-Suites.

01234
56789

$$ $$
$$ $$

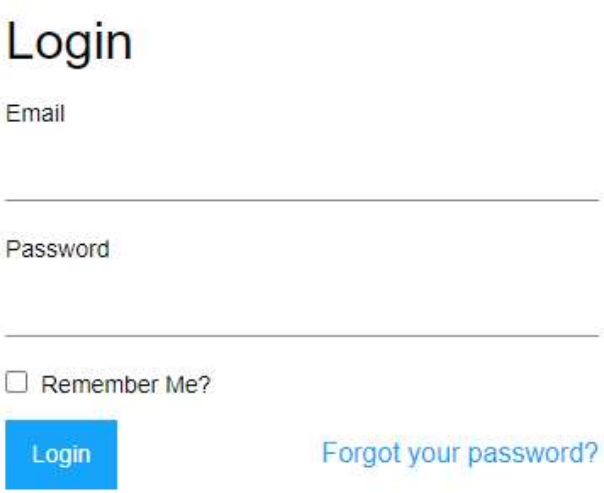
What the Pros Use: FAIR

One globally recognized security risk quantification methodology is the **Factor Analysis of Information Risk (FAIR™)**. It is a model that codifies and monetizes risk.

In other words, it breaks down risk by identifying and defining the building blocks that make up risk and their relationship to one another. The relationships between each building block or element of risk can be measured mathematically and assigned dollar values, so that ultimately risk can be calculated as financial loss exposure.

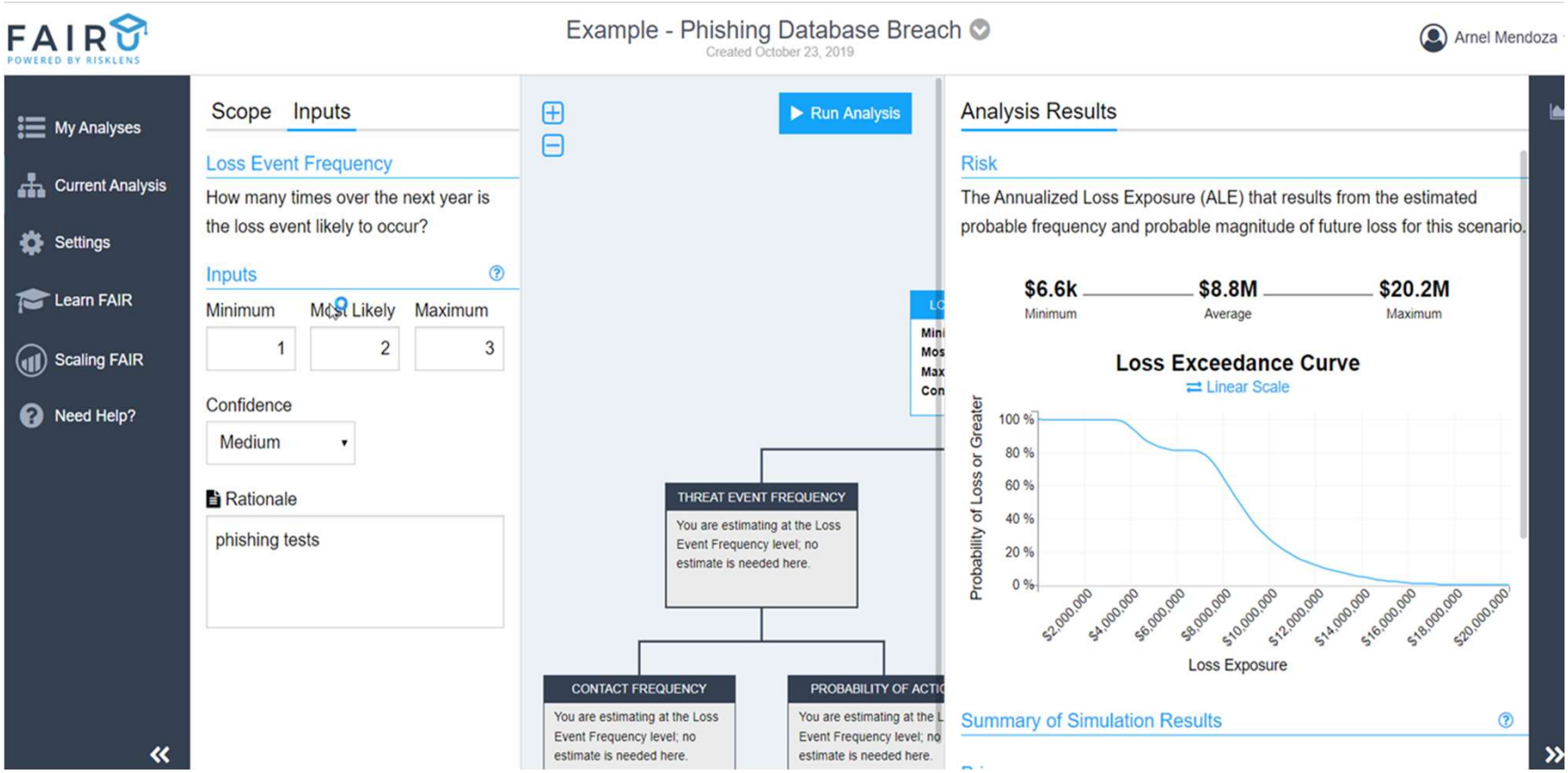
The Tool <FREE!>

FAIR U
POWERED BY RISKLENS



https://app.fairu.net/

FairU Example



The Gold Standard

Source: RiskLens

Where Does A Data Breach Start?

Source: HIMMS Cybersecurity Survey 2021

Phishing Statistics

- According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing.

- According to Verizon's 2021 Data Breach Investigations Report, 85% of breaches involved the human element.

The Human Error Factor

• Unintentional human error can be due to lack of organized knowledge or operating skills. This error may remain unintentional or transforms to another type (intentional or malicious).

• Intentional human error is caused by a user who knows of risky behavior but acts on it, or misuses assets. The wrong action may not necessarily bring a sudden harm to the organization, but it may still breach of existing laws or privacy.

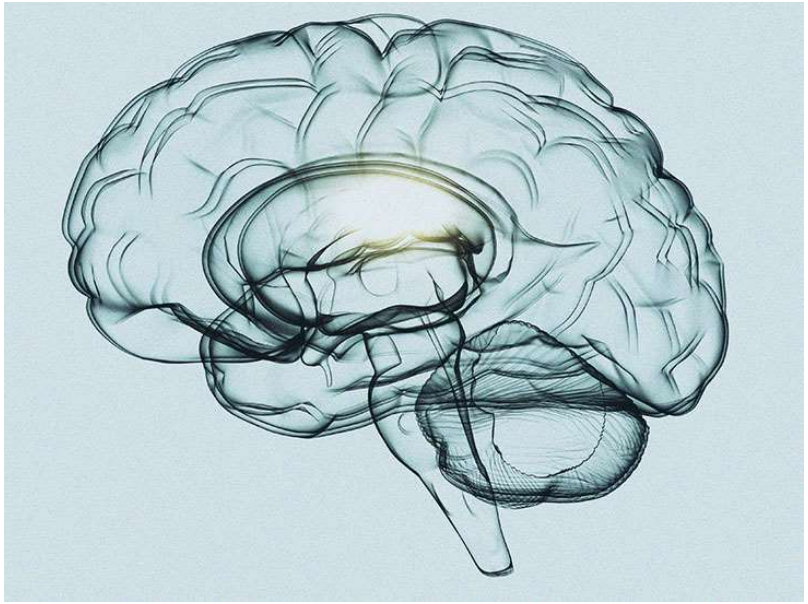
• Malicious human error is the worst error as it is intentional with specific and damaging consequences in mind.

What Did That Click Cost?

From the report Sophos State of Ransomware 2021, the average ransom paid by mid-sized organizations was **$170,404** while the average cost of resolving a ransomware attack was **$1.85 million**. This cost includes downtime, people time, device cost, network cost, lost opportunity, ransom paid, higher cybersecurity insurance premiums.

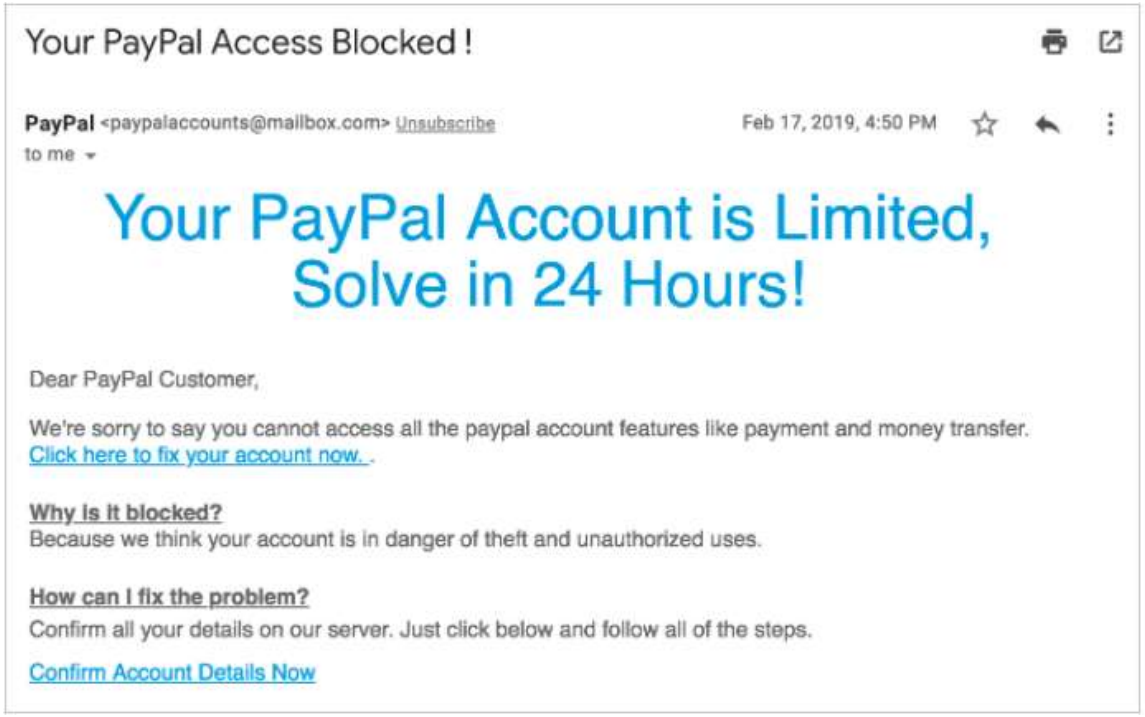
Why Do People Click? A Little Brain Science

Fact: The emotional brain is both quicker and stronger than the logical brain. Emotions, like fear and urgency, sidestep the frontal lobe and smack us right square in the amygdala, triggering a Fight or Flight Response



Continued:

Hackers trying to get access to your information, will introduce a psychological stressor, say in the form of a threatening email…



Your PayPal Access Blocked !

PayPal <paypalaccounts@mailbox.com> Unsubscribe

Feb 17, 2019, 4:50 PM

to me

Your PayPal Account is Limited, Solve in 24 Hours!

Dear PayPal Customer,

We're sorry to say you cannot access all the paypal account features like payment and money transfer.
Click here to fix your account now. .

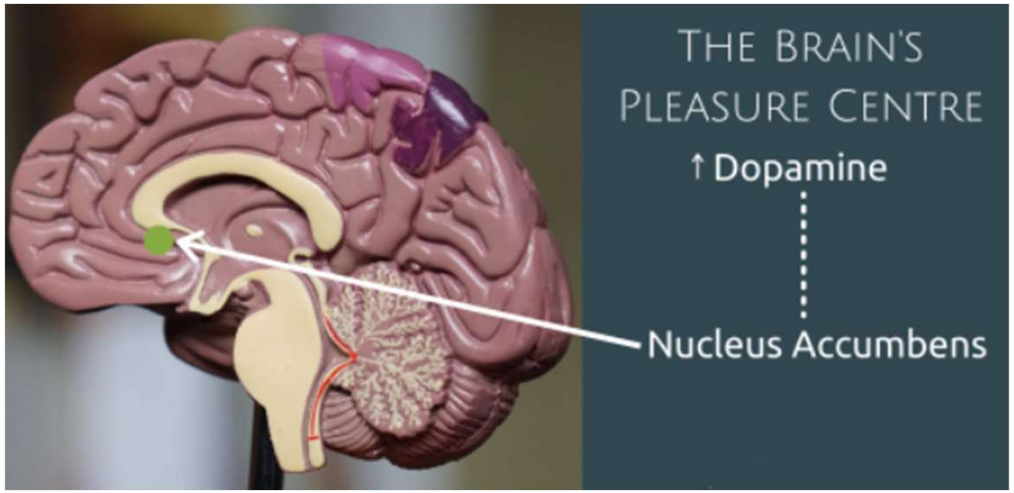
Why is it blocked?
Because we think your account is in danger of theft and unauthorized uses.

How can I fix the problem?
Confirm all your details on our server. Just click below and follow all of the steps.

Confirm Account Details Now

Other Brain Hijacks

Humans have been found to have similar reactions to surprise rewards – specifically the anticipation of the reward. A pleasure center of the brain called the nucleus accumbens is highly activated by the possibility of receiving a reward.



Unexpected Rewards

Claim Your Tax Refund Online

We identified an error in the calculation of your tax from the last payment, amounting to $ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

When Emotions Take Over People Click

- **STRESS** Too busy/pre-occupied to pay close attention
- **FEAR** "Do this now, or else…"
- **OVERCONFIDENCE** Overly optimistic at our ability to recognize a phishing email
- **GREED** The unexpected reward
- **HIERARCHY AND AUTHORITY** People tend to comply with requests from authority figures, particularly in the organization

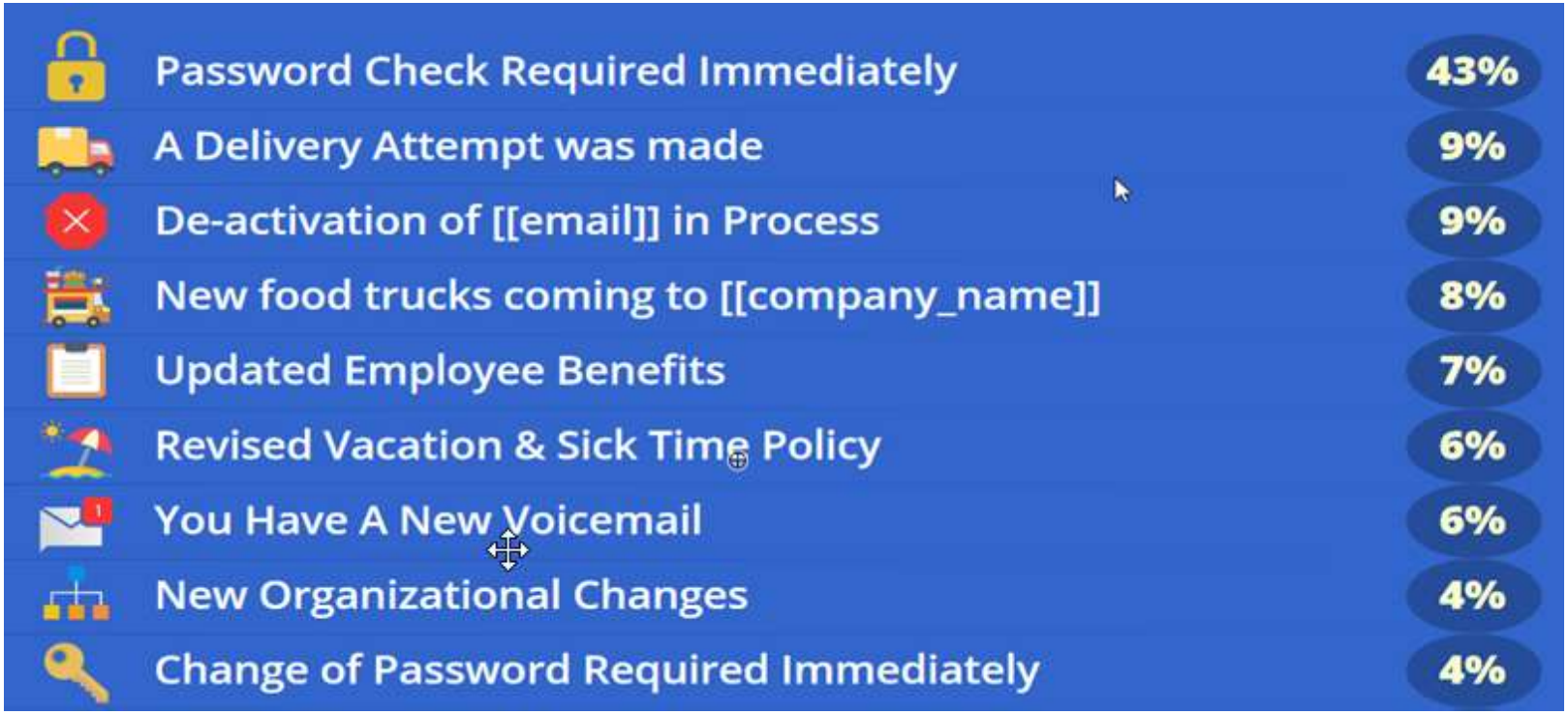
The Power of Authority

Excellent, I need you to head to the nearest store and make a purchase of 10 Visa or Amex gift cards at $500 face value each since they'll have a different selection of gift cards. How soon can you get it done? Because I'll be glad if you can get the purchase done ASAP.

Also, you are getting your payback by the end of the day, So you have nothing to worry about your reimbursement. I assure you of this. And guess what? I also have a surprise for you.

I want this to come as a surprise pending when the lucky ones receive it since we understand it's to come as a surprise to them.

Top Phishing Email Subjects



How Do You Cultivate A Culture of Cybersecurity Awareness?

- A one-hour training given annually is not enough.
- A culture of cybersecurity awareness is something that is cultivated.
- You MUST train like a NINJA!

THE SINGLE MOST IMPORTANT SKILL

HOVER over a link

- If the email appears to be coming from a company, **does the hover link match** the website of the sender?
- Does link have a **misspelling** of a well-known website (Such as Micorsoft.com)?
- Does the link **redirect to a suspicious external domain** appearing to look like the sender's domain (i.e. micorsoft-support.com rather than microsoft.com)?
- Does the hover link show a URL that **does not match where the context** of the email claims it will take you?
- Do you **recognize** the link's address or did you even **expect to receive** the link?
- Did you receive a **blank email** with **long hyperlinks** and no further information or context?

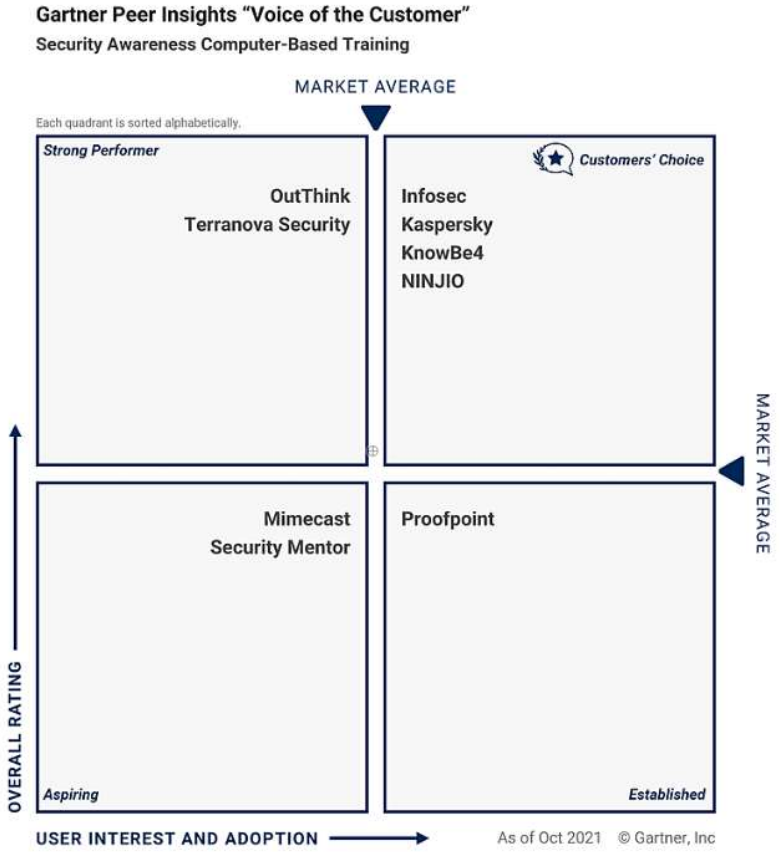
The OTHER Single Most Important Skill

Research shows that it takes 6 seconds for the brain chemicals that caused the brain hijack to diffuse.

Good Email Anti-Phishing Hygiene

- Assume that there's something phishy about every link in every email
- Pay attention
- What is the email trying to get you to do?
- How is it trying to get you to do it?
- Remember the 6-second rule.

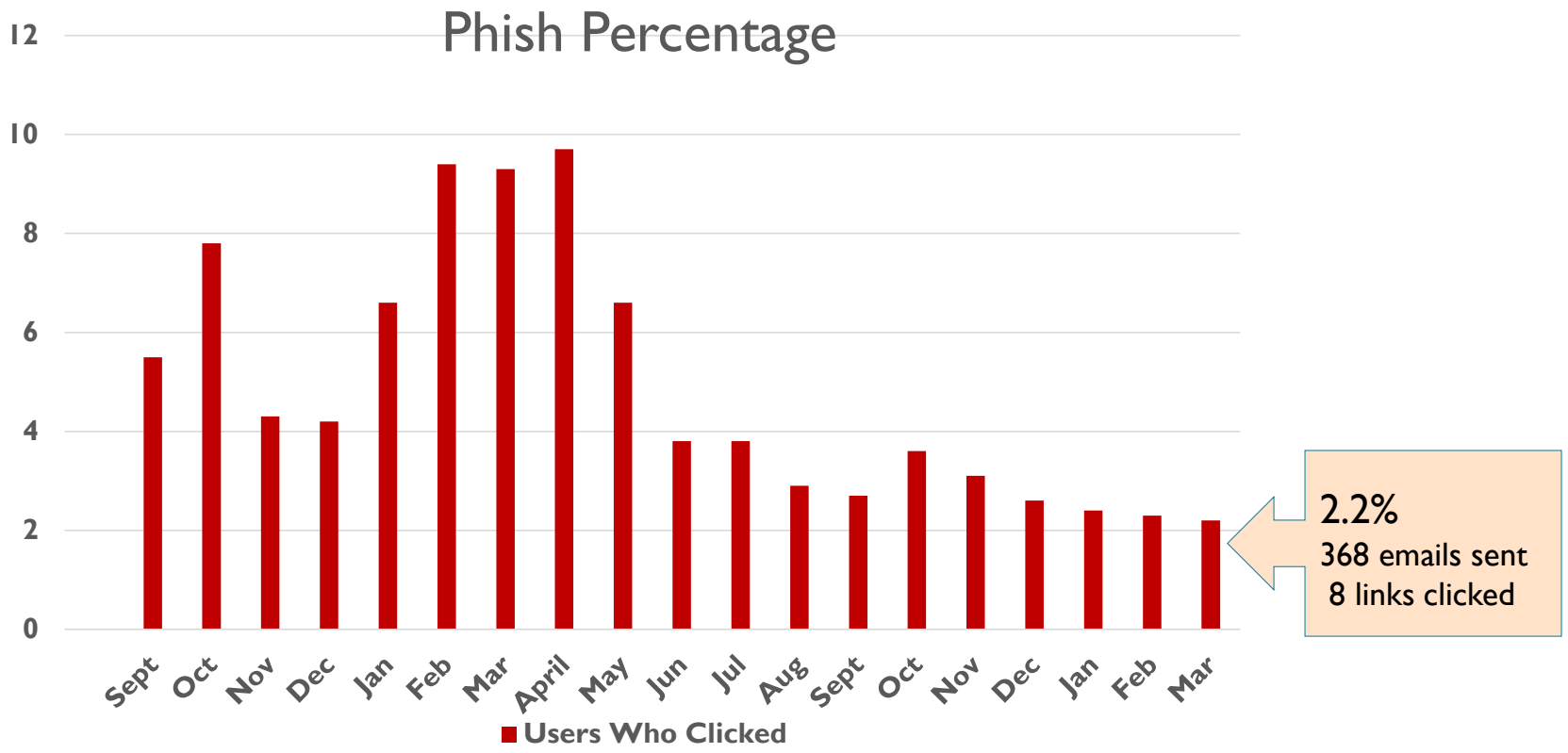
Security Awareness Platforms



Cultivating a Cybersecurity Awareness Culture

- Phishing Tests done monthly
- “Clickers” automatically have to take online training class.
- Supervisors are notified and will get reminders if their staff do not complete training.
- Targeted mini-trainings implemented for groups identified as high-risk (e.g. MAs that have been with the company less than 6 mos., or users that have clicked 3x in the past year)

Testing Is Essential



Source: QueensCare Health Centers

Identify Patterns

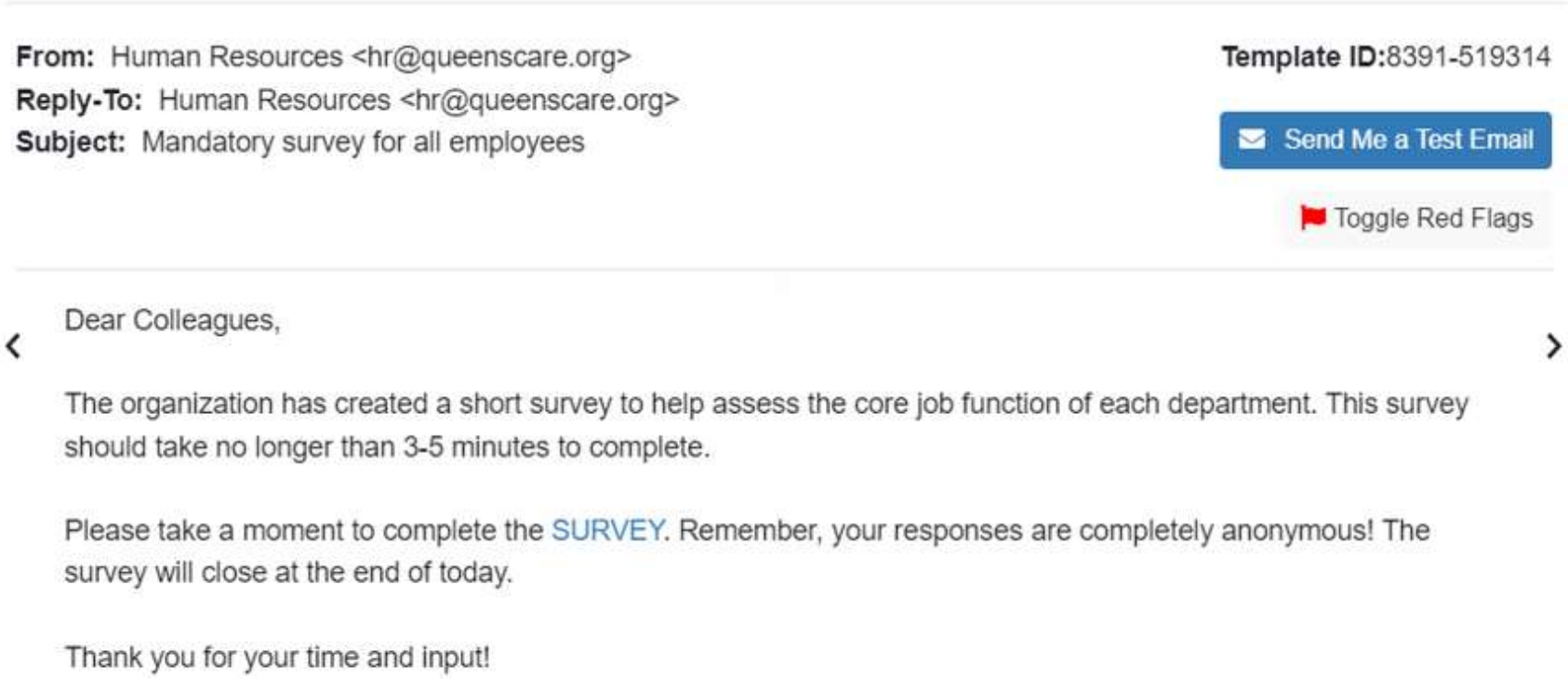
By Job Group

Community Health	1
MA/DA	4
Provider MD/NP/DDS/MH	0
HA/PSR/PAC/CTS	1
Admin/Finance/HR/ Business Services/Fac/ Executive Mgmt	2

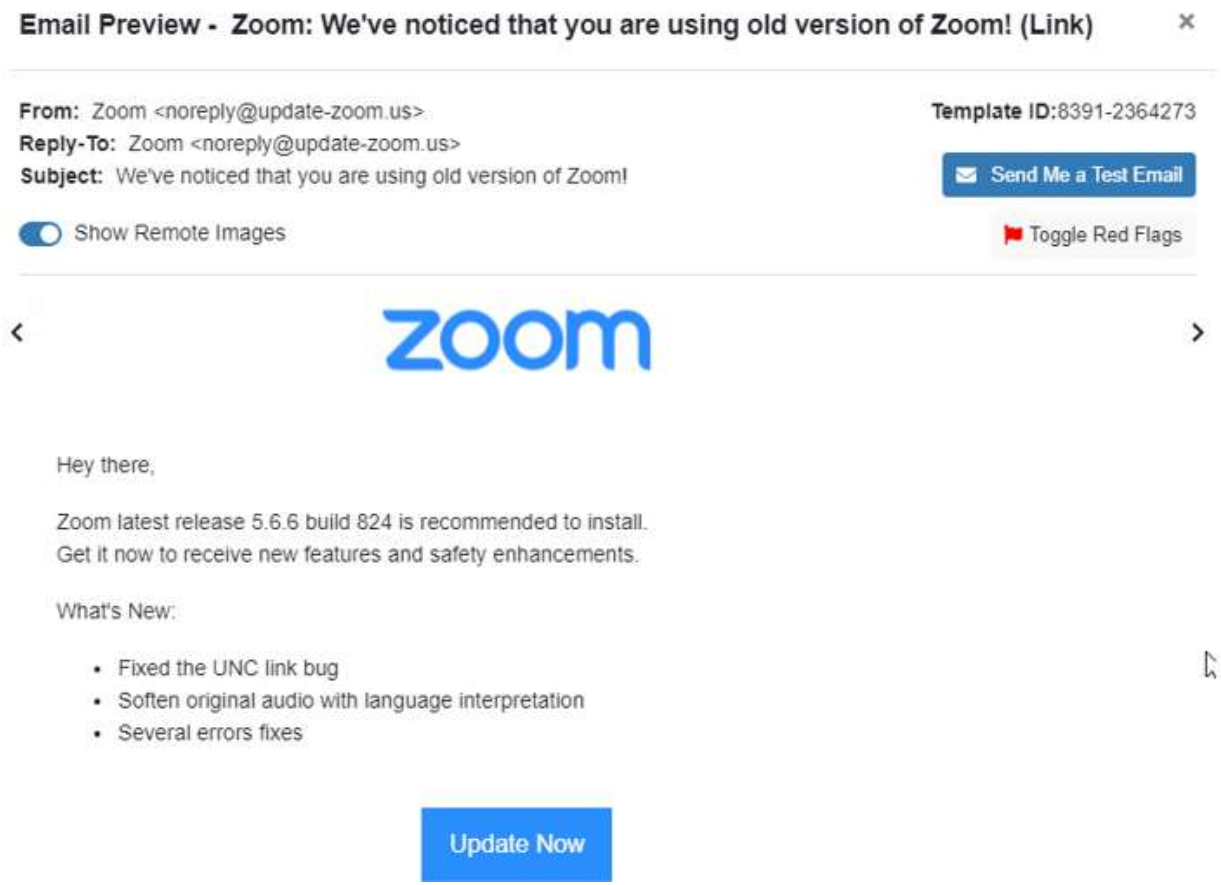
By Location

Location 1	4
Location 2	0
Location 3	0
Location 4	1
Location 5	1
Corporate Office	2

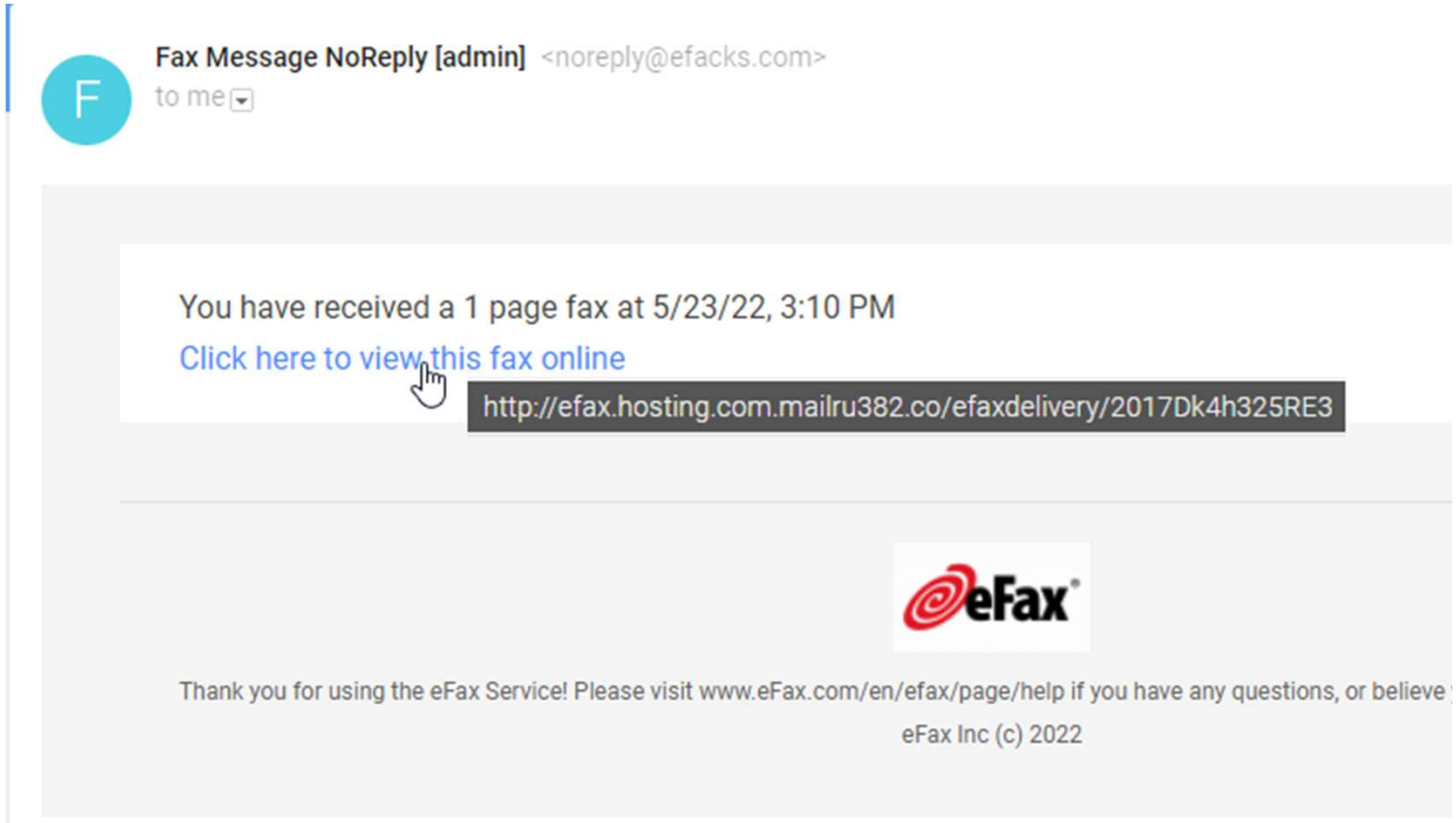
Let Them Know What They Clicked On



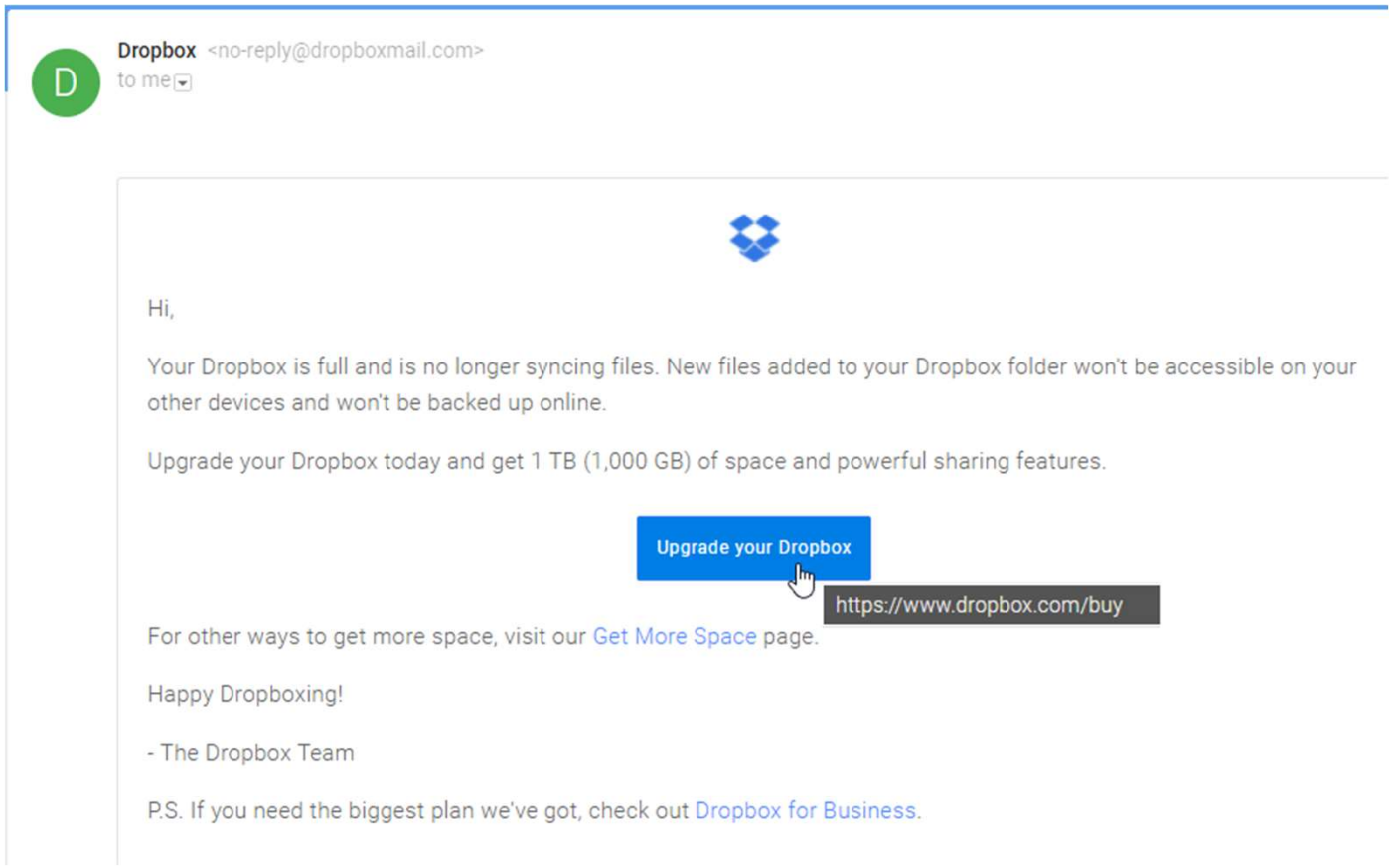
Examples - Continued



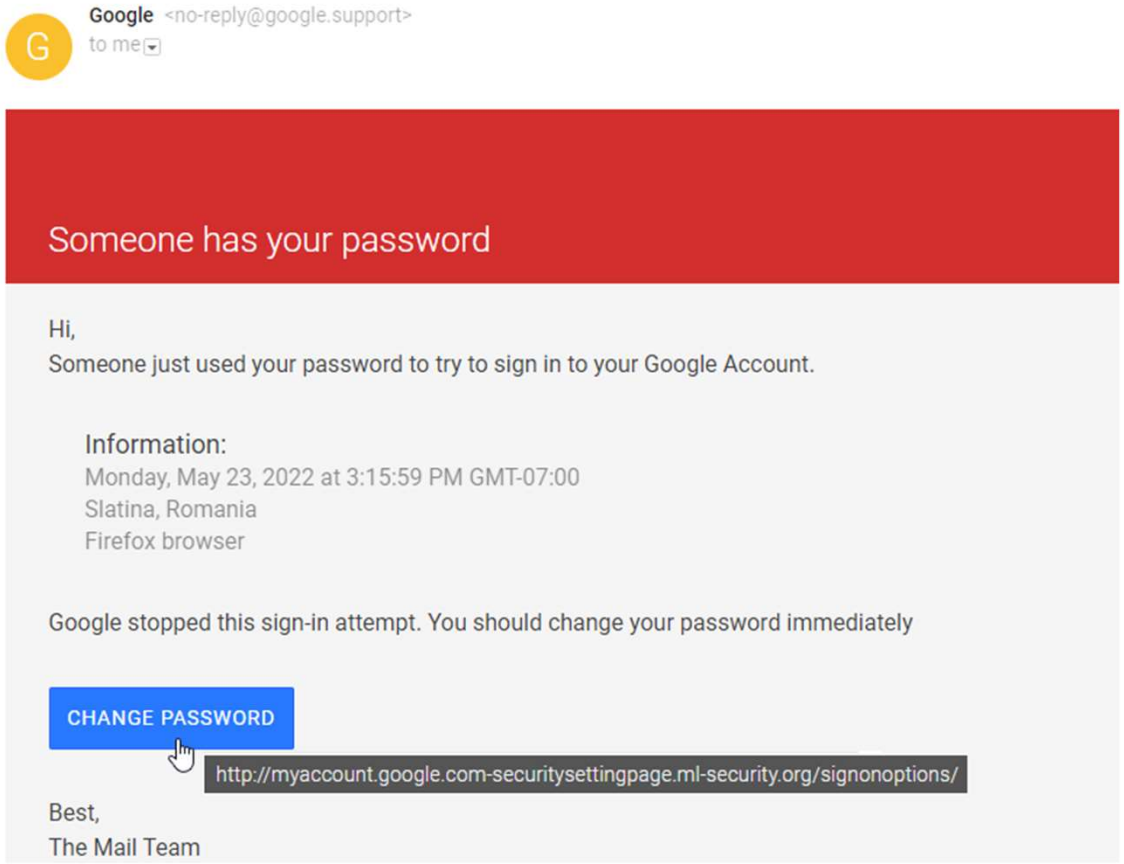
TABLETOP EXERCISE



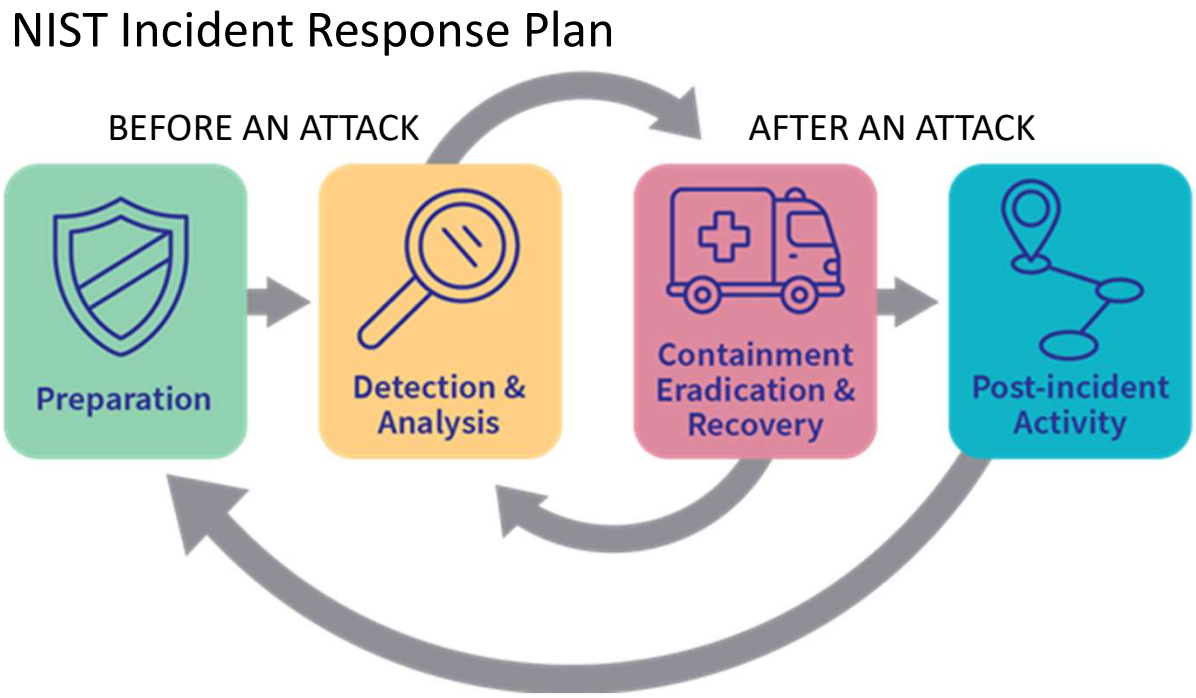
TABLETOP EXERCISE



TABLETOP EXERCISE



WHAT HAPPENS WHEN SOMEONE CLICKS



Who Do I Need To Contact In The Event of A Data Breach

Breach Notification Rule: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html#:~:text=If%20a%20breach%20affects%20500,breaches%20on%20an%20annual%20basis.

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to **notifying the affected individuals**, required to **provide notice to prominent media outlets serving the State or jurisdiction**. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in **no later than 60 days following the discovery of a breach** and must include the same information required for the individual notice.

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form.

BE Prepared

- Compile a list of IT assets such as networks, servers and endpoints.
- Identify their importance and which ones are critical or hold sensitive data.
- Set up monitoring so you have a baseline of normal activity. Determine which types of security events should be investigated.
- Create detailed response steps and communication guidelines for common types of incidents.

Detection and Analysis

- Implement monitoring systems for networks, systems, and logs in order to detect, alert, and report on potential security incidents.

- Identifying a baseline or normal activity for these systems. You must be able to correlate related events and see if and how they deviate from normal behavior.

Containment, Eradication, Recovery

- The goal of **containment** is to stop the attack before it overwhelms resources or causes damage. Your containment strategy will depend on the level of damage the incident can cause, the need to keep critical services available to employees and customers, and the duration of the solution—a temporary solution for a few hours, days or weeks, or a permanent solution.
- Containment methods include a **co-ordinated shutdown** and **blocking communication channels** and **network routes** once compromised systems are identified.
- **Eradication** step removes all elements of the incident from the environment, including malware from all compromised hardware.
- Login credentials must be changed on all compromised accounts.
- Once the threat is eradicated, the goal is a **recovery** to normal operations as quickly as possible.

Post Incident Activity

Questions to ask

- What happened, and at what times?
- How well did the incident response team deal with the incident? Were processes followed, and were they sufficient?
- What information was needed sooner?
- Were any wrong actions taken that caused damage or inhibited recovery?
- What could staff do differently next time if the same incident occurred?
- Could staff have shared information better with other organizations or other departments?
- Have we learned ways to prevent similar incidents in the future?
- Have we discovered new precursors or indicators of similar incidents to watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?

Sample Incident Response Plan Template

California Government Department of Technology Incident Response Plan – includes 17-step incident response procedure, with more detailed plans for specific incident types. Download .DOC file

https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: What is the easiest, most common way to steal credentials?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: What is the first thing you should do if you discover you've introduced malware to your network?

Protect Yourself, Cyber Insurance

- Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records.

NATIONAL ASSOCIATION OF Community Health Centers®

Health Choice Network
a Family of Health Centers
25+ Years of Service

Getting Cyber Insurance Right

- General Liability insurance usually does not cover cyber crimes
- Ask insurers to approve your preferred legal counsel and other service provider
- Invest time when answering the insurer's questionnaire about the company's IT security
- Pay close attention to the exclusions
- Do not simply automatically renew the cyber policy annually.

NATIONAL ASSOCIATION OF Community Health Centers®

Health Choice Network
a Family of Health Centers
25+ Years of Service

How Much Cybersecurity Is Enough?

- How much risk can your organization tolerate?
- How much can you afford to lose?

Live Content Slide

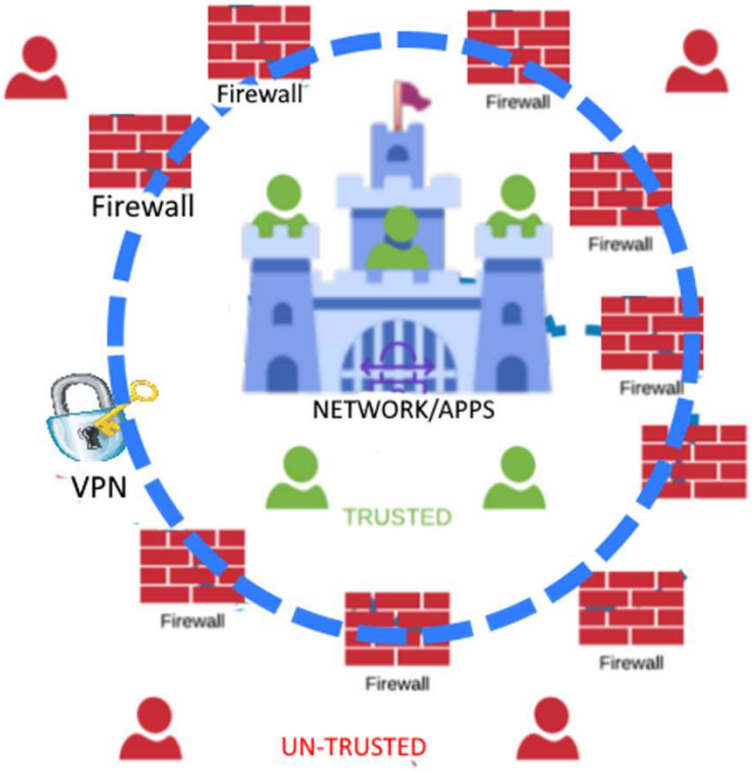
When playing as a slideshow, this slide will display live content

Poll: You (IT) get a call from one of your providers. Their company provided laptop got stolen from Starbucks. You're not worried because:

Future Proofing Cybersecurity: Zero Trust

The core concept of zero trust is simple: assume everything is hostile by default.

Traditional Network Security



The Castle and Moat Approach: Everyone inside the Moat is trusted, Everyone outside is untrusted

You get access to the inside by being already inside OR by connecting via the VPN.

Weaknesses

This approach does not accommodate for non-traditional workmodes (e.g. BYOD, remote work) well.

VPN bandwidth can be a limitation.

Single point of failure: An attacker can compromise a single endpoint within the trusted boundary and create/expand a foothold inside.

Note: Single largest reason for a data breach (9 out of 10 times) is a phishing email on one single user.

Zero Trust Model – What It Isn't

It is not a piece of technology or any one Software implementation.

It is rather a framework that can be implemented by incorporating several security technologies that already exist and are already being used standalone or in some combinations.

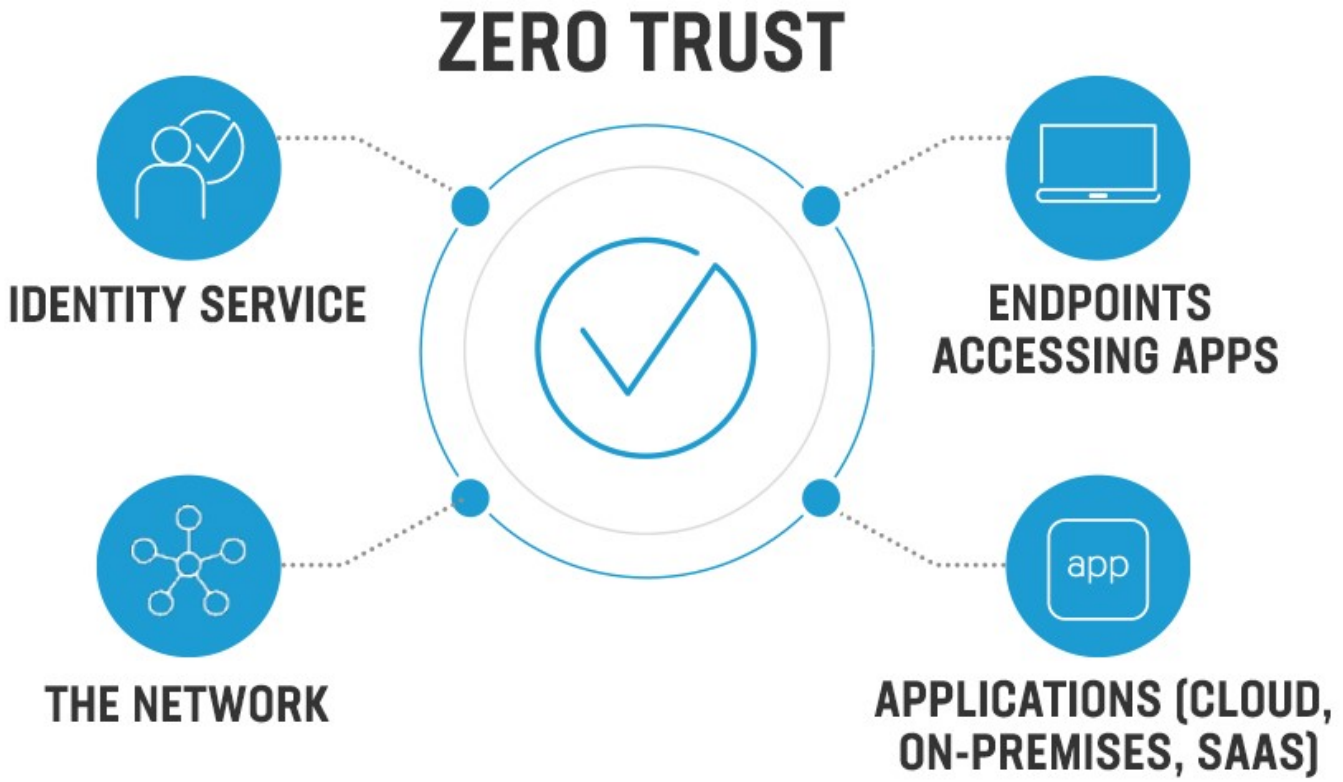
Zero Trust Model Principles

Trust No One. Always Verify.

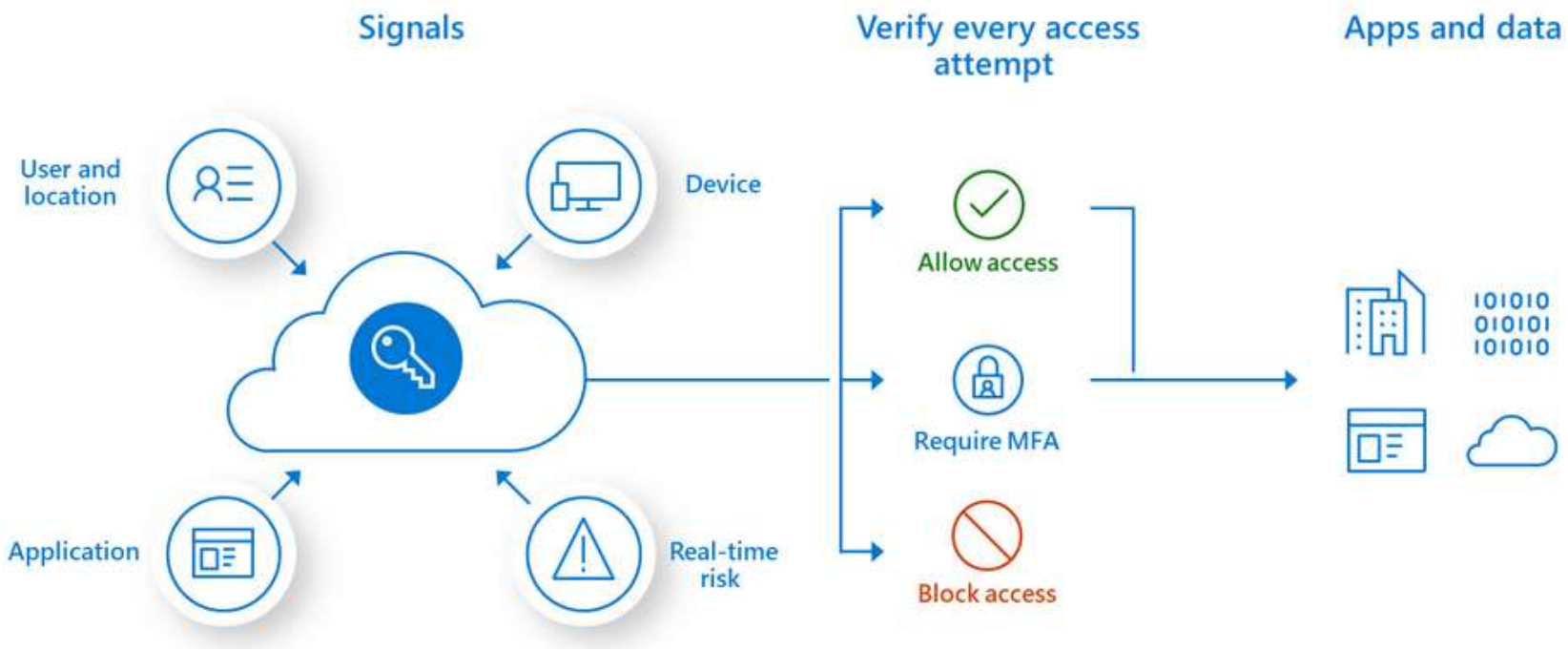
Use Least Privilege Access. Restrict User/Device to the MINIMUM permission required.

Assume breach. Every access attempt is considered hostile until verified otherwise.

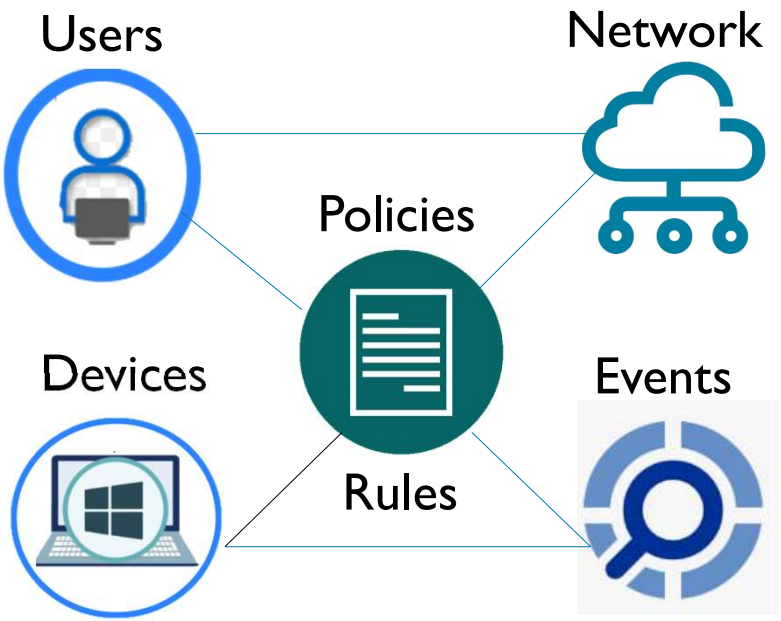
Zero Trust Components



Zero Trust – Practical Application Workflow

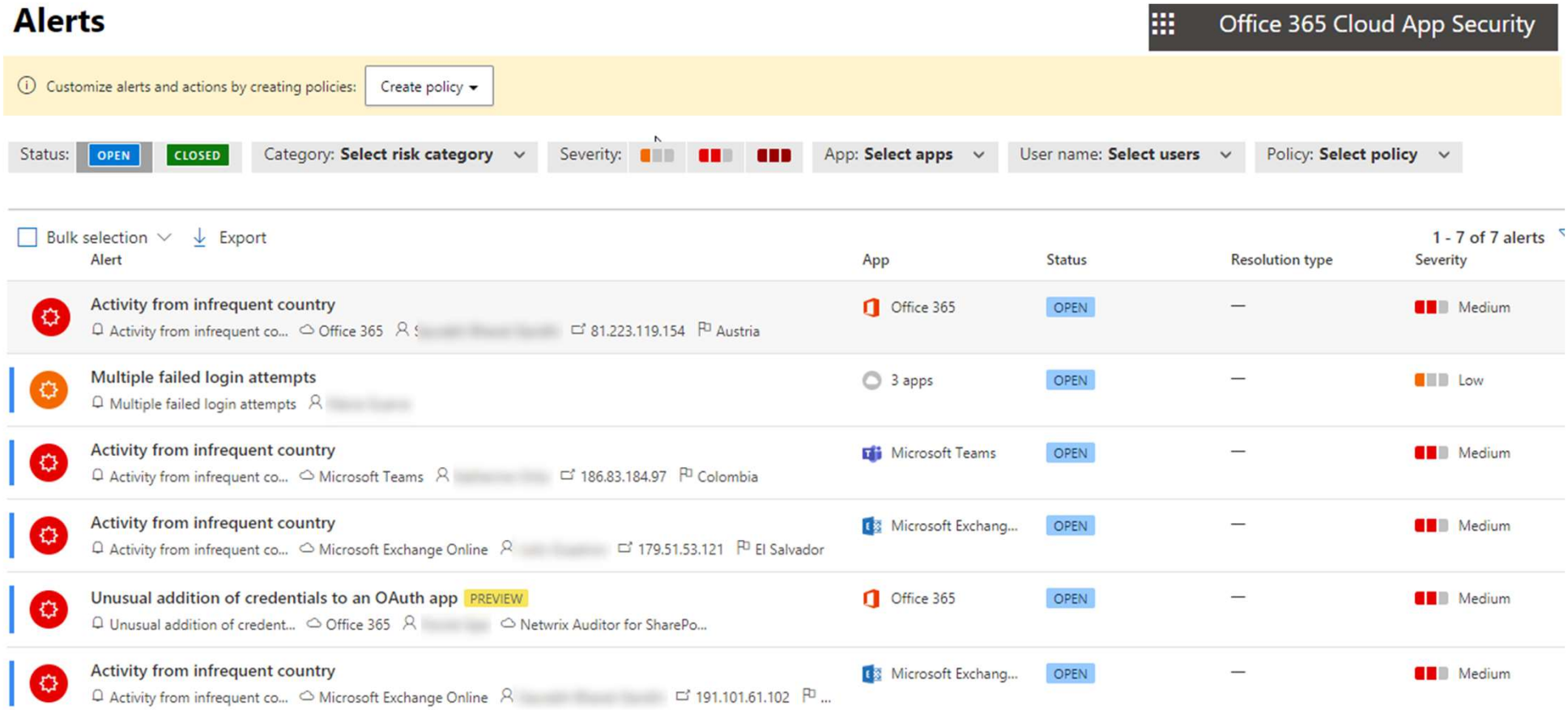


Zero Trust Framework – Interactive Parts

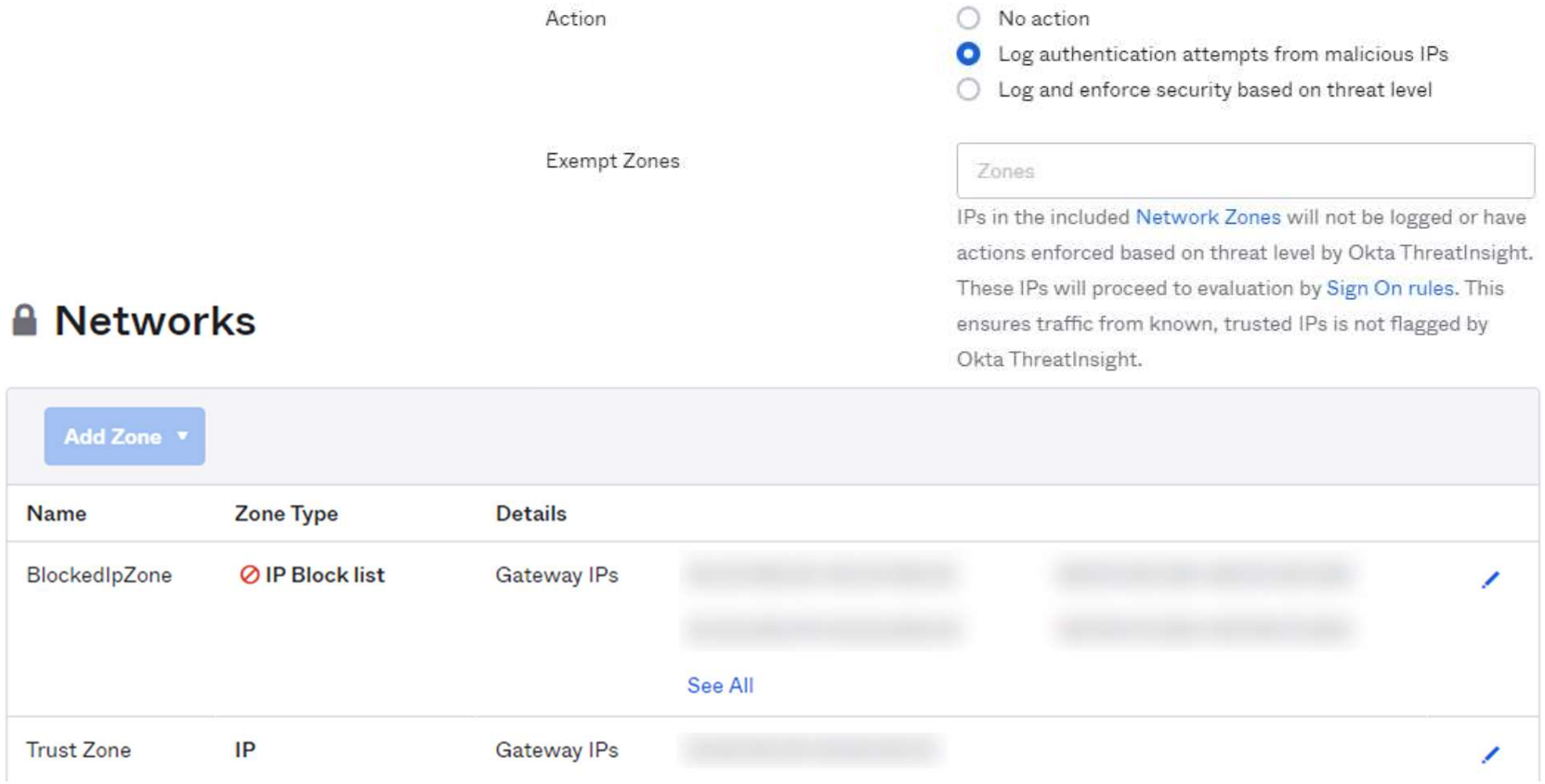


Rules:
Let in only specific users, IP Addresses, MAC addresses, geographic locations to specific networks, apps, and systems.

What Does It Look Like In the Real World

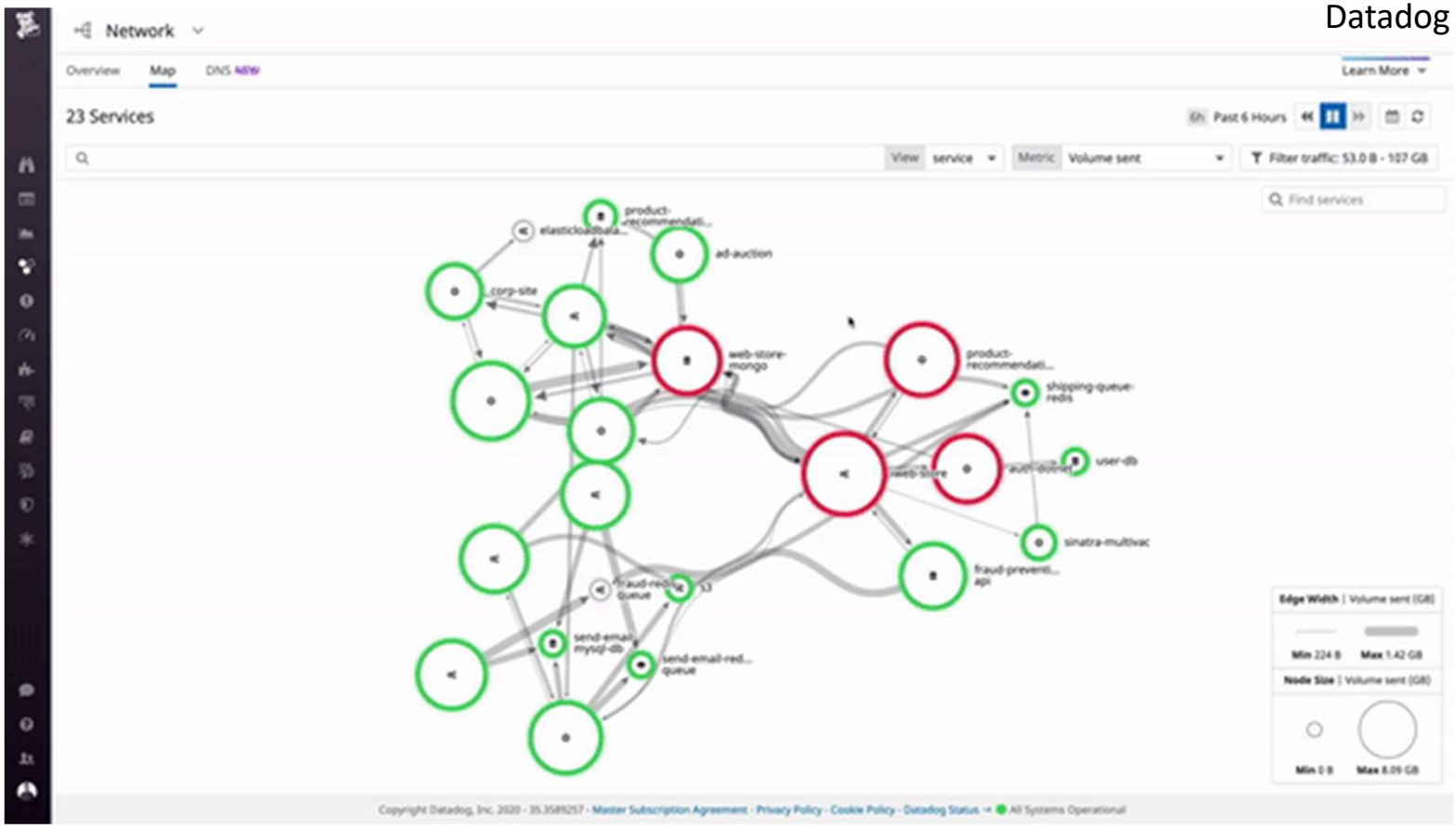


Example: Okta



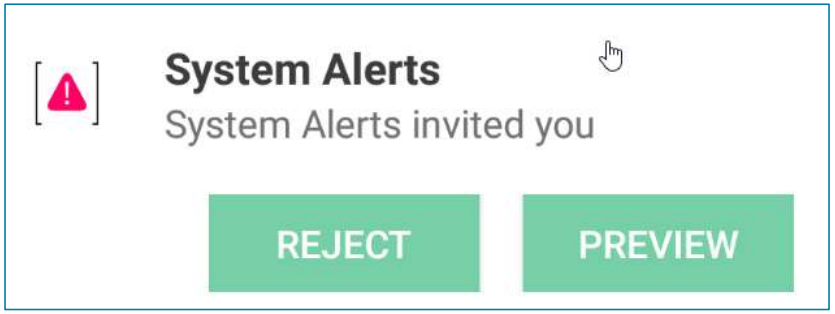
Network Bandwidth Analyzer

Datadog



New World of IT Maintenance

You will get LOTS more warnings and alerts.

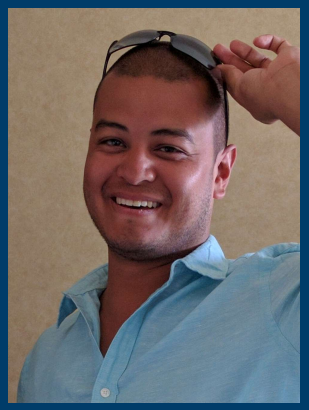


You will sleep better at night.

Thank You!

Questions and Answers?

How Can You Contact Us?



Nick Rosario
chen@synshop.org

Arnell Mendoza
Amendoza@queenscare.org

NATIONAL ASSOCIATION OF Community Health Centers®

ARE YOU LOOKING FOR RESOURCES?

Please visit our website **www.healthcenterinfo.org**

HEALTH CENTER RESOURCE CLEARINGHOUSE

Twitter.com/NACHC

Facebook.com/nachc

Instagram.com/nachc

Linkedin.com/company/nachc

YouTube.com/user/nachcmedia