



YOUR DELAWARE ADVANTAGE

Data Breach and Vendor Risk Management

2016 Secure Delaware Workshop
September 7, 2016

William R. Denny, Esquire
Potter Anderson & Corroon LLP



Not Just Blue Chip Companies

- Small business cyber attacks are on the rise
 - 28 million small business owners have no confidence in their security.
 - 43% of cyber attacks worldwide struck companies with less than 250 workers.
 - 1 in 5 small businesses reported a cyber attack.
 - 7,000 U.S. companies of all sizes fell victim to phishing email scams with losses of more than \$740 million.
 - 30% uptick in cyber attacks from 1Q 2015 to 1Q 2016.
 - 63% of small businesses have been victims of cyber attacks in the last 12 months.
 - 48% reported cyber attacks caused service interruption.
 - Average cost of a breach for small to mid-sized businesses was over \$180,000.



Why Information Security?

- Challenges include:
 - Increasing threats
 - Heightened expectations from customers, shareholders, employees, business partners and regulators
 - Lack of communication among legal, IT and business leadership
 - Demands of changing technology and risk management

- Growing body of law demands attention
 - State data breach disclosure laws
 - State data security laws
 - Federal law focuses on FTC enforcement and sector-specific requirements.



State Data Security Laws

- Data security laws generally require businesses to:
 - Maintain appropriate security policies, procedures and safeguards,
 - Train employees,
 - Oversee service providers,
 - Periodically assess risks, and
 - Monitor their programs.
 - Massachusetts requires a **written information security program (WISP)**

- California sets a **baseline** for reasonable security practices: “CIS 20 Critical Security Controls.”



Massachusetts Data Security Regulations

- Companies must develop, implement and maintain a comprehensive written information security program (WISP)
 - Designate employees to maintain the WISP
 - Identify and assess reasonably foreseeable internal and external risks: data mapping
 - Develop security policies and training for employees
 - Oversee third party providers
 - Regular monitoring
 - Establish and maintain up-to-date computer security systems
 - Encryption
 - Backup tapes



Federal Laws

- FTC takes data security enforcement actions under its authority to address unfair or deceptive trade practices
 - Focus on businesses that fail to keep their security commitments or implement reasonable safeguards to protect PII.
 - FTC follows a **reasonableness standard**.
 - Guidance: “Start with Security: a Guide to Business.”
- Sector-specific data security laws include:
 - HIPAA/HITECH (healthcare)
 - GLBA (financial services)
 - COPPA (children’s online privacy)
 - FERPA (student information)
 - Telecommunications, etc.



Information Security Policies

- WISP laws call for policies
- Reasonable security practices are generally understood to include policies and related training
- Other reasons to implement policies:
 - Sector-specific regulations
 - Critical infrastructure obligations
 - Public company risk disclosures
 - Trade secret protection
 - Contractual obligations
 - Litigation and enforcement risk management



Cyber Risk Governance Models

- Pick one standard and follow its structure and terminology.
 - NIST Framework for Improving Critical Infrastructure Cybersecurity
 - SANS Institute Risk Management Framework
 - ISO Standards 27001 through 27008
 - FAIR (Factor Analysis of Information Risk) Information Risk Management Model



Developing, Implementing and Maintaining a Policy

- Designate and empower a **policy owner**
- Policy development follows a 5-step process:
 1. Identify stakeholders, build collaboration and gather information
 2. Identify legal obligations
 3. Develop policy content
 4. Implement the policy and supporting processes
 5. Periodically review and update policy



Practice Tips for Effective Policies

- Policies should:
 - Have clear ownership coupled with collaborative development;
 - Be based on detailed information gathering and informed decisions;
 - Be written in plain language and be easily accessible;
 - Apply to current environment but evolve as business changes;
 - Set standards that are feasible to implement;
 - Contemplate exceptions and their management;
 - Be supported by responsive experts and processes;
 - Be monitored for compliance and consistently enforced;
 - Explain policy decisions where appropriate;
 - Help demonstrate information security's value to the organization.



Cyber Incident Response Plan

- WISP should require an Incident Response Plan (IRP)
- To build an IRP, companies must:
 - Identify and locate its data;
 - Evaluate the data held;
 - Reduce and eliminate unnecessary data;
 - Secure the company's network and the data located on it; and
 - Plan for possible incidents.
- Incident Response Team (IRT) should develop the plan.
 - IRT should include key people with authority and availability.
 - Each member should be assigned distinct responsibilities and have authority to act within scope of assignment.



Preparing for Cyber Incident Response

- The Incident Response Team should:
 - Identify necessary outside resources.
 - Meet at least monthly to prepare and make decisions in advance of an incident;
 - Designate one person as primary point of contact;
 - Pre-draft all important communications;
 - Plan what to do if electronic communication systems are unavailable;
 - Evaluate cyber insurance coverage;
 - Impose contractual obligations on third party contractors;
 - Evaluate capacity for handling a call center;
 - Identify criteria for notifying law enforcement and regulatory agencies;
 - Identify who will physically secure premises; and
 - Identify who will isolate affected equipment.



Responding to a Cyber Security Incident

- The hours following an incident are critical to reestablish security, limit liability, preserve evidence and protect reputation.
- Plan to:
 - Fix the problem;
 - Implement the plan;
 - Identify the facts;
 - Move to the second stage (notifications, press releases, law enforcement, contractual obligations, review and update policies).



Checklist for Drafting an Effective IRP

- The plan
 - Assigns a specific person to lead the investigation;
 - Provides a clear plan for escalating information;
 - Discusses the need for preserving evidence;
 - Incorporates legal where appropriate to preserve attorney-client privilege;
 - Discusses how the organization will communicate externally concerning the incident;
 - Includes contact information for internal resources;
 - Includes contact information for pre-approved external resources;
 - Is reviewed annually; and
 - Is tested.





Managing Vendor Cyber Risk



Outsourcing Provides Notable Rewards

- Reduced Operating Costs
- Streamlined Operations
- Business Improvement
- Time to Market
- Flexibility



. . . And Creates Notable Risks

- Weak link in the security chain
- Data breach requiring notification
- Failure to comply with laws and regulations
- Loss of trade secrets
- Failure to meet contractual obligations
- Reputational loss
- Liability to customers, stockholders, business partners



Third Party Risk Management is a Hot Topic

- Third Party Risk is one of the largest drivers of data breaches
 - Focus on third party service relationships is increasing
 - IBM hardware business dropped by \$1B, its cloud business increased by \$1B
- Target breach started through lack of security control by a vendor
 - Cost the CEO his job.
 - \$100 million in damages paid



TARGET



Who Is Getting Targeted by Hackers?

- Size of organizations getting impacted has changed dramatically. Smaller organizations getting targeted. These are your vendors.
- Regulatory pressure is increasingly focused on third party risk management
 - Federal Trade Commission (FTC)
 - Payment Card Industry Data Security Standard (PCI DSS)
 - Office of the Comptroller of the Currency (OCC)
 - Consumer Financial Protection Bureau (CFPB)
 - HIPAA Rulemaking by Office for Civil Rights (OCR)
 - NIST Cybersecurity Framework
- How do you manage this?



FTC Guidance (“Start with Security”)

- Make sure your service providers implement reasonable security measures.
 - Put it in writing
 - Verify compliance



PCI DSS – Third Party Risk Highlights

- Must maintain a written agreement
- Must perform due diligence
- Must maintain a program to monitor vendor's PCI DSS compliance at least annually
- Must maintain information about which PCI DSS requirements are being managed by each provider



OCC and Third party Risk Highlights

- Banks should adopt risk management processes commensurate with the level of risk and complexity of its third party relationships
- A bank should ensure comprehensive risk management and oversight of third party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship includes:
 - Plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses and oversees the third party.
 - Proper due diligence in selecting a third party.
 - Written contracts that outline the rights and responsibilities of all parties.
 - Ongoing monitoring of the third party's activities and performance.
 - Contingency plans for terminating the relationship in an effective manner.
 - Clear roles and responsibilities for overseeing and managing the relationship and risk management process.
 - Documentation and reporting that facilitates oversight, accountability, monitoring and risk management.
 - Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.



HIPAA Privacy, Security and Enforcement Rules

- **Business Associates**

- Direct Liability
- Expanded Definition
- Business Associate Agreement

- **Redefinition of when you need to notify of a breach**

- Willful neglect: conscious, intentional failure or reckless indifference. This includes failure to run a proper due diligence process.
- Presumption of reportable breach, unless there is **low probability** the PHI has been **compromised** after risk assessment.
- OCR will investigate all cases of possible willful neglect and impose penalties on all violations.



Where to start on vendor risk

- Questionnaires?
- Annual assessment of vendors?
- How do companies get to scale and manage this?
- Most companies are not properly assessing third party risk
 - 90% of organization have been compromised in some fashion
 - 76% of data breaches resulted from a third party which introduced the security deficiencies that were exploited.
 - Only 24% require third party suppliers to comply with baseline security procedures.



Three Basic Elements of Vendor Risk Management

1. Do your homework about the vendor – due diligence.
2. Make a plan to manage risk – start with the contract.
3. Check on your vendors – are they doing what they're required to do?



Do Your Homework – Due Diligence

“An ounce of prevention is worth a pound of cure.”

- Reputation
- Financial condition and insurance
- Information security controls, including business continuity
- Vendor incident response plan
- Employee training and awareness
- How are they monitoring themselves?



Make a Plan – The Vendor Contract

“One size does not fit all.”

- Definitions
- Minimum necessary access and no further use
- Use of subcontractors
- Who owns the data?
- Confidentiality
- Security program
- Monitoring and assessment
- Requirement to notify and disclose security incidents
- Termination
- What happens when something goes wrong?



Check In – Monitoring Vendor Information Security

“Play nice.”

- As-needed reporting
- Training and awareness
- Independent reviews
- Regularly scheduled checkups



Takeaways

- Do your homework
- Get the right contracts in place
- Monitor vendor performance



What can you do?

- Consider the following questions in your vendor relationships:
 - Does the vendor have the right to use your data?
 - Is the vendor required to protect your data?
 - Is your data stored in the cloud?
 - Are you uploading data to a third-party site that will then be manipulated or placed in some type of report and returned?
 - Is the vendor required to notify you in the event that the vendor has a security breach which might involve your data?
 - Does the vendor subcontract or allow others access to your data?
 - Is the vendor using the data for its own business and not just to provide the services to you?
 - Do your practices in collecting, using and transferring data match your vendor's?



To reach us

William R. Denny
Direct dial: (302) 984-6039
wdenny@potteranderson.com

Potter Anderson & Corroon LLP
1313 North Market Street
P.O. Box 951
Wilmington, DE 19899-0951
www.potteranderson.com

