



YOUR DELAWARE ADVANTAGE

Changing Legal Landscape in Cybersecurity: Implications for Business

Delaware Cyber Security Workshop
September 29, 2015

William R. Denny, Esquire
Potter Anderson & Corroon LLP



Agenda

- Growing Cyber Threats and Risks to Enterprise
- Principles for Approaching Cyber Risks
- Recent Legal Developments in Cyber Security
- Guidelines and Best Practices
- Where Do We Start?



Recent Major Incidents

- Attack on Sony Corporation destroying 70% of its computers and publishing thousands of sensitive emails.
- Compromise of personal information of 100 million Anthem customers and employees
- Theft of information from the IRS and Office of Personnel Management
- Dating website Ashley Madison lost control of 30 GB of data containing sensitive information about customers
 - People's most intimate secrets exposed in a way that credit protection tools or cyber insurance policies cannot address.



And Growing Financial Risk Following Breach

- Target reached settlements of \$67 million with Visa and \$10 million with consumers for losses sustained as a result of 2013 data breach.
 - Possible benchmark in future claims by issuing banks arising out of payment card data breaches
 - Demonstrates that merchants accepting credit cards may be liable for significant damages



Cybersecurity is Not Just an IT issue

- Cyber risks pose serious threats to business operations. Risks include:
 - Reputational injury
 - Financial losses
 - Damage to infrastructure
 - Shareholder suits for breach of duty of care or duty of loyalty
 - Regulatory enforcement actions
- Senior management must consider cybersecurity as part of its enterprise risk management duties.



Constraints on Cybersecurity Initiatives

- Businesses and hackers share an asymmetric relationship that sharply favors hackers.
- Recent experience of companies affected by data breaches do not suggest that cost of such a breach warrants massive additional investment in data protection.
- How Much Data Security Is Enough?
 - Insufficient security may expose company to reputational risk and possible liability in event of an attack.
 - Too much investment in security may result in waste, as no data security system can ever promise complete protection.



Cybersecurity Has Become a Legal Issue

- Legal compliance:
 - Federal, state and international laws, regulations and rules
 - Contracts with third party providers
 - Information security programs and privacy policies
 - Data breach policies
- Litigation, enforcement actions and investigations



Major Legal Developments in Cybersecurity

- Congressional Action
- Section 5 of the FTC Act
- SEC's Disclosure Guidance
- NIST Framework
- State Laws on Data Security and Privacy
- Various other guidance:
 - DoD Cyber Strategy
 - U.S. DOJ Best Practices Guide
 - U.S. Chamber of Commerce Internet Security Essentials for Business
 - New York Department of Financial Services Guidance Letters



Lack of Federal Legislation

- Congress has not passed major cybersecurity legislation since 2002, so many states have passed their own laws.
- Recent legislative proposals relating to cybersecurity concentrate on these issues:
 - National strategy and the role of government
 - Reform of the Federal Information Security Management Act of 2002
 - Protection of critical infrastructure
 - Information sharing and cross-sector coordination
 - Breaches resulting in theft or exposure of personal data
 - Cybercrime offences and penalties
 - Privacy in electronic commerce
 - Research & development
 - Cybersecurity workforce



FTC Has New Mandate to Regulate Cybersecurity

- FTC Act
 - Section 5 prohibits unfair or deceptive acts or practices in or affecting commerce.
 - To be “unfair,” (1) an act must be likely to cause substantial injury to consumers, (2) consumers cannot reasonably avoid the injury, and (3) the injury must not be outweighed by benefits to consumers and competition.
- Third Circuit affirmed in *Wyndham* on August 24, 2015, that FTC has authority to regulate cybersecurity under Section 5 of the FTC Act.
- The fact that the company is a victim of a cybersecurity attack will not likely be viewed as a defense to liability. Companies should expect attacks and plan accordingly.



FTC Regulation of Cybersecurity – What To Do?

- Proactively consider potential privacy and data security issues at every stage of company, product or service development. (*“Privacy by Design”*)
- Consider whether your cybersecurity practices could survive the cost-benefit analysis that weights (a) risks to consumers presented by cybersecurity practices against (b) benefits to consumers and competition?
- Consider whether your cybersecurity practices conform with the guidance of the FTC’s 2007 guidebook entitled “Protecting Personal Information: a Guide for Business.”



SEC Cybersecurity Initiatives

- SEC Division of Corporation Finance: disclosure guidance for cybersecurity risks and incidents issued October 2011.
- Rule 30(a) of Regulation S-P: every broker, dealer and investment company must adopt written policies and procedures implementing administrative, technical and physical safeguards for the protection of company records and information.
- Enforcement action:
 - On September 22, 2015, an investment advisor company settled charges of failing to establish cybersecurity policies and procedures.
 - Company also failed to conduct periodic cybersecurity risk assessments, encrypt PII stored on third party servers, implement a firewall or maintain a response plan for cybersecurity incidents.



Reg. SCI

- The SEC issued *Regulation System Compliance and Integrity* (Reg. SCI) in November 2014.
 - Requires enhanced business continuity and disaster recovery (BC/DR) planning and testing participation to close the apparent gap between BC/DR and demonstrable resilience.
 - Designed to reduce the frequency and impacts of failures, disruptions and delays and cyber intrusions into automated systems and enhance resilience of operations to ensure rapid recovery from disruptions.
- Entities must:
 - Establish, maintain and enforce written policies and procedures to ensure that its systems have high levels of capacity, integrity, resiliency, availability and security.
 - SCI event triggers three obligations: corrective, SEC notification, and dissemination to other SCI entities.



NIST Framework

- In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity
 - Not a regulation, but it may become a *de facto* standard of care
 - Provides a methodological roadmap for planning and implementing a company's compliance plan.



What should Business Know about the NIST Cybersecurity Framework?

1. It is actionable and allows you to assess your organization's risks in five core functions: Identify, Detect, Protect, Respond and Recover.
2. It leverages industry best practices and standards.
3. It helps you focus and prioritize important cyber-related investment decisions.
4. It can help reduce legal risk with evidence of your good faith efforts to manage cybersecurity risk.
5. It is flexible, allowing businesses in different industries to adapt the Framework and make it work for them.



Unanswered Questions about the NIST Framework

- Voluntary or mandatory?
- Compliance or security?
- Duplicative or contradictory function?
- Set standards or have them set for you?
- Liability protections



Liability Concerns

- Potential tort liability for commercially unreasonable cybersecurity practices based on the Framework
 - Key is risk management – not implementing the entire Framework
 - Problem if you haven't documented a risk management process
 - Every entity has different needs and interests
- Possible basis for regulations or enforcement actions
 - Harmonization with existing requirements
 - DOD recommended that government should only do business with companies that meet baseline requirements



Patchwork of State Laws

- New Delaware Laws in 2015 Relating to Cybersecurity:
 - Safe Destruction of Records Act
 - Online and Personal Privacy Protection Act
 - Student Data Privacy Protection Act
 - Employee/Applicant Protection for Social Media Act
 - Victim Online Privacy Act
- Connecticut will become the first state on October 1 to require identity theft prevention and mitigation services in response to a data breach.



DHS Cyber Resilience Review

- Tool offered by Department of Homeland Security to perform a self-assessment to evaluate operational readiness and cybersecurity capability within Critical Infrastructure and Key Resources sectors, as well as state and local governments.
- Goal is to develop understanding of organization's operational resilience and ability to manage cyber risk to its critical services.



Department of Defense Guidance

- Cyber Strategy released April 2015, exhorting companies and governmental bodies to focus on developing **resilience** needed to continue operations if post-attack critical infrastructure services cannot be restored to pre-attack levels.
- Interim rules for DoD contractors issued August 2015
 - Requires reporting on network penetrations
 - Contains policy on purchase of cloud computing services
 - Will require careful assessment by contractors to develop mechanisms for identifying and reporting incidents



U.S. Department of Justice Best Practices Guide

- Best Practices for Victim Response and Reporting of Cyber Incidents, Version 1.0.
 - Assist organizations in preparing a cyber incident response plan and preparing to respond to a cyber incident.
 - Details steps that organizations should take before a disruptive cyber intrusion and the crucial elements that an actionable incident response plan should contain.



U.S. Chamber of Commerce guidance

- Internet Security Essentials for Business 2.0
 - Urges businesses to adopt fundamental internet security practices
 - The guide focuses on preparedness, defense and resilience:
 - Set up a secure system
 - Protect business data
 - Train your workforce
 - Be prepared
 - Multiple internet resources listed



New York Department of Financial Services

- Guidance letter to banks issued March 2015 with a new cyber security assessment process.
 - Outlines specific issues and factors on which all banks will be examined as part of new DFS cyber security preparedness assessments.
 - 11 topics, including “incident detection and response processes, including monitoring.”
 - DFS will schedule IT/cyber security examinations following the comprehensive risk assessment of each institution and will seek responses to cyber security assessment questions.
 - Encourages the view that cyber security is not a subset of information technology (IT) functions, but as integral to overall risk management strategy.



Principles for Directors in Approaching Cyber Risk

- Understand cybersecurity as an enterprise-wide risk management issue, not just an IT issue
- Understand the legal implications of cyber risks as they relate to the company's specific circumstances
- Give adequate meeting time on a regular basis to discussions of cyber risk management
- Establish an enterprise-wide cyber risk management framework with adequate staffing and budget
- Identify which risks to avoid, accept, mitigate, or transfer through insurance, and plan for each approach



Basic Corporate Governance – Where Do We Start?

- Determine the location of sensitive data
- Evaluate network security
- Monitor network activity
- Restrict access to sensitive data
- Require secure user-authentication tools
- Manage vendor security
- Develop an incident response plan
- Develop data destruction policies and procedures
- Train employees and executives



Corporate Counsel's Role

1. Fulfill fiduciary duty of board and management
2. Address disclosure obligations and communications
3. Guide interactions with law enforcement
4. Achieve regulatory compliance
5. Provide counsel to cybersecurity program
6. Prepare to handle incidents and crises
7. Manage cybersecurity-related transactional risks
8. Effectively use insurance
9. Monitor and strategically engage in public policy
10. Discharge professional duty of care



Liability Exposure Through Vendors

- According to Trustwave's 2013 Global Security Report, in more than 60% of cases, hackers obtained access through security deficiencies of vendors engaged to provide system support, development or maintenance.
- If agreements with vendors do not address cybersecurity issues and standards, *all of the risk* may remain with the data owner, because the vendor has no contractual requirement to protect the data or accept some of the risk in event of breach.
- Possible actions from customers, employees, Federal Trade Commission



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

