2023
California Area
IHS Tribal
Leaders
Meeting

Cybersecurity Hot Topics

Ransomware, MFA & Cyber-Insurance

Reese Weber, MBA, CISSP
Chief Information Security and Privacy Officer
California Area Indian Health Service

Ransomware

What keeps you up at night...

What are the potential threats to your operations?

Ransomware

By the numbers…

Ransomware represents over 70% of healthcare breaches

Frequency of attacks doubled from 2020 to 2021

Several IHS clinics have been hit with ransomware in the last couple of years – at least 2 in California Area

Ransomware

The bad guys know no boundaries – they know the small clinics are often the easiest targets

2/3 of healthcare orgs hit with ransomware in 2021

2/3 of *those* resulted in encryption of health records

Ransom paid was averaged at $197K

Recovery costs avg $900K

HHS HIPAA Individuals Breach Reporting Requirements

Ransomware is always considered a breach

For all breaches:

- Notify affected patients by 1st class mail
- Post front page of website for 90 days
- Report via major media broadcasting

HHS HIPAA Other Breach Reporting Requirements

For breaches affecting 500+ patients

- Report to HHS Secretary within 60 days
- Media notification - Press release to local, major news outlets

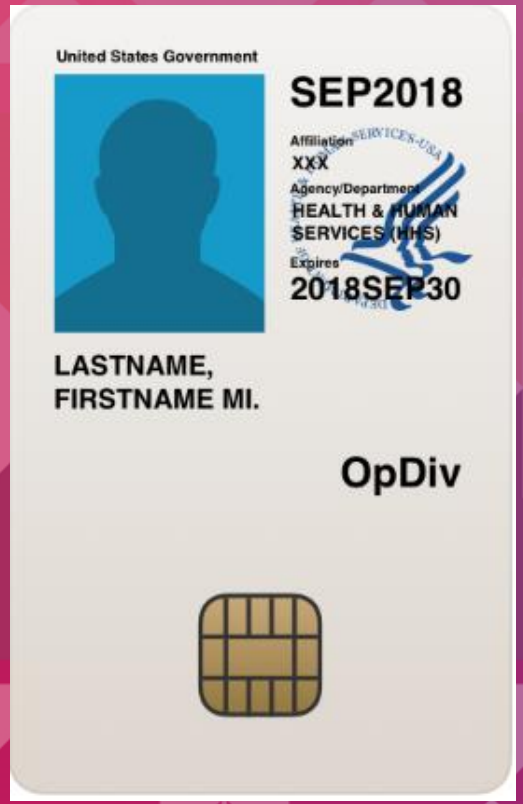
Multi-factor authentication and email security

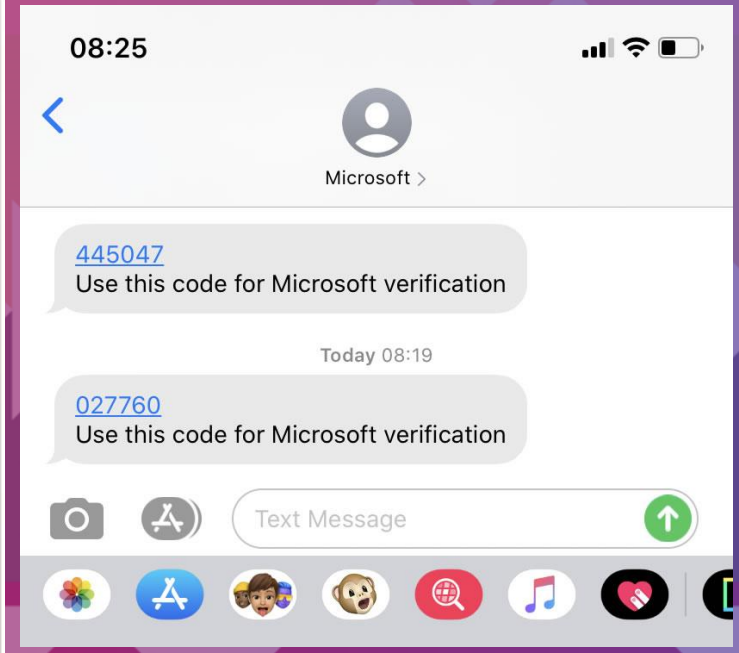
The first lines of defense

90% of ransomware attacks come from phishing emails

Multi-Factor Authentication

Requiring a combination of 2 or more credentials





E-Mail Security

Locking your largest door

- Primary communication tool in the workplace
- 300+ billion emails sent and received DAILY
- Employees receive an average of 120 emails a day.
- 94% of cyberattacks start with a malicious email.
- Cybercrime cost more than $4.1 billion in 2020

E-Mail Security

Locking your largest door

- Choose a reputable email host
- Outsource your email security by using cloud email products like Office 365
- Take advantage of advanced threat protection offerings
- Require Multi-Factor Authentication
- Train folks on incident response by holding phishing exercises
- User Awareness (ISSA)
- Invest in protections against e-mail spoofing/impersonation

Cyber Insurance: Liability insurance to cover attacks, malware and breaches.

Where does insurance fit in?

Cyber Insurance

What does a typically policy cover?

Policies typically cover costs that are directly associated with a security breach: documenting and investigating the attack, data recovery and hardware repairs, notifying consumers and regulatory agencies, crisis management and PR damage control, etc.

Depending on your provider, cyber insurance plans may also offer additional forms of first-party and third-party coverage, including paying for the lost income of your business or covering fines, legal fees and settlements that result from a breach.

Cyber Insurance

What does a typically policy cover?

Data breaches

Theft or loss of client information

Business interruption costs

Forensic investigation

Data recovery

Extortion

Fines & penalties

Crisis management costs

Potential legal costs

Cyber Insurance

What DON'T the policies typically cover?

- Bodily injury
- Property damage
- Intentional dishonest acts by the insured
- Acts of war and terrorism
- Utility failure

Cyber Insurance

Qualification Process

- Employees must receive regular awareness training
- All PCs must have AV be kept up to date
- All PC's must have endpoint protection
- Central patch management to ensure critical updates are applied in time.
- Must have a network firewall
- Data Backups
- Vulnerability scanning/pen testing
- User accounts and permissions must be actively managed and audited
- Admin and other privileged accounts must be secured using MFA

Cyber Insurance

Disadvantages for small clinics

Many healthcare organizations, particularly rural health networks and community hospitals, are seen as softer targets because their IT budgets are relatively limited, and they are more likely to be using dated systems that are more difficult to protect.

This creates challenges when they shop for cybersecurity insurance, as carriers may charge higher premiums or deny coverage outright based on the higher perceived risk.

Cyber Insurance

How to potentially reduce your premiums and increase chances of coverage

- Implement a Zero Trust architecture
- Create, test and maintain a robust Disaster Recovery Plan, COOP plan, and Incident Response Plans.
- Implement, document and test Backup and Recovery solutions
- Have I mentioned MFA? MFA for all users!
- Perform a HIPAA Secure Risk Assessment
  - Use the reported feedback to identity weaknesses and harden your operations as much as possible

Cyber Insurance

How to potentially reduce your premiums and increase chances of coverage using internal audits and certifications

- Obtain ISO 27001 Certification
  - A standard for IT security procedures developed by the International Organization for Standardization (ISO) in collaboration with the International Electrotechnical Commission (IEC). The ISO 27001 framework sets out requirements for the implementation, operation and continuous improvement of an information security management system
- Be SOC-2 or SOC-Cybersecurity Compliant
  - American Institute of CPAs (AICPA) offers Systems Organization Controls (SOC) reports
  - Reports contain detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

Cyber Insurance

How to potentially reduce your premiums and increase chances of coverage using internal audits and certifications

- Obtain NIST CSF Compliance
  At its core, the NIST CSF covers 5 key functions that an organization's cybersecurity program should address: Identify, Protect, Detect, Respond, Recover. These five areas are subdivided into categories (larger topics such as Asset Management or Detection Processes) and subcategories (specific requirements such as "Response and recovery plans are tested"). To assess how well your business meets these targets, the framework measures successful implementation of these criteria in 4 tiers.

Cyber Insurance

Cost Benefit Analysis

- Healthcare ransomware attacks cost between $1M-$10M
- Insurance premiums have steadily raised over the years
- Insurance providers continue to add more requirements and stipulations for coverage, which can limit access to coverage
- Consider the cost of premiums versus the potential costs of a breach
- Consider the costs of conforming to insurance company's standards

Questions?

THANK YOU!

Reese Weber, MBA, CISSP
Theresa.weber@ihs.gov

Resources:

Ransomware Attacks on Hospitals Have Changed | Cybersecurity | Center | AHA
Ransomware attacks against healthcare organizations nearly doubled in 2021, report says - Thomson Reuters Institute
Breach Notification Rule | HHS.gov
U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)
Multi-Factor Authentication Fact Sheet (cisa.gov)
What is Email Security? | Microsoft Security
Cyber Insurance for Healthcare: Benefits, Requirements, Premiums | HealthTech (healthtechmagazine.net)
Quarterly Cyber Insurance Update: February 2023 (wsj.com)
What you should know when considering cyber insurance in 2023 | CSO Online
SOC 2® - SOC for Service Organizations: Trust Services Criteria (aicpa.org)

THANK YOU!

Reese Weber, MBA, CISSP
Theresa.weber@ihs.gov