Cybersecurity Breach Avoidance and Response

Presented by:

Scott J. Hyman, J.D., CIPP/US, CIPM
Shareholder, Severson & Werson

David A. Trepp, M.S.
Partner, BPM LLP

May 9, 2019

BPM

Severson & Werson
A Professional Corporation

Housekeeping

- **Questions and Comments**
  - Please have your microphone muted when you are not speaking to the group
  - Feel free to unmute and speak up when you have a question

- **CPE Credit Rules**
  - You will need to listen for & write down **3 code words** throughout the class in order to receive CPE credits for the one hour of training; the code words will be in **bold, underlined, in red font**
  - At about five minutes before the end of the class, you will receive a survey from Survey Monkey
  - You will need to type in each of the code words and submit the survey in order to receive CPE
  - The expectation is that you complete the survey as soon as you receive it. We will only leave the survey open until half an hour after the class ends, and CPE will not be granted after this time

A Webinar In Two Parts

- Administrative and Human Considerations
  - Scott Hyman
- Technical Considerations
  - David Trepp

Today's Co-Presenter

Scott Hyman is Severson & Werson's Data Protection Officer, is a Certified Information Privacy Professional and Certified Information Privacy Manager, and is Vice-Chair of the Firm's Financial Services Practice Group.

Mr. Hyman heads the Firm's Cybersecurity and Data Privacy Group, which is comprised of attorneys from multiple legal disciplines, including employment law, financial services law, cyber-insurance coverage, and regulatory practices.

Administrative and Human Considerations

Culture of Privacy

- C-Suite
- Compliance/DPO
- Legal
- MIS
- Security
- Human Resources
- Mid-Level Management
- Employees
- Vendors

Assembling the Team

- C-Suite Buy-in
- Human Resources
- Legal
  - Employment
  - Privacy
  - Regulatory
  - Insurance
- Management Information Systems
  - Safety & Soundness
  - MIS
  - Forensic
- Data Protection Officer
  - Enterprise security leadership role required by the General Data Protection Regulation (GDPR)
  - Responsible for overseeing data protection strategy and implementation to ensure compliance with legal requirements.

Inventory

- Coordination and Unification
- Integrated Information Management Program
  - Acceptable Use Policy
  - Employee Handbook
    - “Culture of Privacy”
    - BYOD
- Privacy Policy
- Hacking/Recovery/Incident Response Policy
- Record Retention Policy
- Corruption/Laundering Policy
- External Privacy Audits
- Vendor Management Policy
- Data Mapping/**Architecture**

Integrated Information Management Program

- Entire Team has a role; no one person can do it all

- Notice, buy-in, agreement, implementation, substantiation
  - Develop consistent business processes
  - Provide ongoing guidance, awareness and training
  - Keep the technology simple
  - Data minimization
  - Avoid over-collection of data
  - Data Retention and destruction
  - Vendor Management

The Employee Handbook

- Potentials
  - Background Investigations
  - Consumer Credit Reports
  - Expectations During Employment (BYOD)

- Current and Former Employees
  - Acceptable Use Policy (current)
  - Security/Duties to Maintain Confidences (current)
  - Duty to Report Breach or Loss (current)
  - ongoing duties (former)
  - Ownership/Segregation of data
  - Ownership of devices
  - Access or Denial of Access
  - “Right to be Forgotten”/“Duty to Delete” Policies
  - Consequences

Mitigating Risk

- Where does the threat start?
  - External Threats
    - Hacking/Theft/Phishing/Spearfishing/Malware
    - Safety & Soundness breaches
    - Vendor management: representations, warranties, and insurance!
    - Landlord/Tenant
    - Records management and disposal
  - Internal Threats
    - Employee negligence – Culture of Privacy?
    - BYOD
      - Policies & Procedures
      - Negligence
    - Disgruntled (former & current) employees

Mitigating Risk Continued

- Identifying Risk
  - Employee Training
    - Onboarding
    - Annual/ “Culture of Privacy”
    - Appropriate to Position: dependent on access to and handling of PII
  - “Turn-key” company-wide response policy and team in place
    - C-suite buy-in/retention/Identification
      - Outside Counsel
      - Public Relations
      - Insurance
      - MIS/Forensic Data
      - Crisis Management Point Person
      - Internal Messaging: substance and means
    - Written procedures, clearly written, openly kept

Mitigating Risk Continued

- Identifying Risk
  - Periodic monitoring
    - Incidents versus breaches
    - “Outliers” and “Trends”
    - Testing/”Fire Drills”
    - Reporting

Mitigating Risk: Response

- Expect the unexpected
  - Type of Breach
  - Nature, volume, & sensitivity of the compromise
  - Identification of affected data subjects/sensitivity of data subjects (children, vulnerable persons, etc.)
  - Consequences of breach
  - Control of the scope of the breach (i.e. technical & forensic response)

- Obligations
  - Legal obligations: Involve legal counsel/know your responsibilities
  - Regulatory reporting
  - C-Suite reporting
  - Investor/Interested party
  - Insurance carrier

Mitigating Risk: Response Continued

- Lead investigator – already part of the team!
  - **Centralize** investigation and internal communications
  - Coordinate internal and external messaging
  - Schedule a forward-looking timeline for investigation, results, and reporting
  - Educate the response team on the scope of attorney-client and work product privilege
  - “Remind” Team of responsibilities (because they already know them)
  - “Remind” of proper protocol for interviewing witnesses and collecting evidence
  - “Remind” of proper guidance for documenting factual findings
  - Follow-up/Report/Record

Technical Considerations

Baseline Your Trusted Computing Environment

- Define What You're Trying to Protect
  - Information asset inventory
  - Information classification scheme
  - Segmentation and boundaries, including vendors

- In order to return systems to a trusted state, one must have normal behavior metrics
  - Normal traffic patterns
  - Normal log entries
  - Normal bandwidth usage
  - Normal performance

Have Tools To Identify A Breach

- Intrusion Detection System (IDS) and/or
- Security Incident & Event Management (SIEM) System in Place
  - Calibrated to distinguish between an incident and a breach
  - Network-based vs. Application-based
  - In-house vs. Outsourced
    - Consider monitoring overhead 24x7

Have A Breach Laptop

- Disconnected From Network
  - System/Domain Administrator Privilege Levels
- Post-Breach Administrative Tools
  - Wireshark
  - Microsoft SysInternals
  - Etc.
- Password Database(s)
  - All Key Systems and Applications
- Backup/Restore Software
- Key Application License Keys, etc.
- Ransomware Eradication Tools

Have Current, Offline Backups

- Air-Gapped
  - Disconnected from network after backup is performed
  - Usually a rotation of hard drives that are encrypted at rest
- Hosted/Cloud Backup
  - Multi-factor authenticated
  - Limit authentication attempts to known sources
    - By IP Address
    - By Computer MAC Address
    - By Certificate or Other Digitally Signed handshake

Defend Against Ransomware

- Control Inbound emails
  - Attachments
  - Links
- Prohibit Macros
  - Word
  - Excel
- Fanatically patch Adobe pdf software
- Harden Browsers
  - Restrict Scripts
- Train Users!
  - What to look for
  - What to do if they let their guard down

Prepare to Respond to Ransomware

How long can we afford to be down?

How quickly can we restore from bare metal?

- Fight (**Eradicate**)
  - Removal Software
    - AVG, Trend Micro, BitDefender, Kaspersky, et al
  - Offline Backups
    - Air-Gapped
    - Cloud/Hosted

- Flight (Pay)
  - Have a cryptocurrency wallet set up
  - No guarantees

Summary

- Have a plan for cybersecurity breaches

- Breach avoidance and response requires a combination of
  - Administrative
  - Personnel and
  - Technical Resources

Thank You!

bpmcpa.com | severson.com