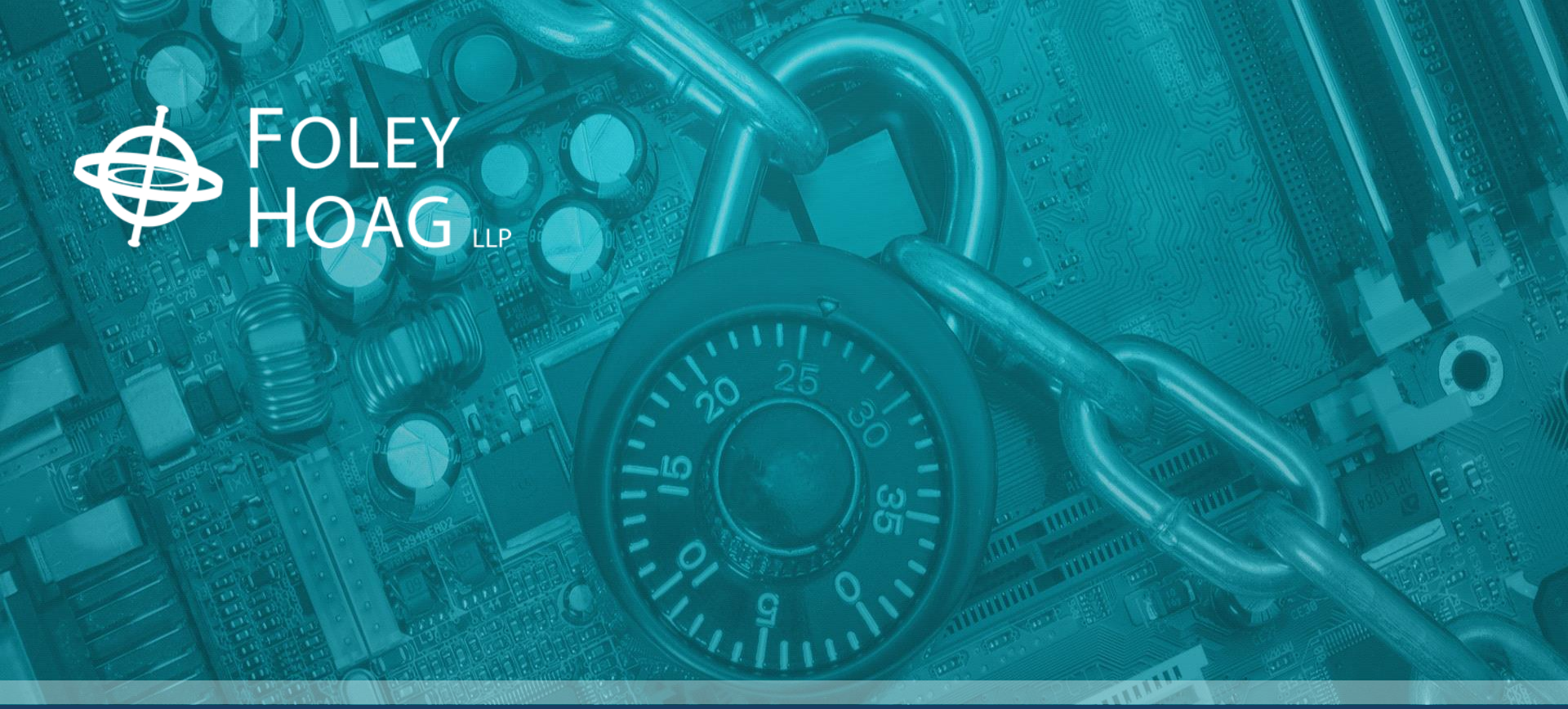

FOLEY HOAG LLP

Avoiding Potential Pitfalls and Protecting Your Company, Clients and Customers

Webinar

May 2, 2017

Speakers

Douglas Bloom

Director, Cybersecurity and Forensics

PwC

Christopher Escobedo Hart

Counsel

Foley Hoag LLP

Stephen Bychowski

Associate

Foley Hoag LLP

Overview

- Summary of the current data privacy and security landscape
- Understanding data breach response
- Key elements of data breach prevention and response

2016: A Busy (and Dangerous) Year

- Breaches and cyber attacks continued to occur at a high frequency
- A number of the known breaches/attacks affected sophisticated organizations, reflecting the difficulty of detection and prevention
- While some attacks are very high tech, low tech attacks are very popular and often successful
- Perpetrators know this and exploit human weaknesses
- Attribution continues to be a serious problem

Some Breaches in the News

- Yahoo
- Verizon
- IRS
- DNC

Regulators, Company Boards, Accountants and Lawyers Are Focusing on Cyber-Security

- Cybersecurity risks are rising to the Board of Directors level
- Cybersecurity reviews are becoming a standard part of M&A due diligence
- FTC, SEC, DHS, HHS and other regulators recognize the centrality of cyber and information security
- Companies are receiving significant penalties from regulators
- Liability could extend to executives

U.S. Industries Affected by Data Loss

- Healthcare
- Education
- Government
- Retail
- Financial and Banking

The Costs of a Breach

- Average Data Breach Costs
- Lost business costs:
  - Loss of customers
  - Impairment of goodwill, reputation
  - Litigation and regulatory action
- Some influences on those costs:
  - Presence of a response plan
  - Business continuity management
  - Legal compliance

Data Breach Case Study #1

Imagine that . . .

- You receive a call from an employee saying that they received a notice from the IRS confirming a request for a tax transcript.
  - Should you be concerned?
  - If not, when?
  - If so, what is your follow up?

Data Breach Case Study #2

Imagine that . . .

- You receive a call from the FBI informing you that they have evidence that your confidential information has been compromised.
  - How should you respond?

Data Breach Case Study #3

Imagine that . . .

- You log into your computer at work and are confronted with a webpage which states that your data has been encrypted and provides instructions for the key to decrypt it in exchange for $25,000 in Bitcoin.
  - How should you respond?

FOLEY HOAG LLP

Keys to Successful Response

- You need to determine if an incident occurred, when it occurred, how it occurred, if insiders were involved, and whether the intrusion has been contained.
- Have resources pre-identified and pre-contracted. You won't have time to deal with contracting delays.
- Check with your insurer in advance to ensure resources are approved. If your preferred providers are not, you can often negotiate getting them covered.
- Cyber forensic investigations can take time. Work with your team to make sure that they are focused on the information and tasks you need.
- Keep track of state/federal notification deadlines.

Keys to Successful Response

- Train IT personnel on best practices for preserving key logs, systems and other pieces of evidence.
  - Electronic resources should be forensically collected.
  - Do NOT disconnect equipment without seeking advice; you can destroy essential evidence and alert the attackers that you are aware of their presence, causing them to escalate the damage.
- Consider the use of network monitoring and endpoint security equipment to look for areas where a latent attack may be present. Sophisticated attackers use multiple simultaneous routes to ensure a persistent presence in your environment.
- Ensure that the IT team knows when to escalate an incident and to whom. They are often the first to see an attack, but good incident response requires an enterprise level response.

A Patchwork of Laws

- **Federal laws**
  - "Sector Specific," not comprehensive
  - Two examples
    - Financial Sector: GLBA
    - Health Sector: HIPAA
  - FTC, SEC and FFIEC have increasing presence in this space
- **State Laws**
  - Where much of the action is
  - Some differences in:
    - How protected information is defined
    - What notification is required
  - Some similarities in:
    - Cooperation with law enforcement
    - Focus on internal policies

Protected Information

- This varies from state to state

SSN, driver's license, financial account numbers, medical information

SSN, driver's license, financial account numbers

SSN, driver's license, financial account numbers

SSN, driver's license, financial account numbers, passwords, mother's maiden name

SSN, driver's license, financial account numbers, medical information, health insurance, passwords, mother's maiden name, date of birth, electronic ID numbers

Key Requirements of the Massachusetts Data Security Regulations

- Develop a written information security policy.
- Designate an individual who will be responsible for your information security program.
- Identify what personal information your business possesses, where it is kept and who has access to it. You should have a process for continuously maintaining this information.
- Place reasonable restrictions on access to personal information: physical restrictions for hard copy files; log-in and password protection for electronic files.
- Take steps to ensure that third party service providers have the capacity to protect personal information consistent with your policies.
- Rapidly remove terminated employees' access to your environment.
- Regularly monitor and update security measures.

Inventory/Audit

- What Information Do We Have?
- Where Is It?
- Who Has It?
- Why Do They Have It?
  - Why Do ***We*** Have It?
- What Are The Risks?
  - How Would Customers and Employees React to Accidental Disclosure?
  - How are potential attackers gaining access to the information?
- What Safeguards Address Them?
  - Governance
  - Physical
  - Technical
- What Are Our Obligations?

Pre-emptive Responses to These Threats

- Move from single to multi-factor authentication for sensitive information
- Patch/update your software on a regular schedule
- Use endpoint protection across computing platforms
- Implement the principle of least privilege
- Continually monitor your systems
- Use encryption of data in transit and at rest where appropriate
- Recognize dangers when traveling.
  - Use secure remote access, and don’t trust personal emails, WiFi, use hotel safes, etc.

Breach Insurance

- Still a developing area
- Limited history of evaluating risk, so premiums can vary widely
- Scope of coverage can vary widely
- Limits vary and can range from $25,000 to $25 million depending on the nature of the policy and business
- What can be covered?
  - Crisis management services
  - Notification of breached parties
  - Credit/public records/fraud monitoring
  - Fraud remediation services
  - Emerging: Data loss and ransoms

Thank you!

Colin Zick
Chair, Privacy & Data Security Practice Foley Hoag LLP
czick@foleyhoag.com | 617.832.1275

Christopher Escobedo Hart
Foley Hoag LLP
chart@foleyhoag.com | 617.832.1232

Stephen Bychowski
Foley Hoag LLP
sbychowski@foleyhoag.com | 617.832.1164

Douglas Bloom
PricewaterhouseCoopers LLP
douglas.b.bloom@pwc.com | 617.331.5563

Read Foley Hoag's cybersecurity blog,
www.securityprivacyandthelaw.com