



YOUR DELAWARE ADVANTAGE

Changing Legal Landscape in Cybersecurity: Implications for Business

Presented to Greater Wilmington Cyber Security Group

Presented by William R. Denny, Potter Anderson & Corroon LLP

May 8, 2014



Topics for Discussion

- Basics of the Cybersecurity Framework
- Impact on Business
- Liability Concerns
- What should you be doing?



Questions About The Cybersecurity Framework

- Will your company be exposed to liability if the Framework is not adopted or is imperfectly implemented?
- Does the Framework establish a de facto standard of care, and if so, will this standard of care extend beyond critical infrastructure?
- Is the Framework cost effective and has adoption been properly incentivized?
- Will agencies base regulations on the Framework?
- What are the ramifications of the Framework's statements on privacy and how will they be harmonized with NIST's upcoming efforts to develop technical privacy standards?



Executive Order 13636: Improving Critical Infrastructure Cybersecurity

- Issued on February 12, 2013
- Calls for a framework of cybersecurity best practices and standards with voluntary adoption by market incentives
 - Directs NIST to develop a Cybersecurity Framework “to reduce cyber risks to critical infrastructure.”
 - Directs DHS to establish a voluntary program to support adoption of the Framework by owners and operators of Critical Infrastructure.
 - Directs DHS to coordinate establishment of a set of incentives to promote participation in this program.



Strategy of Executive Order

- Framework should be cost effective
- Voluntary adoption should be motivated by incentives
- Wide range of incentives is being considered
 - Liability protections
 - Procurement advantages
 - Additional intellectual property protections
 - Forbearance of regulatory enforcement
- EO attempts to coax companies into making substantial changes in their security habits through
 1. Sharing cyber intelligence reports with private industry, and
 2. Assembling standards and best practices



Three Kinds of Information Sharing Specified in EO

- *Classified Information Sharing through Third Party Vendors*
 - Classified cyber threat and technical information to eligible third party vendors to critical infrastructure
- *Catastrophic Target Notices*
 - Unclassified reports to targeted entities of cyber threats to the U.S. homeland that identify that specific targeted entity
- *Imminent Target Notices*
 - Confidential notice to owners and operators of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic effects
 - Owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications
 - IT service companies are exempt from this notice!!!



Basics of the Cybersecurity Framework

- Leverages existing cybersecurity best practices (ISO 27001/2, SP800-53, COBIT, ISA 99, etc.)
- Instructs organizations on how to assess their current level of cybersecurity, set goals for improvement and create a plan for implementing these goals.
- Three main elements are
 1. Framework core
 2. Tiers
 3. Profiles



Final Framework

- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 released February 12, 2014
- Same Day:
 - DHS: Critical Infrastructure Cyber Community (C³) Voluntary Program
 - NIST: Roadmap for Improving Critical infrastructure Cybersecurity



Basics of the Cybersecurity Framework (cont.)

- Controls are divided into five “core functions,” each with its own categories, sub-categories and informative references
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover
- Tiers represent how organizations view and respond to risk.
- Profiles facilitate customization and improvement
 - Current profile
 - Target profile



Notable Changes from Preliminary Version

- Removes controversial privacy appendix that went beyond what U.S. law requires to protect PII
- New section provides methodology to ensure that privacy and civil liberties are adequately protected.
- Increased focus on business case for cyber risk management (“bottom line,” “overinvestment,” “business needs,” “economies of scale”)
- Increased focus on flexibility
- Framework references potential for international application and cooperation to improve security worldwide.



Privacy and Civil Liberties Methodology

- Origin: Executive Order 13636 – 7(c)
 - “Framework shall include methodologies to . . . Protect individual privacy and civil liberties.”
- First take: Appendix B of Preliminary Framework
 - Fair Information Practice Principles (FIPP) controls mapped to Framework Core
- Industry concerns over scope and details
 - Scope of application: apply only to critical infrastructure sector?
 - Appendix B referenced PII. Now term “personal information” is used and is not defined. Appropriate for an evolving concept.
 - Civil liberties apply to protection from state action, not applicable to private sector.
- Final methodology: Mostly reflects industry input.



Unanswered Questions

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



NIST Roadmap

- States that current recommendations are not exhaustive
- Outlines future focus areas
- Emphasizes the importance of private sector involvement
- Suggests that future governance may shift to an NGO, which may be more capable of working closely with international organizations



Much More To Do

- The problem is NOT faulty design (like product safety)
- Cybersecurity is a competition
 - The system is under attack
 - Cyber attack teams are getting much better all the time
 - APT (advanced persistent threat) now showing up everywhere. They will penetrate all perimeter defenses to compromise target systems.



Impact on Business

- Implementation of Framework is left to entity's discretion
- But some expectations are made explicit:
 - “Organizations responsible for Critical Infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk.”
 - In performing a self-assessment, an “organization may determine that it has opportunities to (or needs to) improve.”
- Security concerns must be managed in a manner commensurate with risk
- Creates expectations for privacy to be incorporated into security operations much more extensively than is likely at most organizations



Big Question: How do we Promote Use

- Can good companies keep up?
 - Incentives all favor the bad guys – attacks are cheap, easy to initiate, are profitable, and are unlikely to be prosecuted.
 - There are economic incentives to be insecure – long, international supply chain, BYOD policies
- Risk management means how much security you can afford to buy.



Problems of Implementation

- No. 1 problem is not lack of information, it's economics.
 - Dividing line is between the sophisticated and unsophisticated companies. Incentive to be less secured.
 - Economic incentives to be insecure – long, international supply chain, BYOD policies
 - Risk management means how much security you can afford to buy
 - Private sector spending has doubled in last 5 years
- Framework is not prioritized, so a company doesn't know where to spend first.



Incentives

- For now, technical assistance is offered through C³
- Federal financial incentives not close to fruition in near term
 - DHS/White House have stated that safety is its own incentive
 - Expectation is that market-based “incentives” will develop organically (better access to insurance, certifications, etc.)
- Legislation needed to expand liability protections
 - *E.g.*, SAFETY Act may eliminate civil liability arising out of acts of terrorism where a company has implemented a qualified anti-terrorism technology.
- To date, lawsuits have not driven cybersecurity. Difficult to determine where liability lies.



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



SEC Analysis

- On April 15, SEC issued an unprecedented blueprint for assessing cybersecurity preparedness in the securities industry
 - High-level series of questions that will form the basis for examinations
 - Follows in part the Cybersecurity Framework
 - Currently targets broker-dealers and investment advisors
 - May expand to all publicly traded companies
- SEC already scrutinizes SEC filings to ensure that companies adequately disclose cyber risk
 - Considering imposing minimum cybersecurity disclosure requirements beyond those contained in the existing guidance.



Other Concerns

- What does adoption mean? Will there be certification/audit requirements to qualify for incentives in the future?
- How will insurers use the Framework? An upcoming *Request for Information* will help answer this.
- Will there be quality incentives, especially liability limitation?



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?



Direction of the Framework

- NIST continues to convene and coordinate
 - Informal comments accepted until formal notice issued
 - Workshop 6 months from release
 - Privacy Engineering Workshop April 9-10, 2014
 - Develop technical privacy standards and best practices
 - Resurrection of Appendix B and FIPPs-based privacy controls?
 - Framework as a “living document”
 - Evolution driven by feedback on implementation
 - Areas for improvement: authentication, data analytics, international, privacy standards, etc.
 - Long-term planning – transfer of governance to NGO



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

