CORPORATE DATA SECURITY: BEST PRACTICES AND LEGAL COMPLIANCE

PAUL C. VAN SLYKE

HOOVER SLOVACEK

HOUSTON TEXAS

OVERVIEW

- 2017 – year of Data Breaches… Equifax, Yahoo (largest in history), InterContinental Hotels, Dun & Bradstreet, Saks Fifth Avenue
- Industries with most breaches: Medical/healthcare, Education, financial services, retail/hospitality, real estate, professional services
- Types of data: employer trade secrets, employer embarrassing information, employee and customer personal data, healthcare data
- For every high-profile data breach, there are dozens of threats to small businesses' confidential information
- In 2016, 50% of all targeted attacks were aimed at businesses with under 2,500 employees
- High cost of a data breach

BEST PRACTICE PROTOCOLS

- National Institute of Technology (NIST) Cybersecurity Frame Work
- Consumer Financial Protection Bureau Principles for Data Aggregation Services
- U.S. Dept. of Justice Best Practices for Victim Response and Reporting of Cyber Incidents
- Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities
- International Chamber of Commerce Cyber-Security Guide
- Nat'l Assn. of Corporate Directors Cyber-Risk Oversight Handbook
- California Attorney General Cyber Security in the Golden State

SOME MAJOR STATUTES

- Healthcare Insurance Portability and Accountability Act – HIPPA
- Gramm Leach Bliley Act (Glibba)
- Federal Identify Theft
- Payment Card Industry Protocols
- Computer Fraud and Abuse Act
- California – Identity Theft, Information Practices Act of 1977

MAJOR REGULATORS

- Federal Trade Commission
  - Representations become misrepresentations –unfairness jurisdiction
  - GLB Act
- California Attorney General- State Acts
- Health and Human Services – HIPPA Act
- U.S. Justice Dept.- Computer Fraud and Abuse Act

MAIN SOURCES OF INCIDENTS

- Low hanging fruit
- Employee Negligence
- External theft of a device (theft of laptop or flash drive)
- Employee theft (terminating employee)
- Internet Phishing (employee training issue)
- Internet Malware

RAPID DETECTION IS CRITICAL

- If a company is slow to detect, or does not detect, it will face at least 4 major issues
  - Misses the opportunity to block the attack before it gets to critical data
  - Forensic data that could be used to precisely determine what occurred may be lost (e.g. logs are overwritten)
  - Story breaking publicity before the company is aware
  - When a third party breaks the story, the company is often force to discuss the incident before it can investigate and contain the incident
- As a result, the company is more likely to be viewed as not handling the incident well

TOP PRIORITY STEPS BEFORE AN ATTACK

- Identify your “Crown jewels”
- Have an action plan in place
- Rehearse you action plan
- Have needed technology and services in place
  - Off-Site backup, intrusion detection, devices for logging network activity
- Ensure legal counsel is familiar with technology and incident response plan
- Engage with law enforcement – have established relationships with particular individuals
- Create a crisis management plan

PRIVACY AND SECURITY STEPS

- Check types of authentication and firewalls
- Passwords sufficiently strong and changed regularly
- When employees leave, is account on the network purged
- Network intrusion detection or prevention system
- Is encryption on network and mobile devices used?
- Is logging enabled and stored for sufficient time?
- Is up-to-date malware protection used?
- Does company delete sensitive data no longer used?

PRE-INCIDENT DUE DILIGENCE

- **Assume you are a target!**
- Identify and map your data
- Develop a records retention policy. If you don't have it, it can't be stolen
- Audit contracts with vendors and business partners
- Develop employee training on cybersecurity
- Compare privacy notices with actual practices
- Review cybersecurity insurance coverage
- Limit access to those who have a need to know
- Create a crisis management plan and team

INCIDENT RESPONSE TEAM

- Create response plan and team leader
- Include a C-Suite Executive
- Define roles for each team member

CREATE A RESPONSE CHECKLIST

- Don’t turn off computer
- Notify managers within the company
- Contact Law enforcement
- Document potential scope of breach
- Determine notification requirements
- Determine whether to contact other victims
- Make a forensic image of affected systems
- Preserve all relevant communications
- Block further access to the network

NOTIFICATION OF THE BREACH

- Evaluate breach notification obligations
- Evaluate coordination with law enforcement/regulators
- Set corporate communications strategy
- Follow crisis management policy

CONCLUSION

- Paul C. Van Slyke, Attorney Cop
- Hoover Slovacek LLP
- vanslyke@hooverslovacek.com
- 713-735-4129