Cybersecurity and the Role of the Trustee

- Cybersecurity landscape
- Regulation, Security Culture and the board's role
- Risk reduction

Tom Hallisey, Digital Health Strategy Director

Agenda

Cybersecurity in the healthcare environment now

- Useful definitions
- Troubling statistics
- Why healthcare

Regulations and standards

- Regulatory justification
- State and federal programs

Managing cyber risk – the board's role

- Building compliance culture
- Providing focus

Cybersecurity in the healthcare environment now

Ransomware attacks in healthcare

- Healthcare is the field most targeted for ransomware attacks.
  - Accounting for more than other industries combined.
- Numbers of attacks and dollar amounts rising for years.
  - Decrease in recent months

What is ransomware?

- Ransomware is malicious software (malware).
- Encrypts a computer or database to deny access or control by the owner until a ransom is paid.

AND/OR

- Steals data and threatens to release if not paid
- First – must gain access through attack vector.
  - Ransomware is not itself a *means* of attack.

Attack vector – employee

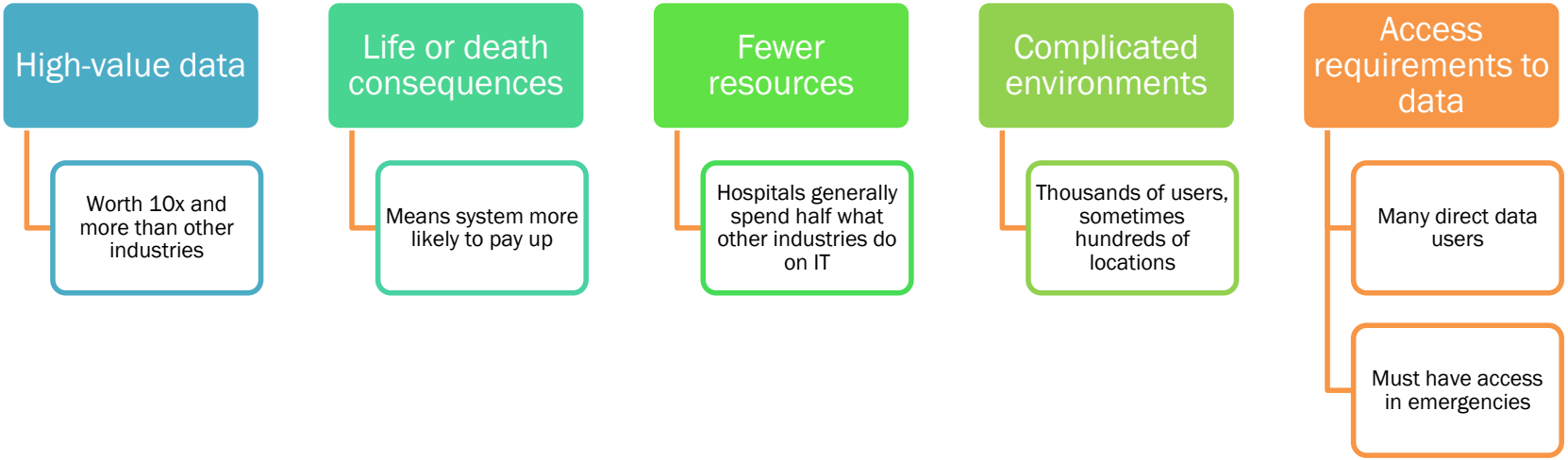
Weakest link or strongest asset?

- **Vector** is a means of network access.
- **Phishing** is the main means of attack.
  - Most often through email, but phone becoming more common; voice increase 10x in past 2 years.
  - Very effective and always adapting.
  - Often called social engineering – attempt to “con” user.
- Bogus links or websites.

Third-party risk

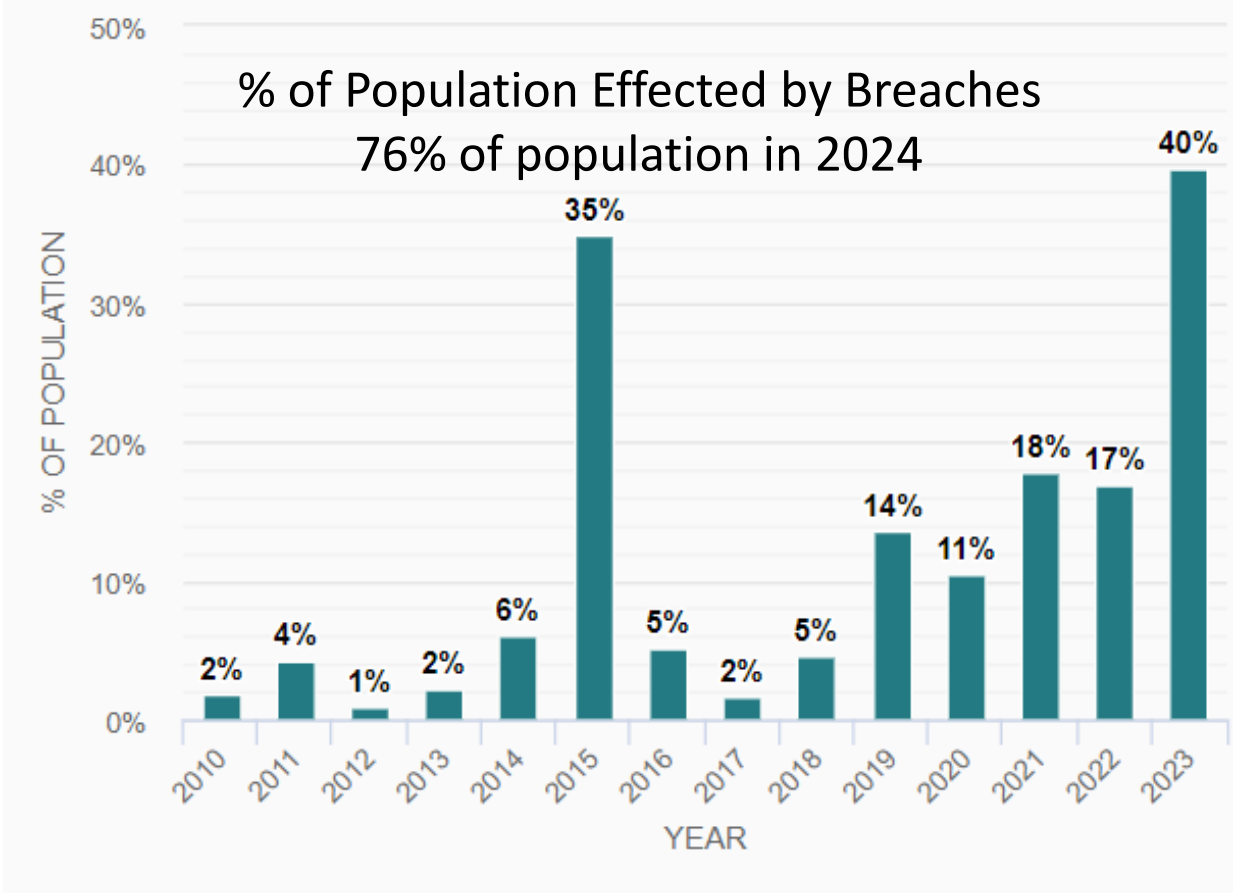
- More than half of incidents and growing.
- Even though the risk of a third-party data breach is high, a survey revealed only 41% of surveyed healthcare companies had a complete inventory of third parties that have been provided with access to their networks.
- To blame for 58% of individual's records affected.

Why healthcare?



Current state

- Cost of over $10 million per incident.
- 276 million patients records breached last year.
  - 20-30 million patients effected this year.
  - 736 incidents.
- Rise of GenAI – vishing 10-fold increase.



Source: https://www.hipaajournal.com/2024-healthcare-data-breach-report

Breaches are costly

Annual reports by IBM calculate healthcare breaches costing over $10 million per incident for 2023.

Financial penalties increase the cost to the breached HCO.

High-profile media releases about individual security incidents damage reputations.

Studies show community health affected by one system downtime.

Factors that increase breach costs

- Supply chain breach
- Security system complexity
- Shadow IT
  - Software and systems outside central IT control

Regulations and standards

Cyber regulatory environment

- Emergency care affected by ransomware.
  - Diversions and cancellations affect whole community.
- Reaction to long EHR downtimes.
- DOH focus on patient care.

Requirements – policies and procedures

- NY Regulations – built on standards
- Not just to meet regulations – good practice.
- Building culture of compliance.
- Based on annual risk assessment.
- Signed off by CISO.
- Reported to and approved by board.
  - At least annually.

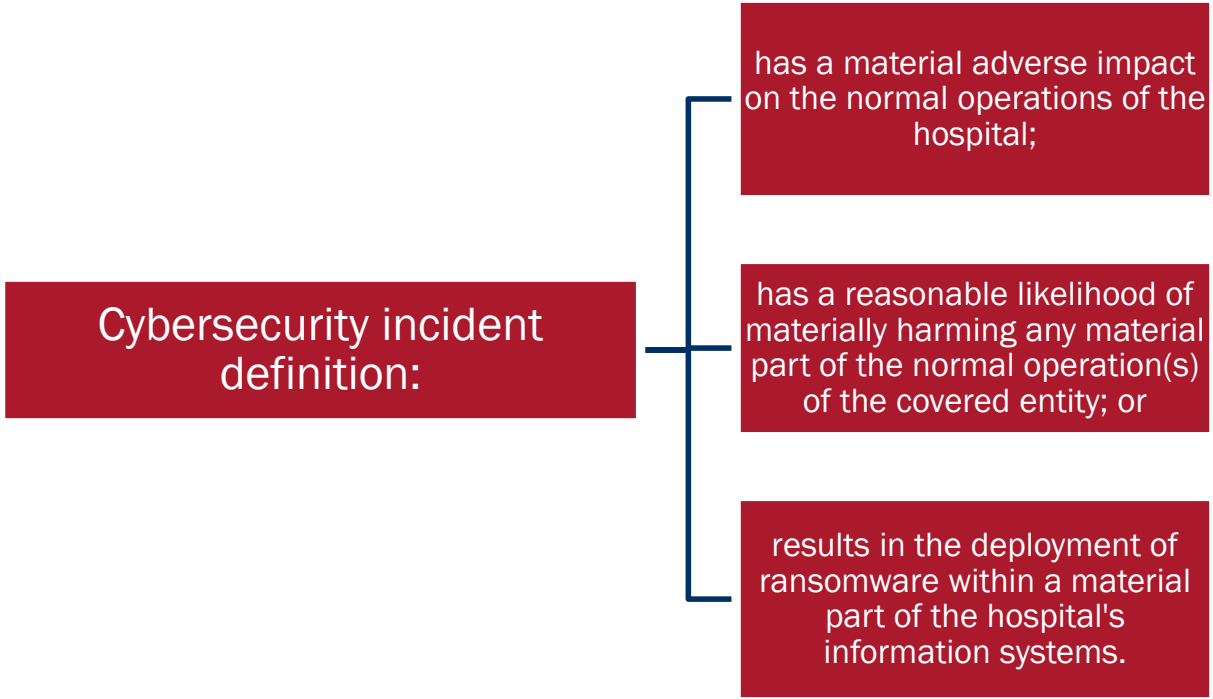
Regulations NY State

Apply only to Hospitals

Based on NIST Standards

- Must report cybersecurity incidents within 72 hours.
- Required to establish a comprehensive program covering risk assessment, response, recovery and data protection.
- Annual risk assessment must be performed.
  - Already a requirement under HIPAA.
- Cyber program and plan must be presented and approved by the board at least annually.
  - Based on risk assessment.
- Hospitals require cybersecurity policies:
  - asset management
  - access and control
  - training
  - monitoring
  - incident response
- Conduct regular cybersecurity testing, including scans and penetration testing.

Must notify DOH within **72 hours** of a determination that a cybersecurity incident has occurred



Regulations NY State

Based on NIST Standards

- The regulations set policies for selecting and monitoring **third-party vendors'** cybersecurity practices.
- Hospitals are required to run tests of their **response plan** to ensure that patient care continues while systems are restored back to normal operations.
- Hospitals are required to establish policies and procedures for evaluating, assessing and testing the security of externally developed applications used by the hospital.
- Hospitals must establish a chief information security officer (CISO) role, if one does not exist already, to enforce the new policies and to annually review and update them as needed. Can be contracted and part time (fractional).
- Hospitals are required to use **multi-factor authentication** (MFA) to access the hospital's internal networks from an external network.

Gaps in cybersecurity programs

- Robust cybersecurity training programs
- Strong/tested incident response plan
- Cybersecurity staffing
- Frequency of vulnerability assessments
- Asset management
- Third-party risk management

Gaps in cybersecurity

For areas of higher risk and non-compliance:

- Perform assessments.
- Leverage a to-and-toward approach — perfection not the goal.
- Focus on high criticality assets first.
- Remember intent and scope.

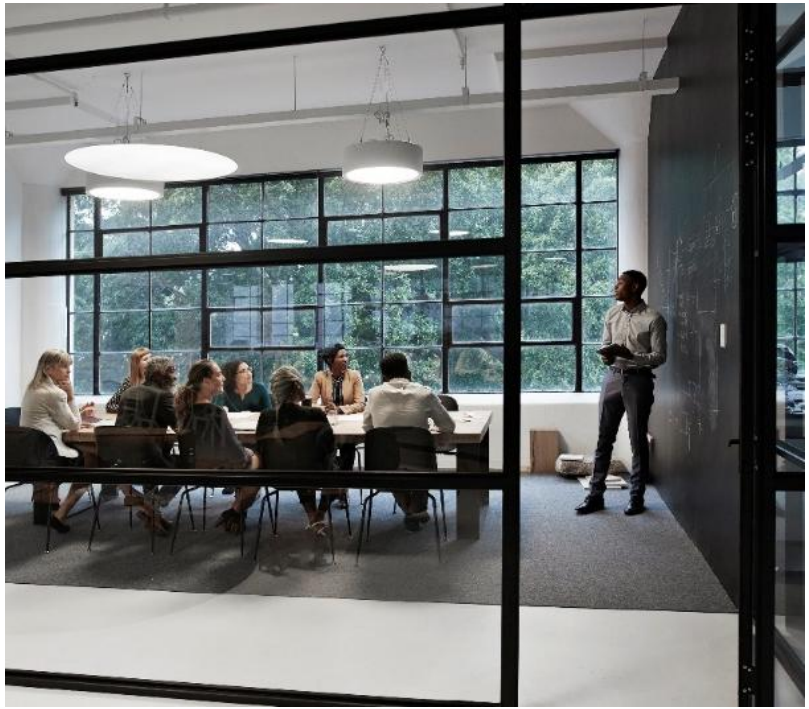
Top risks

- More User ID, less malware.
  - Social engineering.
  - Vishing – 10x increase
  - Target human weakness or error rather than a flaw in software.
- Third-party attacks – supply chain.

Managing cyber risk – the board's role

The board's role in compliance

- Similar to other risks and regulations such as HIPAA.
  - Create accountability.
  - Understand that compliance is a journey.
  - Familiarize yourself with the regulations.
  - Risk mitigation program – may save millions.



The board's role in compliance

What questions should be asked?

- Is there an annual risk assessment conducted by outside vendor? Penetration tests conducted by third parties?
- Do you see the cybersecurity strategic plan and is it based on the risk assessment?
- What are the top vulnerabilities and what are the mitigations planned for each?
- How are you meeting DOH regulations and what other frameworks is your plan based on? (NIST, HICP)

The board's role in compliance

- What workforce training and awareness are occurring?
- Do you have third-party management assessment and management plan?
- Business continuity and disaster recovery plan created and tested
  - Based on recovery time objectives
  - Include outreach to FBI, DOH, Insurer
- What compliance audits and external reviews are ongoing?
- What is the budget and resource allocation?

Resources

- HTNYS - Cybersecurity Oversight
- DOH - Cyber Regulations
- Health Sector Coordinating Council

Thank you

Thomas Hallisey
thallise@hanys.org
518.431.7719

The Statewide Voice for New York's Hospitals and Health Systems