NM Healthcare Financial Management Association Conference - 2022

Data Protection, Privacy, and Cybersecurity Risks – What and Where to Focus for 2023

Timothy Smit

Global Privacy and Cyber Risk Consulting Practice Leader

Lockton Companies

LOCKTON®

Outline

1) Current privacy and cyber risks
2) Best practices for Covered Entities and Business Associates
3) Recommended Controls (addressing current and future privacy and cyber risks)
4) Questions

Current privacy and cyber risks

The Global Cybercrime Pandemic

39 seconds

2007

Attacks were occurring every 39 seconds in 2007.

1.12 seconds

2020

In 2020, attacks were occurring every 1.12 seconds.

$10.5T

2025

By 2025, costs are anticipated to be $10.5 trillion.

Who are they?

- Threat groups or threat actors are everywhere
  - Asia, Europe, Africa, United States
  - Most are independent groups
  - Some are state-sponsored
  - Run like corporations, including customer service!

Why are they doing this?

- Origins of “hacking” was based on bragging rights
- Today, nearly every attack is financially motivated
  - Some may be espionage, masked with a financial demand
- Opportunity – Years of businesses being warned with little to no action towards additional security
- COVID-19 remote workforce transition

Why us?

Generally, not a targeted attack.

Healthcare, Higher Education, Retail, and Auto industries ARE the target for 2023!

Lack of resources; Culture; New technologies; Lack of security adoption due to culture; False sense of security with 'cloud' operations.

Medical devices – easy entry into organizations.

How does this happen?

Poor security controls

Old technology or lack of investment in security solutions.

Unresolved vulnerabilities such as missing patches, default settings, lack of knowledge.

End-of-Life technology used in production without any updated security controls.

(EoL = Non-compliant to HIPAA Security Rule)

Do not know what data you have, where it goes, who has access to it and retain outdated and obsolete information. (DATA MAP)

Cybersecurity misconceptions

"We are too small to be a target"

"We have all of our data in the cloud"

"We passed our audit"

"We are HIPAA Compliant"

Social engineering

The volume of daily email makes everyone susceptible to a "fake" malicious email.

Email attachments: "Hmm, this attachment from Bob that I wasn't expecting must be really important, it's making me enter my password to open it!"

Third party origin

Business Associates, Technology service providers, cloud hosts, vendors

Best practices for Covered Entities and Business Associates

CE and BA recommendations to consider

1. Complete list of Business Associates and review all agreements
   A. Ensure explicit language around incident response requirements
   B. Ensure explicit language around data protection measures
2. Covered Entity
   A. Engage your local OCR team *before* an incident
   B. Asset Inventory
      i. IF any End-of-Life equipment touches or stores **any ePHI,** your company is **non-HIPAA compliant.**
      ii. If you don’t have a data flow map – how do you know and prove that you are protecting all ePHI adequately?
      iii. Data backups – when did you last restore critical data from your data backups?
   C. Breach Coach – who is yours? If you don’t know right now, that is your homework before you leave here today – to identify who that is.

Recommended Controls and Focus

Protections

Priority

- Business Associate Agreements/Language/Requirements
- Data Map
- Data Classification
- Asset Inventory

Focused Controls

- Operationalize Privacy and Data Protection (Processes)
- Encryption
- Unique credentials (internal and external)
- Multi-factor authentication
- Endpoint protection and monitoring
- Alert monitoring
- Rapid patching of vulnerabilities
- Backups – Safe, segmented, inaccessible
- Education – Cyber awareness, phishing training

Readiness

Incident response planning – Proactive – Preparation and PRACTICE!

This is a business exercise, not a technical exercise.

Identify, Contain, and Respond!

1	2	3	4
Do not communicate over business email during an incident.	Who are the key department representatives that will be on the response team? • Legal • HR • Technical • Finance • Privacy • Who Else??	Who is your first external call to?? a) Insurance Carrier b) Insurance Broker c) Incident Response Vendor d) Breach Coach/External Law Firm	Who do you contact at your insurance broker?

Incident response

- Breach Coach/External Counsel
- Forensic IT firms
- Ransom
  - Threat actor negotiations (if needed)
  - Payment
    - Cryptocurrency – good and bad
    - OFAC
    - Trust in the threat group “keeping their word”
- Recovery
- Reputational Damage/Fallout
- Insurance

Questions

Independence changes everything.

LOCKTON®

UNCOMMONLY INDEPENDENT

© 2022 Lockton Companies. All rights reserved.