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
Understanding the Essentials

1. Data Breaches: Who Do They Affect?
2. How Do Hackers Find Their Targets?
3. Cybersecurity 101: Basic Toolsets
A DECADE OF DATA BREACH ...AN EVOLUTION

First identified as an industry issue in 2003, data breaches have now become part of consumer vocabulary. Data breaches have evolved from credit card fraud with financial consequences to medical identity theft with life-threatening implications.
Have you been affected by a Data Breach?

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

<table>
<thead>
<tr>
<th>Yes</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>B</td>
</tr>
</tbody>
</table>
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.
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

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

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

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

This message arrived from outside of our secured HiNetwork email network domain. Prior to following links or responding please review CAREFULLY the sender email address, hyperlinks, and grammatical errors for accuracy. If you have any questions regarding this email message or require further assistance please contact your MSX staff.

Microsoft 365 Email Essentials

Confirm Your Email securityteam@hcnetwork.org

Your incoming emails are queued and pending delivery to your account securityteam@hcnetwork.org.

We require you to login and confirm your Citrix account with a security challenge. Please login with you Citrix account to receive your emails.

Confirm Account

Thanks,

The Microsoft account

This email is for security.

Powered by Microsoft 365
Malware Bots Are Easily Bought

Source: Genesis Marketplace Help Page (Dark web)
Have Your Credentials Been Stolen?

'https://haveibeenpwned.com'

Check if your email address is in a data breach

email address pwned?

https://haveibeenpwned.com
Global Cost of Cybercrime
What do C-Suites Think?

55% of C-Suite respondents support the statement that data breaches are not a big deal blown out of proportion

Source: Shred-It Data Protection Report 2019

4 OUT OF 10 BUSINESS LEADERS rate the risk of an attempted data breach in the next 12 months as a 4 or 5 on a 5-point risk scale

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

Remote work due to COVID-19 increased cost

Compromised credentials caused the most breaches

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.

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.

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?

Mandiant Security Effectiveness Report

DEEP DIVE INTO CYBER REALITY

53% of 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
• Combined, that is an ENTIRE YEAR

Source: ©IBM Security Cost of a Data Breach Report 2020
From the California Attorney General’s Website

<table>
<thead>
<tr>
<th>Organization</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advent Health Partners, Inc.</td>
<td>07/14/2021, 08/27/2021</td>
<td>04/27/2022</td>
</tr>
<tr>
<td>Los Angeles County Department of Mental Health</td>
<td>10/18/2021</td>
<td>04/20/2022</td>
</tr>
<tr>
<td>Sea Mar Community Health Centers</td>
<td>12/12/2020, 03/15/2021</td>
<td>04/01/2022</td>
</tr>
<tr>
<td>Super Care, Inc. dba SuperCare Health</td>
<td>07/23/2021</td>
<td>03/25/2022</td>
</tr>
<tr>
<td>Comprehensive Health Services</td>
<td>04/09/2020, 10/22/2020</td>
<td>03/16/2022</td>
</tr>
<tr>
<td>Entira Family Clinics</td>
<td>12/04/2020</td>
<td>01/13/2022</td>
</tr>
<tr>
<td>Scripps Health</td>
<td>04/29/2021</td>
<td>06/01/2021</td>
</tr>
<tr>
<td>Rady Children’s Hospital San Diego</td>
<td>06/20/2019, 01/03/2020</td>
<td>02/21/2020</td>
</tr>
<tr>
<td>Rady Children’s Hospital-San Diego</td>
<td>03/29/2018</td>
<td>05/03/2018</td>
</tr>
<tr>
<td>Rady Children’s Hospital – San Diego and Rady Children’s Hospital Foundation – San Diego</td>
<td>02/07/2020, 06/04/2020</td>
<td>10/29/2020</td>
</tr>
</tbody>
</table>
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

1. Research
   - Attacker looks for weaknesses he can exploit

2. Stage Attack
   - Social Engineering
     - Phishing email, spam with malware, phone call, dress like the night janitor, etc.
   - Infrastructure Weakness
     - SQL injection, vulnerability exploitation, session hijacking, etc.

3. Exfiltrate
   - Database and File Servers
     - Personally Identifiable Information (PII), credit card numbers, email addresses, other social details, etc.
   - HTTP-based path, FTP, email, etc.
   - Accessed data is exfiltrated back to attacker

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 don’t have to run faster than the bear to survive. You just have to run faster than the guy next to you.

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
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

- 22 Sub-Categories
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy
  - Access Control
  - Awareness and Training
  - Data Security
  - Info Protection Processes and Procedures
  - Maintenance
  - Protective Technology
  - Anomalies and Events
  - Security Continuous Monitoring
  - Detection Processes
  - Response Planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements

www.nachc.org
NIST Framework: Baseline Assessment

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

0: Nope, we’re not doing this at all
1: It’s ad hoc, we only do it in cases where we have to
2: We do it... but it’s not consistent or structured
3: We do it consistently... but it’s not best practice and it could be better aligned with the business
4: We do it well and I wouldn’t be ashamed to show this to my peers
5: 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 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 Encryption
- 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
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

Create 3 copies of data (1 primary and 2 back ups)
Keep data on at least 2 types of storage media (local drive, NAS, tape etc)
Store 1 of these offsite (secure storage, cloud etc)
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.
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.
# Tabletop Exercise

What is the easiest, most common way to steal credentials

<table>
<thead>
<tr>
<th>Method</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brute Force (Guessing a password)</td>
<td>A</td>
</tr>
<tr>
<td>Malware/Bots</td>
<td>B</td>
</tr>
<tr>
<td>Phishing</td>
<td>C</td>
</tr>
</tbody>
</table>
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?

Michael Sanguily
MSanguily@hcnetwork.org

Arnell Mendoza
Amendoza@queenscare.org
ARE YOU LOOKING FOR RESOURCES?

Please visit our website www.healthcenterinfo.org