



NATIONAL ASSOCIATION OF
Community Health Centers®

Health Center Cybersecurity

Investing to Safeguard Protected
Health Information



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.



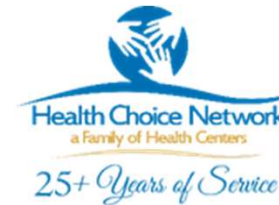
Meet Your Speakers



Arnel Mendoza
Director of Information Systems
QueensCare Health Centers



Michael Sanguily
Director of CISO Services
Health Choice Network



IT Budgets: The 30,000 ft View

- The Language of the C's
- IT spending varies by organization size. Because of this, IT spending should not be benchmarked just by percentage of revenue but by other ratios such as IT spending by user or IT spending per desktop.

**IT Spending Ratios
Between 25th and 75th Percentiles, by Industry**

IT Spend as...	Discrete Mfg	Fin'l Services	High Tech	Retail	Health care
Percentage of Revenue	1.4%-3.2%	4.4%-11.4%	2.6%-4.7%	1.2%-3.0%	3.0%-5.9%
Per User	\$3,733-\$9,864	\$13,772-\$26,667	\$6,191-\$11,653	\$3,913-\$14,685	\$3,157-\$6,143
Per Desktop/Laptop	\$4,658-\$9,395	\$12,171-\$23,882	\$5,452-\$9,218	\$4,806-\$13,533	\$3,280-\$7,273

Source: *Computer Economics, 2019*

Figure 1

Budgets = Priorities

- What are the priorities for IT? It depends.

- Compliance and Audit
- Contractual Obligations
- Business Critical Activities and Initiatives
- Strategic Plan Implementations

IT Budgets: The 20,000 ft View

What To Spend. This was a typical IT budget template in 2013. Expense categories were broad. Cybersecurity was not considered a category.

Categories	Hardware	Software	Network Equipment	Services	Staffing	Training	Yearly Subtotals
Year 1	\$370,000	\$76,800	\$12,300	\$6,100	\$275,000	\$48,000	\$788,200
Year 2	\$13,700	\$12,644	\$1000	\$4,900	\$298,700	\$48,000	\$378,404
Year 3	\$13,700	\$12,644	\$1000	\$4,900	\$307,661	\$48,000	\$390,321
Year 4	\$176,250	\$57,000	\$12,010	\$4,900	\$316,891	\$48,000	\$615,051
Year 5	\$203,750	\$15,300	\$1,000	\$4,900	\$326,398	\$48,000	\$598,508
5 Yr Subtotals	\$777,400	\$177,644	\$27,310	\$25,700	\$1,524,649	\$240,000	\$2,770,483

IT Budgets: The 10,000 ft View

- Where is Cybersecurity?

5 years ago cybersecurity consisted of:

- Firewall
- Antivirus
- Identity Management (Windows Active Directory)
- Email encryption
- Database encryption
- VPN for remote access

All could be lumped into hardware/software OR both OR services if they were outsourced

What has happened in the last 5 years?

- The bad guys got better at being badder, FASTER.
- Cybercrime is now more profitable than the Global Drug Trade!
- Cybercrime costs more per year than ALL NATURAL DISASTERS combined.



Industry Impact: Colonial Pipeline

- In May 2021, Colonial Pipeline which operates out of Houston, Tx and carries gasoline to a good part of the Southeastern US suffered a ransomware cyberattack, forcing operations to shut down for 5 days.

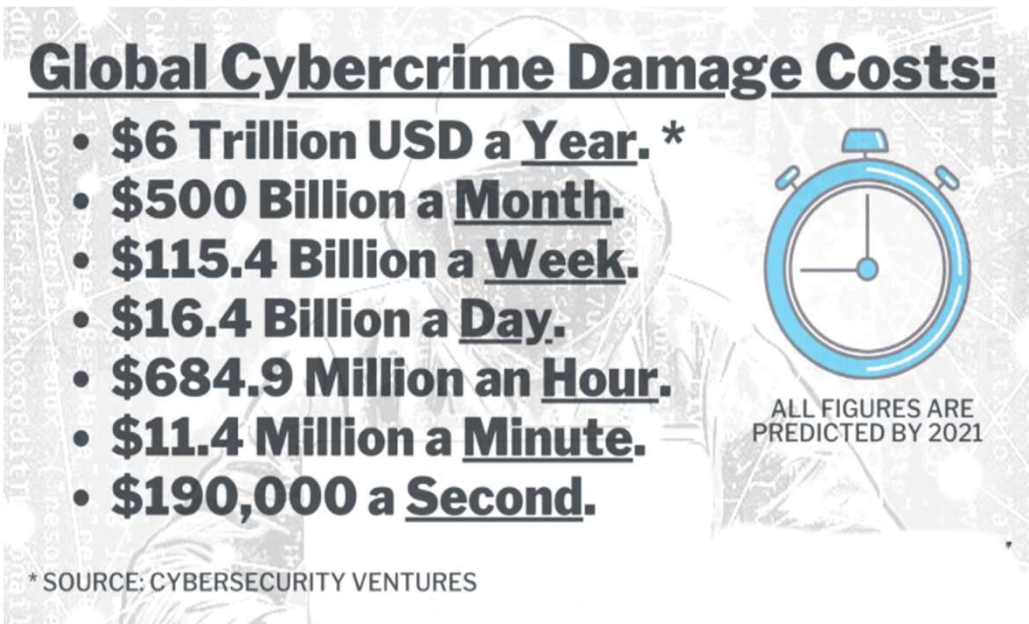
- Flight schedule changes and delays
- Airports had to scramble for other fuel suppliers
- Fuel shortages began to occur at filling stations amid panic buying
- Average fuel prices rose to their highest levels since 2013

Industry Impact: XXX Community Health Center

- 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

The Evolution of Cybersecurity



- Sharp increase in the number of cyberattacks.
- Corresponding decrease in revenue due to losses as a result of cyberattacks.
- Increased awareness at the C-suite level.
- Cybersecurity has NOW become an important part of an organization's operating strategy.

A Warning to the C-Suites



While the responses from the C-Suites indicate that they recognize data security risks, they underestimate consequences, creating a worrisome disconnect. Simply put, a data breach is a trust breach, and consumers will take their business elsewhere if they lose confidence in an organization.”

Source: Shred-It Data Protection Report 2019

How effective are your defenses?

Mandiant Security Effectiveness Report

DEEP DIVE INTO CYBER REALITY

53%

ATTACKS INFILTRATE
UNNOTICED

68%

OF RANSOMWARE ATTACKS
UNNOTICED

91%

OF ATTACKS DID NOT
GENERATE AN ALERT

Data Breach Response Times

Healthcare Industry Statistics:

- Average Number of Days to Detect a Data Breach:
255
- Average Number of Days to Contain a Breach:
103

Source: ©IBM Security Cost of a Data Breach Report 2020

Data Security Breach Report: California Dept of Justice

Organization Name	Date(s) of Breach	Reported Date ▼
Metabolic Maintenance Products, Inc.	05/01/2020, 07/09/2021	09/16/2021
King's Seafood Company	06/04/2021	09/15/2021
Eastern Los Angeles Regional Center	07/15/2021	09/13/2021
Dick Blick Holdings	03/11/2020, 12/15/2020	09/13/2021
HCI, LLC	09/02/2020	09/13/2021
Nations Lending Corporation	07/26/2021	09/10/2021
Buddhist Tzu Chi Medical Foundation	07/15/2021	09/09/2021
Cedarlane Natural Foods, Inc.	05/20/2021	09/09/2021
UC San Diego Health	12/02/2020, 04/08/2021	09/09/2021
California Massage Therapy Council	11/04/2020	09/08/2021
Resource Anesthesiology Association of California, a Medical Corporation	07/08/2021	09/05/2021
K and B Surgical Center, LLC	03/24/2021, 03/30/2021	09/03/2021
Smile Brands Inc.	04/23/2021, 04/24/2021	09/03/2021
CA Department of State Hospitals - Coalinga	08/27/2019, 10/12/2016, 07/21/2013	09/03/2021
Sequoia Concepts, Inc.	06/28/2021, 07/01/2021	09/02/2021
County of Los Angeles Fire Department	07/13/2021	09/01/2021
DuPage Medical Group, Ltd.	07/12/2021, 07/13/2021	09/01/2021
MFA Financial, Inc.	03/10/2021	09/01/2021



1 out of 2 organizations listening to me today are **ALREADY** infected with malware, most don't know it yet.

No-Win Scenario



Even The Mighty Have Fallen



What is the strategy in a no-win scenario?



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

You Must Use Data

- You can't manage what you can't measure.
- If you can't measure it, you can't improve it.

A photograph of a dark chalkboard with a white line graph drawn on it. The graph shows an upward trend with some fluctuations. A blue ruler is placed horizontally across the graph, and two hands are visible, one holding the ruler at the bottom left and the other at the top right, as if measuring the length of the graph. The text "You can't manage what you don't measure" is written in white chalk on the board.

You can't manage
what you
don't measure

What is the Cost of a Data Breach?

\$7.13 million

The average cost of a data breach in the healthcare industry, an increase of 10% compared to the 2019 study

80%

Share of breaches that included records containing customer PII, at an average cost of \$150 per record

\$150

Customer PII avg. cost per record

Source: Ponemon Report 2020 United States Averages

Quantifying the Cost of a Data Breach



My Analyses

Current Analysis

Settings

Learn FAIR

Scaling FAIR

Need Help?

Scope Inputs

Loss Event Frequency

How many times over the next year is the loss event likely to occur?

Inputs

Minimum	Most Likely	Maximum
1	1	2

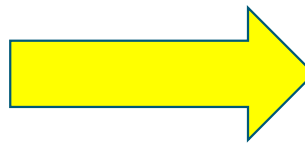
Confidence

Medium

Rationale

phishing tests

Inputs:
Loss of 1 day of
Productivity +
Cost of response



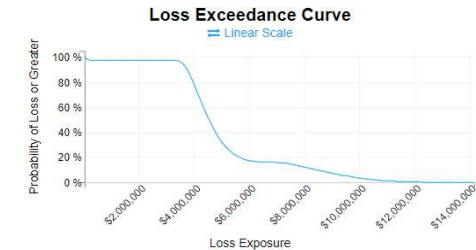
Not quantified:
Loss of reputation
Market Loss

Analysis Results

Risk

The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario

\$41.2k Minimum \$5.1M Average \$14.0M Maximum



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	1	1.17	2
Loss Magnitude	\$36.8k	\$53.4k	\$79.2k

<https://www.fairinstitute.org/>



www.nachc.org

@NACHC | 22

So How Much Do I Need To Spend on Cybersecurity?

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



Cybersecurity: A Risk-Based Approach

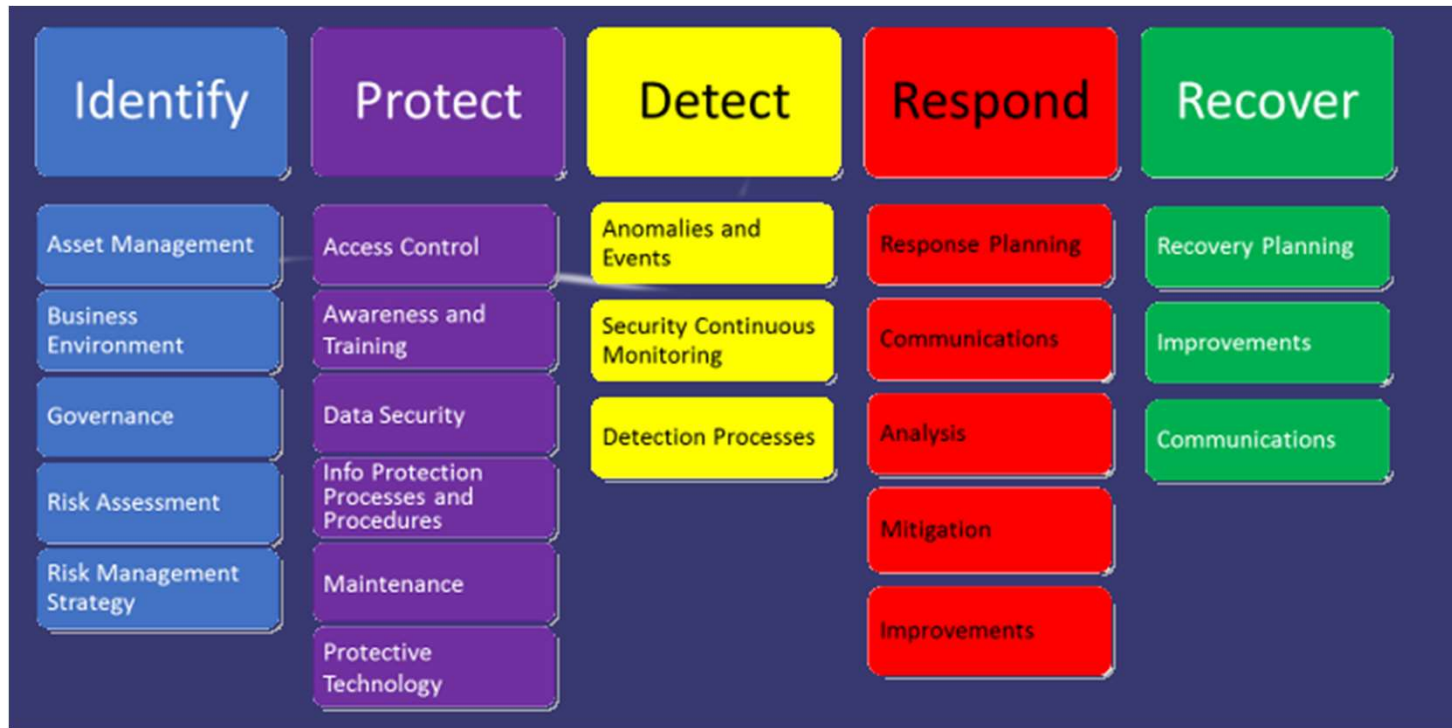
NIST Cybersecurity Framework

- A set of industry standards and best practices to help organizations manage cybersecurity risks
- A framework to document and assess cybersecurity controls in an organization
- Organizations assess themselves on a 1-5 scale through 98 sub-categories
- The outcome is an average score for each of the five functions of the framework (Identify, Protect, Detect, Respond, Recover)
- The GOLD STANDARD of cybersecurity risk assessment
- Allows cybersecurity spending to be driven by standards and an accepted framework

Quantifying Risk: NIST Framework

5 Categories

22 Sub-
Categories



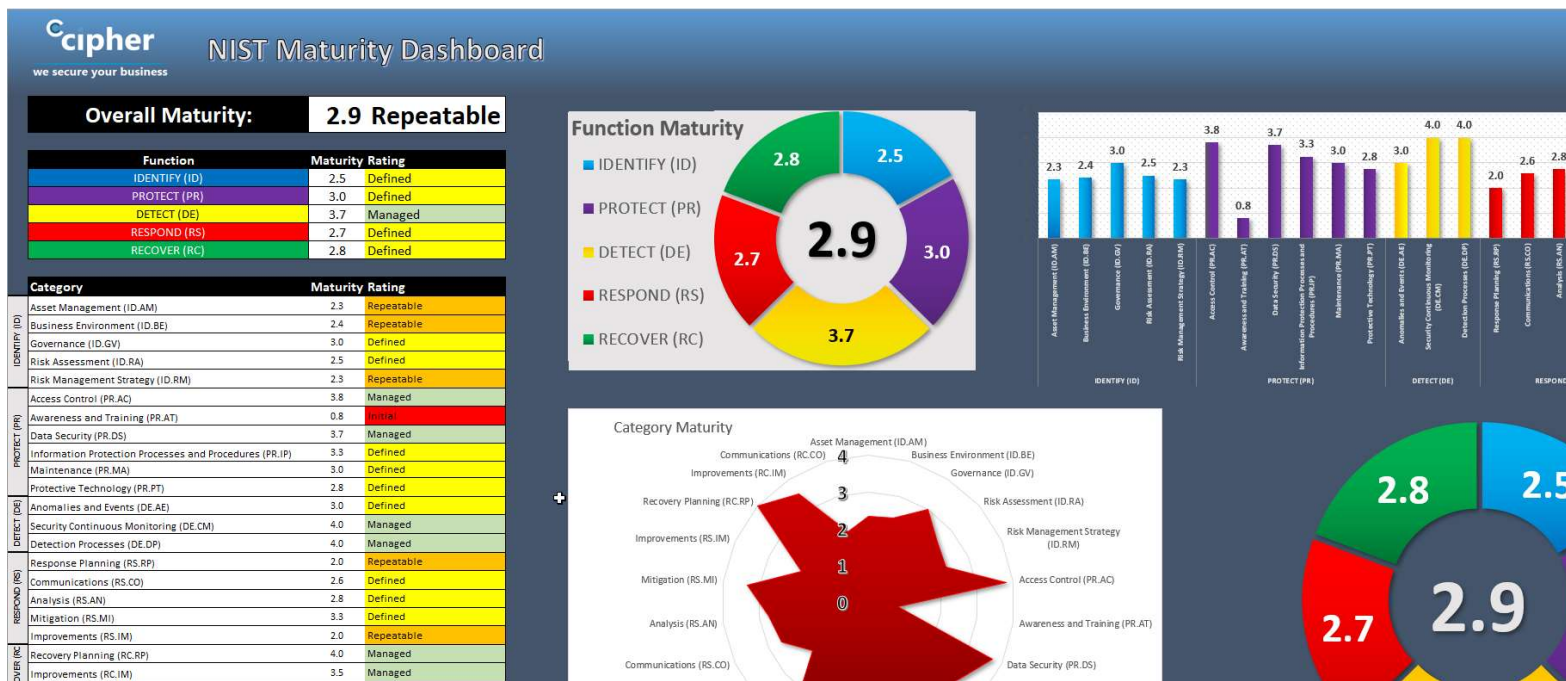
NIST Framework: Baseline Assessment

Function	Category	Subcategory	Maturity
PROTECT (PR)	Access Control (PR.AC)	PR.AC-2: Physical access to assets is managed and protected	2 - Repeatable
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	4 - Managed
PROTECT (PR)	Access Control (PR.AC)	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	4 - Managed
PROTECT (PR)	Access Control (PR.AC)	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	4 - Managed
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-1: All users are informed and trained	0 - Non-Existent
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-2: Privileged users understand roles & responsibilities	1 - Initial
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	0 - Non-Existent
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-4: Senior executives understand roles & responsibilities	2 - Repeatable
PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-5: Physical and information security personnel understand roles & responsibilities	1 - Initial
PROTECT (PR)	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	4 - Managed
PROTECT (PR)	Data Security (PR.DS)	PR.DS-2: Data-in-transit is protected	4 - Managed
PROTECT (PR)	Data Security (PR.DS)	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	4 - Managed
PROTECT (PR)	Data Security (PR.DS)	PR.DS-4: Adequate capacity to ensure availability is maintained	2 - Repeatable

0	1	2
Nope, we're not doing this at all	It's ad hoc, we only do it in cases where we have to	We do it ... but it's not consistent or structured

3	4	5
We do it consistently ... but it's not best practice and it could be better aligned with the business	We do it well and I wouldn't be ashamed to show this to my peers	We're world class (as in, we're one of the best in the world)

Result: SWOT Analysis on your Cybersecurity Posture



<https://cipher.com/blog/a-quick-nist-cybersecurity-framework-summary/>

Cybersecurity Incidents: Initial Point of Compromise

Table 5: Significant Security Incidents – Initial Point of Compromise

Initial Point of Compromise	N	%
E-mail (e.g., phishing e-mail)	105	89%
Human error	41	35%
Telephone system	21	18%
Website	17	14%
Vendor or consultant	17	14%
Mobile device	16	14%
Social media	14	12%
Remote access server	12	10%
Third party website	11	9%
Internet of Things device	8	7%
Cloud provider/service	8	7%
"Off the shelf" hardware or software (e.g., malware)	8	7%
Medical device	6	5%
Client or customer	5	4%
Building automation system or other industrial control system	3	3%
Videoconferencing system	2	2%

Source: HIMSS 2020 Cybersecurity Survey

Budget Choices and Realities

- \$30K+ spent on hardware and software for a firewall to protect your network perimeter just got rendered ineffective because someone clicked on a bad link or attachment in an email.
- Comprehensive Security Awareness program is approx. \$5K.

Tying Strategy to Toolsets: The Basic Minimum Required

- Firewall: Perimeter Network Security
- Antivirus/AntiMalware/Endpoint Security
- Intrusion Detection/Prevention System [Network Monitoring]
- Endpoint Security: Data/Disk/Device Encryption
- Endpoint Security: System and Application Patching
- Endpoint Security: Host Intrusion Detection/Prevention [Can be integrated with endpoint security]
- Security Awareness Training (The Human Firewall)
- Audit Log/Log Monitoring [SIEM]

Other Budget Considerations

- Backup Backup Backup
- Best practice is the 3-2-1 Strategy



Know Your Vulnerabilities

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

More Budget Considerations: Identity Management



- Federated Single Sign-On
- Multi-Factor Authentication
- Most effective if software apps are already in the cloud (e.g. O365).

More Budget Considerations: DIY vs Managed

- DIY = FTE/Internal Staff
- There are lots of FREE tools and resources, most have a learning curve to be used effectively.
- Managed = Migrate to the Cloud

Beyond Basics: Technology Evolution

- Perimeter-based security and end-point based security is no longer effective.
- Moving towards Zero Trust Model.

Zero Trust Security Model

- Zero Trust = Don't trust anyone. You must prove you are who you are every time.
- No access to anything until you prove it's you. No single point of entry for full access (e.g. VPN).

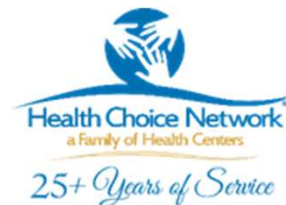
- Yes, remember this computer.**
Trust this computer when I sign in.
- No, don't remember this computer.**
Ask me to verify my identity each time I sign in.

How Much Cybersecurity Is Enough?

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

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.



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®



What is your information worth?

Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:



Social security number



\$1

Online payment services login info
(e.g. Paypal)



\$20-\$200

Credit or debit card
(credit cards are more popular)



\$5-\$110

With CVV number
\$5

With bank info
\$15

Fullz info*
\$30

Drivers license



\$20

Loyalty accounts



\$20

General non-financial institution logins



\$1

Diplomas



\$100-\$400

Passports (US)



\$1000-\$2000

Subscription services

\$1-\$10

Medical records

\$1-\$1000**

From Data Breach to the Dark Web



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Date>>

Dear <<Name 1>>:

Maintaining the confidentiality and security of our patients' information is something Scripps Health takes very seriously. Regrettably, we are writing to inform you of an incident involving some of that information.

On May 1, 2021, we identified unusual network activity. We immediately initiated our incident response protocols, which included isolating potentially impacted devices and shutting off select systems. We also began an investigation with the assistance of computer forensic firms. The investigation determined that an unauthorized person gained access to our network, deployed malware, and, on April 29, 2021, acquired copies of some of the documents on our system. On May 10, 2021, we discovered that some of those documents contained patient information. Upon conducting a review of those documents, we determined that one or more files may have reflected your name, address, date of birth, health insurance information, medical record number, patient account number, and/or clinical information, such as physician name, date(s) of service, and/or treatment information.

We have **no** indication that any of your information has been used to commit fraud. However, we recommend that you review the statements you receive from your healthcare providers and health insurer. If you see any medical services that you did not receive, please call the provider or insurer immediately. To help prevent something like this from happening again, we are continuing to implement enhancements to our information security, systems, and monitoring capabilities.

We deeply regret that this incident occurred and for any concern this may cause you. We value your trust and confidence in Scripps Health, and look forward to continuing to serve you.

Medical Records For Sale

[Home](#) > [Fraud](#) > [Accounts & Bank Drops](#) > [Accounts & Bank Drops](#) > [Medical Fullz](#)

LISTING OPTIONS


Contact Seller

Favorite Listing

Favorite Seller

Alert when restock

Report Listing



Medical Fullz

PatID,FirstName,LastName,Soc,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,Email,LastApptDate,LastVisitType,NextApptDate,NextVisitType,LastDOS,FollowUpDate,BirthDate,Ins,InsID1,InsID2,RefPhysCode,FirstLast,Title,LastNO Refund.

Sold by **badmans** - 3 sold since Jul 7, 2016 Vendor Level 5 Trust Level 5

Product class	Features	Origin country	Features
Quantity left	Digital goods	Ships to	Worldwide
Ends in	Unlimited	Payment	Worldwide Escrow

Purchase price: USD 5.00

Qty: Buy Now Queue

0.0088 BTC / 0.0053 XMR

[Description](#) | [Bids](#) | [Feedback](#) | [Refund Policy](#)

Product Description

PatID,FirstName,LastName,Soc,Addr1,Addr2,City,State,Zip,HomePhone,WorkPhone,Email,LastApptDate,LastVisitType,NextApptDate,NextVisitType,LastDOS,FollowUpDate,BirthDate,Ins,InsID1,InsID2,RefPhysCode,FirstLast,Title,LastPract,LastBase,LastTotal

NO Refund.

Image via ICIT of TheRealDeal stolen record package

Credentials For Sale

The screenshot shows a forum post with the following details:

- Title:** USA Hospital RDP For Sale - Больница США RDP на продажу
- Author:** hardknocklife, 4 сентября в Аукционы
- Profile:** hardknocklife, 1 мегабайт, 00 публикаций, 22.04.2019 (ID: 112.321), Дятельность: виртуозный / палеолог
- Post Content:**
 - Опубликовано: 4 сентября (изменено)
 - Сelling RDP of a US Hospital.
 - On the RDP has a lot of patient records and also active software client which shows full medical records of patients etc.
 - I have no use for this topic. You will receive login information of the RDP in one hand.
 - Willing to work through escrow/guarantor (buyer pays fees)
 - Start: \$ 500
 - Step: \$ 100
 - Blitz: \$ 5000
 - Auction is valid only for 24hours!
- Second Post Content:**
 - Продам РДП больницы США.
 - На RDP есть много записей пациентов, а также активный программный клиент, который показывает полные медицинские карты пациентов и т. Д.
 - Мне эта тема не нужна. Вы получите данные для входа в RDP в один руки.
 - Готовность работать через эскроу / поручителя (комиссия оплачивает покупатель)
 - Старт: \$ 500
 - Шаг: \$ 100
 - Блиц: \$ 5000
 - Аукцион действителен только 24 часа!

Image from IntSights Report: Selling Breaches: The Transfer of Enterprise Network Access on Criminal Forums

5 Laws of Cybersecurity

Law 1: If there is a vulnerability, it will be exploited.

Law 2: Everything is vulnerable in some way.

Law 3: Humans can trust when they shouldn't.

Law 4: With innovation comes opportunity for exploitation.

Law 5: When in doubt, see law 1

Source: Nick Espinosa @ TEDxFondduLac

Securing Your Organization – Vulnerability Assessments

How Does a Vulnerability Assessment Help?

- Understand your risk and vulnerabilities that you may have
- Target low-hanging fruit
- Maintaining a strong vulnerability assessment program will decrease your chances of a breach
- Preparation for a penetration test
- Keep yourself up-to-date with the latest looming vulnerabilities
- The technical aspect of your cybersecurity risk assessment

The Importance of Cybersecurity Awareness

- **94%** of malware is delivered via email [CSO online]
- Human error was a major contributing cause in **95%** of all data breaches [IBM Cyber Security Intelligence Index Report 2020]

A Culture of Cybersecurity Awareness is Essential

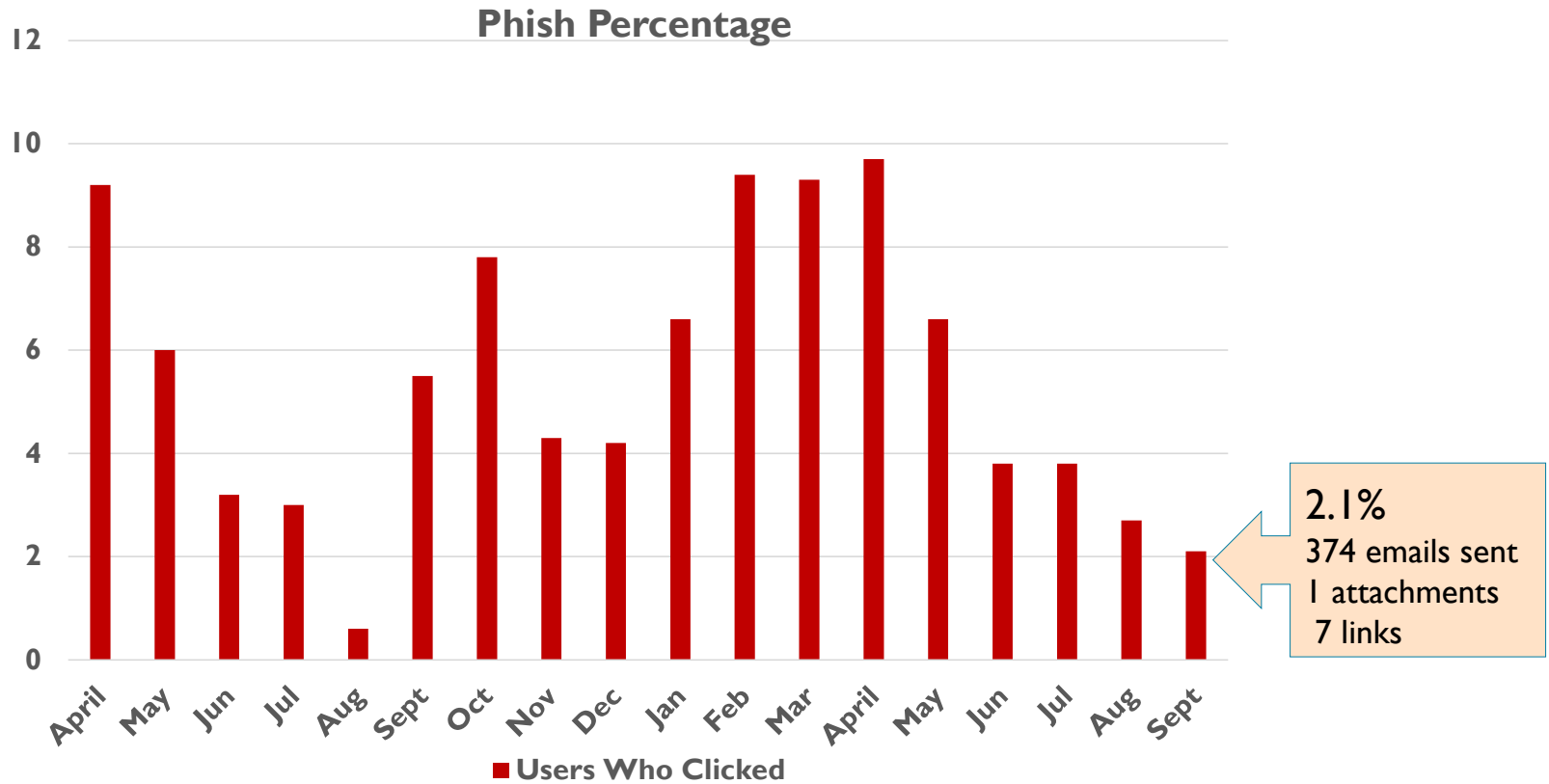
- A one-hour training given annually is not enough.
- A culture of cybersecurity awareness is something that is cultivated.

What Does Culture Look Like

Construction Example



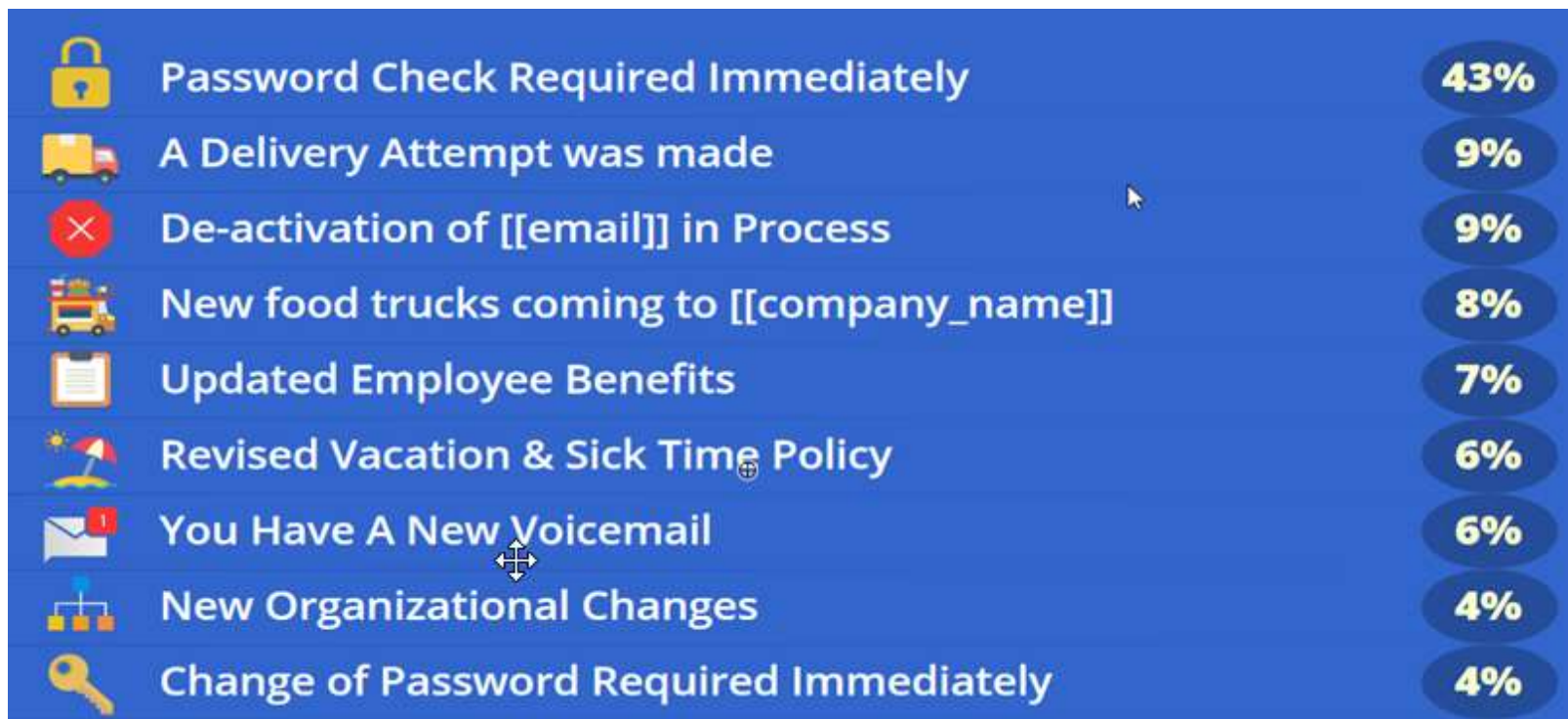
Cultivating a Cybersecurity Awareness Culture



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)

Top Phishing Email Subjects



Testing Your Organization— Penetration Testing

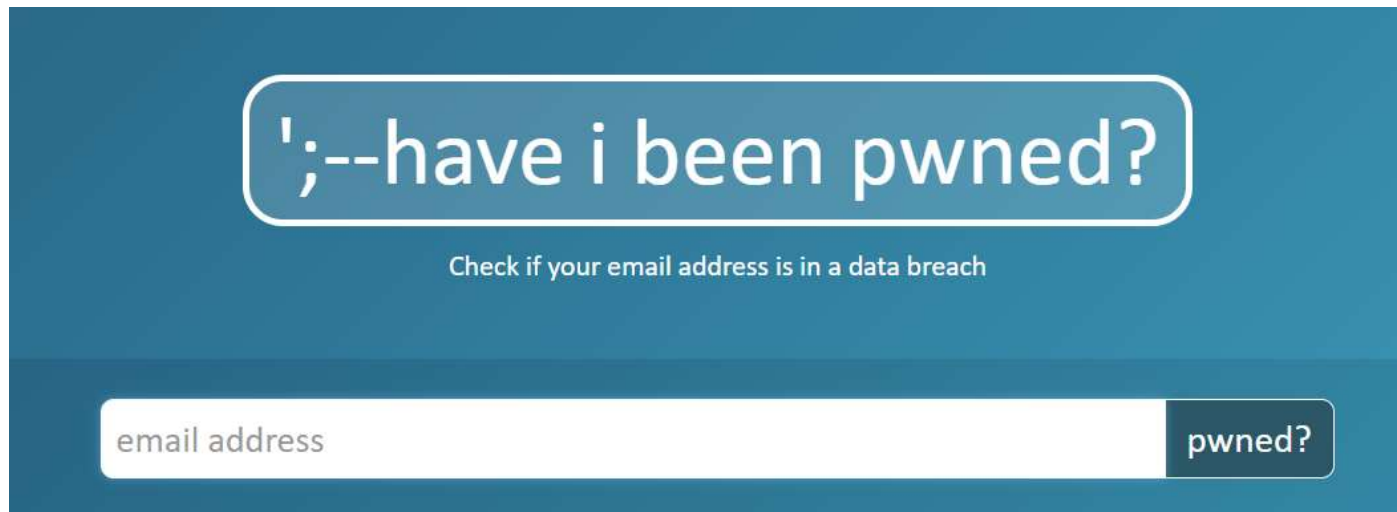
- Assessing the true security of your Organization
- Mimic what a true malicious actor would do when targeting your network
- Ensure Compliance
- Create an Action Plan to prioritize your vulnerabilities as part of your security program
- Test all aspects of your security posture – Network, Applications,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



NATIONAL ASSOCIATION OF
Community Health Centers



Have YOU been breached?



<https://haveibeenpwned.com>

Security Awareness Training

Virtual or on-site, education for employees on the ongoing cyber security threats and how to identify them via our healthcare specific **Security Awareness Training** offered by Health Choice Network. This is an annually mandated training for all health center associates under the HIPAA training provision for HIPAA security policy regulations.

Training Objectives will focus on:

- How to identify phishing emails and malicious websites
- Tips and tricks on identifying social engineering scams in person or by phone
- How to properly respond and report security threats
- Review your organizations Phishing Simulation Attacked Report*
- Industry trending security threats

Annual Trainings should be provided to keep organizations updated on current and latest threats to the industry, their working environment and for HIPAA regulation compliance.

* Phishing Simulation Attack service is required for report review during Security Awareness Training.

Phishing Simulation Attack

Phishing attacks are the number one cause for data breaches in our industry. An annual phishing simulation is important to help demonstrate this type of attack and how to identify them. Health Choice Network provides a phishing simulation to all health center associates, using a realistic email communication with malicious links. Associates who open or click on the simulated malicious links will be identified and flagged for additional training needs during the presentation of the Phishing Simulation Attacked Report. The phishing simulation service is highly recommended in conjunction with our security awareness training in order to provide the complete experience for health center associates.

Additional information available upon request.

Vulnerability Assessment

An annual vulnerability assessment is a critical part of organizations HIPAA security risk plan. The Health Choice Network assessment performs specific industry examinations and searches all devices on your local network for vulnerabilities that perpetrators can exploit and use to gain unauthorized access to Patient Health Information (PHI) or sensitive business data. The assessment provides a risk level rating (HIGH to LOW) of recommended actions required in order to prevent unauthorized access to include software updates needed, security concerns related to aging technology and hardware, and configuration changes recommended.

Penetration Testing

Our annual penetration testing simulates an attack on your networks access points. Several subject matter experts will work to exploit known vulnerabilities in the technology and configuration deployed within your organizations network. If CISO team gains access, our penetration testers will document access to various systems while continuing to gain access to as many network and systems possible during the engagement period. A report will be generated of the simulation and used to educate and prioritize systems and configuration while securing your network; ultimately preventing this form of attack.



9064 NW 13 Terrace | Miami, FL 33172
www.hcnetwork.org

© 2020 Health Choice Network, Inc. All Rights Reserved.

Thank You!

Questions and Answers?

How Can You Contact Us?



Michael Sanguily
MSanguily@hcnetwork.org



Arnell Mendoza
Amendoza@queenscare.org



ARE YOU LOOKING FOR RESOURCES?

Please visit our website www.healthcenterinfo.org



**HEALTH CENTER
RESOURCE
CLEARINGHOUSE**



[Twitter.com/NACHC](https://twitter.com/NACHC)



[Facebook.com/nachc](https://facebook.com/nachc)



[Instagram.com/nachc](https://instagram.com/nachc)



[Linkedin.com/company/nachc](https://linkedin.com/company/nachc)



YouTube.com/user/nachcmedia

