A Primer on Cybersecurity and Data Privacy Law

Antony K. Haynes

August 5, 2016
Attacks

In 2015, an unknown group infiltrated hundreds of banks in multiple countries, swiping somewhere in the neighborhood of $1 billion.

HEALTH

US health insurer Anthem hit by massive cyberattack: 80 million customers' private data exposed

Antony K. Haynes
Goals

1. Gain knowledge and understanding of key cybersecurity and data privacy issues facing corporate counsel.

2. Begin a conversation and information sharing around best practices for cybersecurity and data privacy.
Agenda

• Corporate Cybersecurity Standards
• National Infrastructure Cybersecurity
• Spectrum of Cyber Attacks
• Computer Fraud and Abuse Act
Corporate Cybersecurity Standards
Corporate Cybersecurity Standards

• Top 10 Issues
• Cyber Risk Checklists
• 16 CFR 314.3 & .4
• Wyndham Worldwide
Top 10 Issues

• Complexity, multi-disciplinary and dynamic nature
• Rapidly evolving cyber threats and threat agents

**Attack Vectors**
- Malware
- Phishing
- DDoS
- APT
- ZDE

**Threat Agents**
- Insiders
- Hacktivists
- Cybercriminals
- Nation Sates

Sources:
Top 10 Issues

**Cybersecurity**: The ability to protect or defend the use of cyberspace from an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

**Cyberspace**: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Source: Committee on National Security Systems Instruction (CNSSI)-4009 (National Information Assurance (IA) Glossary
Top 10 Issues

**Information Security**: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3) availability, which means ensuring timely and reliable access to and use of information.

Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66 (Information Security); 44 U.S.C., Sec 3541
Top 10 Issues – 1. Increased Regulation & Compliance Requirements

FTC
- Most common actions due to insufficient cybersecurity practices and failure to disclose breaches involving consumer information
- 3rd Circuit in *Wyndham Wordwide*
- $100M settlement in 2015 with LifeLock Inc.

FCC
- $10M fine in 2014 against TerraCom, YourTel - stored PII in clear on internet
- $25M fine in 2015 against AT&T - employees sold 280,000 customer SSANs
Top 10 Issues – 1. Increased Regulation & Compliance Requirements

SEC’s Division of Investment Management
- RT Jones (investment advisor) fined $75k for “failure to adopt policies reasonably designed to protect consumer records and information”
- → SEC’s IM Guidance Update for Cybersecurity

DOJ’s Cybersecurity Unit
- → Best Practices for Victim Response and Reporting of Cyber Incidents

California State AG
- → 2016 California Data Breach Report
- Recommendations: (1) Implement 20 CIS Critical Security Controls (2) Expand use of multi-factor authentication (3) Use strong encryption to protect PII in portable devices and (4) Encourage consumers’ use of credit file fraud alerts
- Failure to implement [applicable] Controls… constitutes a lack of reasonable security
Top 10 Issues – 1. Increased Regulation & Compliance Requirements

• Recommended Actions
  • Identify industry’s regulator’s guidelines and relevant data security and privacy laws and regulations applicable to your organization
  • Determine regulatory compliance obligations for cybersecurity
  • Streamline existing regulatory compliance processes
  • Train incident response team compliant with breach notification laws
Top 10 Issues – 2. Increased Litigation Exposure

• Cost = ~ $145 per stolen/lost record
• Target
  • $39M settlement with MasterCard banks’ class action lawsuit
  • $10M settlement with customer class action lawsuit at MTD
• Neiman Marcus
  • 7th Circuit ruled customers had standing for class action
  • Mere theft of PII constitutes imminent risk of suffering a concrete injury
• Spokeo Inc. v. Robins
  • USSC remanded standing issue to 9th Circuit (FCRA)
  • A realistic threat of actual injury is necessary but “intangible injuries can nevertheless be concrete”

• Standard of care
  • Regulators expect boards actively manage cyber risk at enterprise level
  • Industry regulations (e.g. HIPPA, GLBA) and standards (e.g. PCI DISS, NIST Framework)
  • FTC’s *Start with Security: A Guide for Business* (listing 10 lessons)
  • SEC OCIE 2015 Cybersecurity Examination Initiative
  • California AG 2016 Data Breach Report

• Recommended Actions
  • Approach cybersecurity as an enterprise risk management issue (not just IT)
  • Understand legal implication of cyber risks as they relate to company’s circumstances
  • Have adequate access to cybersecurity expertise and provide regular and adequate time on board meeting agendas for cyber risk discussions
  • Set expectation for management to established enterprise risk management framework with adequate staffing and budget
  • Cyber risk discussion includes identification of risks to avoid/ accept/ mitigate/ transfer and specific plans associated with each approach

• Questions boards should ask
  • Governance
  • Critical asset review
  • Threat assessment
  • Incident response preparedness
  • Employee training – Employee error is the most common reason for a breach
  • Third-party management
  • Insurance
  • Risk disclosure
Top 10 Issues – 4. Counseling the C-Suite

• Goal: Provide legal advice at both a strategic and day-to-day operational level to various members of the C-Suite

• Issues

• Stakeholder Interactions

• Recommended Actions:
  • Appoint counsel to be responsible for legal issues related to cyber security and the company’s security program
  • Bring novel issues of policy and legal risk to senior leadership and board
Top 10 Issues – 5. Cyber Insurance

• Duty of Care:
  • Boards actively engaged in monitoring have low personal liability risk—
  • “acted in a deliberate and knowledgeable way, identifying and exploring alternatives”

• Issues – Type of Coverage:
  • First Party coverage (crisis management and identity theft response, cyber extortion, data asset protection)
  • Third Party coverage (network security liability, privacy liability)
  • Specific Policies (underwriting, claims, exclusions, coverage, requirements)

• Recommended Actions:
  • Review efficacy of cyber-risk insurance for your organization’s purposes. Pay particular attention to exclusions and conditions imposed.
Top 10 Issues – 6. Commercial Transactions

- Transactions Implicated:
  - M&A
  - Vendor/Supplier contracts
  - Customer/Client contracts

- Recommended Actions:
  - Update due diligence checklist to include cybersecurity issues
  - Review key contractual provisions used in transactions
  - Review vendor oversight program to include cybersecurity risk assessments
Top 10 Issues – 7. Information Sharing with Law Enforcement

• Governments Compel Decryption
  • China’s counterterrorism law can compel decryption of communications
  • FBI’s request that Apple install iPhone “back door”

• Recommended Actions
  • Confirm company’s information sharing partnerships with industry and government benefit the company and do not put it at undue risk
  • Provide regular legal oversight and training of relevant personnel
  • Appoint counsel for issues arising out of law enforcement interactions
  • Develop law enforcement contacts and relationships prior to needing them
Top 10 Issues – 8. Incident Preparation & Response

• Recommended Actions
  • Appoint counsel to help lead the incident response team and process (should be familiar with cybersecurity concepts, fact patterns and terms)
  • Retain key internal and external resources (forensics, counsel, PR)
  • Conduct regular exercises, including senior leaders, to prepare for incidents
  • Prepare for key legal issues in advance, e.g. attorney-client privilege, communications with senior management, criteria for incident disclosure
Top 10 Issues – 9. International Data Transfers

• Trans-Atlantic data transfers face a period of continued uncertainty
  • ECJ in *Schrems* (Oct. 2015) invalidated data transfer safe harbor

• EU-US Privacy Shield proposed in February 2016
  • FTC enforces “strong obligations on companies handling Europeans’ personal data”
  • US agrees to prohibit mass surveillance of EU personal data, subject to “clear limitations, safeguards and oversight mechanisms”
  • EU citizens may seek redress in FTC, free ADR, or in intelligence agency ombudsperson
  • In June, the EC proposed further data sharing limitations on companies ability to transfer data to third parties and on ombudsperson independence.

• Recommended Actions:
  • Anticipate impact of EU-US privacy shield on business operations
Top 10 Issues – 10. Internet of Things

• Limited regulation (currently)
  • FTC’s *Trendnet* enforcement action in 2013 only significant case

• Recommended Actions:
  • Review company’s use or production of mobile data collection for cybersecurity issues
  • Consider evolving standards on data collection, unexpected uses of consumer data and/or heightened security risks
Cybersecurity Self-Assessment

<table>
<thead>
<tr>
<th>Organizational Prevention and Preparedness</th>
<th>Organizational Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization conducts a cybersecurity audit of the entire organization at least annually</td>
<td>Password policy</td>
</tr>
<tr>
<td>A member of the legal department is on the company's data breach response team</td>
<td>Social media policy</td>
</tr>
<tr>
<td>Organization has cybersecurity insurance</td>
<td>Document retention policy</td>
</tr>
<tr>
<td>Organization has mandatory training on cybersecurity for all employees</td>
<td>Website privacy policy</td>
</tr>
<tr>
<td>Organization tests employee preparedness/knowledge of cybersafety practices/data policies at least annually</td>
<td>Employee manual acceptance policy</td>
</tr>
<tr>
<td>Organization retained outside counsel to assist you should a breach occur</td>
<td>Internet privacy policy</td>
</tr>
<tr>
<td>Company collaborates proactively with law enforcement or other governmental agencies to address cybersecurity risks</td>
<td>Identity and access management</td>
</tr>
<tr>
<td>Organization retains a forensic company to assist should a breach occur</td>
<td>BYOD policy</td>
</tr>
<tr>
<td></td>
<td>Data map</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organizational Staffing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Information Officer (CIO)</td>
</tr>
<tr>
<td>Privacy/Security Manager</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
</tr>
<tr>
<td>Chief Risk Officer (CRO)</td>
</tr>
<tr>
<td>Chief Privacy Officer (CPO)</td>
</tr>
<tr>
<td>Chief Security Officer (CSO)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organizational Preparedness Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct cybersecurity audit of entire organization at least annually</td>
</tr>
<tr>
<td>Use a standard (e.g., SAE, NIST, ISO) to prepare for, manage, and reduce cybersecurity risk</td>
</tr>
<tr>
<td>Track mandatory training requirement and attendance for all employees</td>
</tr>
<tr>
<td>Test employees’ knowledge of mandatory training</td>
</tr>
<tr>
<td>Conduct mock security event</td>
</tr>
<tr>
<td>Conduct tabletop exercises</td>
</tr>
<tr>
<td>Review disciplinary actions for violations</td>
</tr>
</tbody>
</table>

Source: ACC Foundation, Key Findings from the ACC Foundation the State of Cybersecurity Report (2016), at 8
Questions for the Board to Ask Management

SITUATIONAL AWARENESS
1. Were we told of cyberattacks that already occurred and how severe they were?
2. What are the company’s cybersecurity risks, and how is the company managing these risks?
3. How will we know if we have been hacked or breached, and what makes us certain will we find out?
4. Who are our likely adversaries?
5. In management’s opinion, what is the biggest vulnerability in our IT systems?
6. If an adversary wanted to deal the most damage to our company, how would they go about it?
7. Has the company assessed the inside threat?
8. Have we had a penetration test or external assessment? What were the key findings, and how are we addressing them? What is our maturity level?
9. Does our external auditor indicate we have deficiencies in IT? If so, where?

CORPORATE STRATEGY AND OPERATIONS
1. What are leading practices for cybersecurity, and where do our practices differ?
2. Do we have an appropriately differentiated strategy for general cybersecurity and for protecting our mission-critical assets?
3. Do we have an enterprise-wide, independently budgeted cyber-risk management team? Is the budget adequate?
4. Do we have a systematic framework, such as the NIST Framework, in place to address cybersecurity to assure
5. Where do management and our IT team disagree on cybersecurity?
6. Do the company's outsourced providers and contractors have cyber controls and policies in place and clearly monitored? Do those policies align with the company's expectations?
7. Does the company have cyber insurance? If so, is it adequate?
8. Is there an ongoing, company-wide awareness and training program established around cybersecurity?
9. What is our strategy to address cloud, BYOD and supply chain threats?
10. How are we addressing the security vulnerabilities of an increasingly mobile workforce?

INCIDENT RESPONSE
1. How will management respond to a cyberattack? Is there a validated corporate incident response plan? Under what circumstances will law enforcement and other relevant government entities be notified?
2. For significant breaches, is our communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and ramifications to the company and the response plan?
3. Are we adequately exercising our cyber-preparedness and response plan?
4. What constitutes a material cybersecurity breach? How will those events be disclosed to investors?
FTC Section 5 Enforcement

• Reasonable Security Standard
  • FTC Allegations of insufficient cybersecurity practices and failure to disclose breaches involving consumer information.
16 CFR 314.3
Standards for safeguarding consumer information

• **Information security program.**
  • comprehensive information security program that is written
  • contains administrative, technical, and physical safeguards appropriate to:
    • your size and complexity,
    • the nature and scope of your activities, and
    • the sensitivity of any customer information at issue.
16 CFR 314.3
Standards for safeguarding consumer information

• *Information security program.*
  • Such safeguards ... shall be reasonably designed to ...  
    • *(1)* Insure the security and confidentiality of customer information;  
    • *(2)* Protect against any anticipated threats or hazards to the security or integrity of such information; and  
    • *(3)* Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

• Such safeguards ... shall include the elements set forth in § 314.4
16 CFR 314.4
Elements of comprehensive information security program

• (a) Designate an employee or employees to coordinate your information security program

• (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

• (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
16 CFR 314.4
Elements of comprehensive information security program

• (d) Oversee service providers, by:
  • (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
  • (2) Requiring your service providers by contract to implement and maintain such safeguards.

• (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
FTC v. Wyndham Worldwide
Wyndham’s Hotel Group Brands
Franchise vs Management Contract

• A franchisee is the buyer of a brand name and remains an independent businessman from the franchiser (who owns the brand)

• In a management agreement, the franchiser provides the same services as a franchise agreement, such as brand, reservation system etc., but on top of this, there is an agency agreement, meaning the brand operates the hotel, making all the day-to-day decisions on behalf of the owner.

• In a franchise agreement fees are collected on a room revenue basis, and in the management agreement, fees are collected on a total revenue basis and on the bottom-line
Wyndham Attacks

• 2008 – 2010 – Wyndham attacked three times
  • Hackers stole PII for over 619,000 customers
• April 2010 – FTC begins investigation under Section 5
  • Wyndham spends over $5 million complying
• June 2012 – FTC initiates legal proceedings
• April 2014 – District court denies Wyndham’s motion to dismiss
• August 2015 – 3rd Circuit Affirms trial court
• December 2015 – Consent Decree
What is the legal standard?

• FTC contends the Court can evaluate the reasonableness of Hotels and Resorts’ data security program in view of the following guidance:

  • (1) industry guidance sources that Hotels and Resorts itself seems to measure its own data-security practices against; and

  • (2) the FTC’s business guidance brochure and consent orders from previous FTC enforcement actions.
Wyndham’s Alleged Cybersecurity Failures

• No firewalls
• Stored payment card info in clear readable text
• Did not require franchisees to have adequate information security policies and procedures
• Allowed franchisees to connect servers with outdated O/S’s
• Used “micros” as username and password for Micros Systems software
• No password policy or requirement for complex passwords
Wyndham’s Alleged Cyber Failures Continued

• Inadequate inventory of connected devices
• No intrusion detection system
• No access segmentation or access restriction or IP filtering
FTC’s Deception Claim

• Hotels and Resorts’ website represents, in part, that
  • “[w]e safeguard our Customers’ personally identifiable information by using industry standard practices” and make
  • “commercially reasonable efforts” to collect personally identifiable information “consistent with all applicable laws and regulations” and, among other things, that
  • “[w]e take commercially reasonable efforts to create and maintain ‘fire walls’ and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy.”
Intrusion Detection System

- Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior based solely on network traffic.
- A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network.
- Using the captured data, the IDS system processes and flags any suspicious traffic.
- Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting. Examples of Network IDS:
Demilitarized Zone (DMZ)

- Outer firewall b/t the Internet and the Web Server processing the requests originating on the company Web site.
- Inner firewall b/t the Web Server and the appl. Server to which it is forwarding requests. Date resides behind this.
Settlement
Conclusion from FTV v Wyndham

- There is a baseline of minimum cybersecurity practices
- Look to industry guidelines and agency consent decrees
- A robust cybersecurity and risk mitigation program require periodic review and iteration to stay up to date with the latest
  - security software and
  - regulatory reports and tools for companies to map policies and practices
Hypothetical 1

• The CEO rushes into your office in a panic. Your company’s clients’ personal information has appeared in the public domain. A reporter has called inquiring about the data breach. A government regulator has emailed an information request.
National Infrastructure
Cybersecurity
National Infrastructure Cybersecurity

• FISMA
• EO 13636
• Critical Infrastructure
• NIST Framework
• EO 13691
• CISA
• CNAP
Cybersecurity— a Legislative Priority in Past Decade

**Timeline of Enacted Cybersecurity Legislation, Executive Orders**

- **2002**
  - Federal Information Security Management Act (FISMA)
    - Establishes a comprehensive, risk-based framework to ensure information security controls over information resources supporting federal operations and assets

- **2006**
  - National Infrastructure Protection Plan
    - Provides framework integrating a range of efforts and partnerships designed to make the nation’s critical infrastructure more safe

- **2008**
  - Comprehensive National Cybersecurity Plan
    - Establishes frontline of defense against network intrusion, enhances U.S. counterintelligence capabilities and expands cyber education

- **2013**
  - Executive Order 13636 “Improving Critical Infrastructure of Cybersecurity”
    - EO requires government to share cybersecurity threats with private sector and directs NIST to create best practices for cybersecurity in the private sector; House passes, but Senate does not take action on, major cybersecurity bill CISPA

Cybersecurity— a Legislative Priority

Timeline of Enacted Cybersecurity Legislation, Executive Orders and Plans

2014
- NIST Cybersecurity Framework v1.0

Early 2015
- Executive Order 13691
  “Promoting Private Sector Cybersecurity Information Sharing”

Late 2015
- Cybersecurity Information Sharing Act

2016
- Cybersecurity National Action Plan

Source:
Federal Information Security Management Act (FISMA):

• Strengthen federal agencies resistance to cybersecurity attacks and lead by example.

• Mandates CIO of each federal agency develop and maintain an agency-wide information security program that includes:
  • periodic risk assessments
  • security policies/plans/procedures
  • security training for personnel
  • periodic testing and evaluation
  • incident detection, reporting & response
  • plan to ensure continuity of operation (during an attack)

• Yearly report to Office of Management & Budget (OMB), tied to procurement.
Executive Order 13636 – Improving Critical Infrastructure Cybersecurity

• Creates information sharing mechanisms between private industry and state and local governments
• Federal agencies develop voluntary cybersecurity guidelines for critical infrastructure
• Identifying critical infrastructure at greatest risk—
  • cybersecurity incident could reasonably result in *catastrophic* regional or national effects on public health or safety, economic security, or national security
Key Government Agencies & Organizations Protect Federal & Private Organizations from Cyber Threats

**Agencies Tasked with Protecting Nation’s Cybersecurity**

**Department of Homeland Security**
- Responds quickly to cyber vulnerabilities
- Partners with owners and operators of critical infrastructure, to release actionable cyber alerts
- Investigates and arrests criminals
- Educates public on cyber safety
- Within DHS, United States Computer Emergency Readiness Team (US-CERT) provides cyber threat warning information and coordinates responses

**Office of Management and Budget**
- Develops and oversees implementation of policies, principles, standards, and guidelines on information security in federal agencies
- Annually reviews and approves agency information security programs

**Department of Commerce**
- Oversees Internet Policy Task Force
- Researches and reviews cybersecurity standards in the commercial sector
- Within the Department of Commerce, the National Institute of Standards and Technology (NIST) develops minimum security standards for agencies and guidelines for identifying information systems critical to national security

Executive Order 13636 –
Improving Critical Infrastructure Cybersecurity

• **Purpose:**
  • Help owners and operators “identify, assess and manage cyber risks”

• **Direction:**
  • NIST to coordinate development of “Cybersecurity Framework”

• **Results:**
  • A set of “voluntary consensus-based standards and industry best practices”
Critical Infrastructure

- Chemical Sector
- Commercial Facility
- Communications
- Critical Manufacturing
- Dams Sector
- Defense Industrial Base
- Emergency Services
- Energy

- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare/Public Health
- Information Technology
- Nuclear Reactors/Materials
- Transportation Systems
- Water Systems
EO 13636, Private Sector Cooperation Is Voluntary

Cybersecurity Executive Order (EO) Flow of Information

**Mandated Course of Action**

**U.S. Executive Branch**
- Ordered National Institute of Standards and Technology (NIST) to create a “cybersecurity framework” to identify threats and establish guidelines for protection; a first draft was released in February of 2014
- Ordered NIST to assess its own performance on privacy
- Directs all government agencies to provide alerts to the private sector in the event of a threat

**Private Sector**
- May help NIST develop framework
- May volunteer to comply with cybersecurity framework
- May help to protect critical infrastructure, e.g., electrical grids, banking systems, and water treatment plants

**Voluntary Course of Action**

Expertise and advice

Analysis

- Obama’s 2013 executive order aimed to enhance cybersecurity by establishing a synergetic framework between the private sector and government agencies
- Government agencies must share information about alerts, threats, and vulnerabilities with private sector
- In return, private sector entities are advised, though not required, to help NIST develop a stronger cybersecurity framework


Source: Cybersecurity Primer, August 15, 2014, National Journal Presentation, David Stauffer and Jessica Guzik
## NIST Framework’s Tiers Rate Organizational Preparedness Against Cyber Threats

<table>
<thead>
<tr>
<th>NIST Tiers</th>
<th>Risk Management Process</th>
<th>Integrated Risk Management Program</th>
<th>External Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier I – Partial</td>
<td>No formalized process, ad hoc and reactive to threats, not informed by organizational needs or current trends</td>
<td>Limited awareness of cybersecurity risk and no organization-wide approach to risk management</td>
<td>No processes in place to participate in coordination with other entities on cybersecurity</td>
</tr>
<tr>
<td>Tier II – Risk Informed</td>
<td>Risk management practices are approved by management but may not be organization-wide policy; risk management may be informed by organizational needs or current trends</td>
<td>Awareness of cybersecurity risk at the organizational level, no organizational approach</td>
<td>The organization understands it is part of a larger ecosystem but has no formal system for external interaction</td>
</tr>
<tr>
<td>Tier III – Repeateble</td>
<td>The organization’s risk management practices are formally approved and expressed as policy, and the organization changes those practices based on updated organizational needs and current trends</td>
<td>A consistent organization-wide approach to risk management</td>
<td>The organization understands its partners and dependencies and receives information from those entities that allows for collaboration and informed responses to threats</td>
</tr>
<tr>
<td>Tier IV – Adaptive</td>
<td>A formalized and continuously updating system of cybersecurity practices based on information from previous and current cybersecurity activities</td>
<td>An organization-wide approach to managing cybersecurity risk using risk-informed policies and procedures, with cybersecurity risk management as a part of organizational culture</td>
<td>Actively shares information with partners to ensure systemic security and defense against a cybersecurity breach</td>
</tr>
</tbody>
</table>

Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing

• Real time information sharing regarding cybersecurity risks and incidents between private and public sector

• Formation of Information Sharing and Analysis Organizations (ISAOs)
Cybersecurity Information Sharing Act (CISA)

• Remove legal barriers for companies to share information about cybersecurity threats and providing liability protection for companies who share such information

• Liability protection would allow protection from civil action, regardless of prior contracts that may prevent sharing information without a customer’s consent (ss 104(a)(1), 106(a))

• Allows companies to directly share information with the Department of Defense (including the National Security Agency) without fear of being sued (ss 102(3), 104(c)(1), 105(a)(1), 106(b))
Cybersecurity Information Sharing Act (CISA)

• Overbroad definition of “cyber threat indicator” (ss 102(6)(g))
• Requirement for private entities to strip out “known” identifying information prior to sharing cyber threat indicators (ss 104(d)(2))
• Authorizes “weaponized” counter-measures “notwithstanding any law” (e.g., Computer Fraud and Abuse Act) (but see ss 102(7)(b))
• Permits law enforcement to use the information for purposes beyond simply fighting cyber crimes (ss 104(d)(4)(a), 105(d)(5)(a))
Cybersecurity Information Sharing Act (CISA)

• Doesn’t address root data breach causes—unencrypted files, un-updated servers, no firewall, no password policy, no segmentation

• How is information sharing supposed to actually improve security?
  • The underlying premise behind information sharing is the fact that hackers tend to use the same methods and programs against multiple targets.
President Obama’s $19 Billion Cybersecurity Proposal Calls for 35% Increase Over 2016 Enacted Level

Major Pieces of the Cybersecurity National Action Plan

$3.1 billion Information Technology Modernization Fund
This fund enables the retirement, replacement and modernization of IT equipment throughout the government. Many see this initiative as overdue as some branches of the government are running antiquated as old as Windows XP which Microsoft stopped officially supporting in 2014.

Full Multi-Step Authentication Rollout
While a large portion of the government uses 2-step or multi-step authentication for internal logins, the initiative plans to extend this extra layer of security to citizen-facing federal government digital services. The President hopes this switch will also increase public awareness of this identity proofing mechanism, encouraging more wide use among private online systems.

EINSTEIN and the Continuous Diagnostic and Mitigation Program
The president proposes allocating increased funding to the government’s primary cyber defense system: EINSTEIN, which has faced significant criticism since it is currently unable to dynamically detect new kinds of cyber intrusions, making it only useful against known threats.

National Initiative for Cybersecurity Education
$62 billion is requested to invest in educating the nation’s next generation of cybersecurity personnel. Proposed programs include the CyberCorps Reserve which would offer scholarships for Americans who wish to obtain cybersecurity education in exchange for civil service in government.

Critiques from the Tech Industry
• While many in the tech industry have applauded the president’s proposal for investment, many of the suggestions are seen as basic and a sign at how woefully behind our government is on cybersecurity. Brian Barrett, a writer for Wired magazine, compares the plan to “standard advice you’d give a tech novice”.
• With the proposal coming from a “lame-duck” president nearing the end of his second term, there is a growing pessimism that pieces that require congressional action will go unfunded.
• Despite being a basic tenet of internet security, encryption is notably absent from the president’s press release. While many in the tech community believe encryption is necessary for continued cyber safety, the topic remains controversial in Congress.
# Education and Public-Private Partnerships Highlight Improvements in Government Cybersecurity Programs

<table>
<thead>
<tr>
<th>Programs</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commission on Enhancing National Cybersecurity</td>
<td>The commission, created through an executive order, will be comprised of “top strategic, business and technical thinkers” from the private sector. The main goal is to establish a link between the federal government and Silicon Valley to provide insight on best practices for federal cybersecurity.</td>
</tr>
<tr>
<td>Cybersecurity Assurance Program</td>
<td>The program, run by the Department of Homeland Security, would test and certify network devices to standardize security standards for internet-connected consumer goods, ranging from refrigerators to medical infusion pumps.</td>
</tr>
<tr>
<td>National Center for Cybersecurity Resilience</td>
<td>The Center is a public-private research and development partnership which will allow the industry and the government to cooperate in developing solutions for high-priority cybersecurity challenges.</td>
</tr>
<tr>
<td>Cyber Mission Force</td>
<td>Comprised of 133 teams and nearly 6,200 military, civilian and contractor personnel, the Cyber Mission Force would take a military and defense approach to support U.S. Government objectives. Plans are to have the group fully operational by 2018.</td>
</tr>
<tr>
<td>Cybersecurity Core Curriculum</td>
<td>The president’s proposal includes a request to develop a set of unified educational goals to ensure that cybersecurity graduates who wish to join the federal government have the requisite skills and knowledge to succeed.</td>
</tr>
</tbody>
</table>

Hypothetical 2

• The NSA has requested that your company provide access to its customer list data as part of an effort to identify potential members of a possible terror cell. Your company’s contract guarantees its customers that their data will never be shared with any outside party, including government entities. One of your biggest customers has threatened to leave if you comply with the NSA request. In addition, the NSA also intends to provide your customer data to the FBI to help the FBI protect the trade secrets of one of your competitors.
Spectrum of Cyber Attacks
Cyberwar “Arrives”?

Pentagon wages cyberwar against Islamic State

Los Angeles Times, February 29, 2016

U.S. commanders mounted a cyber offensive against Islamic State in Syria for the first time in recent weeks by deploying military hackers against the extremist group’s computer and cellphone networks, according to the Pentagon.

The digital assault, launched from Ft. Meade in Maryland, marked the first major integration of U.S. Cyber Command into a major battlefield operation since the command was established in 2009.

More importantly, Secretary of Defense Ashton Carter’s disclosure of a government-sanctioned cyberattack represents a shift in America’s warfare-fighting strategy and power projection. No other nation has publicly acknowledged launching cyberwar.
Carter said Monday at the Pentagon that the goal was to "overload their networks" and "interrupt their ability to command and control forces" with jamming and other cybertools.

... 

U.S. officials said targeted denial of service and other cyberattacks, plus more than 85 coalition airstrikes, helped U.S.-backed Syrian rebels retake the strategic town of Shaddada and nearby oil fields in mid-February, a major prize in the war.

The officials, who were not authorized to speak publicly about ongoing operations, said teams working from Ft. Meade identified and jammed Islamic State online communication networks during the four-day battle.
Lewis: “Cyber War Has Not Begun”/
Rid: “Cyber War Will Not Take Place”

**Four kinds of threats:**

- Crime
- Espionage (e.g. GhostNet)
- Subversion (e.g. Anonymous, DNC Hack)
- Sabotage (e.g. Stuxnet)

**None qualify as “war”:**

- War = (1) violence (2) instrumental (3) political attribution
Cyber Attack Case Studies

**Estonia (April 2007):**
- DDoS shuts down parliament, banks, ministries, newspapers and broadcasts → appeal to NATO for help.

**Georgia (August 2008):**
- Government and commercial websites shut down by DOS in concert with Russian ground troops invasion.

**Iran (June 2010):**
- “Stuxnet” worm damaged Iranian nuclear facility
“Law for Cyberwar”

**Dunlap:**

- Tenets of LOAC are sufficient to address most issues of cyberwar
  - Difficulty is not “law” but determining facts needed for judgments
  - “act of war” → National security response vs law enforcement action

- UN Charter art 51: “armed attack”
  - Schmitt: “CNA ... cause physical damage to tangible property or injury or death to human beings”
  - DoD JP 3-12: “actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction)” (p II-5)
“Cyberspace is not a Warfighting Domain”

**Libicki:**
- Cyber “war” is an engineering endeavor—safety engineering for defense and reverse engineering for vulnerabilities for offense
  - “highly malleable by its owners,” “not a given environment” (p 324)
  - “composed of multiple media” that advantage owners-operators (p 328)
- Defense: “change the particular features of one’s own portion of cyberspace itself so that it is less tolerant of attack” (p 326)
  - Overall: safety engineering, architecture, administration, policies (p 329)
- Offense: “creating useful effects in your adversaries’ systems” (p 328)
  - “the military metaphor just does not fit it” (p 329)
  - cyberspace superiority is likely of “modest military value” (p 327)
Responses to Cyber Attacks - Deterrence

**Baker:**
Exploit attribution of cyber espionage for deterrence
- Impose sanctions on foreign hackers and their customers
- Use “S” visas to recruit most skilled foreign hackers
- Pass laws to allow victims of data theft to sue foreign companies
- Require DOJ/FBI to issue letters of marque to create privateers
“Future of All Things Cyber”

**Hayden:**
- **Lack of attribution?** See Baker.
- **Is cyber a domain?** See Libicki.
- **Privacy?** See CISA (Dec ‘15), EO 13636 (Feb ‘15).
- **Is cyber “war” a threat?** See McConnell; *contra* Rid.
- **Private sector’s role?** See FTC actions; NIST framework; CIS controls.
- **Classification?** See PPD 20 (Snowden leak).
- **Self Defense?** See Baker; CISA; PPD 20.
- **International Law/ LOAC?** See Dunlap; Tallinn Manual.
Cyberspace and Cyberspace Operations

DoD JP 3-13 (p II-9):

Cyberspace:
- “A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

Cyberspace Operations: “deny or manipulate adversary or potential adversary decision making, through targeting
- an information medium (such as a wireless access point in the physical dimension),
- the message itself (an encrypted message in the information dimension), or
- a cyber-persona (an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension).”
Cyber Terrain

Layer | O/S | Internet | Data Format | Protocols |
------|-----|----------|-------------|-----------|
1     | Physical | Hardware, Cables (fiber, copper, etc.) |
2     | Data Link | Network Access | Frames |
3     | Network | Internet | Packets |
4     | Transport | Host-Host | Segments or Diagrams |
5     | Session | | |
6     | Presentation | | |
7     | Application | | |
8     | Machine Language | 01010101010100001010010 |
9     | Operating System | Win / *nix / Android / IOS / etc. |
10    | Software Application | Browsers, Office Products, etc. |
11    | Persona | User IDs, Emails, Phone Numbers |
12    | People | Supervisory | Temporal |
13    | Organization | Org. Cyber Policies, Procedures, Information Sharing Agreements, etc. |
14    | Government | Govt. Cyber Laws, Regulations, Policies, Frameworks, Agreements, etc. |

Go to www.securitytodayinfo.com
Convergence of EW and IO

SOURCE: CERDEC I2WD.
RAND MG1113-5.2
DoD and U.S. Cyber Command

**Responsibilities:**
- Cyber Command - .mil domain
- DHS - .gov domain
- Individual companies - .com domain

**Cyber Command vs NSA:**
- Title 10 vs Title 50
- CNA vs CNE
- Clandestine vs Covert
PPD-20 U.S. Cyber Operations Policy

This directive provides a procedure for cyber collection operations that are reasonably likely to result in “significant consequences.”² (S/NF)

Significant Consequences: **Loss of life**, significant responsive actions against the United States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States.
Offensive Cyber Effects Operations (OCEO)

OCEO can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging. The development and sustainment of OCEO capabilities, however, may require considerable time and effort if access and tools for a specific target do not already exist. (TS/NF)

The United States Government shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive. (TS/NF)
Cyber Operations Targeting

The Secretary of Defense, the DNI, and the Director of the CIA – in coordination with the AG, the Secretaries of State and Homeland Security, and relevant IC and sector-specific agencies – shall prepare for approval by the President through the National Security Advisor a plan that identifies potential systems, processes, and infrastructure against which the United States should establish and maintain OCEO capabilities; proposes circumstances under which OCEO might be used; and proposes necessary resources and steps that would be needed for implementation, review, and updates as U.S. national security needs change.  
[Action:  DOD, Office of the DNI, and CIA update to Deputies on scope of plans; 6 months after directive approval]  (TS/NF)
Hypothetical 3

- As part of a promotional campaign, your company released a video featuring well-known comedians mocking the country of Ruskiya and its glorious leader. The video went viral, becoming an international hit, but it irreparably damaged Ruskiya’s reputation and caused its currency to crash. Ruskiya’s glorious leader promised revenge. Soon after, a DDoS shuts down hospitals, banks, airports, and newspapers in the U.S., causing billions of dollars of financial losses; and a hospital patient died when given the wrong mediation.
Computer Fraud and Abuse Act
Computer Fraud and Abuse Act (CFAA)

- 18 USC 1030
- *Aaron Schwartz* (2013)
- *Nosal I* (9th Cir. 2012)
- *Valle* (2nd Cir. 2015)
- *Nosal II* (9th Cir. 2016)
18 USC 1030

• Originally narrow—enacted in 1984 to protect national security, financial records, and government property
• Now broad—regulates every use of every computer in U.S. (and potentially around the world)
• Key phrase “unauthorized access” is vague, ambiguous
• Users sometimes cannot know if use if “authorized”
18 USC 1030

• (e)(6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
Lori Drew

**Background**
- In 2006, created a fake MySpace account of non-existent 16-year-old boy to discover whether daughter’s friend was spreading false information about daughter
- Used fake account to flirt for months with daughter’s friend and then told daughter’s friend the world would be a better place without her.
- Daughter’s friend then committed suicide.

**Trial Court**
- Jury convicted Drew of violating CFAA under theory Drew violated terms of service (TOS) of MySpace

**Appellate Court**
- On appeal, the court vacated conviction because TOS did not govern “authorization” and the broader interpretation would render the statute void for vagueness
Aaron Swartz

• In 2011, downloaded 2.7 million academic papers from JSTOR via his MIT account
• All academic papers were freely available
• JSTOR did not pursue a complaint
• DOJ prosecuted under CFAA “exceeds authorized access” → up to 50 years sentence and $1 million fine
• Committed suicide before trial
Nosal I

Background
• In 2004, resigned from Korn/Ferry and agreed to serve as a paid, independent contractor for one year, with a non-compete

• After leaving, Nosal had three Korn/Ferry employees help him start a competing executive search business

• Before leaving, the three employees downloaded “confidential and proprietary” data, including source lists, names, and contact information for executives

District Court
• Initially found against Nosal; held, “when a person access a computer ‘knowingly and with the intent to defraud ... [it] renders the access unauthorized or in excess of authorization.”

• Then reversed itself, on reconsideration, following 9th Circuit’s Brekka decision and government appealed.
Nosal I

Appellate Court

• Held: Current employee of a company did not violate CFAA (did not “exceed[] authorized access”) when he was authorized to access the company’s computers but did so in a way that violated use restrictions listed on the company’s website and in the employee handbook.

• Rationale: Applied rule of lenity because statute open to two contradictory interpretations

• Observation: “government’s interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute”
Valle

Background
• In 2012, while NYPD officer, fantasized online at DFN about engaging in cannibalism and sexual violence against women
• Used his access to law enforcement databases to search for home address of high school classmate he desire to kidnap

District Court
• Denied MJA; found Valle violated CFAA because he had not been authorized to search for classmate without a law enforcement reason

Appellate Court
• On appeal, the court reversed, finding the statute was ambiguous and the rule of lenity required ruling in favor of defendant
Circuit Split

**Issue:** statutory interpretation of “exceeds authorized access”

1st, 5th, 7th and 11th Circuits
- “interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty”
- “these courts only looked at the culpable behavior of the defendants”

2nd, 4th and 9th Circuits
- “risk of criminalizing ordinary behavior inherent in [the government’s] broad construction”
- “we must construe ambiguous statues narrowly”
Nosal II

Appellate Court

• *Held:* Former employees of a company violated CFAA (acted “without authorized access”) when they subsequently used passwords of a current employee, with the employee’s permission, to access the company’s computers.

• “[A] person uses a computer ‘without authorization’ under [the CFAA] . . . when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.”

Consequences

• Appears to criminalize password sharing (*but see Facebook v. Power Ventures* (9th Cir. July 12, 2016))

• Expands scope of CFAA from “breaking into” computer systems into policing what legitimate users know or are told → What constitutes ‘notice’?
Hypothetical 4

• A senior manager has figured out how to use your company’s access to a third party’s database of prospects to download the entire database. While the legitimate access was limited to only a tiny portion of the database, the manager was able to circumvent this limitation relatively easily. The manager then provided this enhanced database access to one of his college friends working for a company on the west coast. The database provider recently contacted your company due to the higher than expected usage of the database.