NATIONAL ASSOCIATION OF Community Health Centers®

Considerations for Sustaining A Culture of Cybersecurity

Part I

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

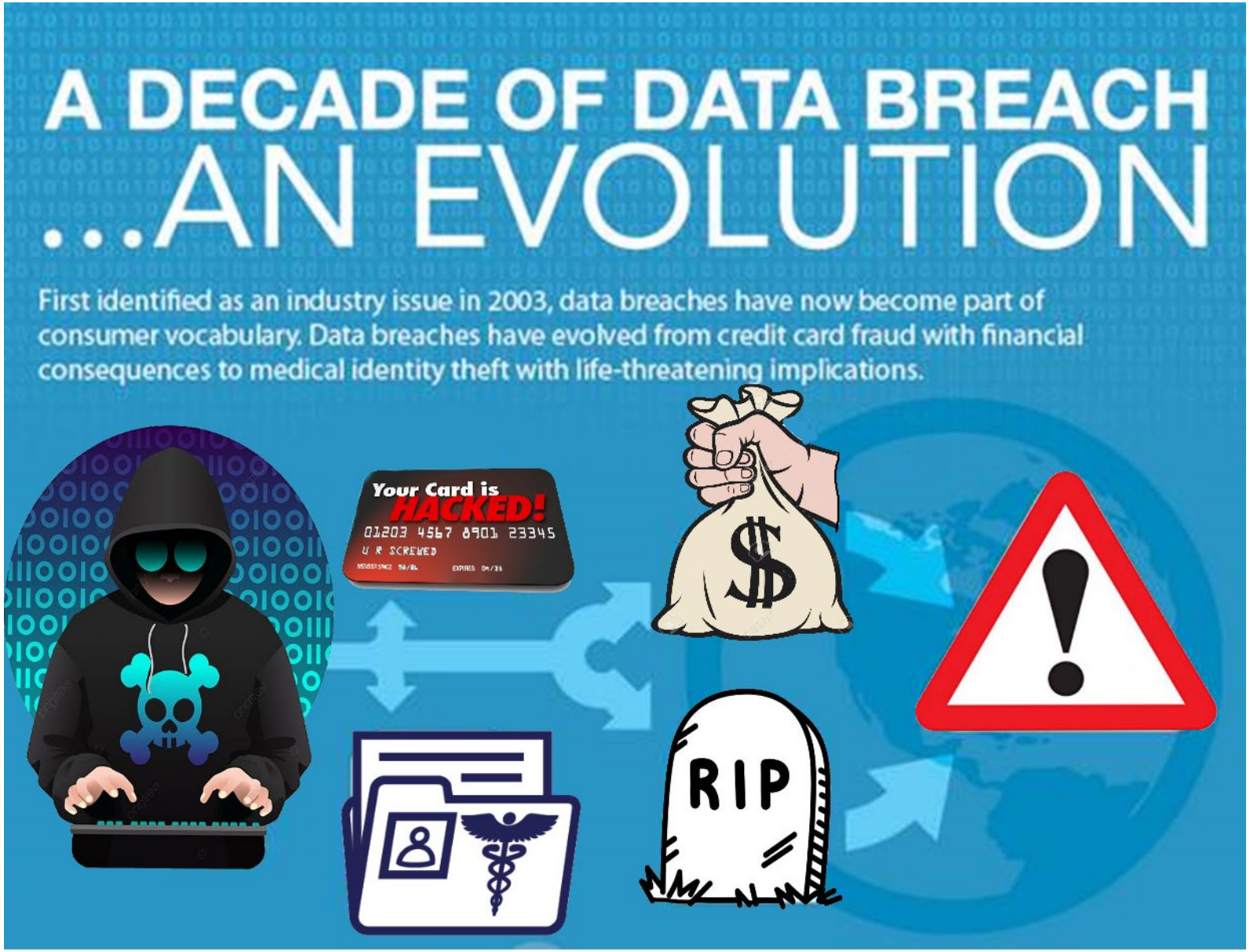
Arnel Mendoza
Director of Information Systems
QueensCare Health Centers

Michael Sanguily
Director of CISO Services
Health Choice Network

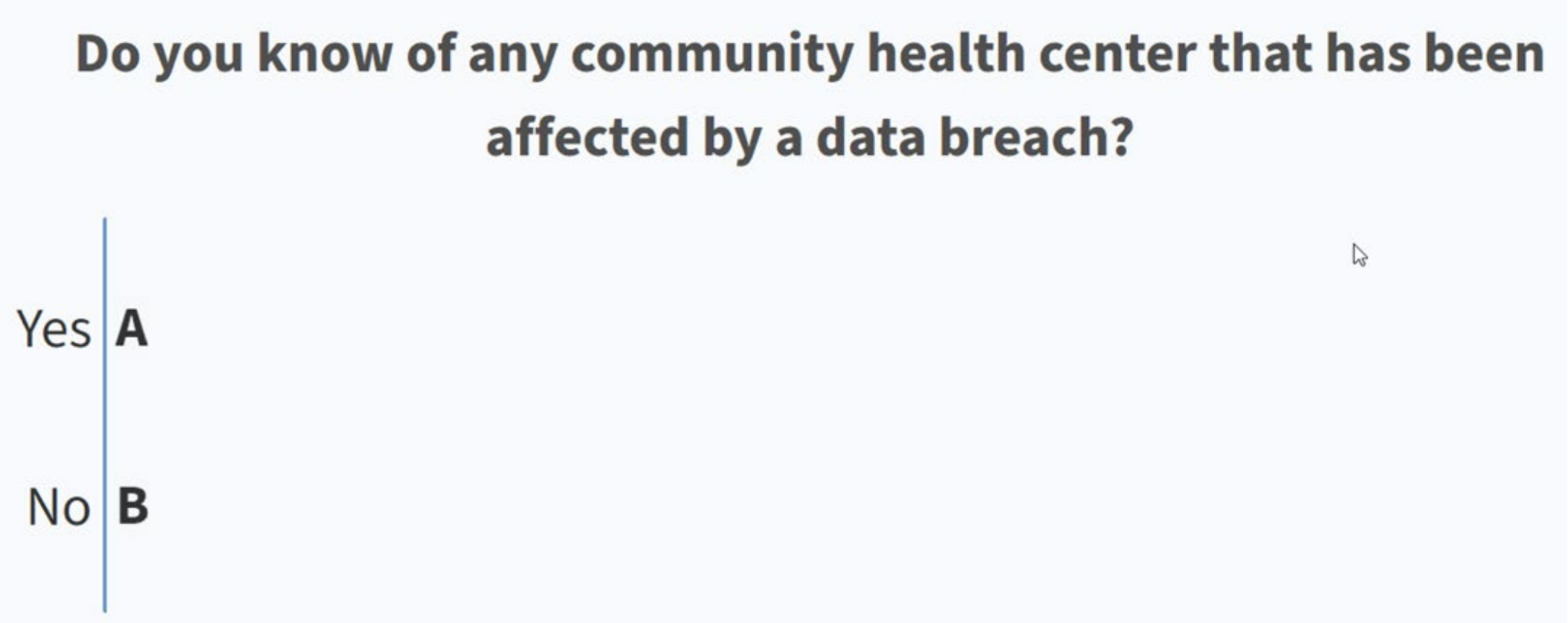
Health Choice Network
a Family of Health Centers
25+ Years of Service

Understanding the Essentials

1. Data Breaches: Who Do They Affect?
2. How Do Hackers Find Their Targets
3. Cybersecurity 101: Basic Toolsets



Have you been affected by a Data Breach?



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

Have You Heard of Lapsus$

In late March 2022 City of London Police said: "Seven people between the ages of 16 and 21 have been arrested in connection with an investigation into the hacking group Lapsus$. They have all been released under investigation. Our inquiries remain ongoing."

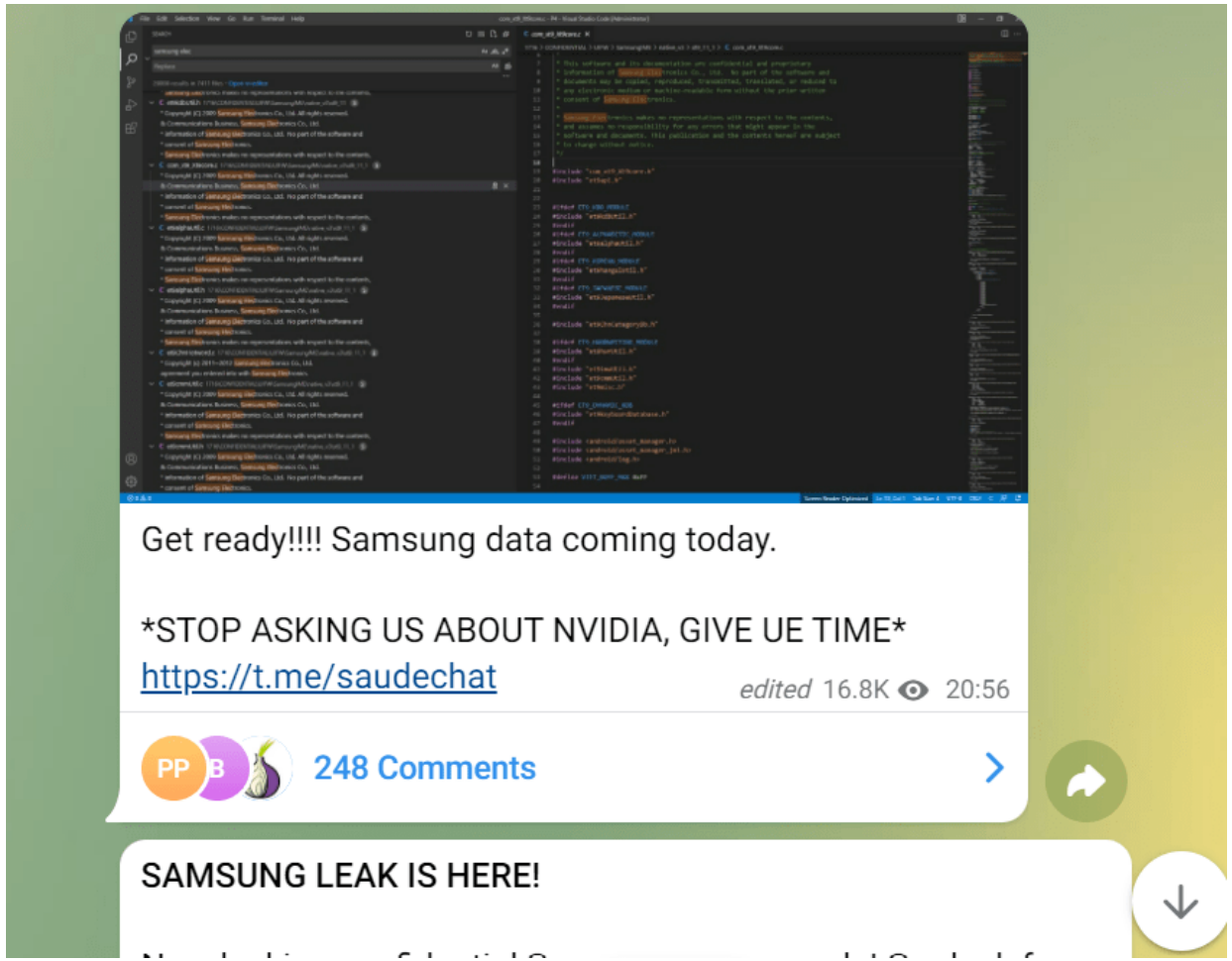
LAPSUS$, in a short time since emerging on the threat landscape in late 2021, has gained notoriety for its breaches of Impresa, NVIDIA, Samsung, Vodafone, Ubisoft, Microsoft, Okta, and Globant… all between November 2021 and March 2022.

The last message was posted on the group's Telegram channel said: "A few of our members has a vacation until 3/30/2022. We might be quiet for some times. Thanks for understand us - we will try to leak stuff ASAP."

Lapsus$ Data Breaches: T-Mobile

- In March 2022, a cybercrime group called Lapsus$ gained access to **Atlas**, a powerful internal T-Mobile system for managing customer accounts.
- Although T-Mobile said at the time that the systems accessed contained no customer or government information or other similarly sensitive information, it admitted that source code for several projects were stolen.
- The Lapsus$ group used access to the systems to perform SIM-swaps [hijacking a target's mobile phone by transferring the number to a device owned by the attacker], which would enable them to bypass Multi-Factor Authentication by intercepting texts to a smartphone

Lapsus$: Samsung Data Breach



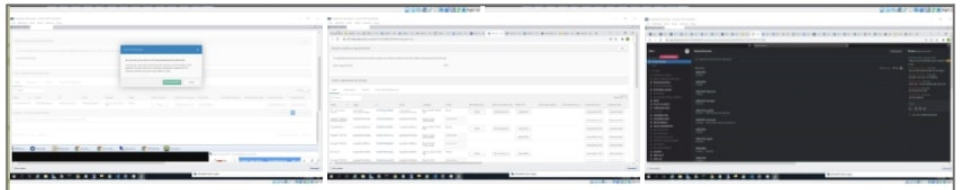
Source: Lapsus$ Telegram channel via Security Affairs

March 2022: Lapsus$ claimed to have stolen a huge trove of sensitive data from Samsung Electronics and leaked 190GB of alleged Samsung data as proof of the hack.

The gang announced the availability of the sample data on its Telegram channel and shared a Torrent file to download it. They also shared an image of the source code included in the stolen data.

Source code included algorithms for all biometric unlock operations and bootloader source code for all recent Samsung devices, including Samsung Galaxy smartphones.

Lapsus$: Okta Data Breach



Just some photos from our access to Okta.com Superuser/Admin and various other systems.

For a service that powers authentication systems to many of the largest corporations (and FEDRAMP approved) I think these security measures are pretty poor.

(yes we know the URL has a email address. the account is suspended - we dont care)

BEFORE PEOPLE START ASKING: WE DID NOT ACCESS/STEAL ANY DATABASES FROM OKTA - our focus was ONLY on okta customers.

In January 2022, Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider.

Further investigation by the service provider determined that an attacker did get access to the support engineer's laptop remotely.

Okta claimed that the scope of the intrusion was limited, and that the breach lasted for 25 minutes and affected only 2 customers.

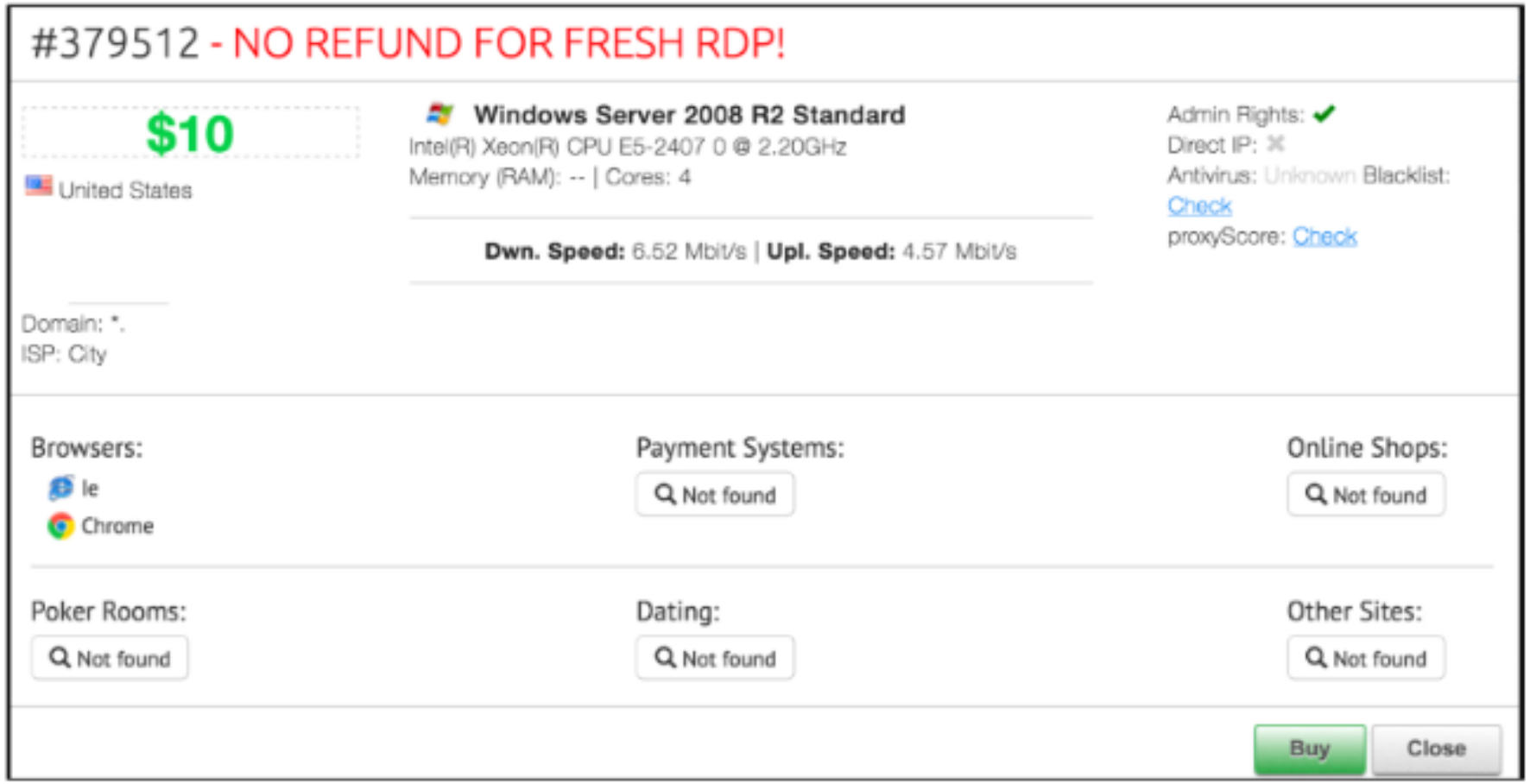
Note: Since my organization uses Okta as our identity management provider, I spent time and effort trying to determine if our organization was part of the breach when it was made public.

How Did They Pull Off Breach After Breach

- For the **T-Mobile** hack, they purchased stolen credentials from the Russian cybercrime market that provided them on a regular basis.

- Compromised credentials allow the threat actor to access internet-facing systems and applications, such as virtual private network (VPN), remote desktop protocol (RDP), virtual desktop infrastructure (VDI), or Identity providers (including Azure Active Directory, Okta).

Corporate Credentials Are Easily Purchased



Source: HelpNetSecurity

Hackers Leverage Stolen Credentials

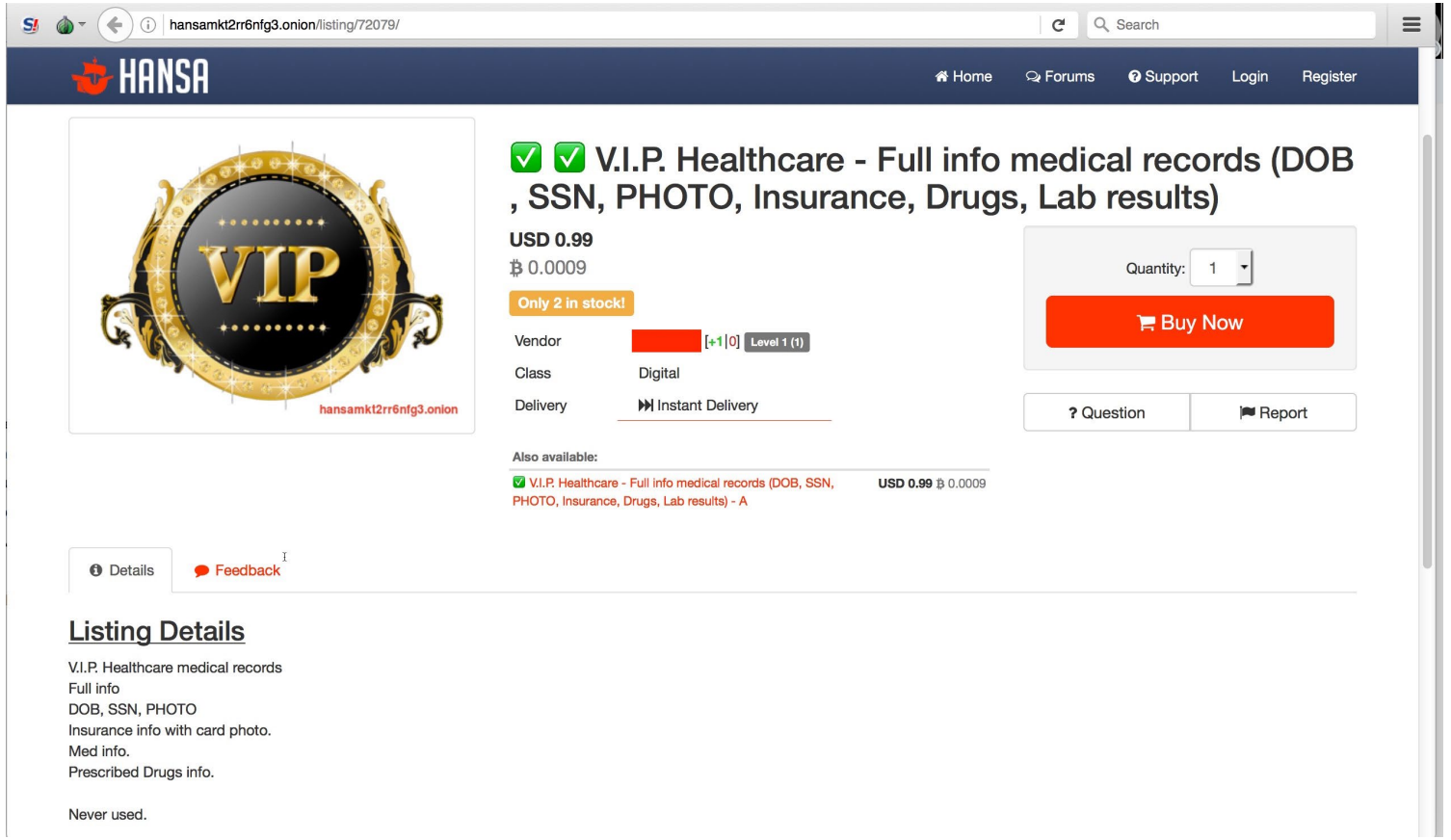
Leveraging stolen credentials is the No. 1 tactic used by hackers in recent years due to its relative ease and effectiveness. And since March 2020, the number of high-severity account takeover exposures where corporate credentials with plaintext passwords were exposed has increased by 429%, according to Arctic Wolf.

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

Where Do Patient Records Go?

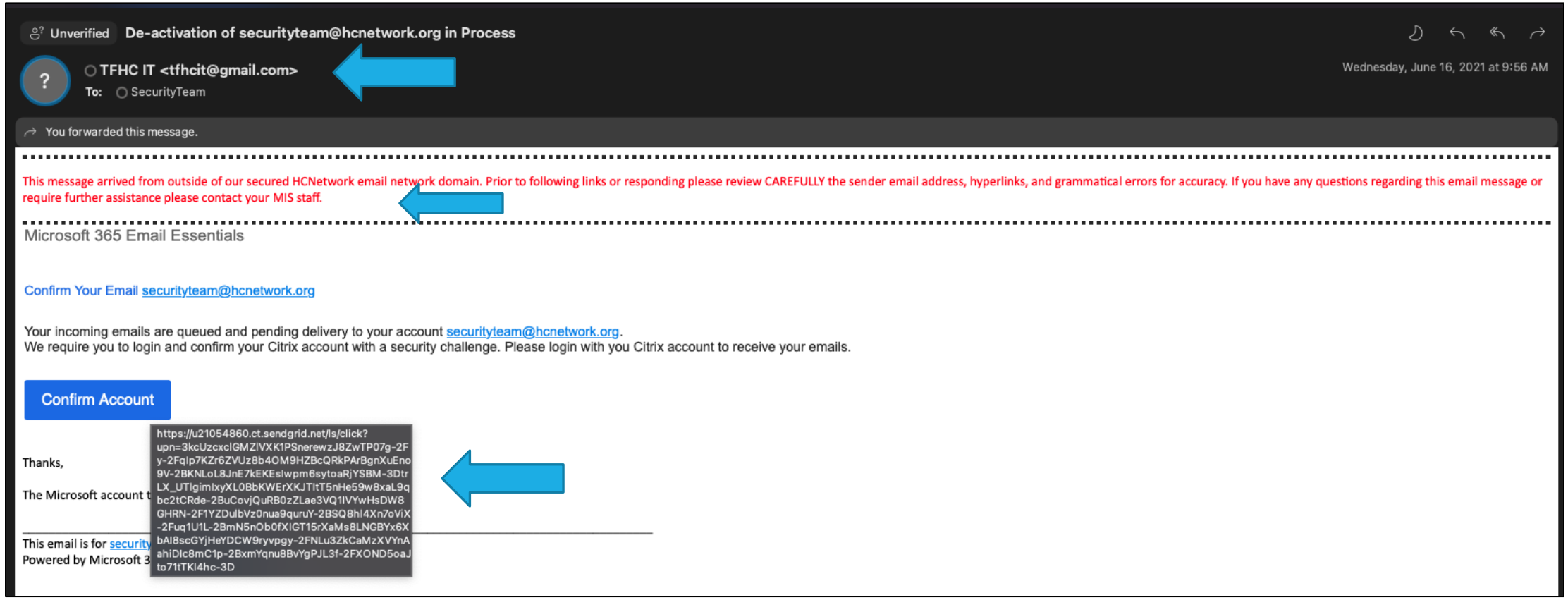


Source: Privacy Affairs

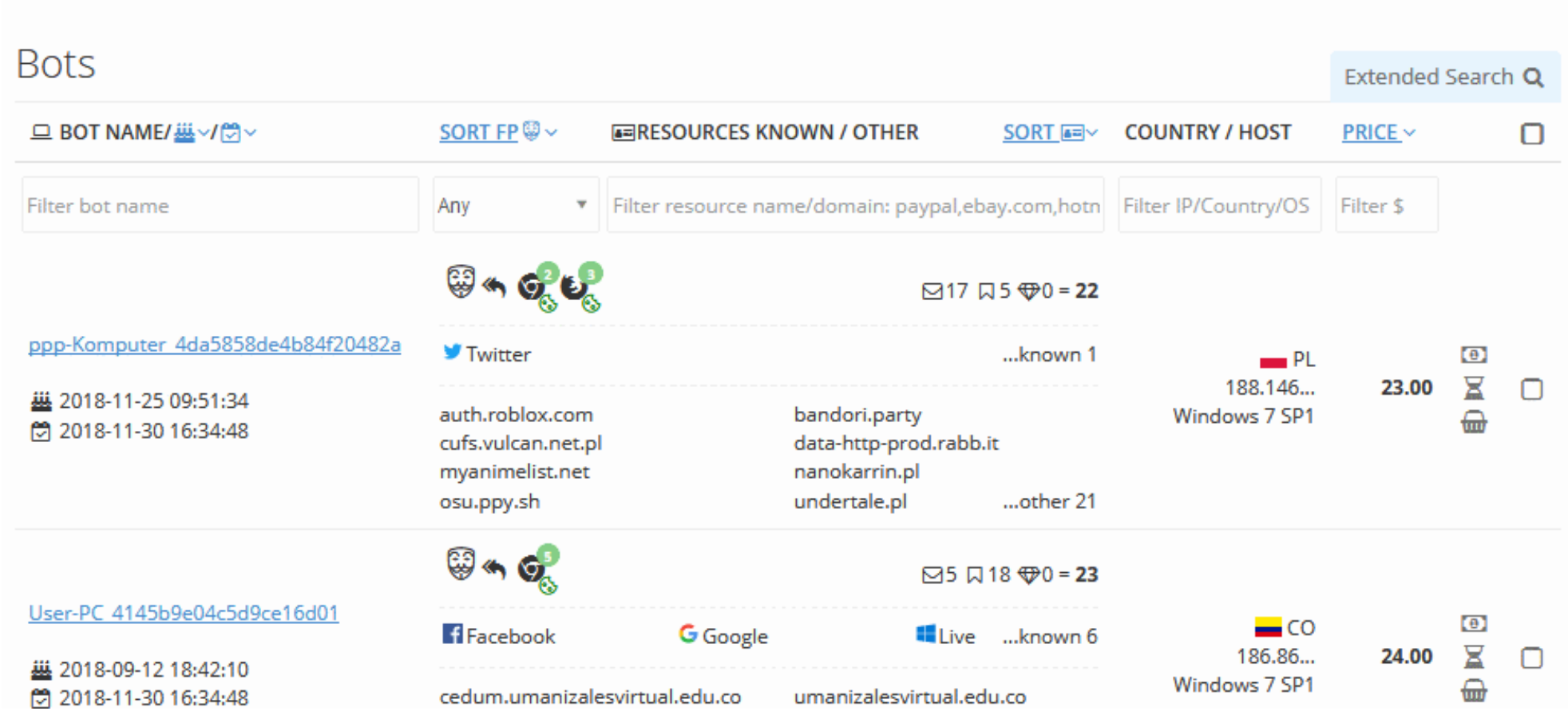
5 Most Common Ways Credentials Are Stolen

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

Spot The Phish

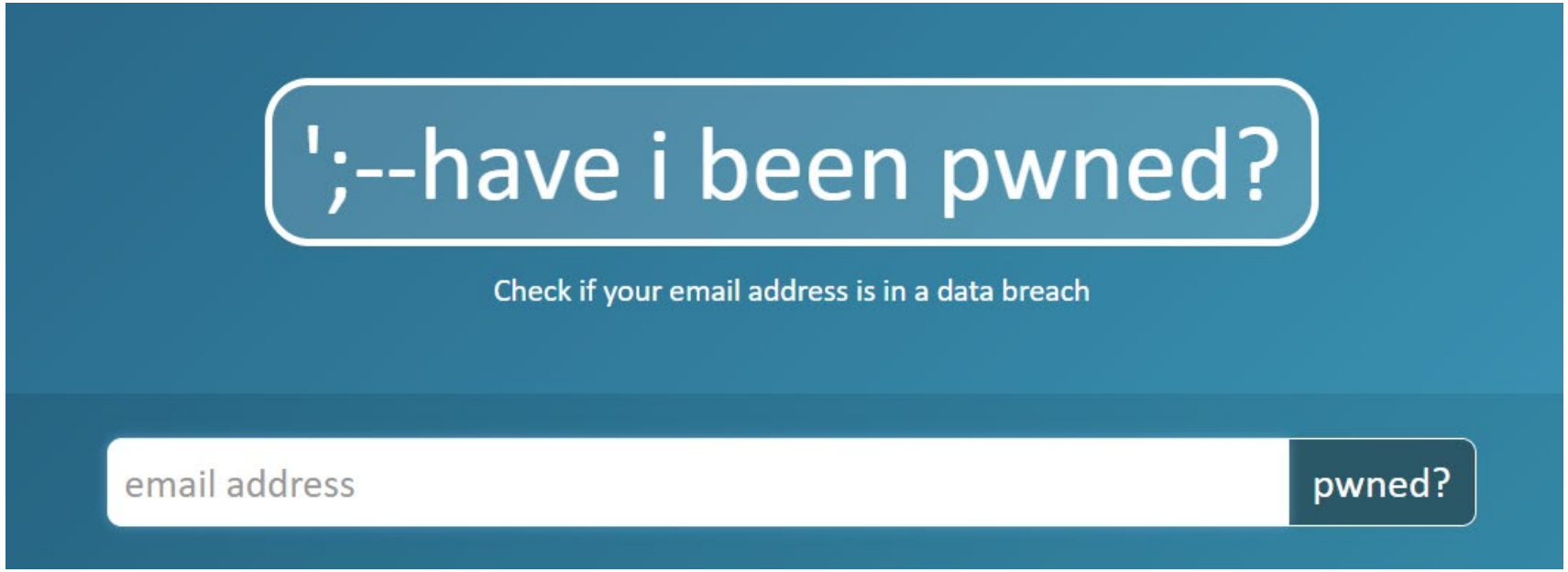


Malware Bots Are Easily Bought



Source: Genesis Marketplace Help Page (Dark web)

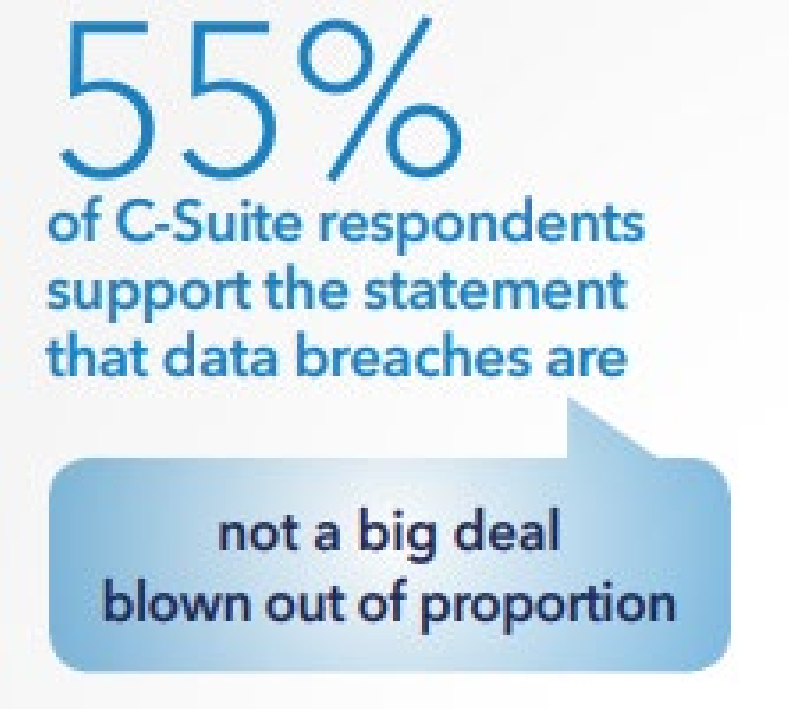
Have Your Credentials Been Stolen?



https://haveibeenpwned.com

Global Cost of Cybercrime

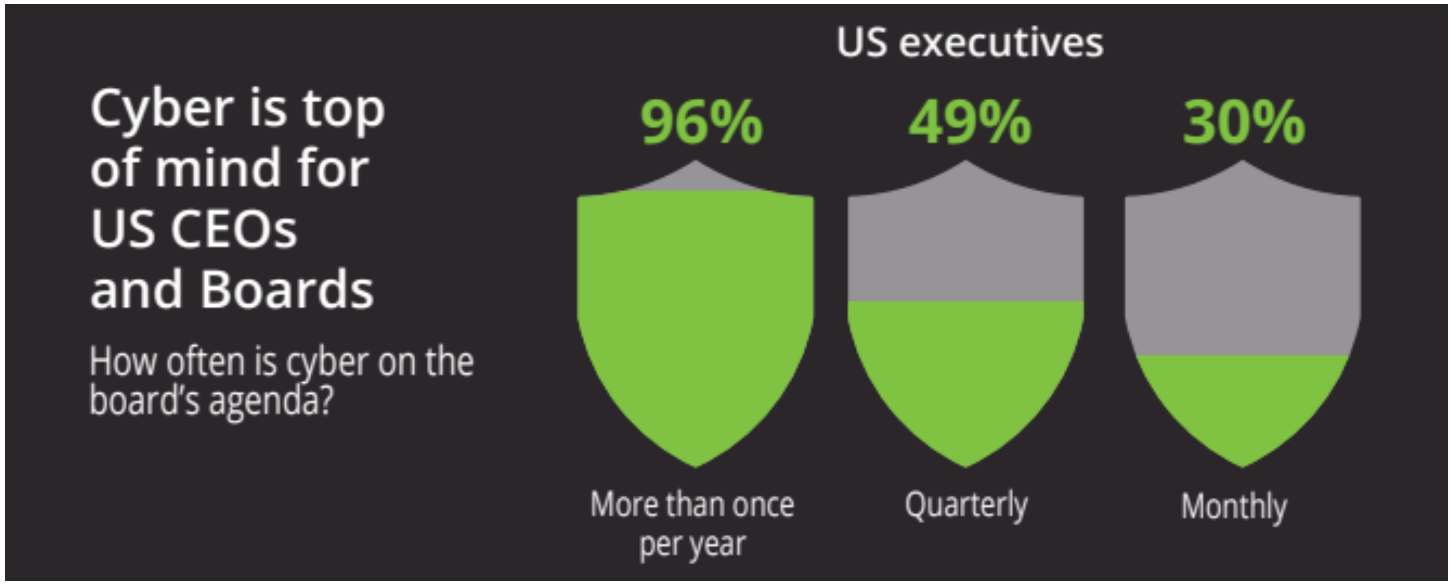
What do C-Suites Think?



Source: Shred-It Data Protection Report 2019

Source: Shred-It Data Protection Report 2021

Disconnect at the Top?

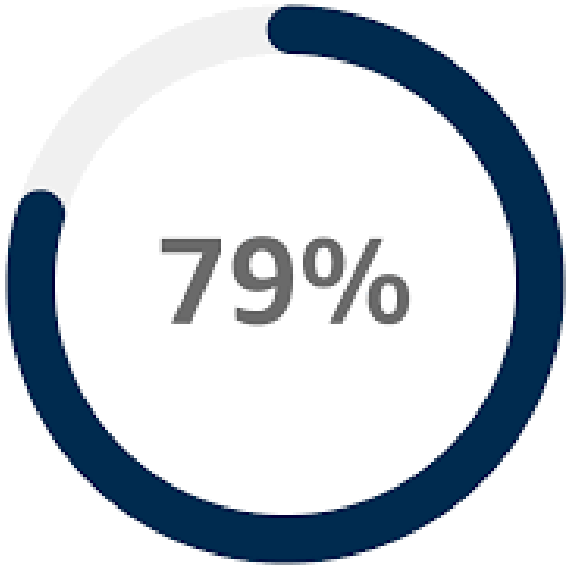


Source: Deloitte 2021 Future of Cyber Survey

More C-Suite responses

According to the Deloitte 2021 Future of Cyber Survey, **98%** of US Executives say their organization experienced one or more cyber incidents in the past year

Different Survey – Technology Leaders



According to Mimecast 2021 State of Email Security Report 79% of organizations (almost 4 out of 5) said their companies were hurt by their lack of cyber preparedness

What are the Obstacles?

38% Increases in Data Management, perimeter and complexities

35% Inability to match rapid technology changes

31% Need for better prioritization of cyber risk across the enterprise

=

New Technology

New Approach

More Resources

Selling to the C-Suites

Cybersecurity 101

Cost of A Data Breach

2021 had the highest average cost in 17 years

Data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17-year history of this report.

Remote work due to COVID-19 increased cost

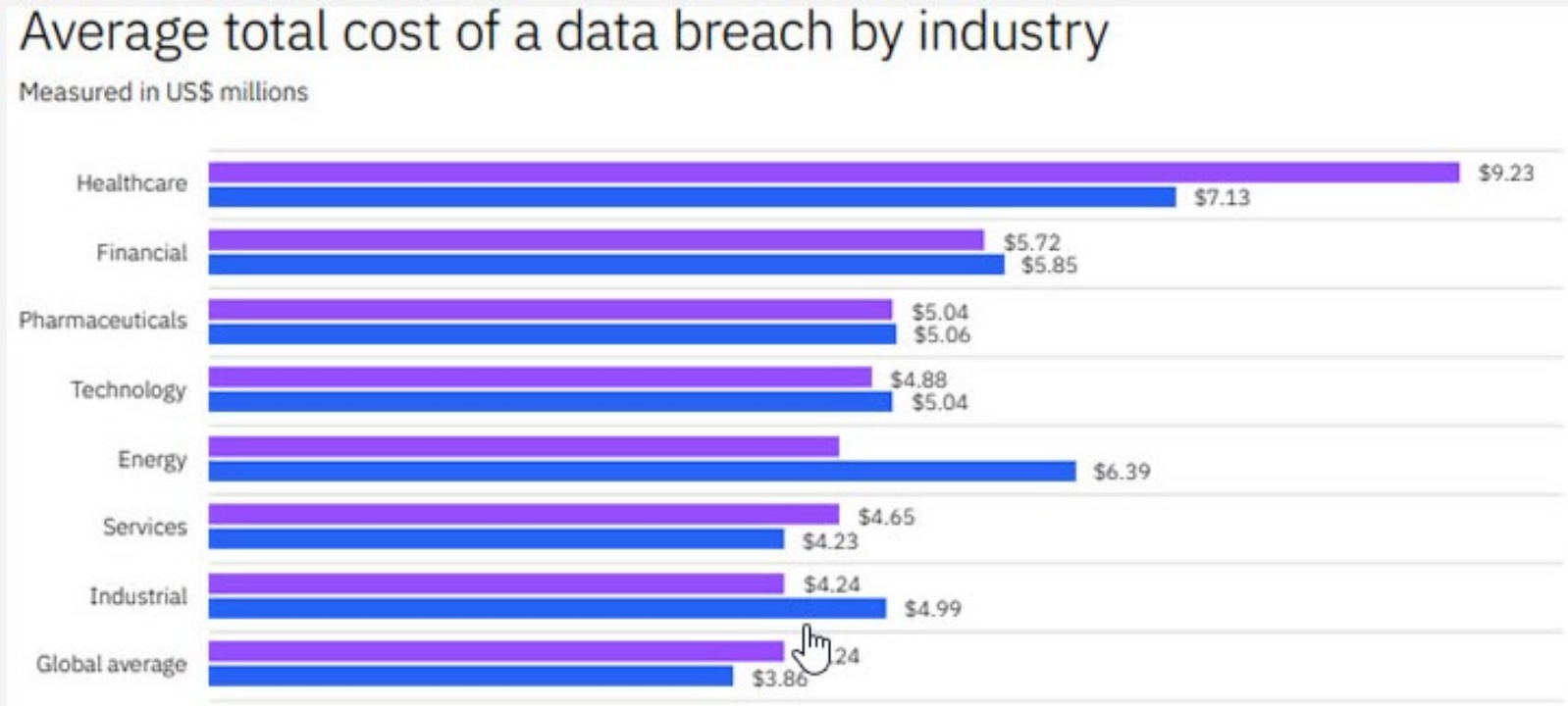
The average cost was USD 1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor.

Compromised credentials caused the most breaches

The most common initial attack vector, compromised credentials, was responsible for 20% of breaches at an average breach cost of USD 4.37 million.

Source: IBM Cost of A Data Breach Report 2021

Healthcare Costs



The average cost of a Healthcare Data Breach has ballooned to **$9.23M**, up 29% from 2020.

Could It Happen To My Organization?

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
- Combined, that is an ENTIRE YEAR

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

From the California Attorney General's Website

Advent Health Partners, Inc.	07/14/2021, 08/27/2021	04/27/2022
Los Angeles County Department of Mental Health	10/18/2021	04/20/2022
Sea Mar Community Health Centers	12/12/2020, 03/15/2021	04/01/2022
Super Care, Inc. dba SuperCare Health	07/23/2021	03/25/2022
Comprehensive Health Services	04/09/2020, 10/22/2020	03/16/2022
Entira Family Clinics	12/04/2020	01/13/2022
Scripps Health	04/29/2021	06/01/2021
Rady Children's Hospital San Diego	06/20/2019, 01/03/2020	02/21/2020
Rady Children's Hospital-San Diego	03/29/2018	05/03/2018
Rady Children's Hospital-San Diego	06/06/2014, 11/30/2009, 11/30/2010, 11/30/2011	06/20/2014
Rady Children's Hospital – San Diego and Rady Children's Hospital Foundation – San Diego	02/07/2020, 06/04/2020	10/29/2020

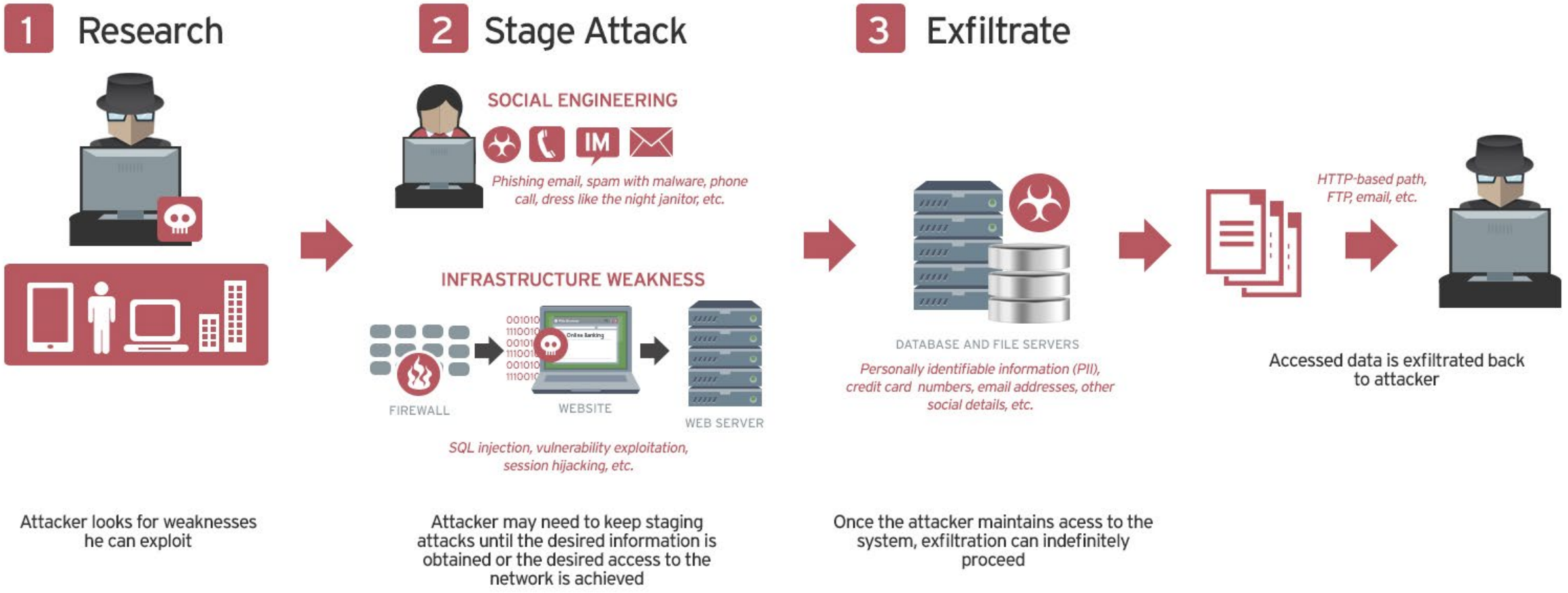
How Do You Know You Haven't Been Breached Already?

How Do Hackers Find Their Targets?

Research:

- A company's organizational structure
  - Who does what in the organization
- Financial information
  - How much do they spend on what
- People no longer with the company
- Posts on Social Media
- Look for any possible vulnerability in a company's IT infrastructure

Anatomy of A Data Breach



Source: Trend Micro

The Easiest Ways To Get Hacked

- Phishing/Social Engineering: It is much easier to hack a human than any IT infrastructure
- Viruses/Worms/Ransomware And Other Malware: Downloaded from websites
- Denial of Service (DDOS) Attacks/Botnets
- Security Vulnerabilities Due to Unpatched Software
- Brute Force: Weak Passwords/Credentials

Don’t Be The Low Hanging Fruit

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

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.

Can Your Risks Be Quantified?

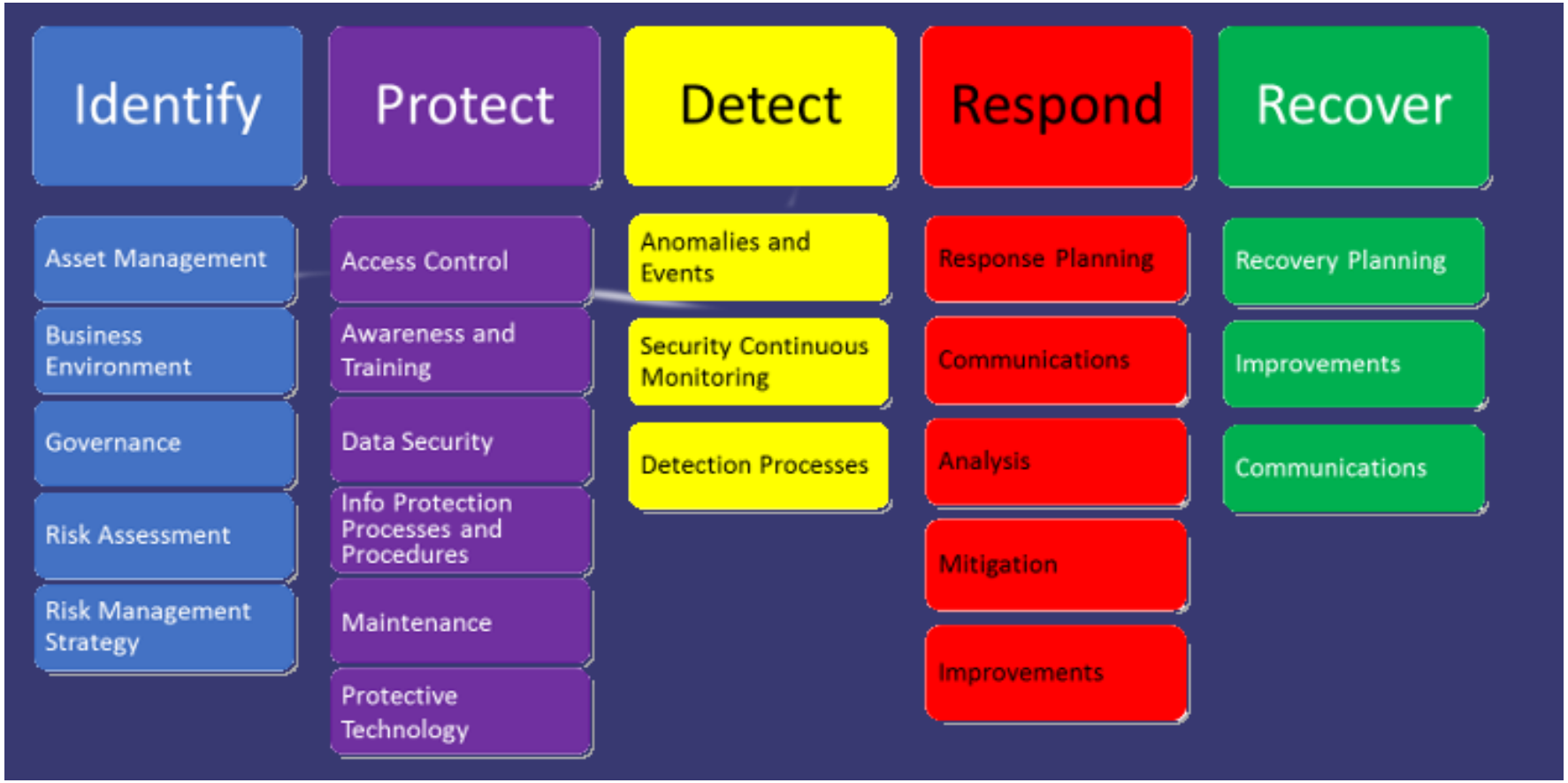
NIST Cybersecurity Framework

- 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



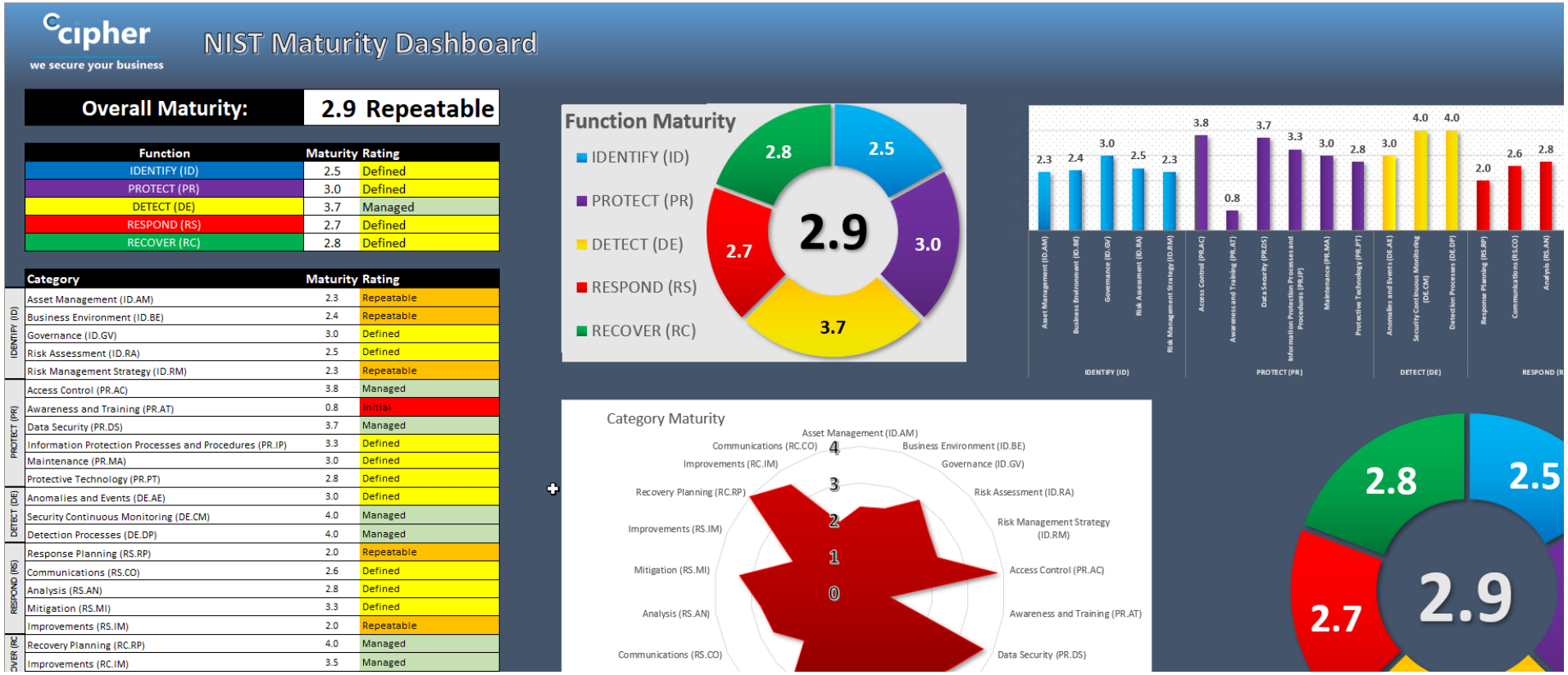
NIST Framework: Baseline Assessment

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



Function	Maturity	Rating
IDENTIFY (ID)	2.5	Defined
PROTECT (PR)	3.0	Defined
DETECT (DE)	3.7	Managed
RESPOND (RS)	2.7	Defined
RECOVER (RC)	2.8	Defined

	Category	Maturity	Rating
IDENTIFY (ID)	Asset Management (ID.AM)	2.3	Repeatable
	Business Environment (ID.BE)	2.4	Repeatable
	Governance (ID.GV)	3.0	Defined
	Risk Assessment (ID.RA)	2.5	Defined
	Risk Management Strategy (ID.RM)	2.3	Repeatable
PROTECT (PR)	Access Control (PR.AC)	3.8	Managed
	Awareness and Training (PR.AT)	0.8	Initial
	Data Security (PR.DS)	3.7	Managed
	Information Protection Processes and Procedures (PR.IP)	3.3	Defined
	Maintenance (PR.MA)	3.0	Defined
	Protective Technology (PR.PT)	2.8	Defined
DETECT (DE)	Anomalies and Events (DE.AE)	3.0	Defined
	Security Continuous Monitoring (DE.CM)	4.0	Managed
	Detection Processes (DE.DP)	4.0	Managed
RESPOND (RS)	Response Planning (RS.RP)	2.0	Repeatable
	Communications (RS.CO)	2.6	Defined
	Analysis (RS.AN)	2.8	Defined
	Mitigation (RS.MI)	3.3	Defined
	Improvements (RS.IM)	2.0	Repeatable
RECOVER (RC)	Recovery Planning (RC.RP)	4.0	Managed
	Improvements (RC.IM)	3.5	Managed

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

Cybersecurity Best Practices

PEOPLE

- Password/User Mgmt
- Security Awareness
- Organizational Culture
- Compliance
- Security Awareness Training
- HIPAA & Cyber Educated staff
- Security Officer/Leader
- Role-Based Access

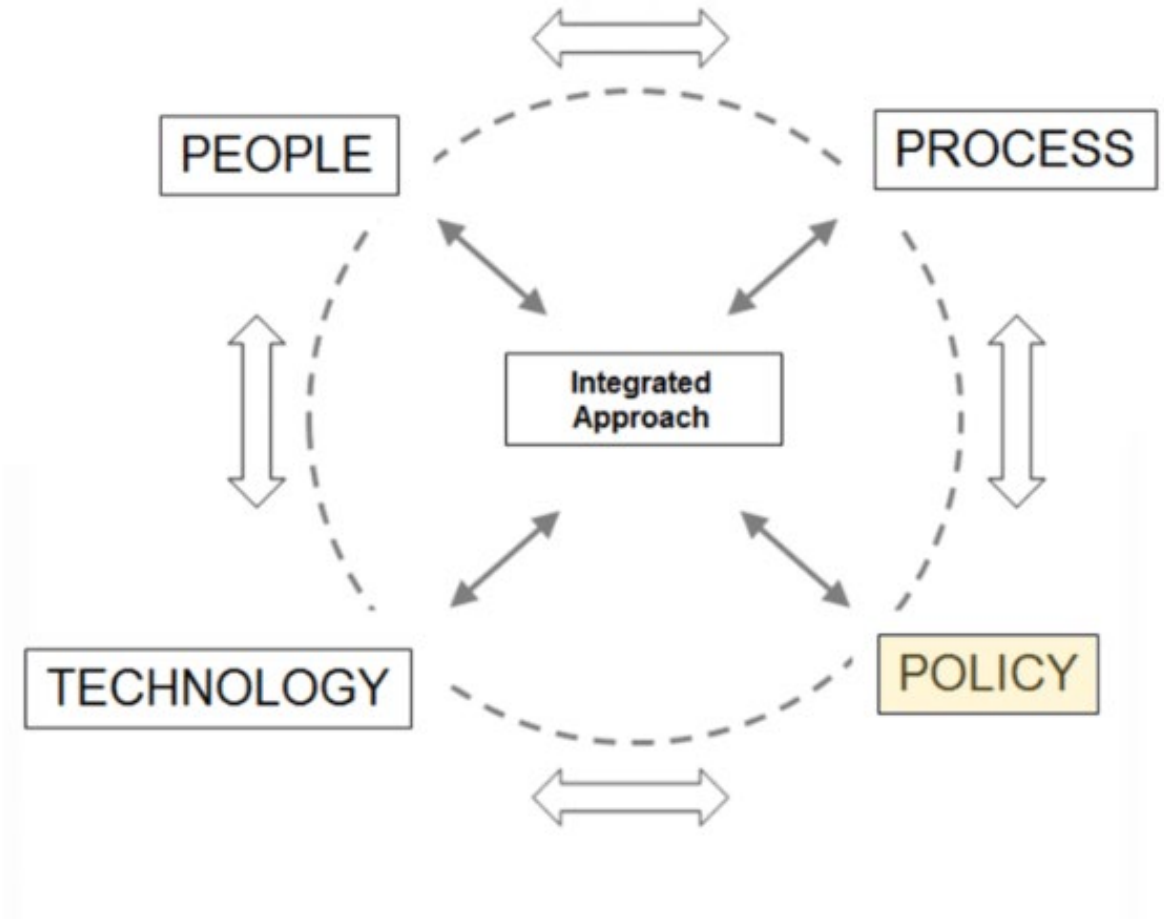
TECHNOLOGY

- Firewall/VPN
- Patch Management
- Mobile Device Mgmt (MDM)
- End-point security
- Security Awareness Training
- Data Protection/DR
- Intrusion Detection Systems
- Intrusion Protection Systems
- Device Encrypsion
- Segmented Networks
- MFA (Multi-Factor Auth

PROCESS

- Ongoing Risk Management
- Data Backup
- Cyber-insurance in place
- Compliance
- Incident Response
- Business Continuity Processes
- Network Pen Testing
- Ongoing Audits

3 P's and a T



A strong cybersecurity posture requires strong policies

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/

Know What You Have

- Identify your devices
- Identify your applications
- Identify your risks

Note: There are a multitude of free tools that can do these

Know Your Risks/Vulnerabilities

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

Testing 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

Maintain Your Defenses

- Secure your perimeter
  - Firewall: Perimeter Network Security
  - VPN: Remote Network Security
  - Antivirus/AntiMalware/Endpoint Security
- Update your devices
  - Endpoint Security: System and Application Patching
- Encrypt your data
  - Data/Disk/Device Encryption
- Secure your websites
  - Encryption Tools
  - External penetration testing

Beyond Simple Passwords

- Implement Strong Passwords
- Manage Your Passwords
  - Tools to generate, store, and manage passwords*
- Tools for 2FA
  - Hardware or SMS authenticators

Prevent Phishing and Malware

- Network Monitoring
  - Intrusion Detection
  - Audit Log/Log Monitoring
- Antivirus and Ad Blockers
  - Spam Blocker
- DNS Security
  - DNS Recursive Service*
- Security Risk Awareness
  - End-User Training

A Word About Security Awareness Training

- $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.

Backup and Recover

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

Protect Your Email and Reputation

- Implement DMARC
  - Domain-based Message Authentication, Reporting & Conformance
- Audit Your Social Media Accounts

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

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.

NATIONAL ASSOCIATION OF Community Health Centers®

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

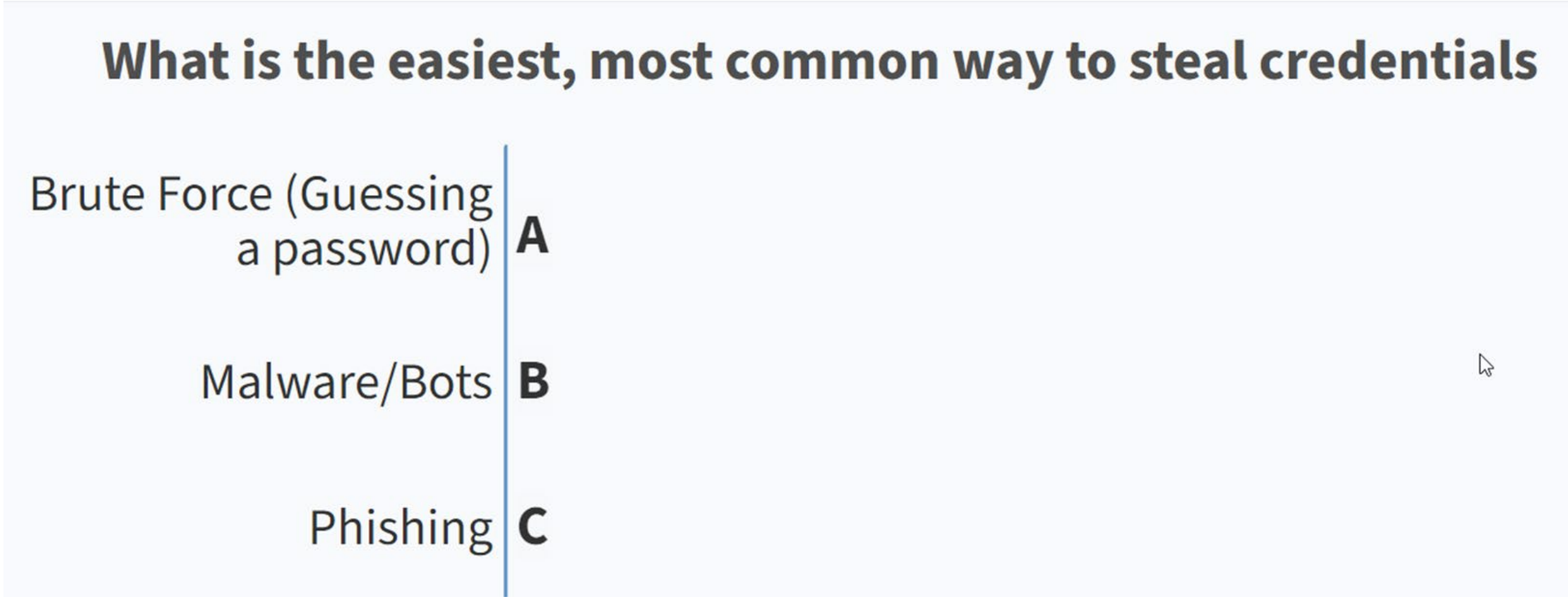
Getting Cyber Insurance Right

- 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

Tabletop Exercise



Tabletop Exercise

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

Call IT	A
Turn off your computer	B
Yell for help	C
Do nothing	D

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

Facebook.com/nachc

Instagram.com/nachc

Linkedin.com/company/nachc

YouTube.com/user/nachcmedia