Data Management and Security: Developing a Strategy for Success

Allison Davis Ward, CISSP, CISA, CISM
Partner, CapinTech
11.10.21

CAPINTECH

The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

Polling Question 1

Do you want CPE?

Discussion for Today

- Recent breaches and threat landscape
- Challenges with data management and security
- Baseline practices and controls
- Advanced protections for securing data

July 2020

- Ransomware attack
- EMR system not breached but attackers potentially accessed Protected Health Information (PHI) of 85 patients due to EMR data **downloaded** in order to send claims to insurance companies
- Separate breach notification sent to over 308k patients believed not to be at risk but advised to be vigilant

July 2020

- “The attack was resolved and access to the electronic files returned. The attacker confirmed that none of the files were used or disclosed to anyone and any files taken were destroyed.”
- Since then…
  - Installed additional electronic safeguards
  - Provided additional employee education
  - Retained cybersecurity experts to aid in monitoring

July 2020

- Reported February 2021
- Server physically stolen
- Included name and SSN (old data, 10 years) that was provided during an application process or as a result of a prior US Bank acquisition

September 2020

- Employee downloaded customer data to a personal storage drive
- Information sent to a third party
- No indication of third party or intended use

Vastaamo.fi

October 2020

- Finnish psychotherapy clinic
- Attack from November 2018 resurfacing
- Ransomware leading to theft of patient data
- Multiple levels of extortion
  - Ransom demanded from clinic
  - Patients contacted directly
- Declared bankruptcy and shut down

Accellion

December 2020

- Secure file sharing and collaboration
- File Transfer Appliance (FTA) product reaching EOL
  - Retirement in April 2021 but only 75% on new system
- Vulnerability in vendor's software allowed exploitation
- Data transferred via FTA was sensitive — jackpot!
- Many industries affected

Metromile

January 2021

- Car insurance startup
- Security flaw on website form allowed hacker to obtain personal information submitted
- Issue present for 6 months (since June 2020)

blackbaud

power your passion

February 2020

- Cloud-based software used for financial and donor management functions
- Ransomware attack in February (undetected until May)
- Data on over 6 million individuals stolen (e.g., names, phone number, DOB, genders, etc.)
- Ransom paid for confirmation that data was destroyed
- Impacted numerous nonprofits

March 2021

- External accountant fell victim to phishing emails spoofing an owner of the business
- Microsoft 365 email credentials captured
- No on-premise or cloud EMR systems compromised
- Notified almost 35,000 patients about a breach that ***potentially*** involved protected health information

March 2021

- "Due to the size of the email system, we were unable to identify all potential patient information that may have been contained in the system."
- Since then…
  - Engaged outside consultant to assess security controls
  - Implemented stricter password policies
  - Enabled multi-factor authentication for mobile access
  - Implemented more robust vendor vetting process

CVS Health

June 2021

- Vendor posted an unsecured database containing 1B+ search records of CVS customers
- Cloud-based misconfiguration issue
  - Database lacked password protection
  - Identity access management not utilized
- No personal information but lots of meta data

Polling Question 2

What threat is most relevant to you and the security of your data?

Takeaways from Breaches

- Data protection relevant to all organizations
- Exposure stems from…
  - Cloud misconfigurations
  - External attacks and ransomware
  - Human error or malicious intent
  - Vendor issues
- Data exposure can be hugely impactful

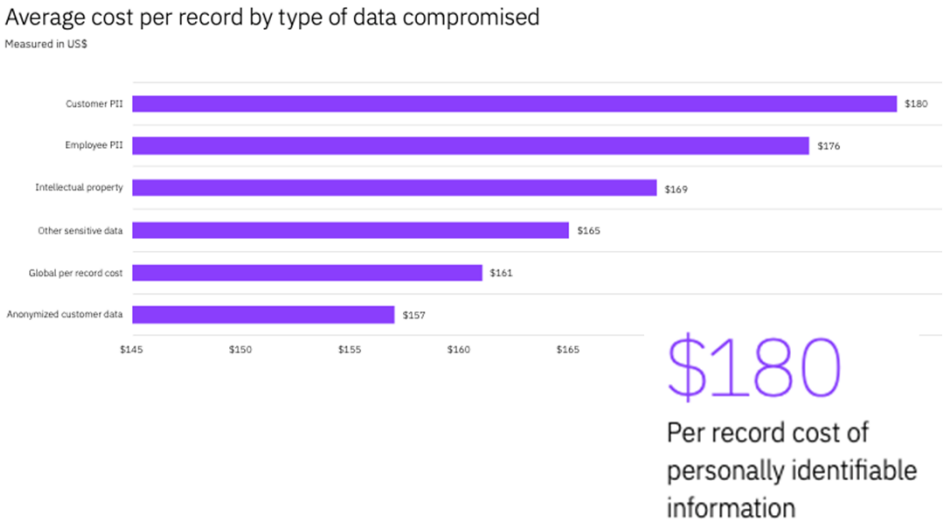
Takeaways from Breaches

- Many incidents can be prevented via baseline controls
  - Physical security
  - Restricting removable media
  - Monitoring for EOL solutions and patching, patching, patching!
  - End-user training
  - Securing cloud infrastructure
  - Multi-factor authentication

Why Managing and Protecting Data Is Important

- Reputational impact and loss of constituent trust
- Breaches are expensive
- IBM's 2021 Cost of Data Breach study
  - Total cost – $4.24M
  - Highest region – U.S. at $9.05M (followed by Middle East at $6.93M)
  - Highest industry – healthcare at $9.23M (followed by financial at $5.72M)

Why Managing and Protecting Data Is Important



Challenges with Data Management

- We have so much of it
- It's mobile (e.g., data transfers, email, file sharing)
- People have access to data they don't need
- Remote work adds complexity
- Data is often duplicated
- Data theft is lucrative, so threats remain relentless

$1.07m

Cost difference where remote work was a factor in causing the breach

What Next?

- Determine the who, what, where, when, and why
- Develop formal policies/procedures and train users
- Establish efficiencies and decrease complexity
- Ensure baseline controls exist to secure the data and support policies and procedures
- Plan for evolving protections

Your Inventory (The What)

- Can't manage what you can't measure
- Are our inventories data-centric?
- Do we know what we have?
  - Public information and general correspondence
  - Constituent, donor, or employee PII
  - Intellectual property

Your Inventory (The Where)

- Do we know where it is?
  - Source applications
  - Databases
  - Server shares
  - Local hard drives of end-user devices
  - Vendor data centers
  - Removable media (e.g., USBs)

Your Inventory (The Where)

- Do we know where it is?
  - Document reproduction technology
  - Backup infrastructure
  - Email or file transfer/cloud storage
  - Meeting solutions, including any recordings and chats
  - Personal devices (e.g., smartphones, tablets, home office devices)

Your Inventory (The Who, When, and Why)

- Do we know who accesses our data in each location and do they have a business need for it?
  - User access management processes should support the principle of least privilege
  - Don’t forget about vendors, consultants, and other non-employee access (e.g., system accounts)
- Do we know when data is accessed?
  - Strong logging capabilities are important in incident investigation and management

Polling Question 3

Do you have a data inventory?

Tips for Inventory Development

- Not a project just for IT
  - Departmental management should aid in identification
- Classify your data based on criticality or risk
  - All levels of data do not present the same level of risk or require the same level of management
- Assign data owners responsible for various data sets
  - Data owner is not always the application or system owner but can be

Tips for Inventory Development

- Identify instances of duplicated data
- Supplement with a data flow diagram to understand how the data moves
  - Into your organization
  - Within your organization
  - Outside of your organization to vendors, consultants, CPA firms, constituents, other applications, etc.

Establish Policies/Procedures and Train

- Define and communicate acceptable use
  - How to send information — internally vs. externally
  - Verification requirements for requests for data
  - Physical security of data and clean desk policies
  - How to handle data stored or accessed in home offices
  - Storing individual, shared, and departmental data

User Access Management Processes

- New hires, job changes, termination, resignations
- Group access profiles vs. granular rights by user
- Principle of least privilege
- Ongoing access reviews

Establish Application-Specific Controls

- Authentication controls
  - Password and lockout
  - Multi-factor authentication
- Retention settings
  - Keep only what you need
  - Reduce impact in event of system compromise

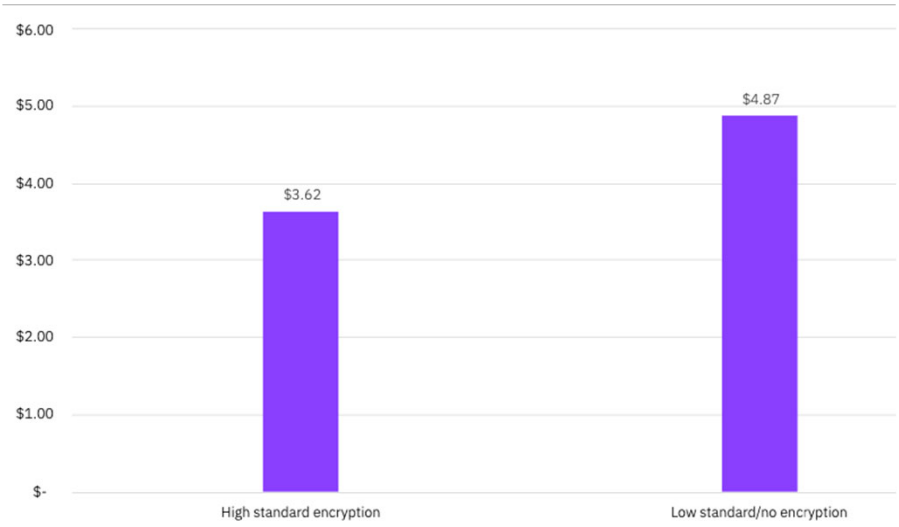
Streamline and Centralize the Data

- Decrease duplication where feasible
- Built-in reports for data that people need frequently
- Capitalize on dashboard capabilities
- Collaborative applications/tools
- Utilize automatic syncing and updates

Secure Data on Endpoints

- Periodically purge items in “Downloads” folders
- Map local folders to secure server shares
- Encrypt relevant hard drives
  - Non-negotiable if you handle sensitive data!
  - Consider the more “mobile” devices (e.g., laptops, USB drives, backup tapes, smartphones, tablets)

Impact of Encryption on Cost of Data Breach



Practice Baseline Cyber Hygiene

- Patch and anti-malware management
  - Critical to reduce risk of data compromise from malware or exploitation of vulnerabilities
  - Don’t forget to monitor vendor updates and releases or if their systems are reaching EOL
- Establish strong backup processes
- Incident response planning

Understand Your Vendor Controls

- Vendor management is key
  - Do you know what they are doing to secure your data?
  - Do you know what their backup practices are?
  - Do you know what they do regarding uptime/availability?
- You cannot outsource the oversight

Polling Question 4

Do we know how our vendors are protecting our hosted data?

Advanced Protections

- Consider three categories:
  - Authentication to access the data
  - Securing places where data is stored
  - Data loss prevention

Authentication to Access the Data

- More stringent authentication parameters
- Single sign-on (SSO) solutions
  - User ID + password (master login)
  - Secondary MFA layer via push, QR code, etc.
  - All other logins tied behind master

Securing Places Where Data Is Stored

- More complex endpoint management solutions
  - Robust anti-malware protections
  - More comprehensive patching
  - Application whitelisting
  - Centralized encryption
  - Behavioral monitoring

Securing Places Where Data Is Stored

- Mobile device management (MDM)
  - Containerization
  - Restricting what can be accessed on device
  - Enforcing critical controls
  - Data loss prevention

Data Loss Prevention

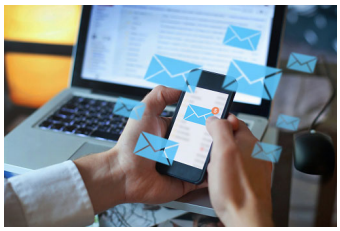
- Identify all the ways data can leave your organization physically or electronically
  - Removable media
  - Data transfers
  - Email and file sharing software
  - Cloud storage solutions and other cloud apps
- Implement controls to reduce the risk (or at a minimum, ensure security in transit)

Data Loss Prevention

- Restricting access to removable media
  - Encrypt authorized media
- Restrict devices from connecting to countries or locations you don't do business with
  - Don't do work in Russia? Why should your computer be sending data to a Russian IP address?

Data Loss Prevention

- Enhanced filtering and flags to meet compliance with GLBA, GDPR, HIPAA, etc.
  - Scanning emails for data that meets a sensitive format (e.g., nine digits could mean SSN)
  - Restrict, review, or auto-encrypt
- Identification of auto-forwarding rules created (key for incident response)



Data Loss Prevention

- Restrict sharing of data to only emails within your organization
- Limit number of downloads of shared files
- Auto-expire shared links after a set period

Data Loss Prevention

- Limit screenshots or access on unauthorized devices
- Make data “read only”
  - Viewable only mobile devices (no downloads)
  - Prevent copying of data out of the network by users who connect via remote access solutions

Join Us for Our Next Cyber Series Webcast

Password Management and Authentication Security
Wednesday, December 1
1:00 – 2:00 p.m. EST

Learn more at capincrouse.com

You Could Win a Free CapinTech Cyber Checkup!

- Receive one entry for each 2021 CapinTech Cyber Series webcast you:
  - Attend live, or
  - Watch the recording of within one week of the webcast date
- Winner announced in December

Thanks!

Allison Davis Ward, CISSP, CISA, CISM
Partner, CapinTech

award@capincrouse.com
505.50.CAPIN ext. 2008

CAPINTECH