Cybersecurity Law and Risk Management

Mr. Keelan T. Stewart

March 21st, 2018

keelan.t.stewart@gmail.com

About the Speaker

- Education and Certification
  - BS, MS in Information Assurance, University of Nebraska Omaha
  - Certified Information Systems Security Professional, CISSP
  - GIAC Law of Data Security & Investigations, GLEG
- Experience
  - Information Security Analyst and Authorizing Official, Boys Town
  - Nuclear and Space Mission Systems Cybersecurity Analyst, U.S. Strategic Command
  - National and Nuclear Command and Control Enterprise and Solutions Architect
- Distinctions
  - Joint Civilian Service Achievement Award (2015)
  - C4 Systems Directorate Civilian of the Quarter (2011, 2014)
  - Walter Scott, Jr. Scholarship (2008)

Agenda

- Identification of Applicable Laws and Regulations
- Information Security Register
- Review of Cybersecurity Law
  - International Laws
  - Federal Laws
  - State Laws
  - Industry Regulations
- Integration with the Risk Management Framework

Identification of Applicable Laws and Regulations

Identification of Applicable Laws and Regulations

- Identify Sources
  - Regulated Industries
  - Legal Jurisdictions
  - Protected Information Types
- Identify Regulators
  - International
  - Federal
  - State
  - Industry

Regulated Industries

- Identify all known industries your organization operates in
  - Think about what products/services you provide
  - Think about what departments you have
- Think broad, then focus in
  - Ex., A bank's industries may include banking, finance (loans), investments, insurance, and storage (safety deposit boxes)
- Major regulated industries:
  - Healthcare
  - Education
  - Infrastructure
  - Finance
  - Commerce

Legal Jurisdictions

- Identify all known legal jurisdictions you operate in
  - Think about where your offices/branches are
  - Think about where your customers live
  - Think about where your interactions with customers are
    - Brick-and-Mortar and Online
- Goal is to identify all countries and states you operate in

Protected Information Types

- Determine intuitive types of information
  - Ex. Cardholder data, medical records, etc.
- Determine formal types of information
  - Reference the Federal Enterprise Architecture and NIST SP 800-60 Volume I and II
    - May require minor tailoring from federal focus
  - Ensures you capture most exception cases
  - Bonus: NIST maps FEA information types to C-I-A impact for security control selection

Protected Information Types

Information Types	Security Objective		
	Confidentiality	Integrity	Availability
Personally Identifiable Information	Moderate	Moderate	Moderate
Protected Health Information	Low	Low	Low
Consumer Financial Information / NPI	Low	Low	Low
Private & Foundation Grants	Low	Low	Low
Knowledge Creation and Management			
Research & Development	Low	Moderate	Low
General Purpose Data & Statistics	Low	Low	Low
Advising & Consulting	Low	Low	Low
Public Affairs			
Product Outreach	Low	Moderate	Low
Information & Technology Management			
Record Retention	Moderate	Moderate	Low
Information Sharing	N/A	N/A	N/A
Security Categorization	Moderate	Moderate	Moderate

Regulators

- Identify all regulators that have jurisdiction over you
  - Consider regulators who have conducted past audits
  - Consider regulators who audit similar organizations
  - Consider regulators who issue guidance in your industry
- Identify which laws/regulations those regulators focus on
  - Typically based on past findings, cases against other organizations
  - Some, like FTC, list their core areas on their website

Information Security Register

The Register

- The Register is your cybersecurity body of knowledge
  - Document and maintain for posterity
- Excel workbook with the following sheets
  - Regulations: document all applicable laws/regulations
  - Systems: document all information systems
  - Controls: document all sets of security control selections
  - Definitions: document all acronyms and definitions
  - Exclusions: document all non-applicable laws/regulations, with justifications
  - Read Me: document basic information about the workbook

The Register: Regulations Tab

Cybersecurity Law Register	Total: 180						
Regulation Name	**Type**	**Code(s)**	**Regulator**	**Overlay**	**Scope**	**Requirements**	**Penalties**
BSA *Bank Secrecy Act*	Federal	31 U.S.C. § 5311 *et seq.*	Treasury		**§ 5312(a)(2):** Financial institutions	**§ 5321(b):** Maintain records about reportable transactions for 6 years	Fine not to exceed $100K per day, per location
CAN-SPAM *Controlling the Assault of Non-Solicited Pornography and Marketing Act*	Federal	15 U.S.C. § 7701 *et seq.*	FTC		**§ 7702(2):** Commercial email - primary purpose is ad or promotion of a product or service *See Notes*	**§ 7704:** Prohibition of false or misleading transmission information; prohibition of deceptive subject headings; inclusion of return address or comparable mechanism (unsubscribe link); allowance to provide detailed unsubscribe; prohibition of transmission of commercial email after objection (unsubscribe) after 10 business days; inclusion of identfier, opt-out, and physical address; prohibition of address harvesting and dictionary attacks; requirement to place warning labels on emails containing sexually oriented material	$250 per email not to exceed $2M; may be blacklisted by ISPs until compliant
CFATS *The Chemical Facility Anti-Terrorism Standards*	Federal	6 C.F.R. Part 27	DHS	NIST SP 800-171	**§ 27.110:** Chemical facilities and covered facilities (energy and utilities, agriculture and food, healthcare)	**§ 27.210:** Complete Top-Screen, security vulnerability assessment, and site security plan every 2-3 years **§ 27.230:** Restrict area perimeter; secure site assets; screen and control access; detect, deter, and delay attacks; secure and monitor shipping, receipt, and storage; deter theft and diversion; deter sabotage; deter cyber sabotage; incident response; monitoring; training and exercises, personnel surety; elevated threat measures; address specific threat, vulnerabilities, and risks; report significant incidents; designate officials; and maintain records **§ 27.255:** Maintain records for 3 years **§ 27.400:** Protect and mark CVI classified information	$25K per day of violation
CIPA *Children's Internet Protection Act*	Federal	47 U.S.C. § 254	FCC		Schools that receive discounted Internet service	**§ 254(h)(5)(B):** (i) enforce a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are (I) obscene (II) child pornography or (III) harmful to minors; (ii) enforce the operation of such technology protection measure during any use of such computers by minors; and (iii) as part of its Internet safety policy is educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.	Loss of discounted Internet service rates
CJIS *Criminal Justice Information Systems*	Federal	28 C.F.R. Part 20	FBI		Collection of fingerprints and use of criminal history record information	**§ 20.21(f):** Access control; physical security; confidentiality; integrity; availability; log unauthorized attempts to access information; personnel security **From 2016 Audit:** third-party agreements with any agency shared CHRI; encryption of CHRI; secure disposal of CHRI to include observing destruction of it in person	Fine not to exceed $11K and may lose state funding and access to CHRI
COPPA *Children's Online Privacy Protection Rule*	Federal	16 C.F.R. Part 312	FTC		Online services that collect info about children under 13 years	**§ 312.3:** Notice on website of privacy policy; obtain parental consent; means for review of information and refusal to continue by parents; establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of child's information **§ 312.8:** Require reasonable security from third-parties who obtain the data **§ 312.10:** Only retain as long as needed; delete using measures to protect against unauthorized access to or use of information during the deletion process	$11K-$16K per violation

The Register: Systems Tab

The Register								
System Name	Information System Security Engineer	Security Control Assessor	Operational Status	Information System Type	Authorization Status	Authorization Date	System Categorization	Last Assessed Risk Level
System Name	Name: Title: Department: Location: Phone Number: Email:	Name: Title: Department: Location: Phone Number: Email:					Confidentiality: Integrity: Availability:	
System Name	Name: Title: Department: Location: Phone Number: Email:	Name: Title: Department: Location: Phone Number: Email:					Confidentiality: Integrity: Availability:	
System Name	Name: Title: Department: Location: Phone Number: Email:	Name: Title: Department: Location: Phone Number: Email:					Confidentiality: Integrity: Availability:	
System Name	Name: Title: Department: Location: Phone Number: Email:	Name: Title: Department: Location: Phone Number: Email:					Confidentiality: Integrity: Availability:	
System Name	Name: Title: Department: Location: Phone Number: Email:	Name: Title: Department: Location: Phone Number: Email:					Confidentiality: Integrity: Availability:	

The Register: Controls Tab

Control Number	Control Name	System 1	NIST SP 800-53 Control Baselines			NIST SP 800-66	NIST SP 800-171	CIS CSC SANS 20	CNSSI 1253F Privacy Overlay				CNSSI 1253 NSS Security Control Baselines								
									PII Confidentiality Impact Level				Confidentiality			Integrity			Availability		
			Low	Moderate	High	HIPAA	CUI/FERPA	CA Laws	Low	Moderate	High	PHI	Low	Moderate	High	Low	Moderate	High	Low	Moderate	High
AC-1	Access Control Policy and Procedures		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
AC-2	Account Management		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management			X	X									X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts			X	X									X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts			X	X									X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions			X	X								X	X	X	X	X	X			
AC-2(5)	Account Management | Inactivity Logout				X								X	X	X	X	X	X	X	X	X
AC-2(6)	Account Management | Dynamic Privilege Management																				
AC-2(7)	Account Management | Role-Based Schemes												X	X	X	X	X	X			
AC-2(8)	Account Management | Dynamic Account Creation									*Not Allowed*											
AC-2(9)	Account Management | Restrictions on Use of Shared / Group Accounts								X	X	X	X	X	X	X	X	X	X			
AC-2(10)	Account Management | Shared / Group Account Credential Termination												X	X	X	X	X	X			
AC-2(11)	Account Management | Usage Conditions				X										X			X			
AC-2(12)	Account Management | Account Monitoring / Atypical Usage				X								X	X	X	X	X	X			
AC-2(13)	Account Management | Disable Accounts for High-Risk Individuals				X				X	X	X	X	X	X	X	X	X	X			
AC-3	Access Enforcement		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
~~AC-3(1)~~	~~Access Enforcement | Restricted Access to Privileged Functions~~		*Withdrawn*			*Withdrawn*			*Withdrawn*				*Withdrawn*			*Withdrawn*			*Withdrawn*		
AC-3(2)	Access Enforcement | Dual Authorization																				
AC-3(3)	Access Enforcement | Mandatory Access Control																				
AC-3(4)	Access Enforcement | Discretionary Access Control												X	X	X	X	X	X			
AC-3(5)	Access Enforcement | Security-Relevant Information																				
~~AC-3(6)~~	~~Access Enforcement | Protection of User and System Information~~		*Withdrawn*			*Withdrawn*			*Withdrawn*				*Withdrawn*			*Withdrawn*			*Withdrawn*		
AC-3(7)	Access Enforcement | Role-Based Access Control																				
AC-3(8)	Access Enforcement | Revocation of Access Authorizations																				
AC-3(9)	Access Enforcement | Controlled Release									X	X	X									
AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms								X	X	X										
AC-4	Information Flow Enforcement			X	X	X	X	X		X	X	X		X	X		X	X			
AC-4(1)	Information Flow Enforcement | Object Security Attributes																				
AC-4(2)	Information Flow Enforcement | Processing Domains																				
AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control																				
AC-4(4)	Information Flow Enforcement | Content Check Encrypted Information																				
AC-4(5)	Information Flow Enforcement | Embedded Data Types																				
AC-4(6)	Information Flow Enforcement | Metadata																				
AC-4(7)	Information Flow Enforcement | One-Way Flow Mechanisms																				
AC-4(8)	Information Flow Enforcement | Security Policy Filters										X										
AC-4(9)	Information Flow Enforcement | Human Reviews																				
AC-4(10)	Information Flow Enforcement | Enable / Disable Security Policy Filters																				
AC-4(11)	Information Flow Enforcement | Configuration of Security Policy Filters																				
AC-4(12)	Information Flow Enforcement | Data Type Identifiers											X									
AC-4(13)	Information Flow Enforcement | Decomposition into Policy-Relevant Subcomponents																				

Review of Cybersecurity Law

Cybersecurity Law

- Laws and regulations exist to protect our rights and prevent unfair and deceptive practices
  - If you are non-compliant with the law, you are breaking it
- Strategic Questions
  - What cybersecurity laws must you comply with?
  - What is your exposure if you are non-compliant?
  - What organizations regulate/audit you?
  - How do you manage all of these requirements?

International Laws

- Two basic legal approaches
  - Common Law – U.S. and U.K.
  - Civil Law – Continental Europe
- E.U. General Data Protection Regulation (GDPR)
  - Applies to any E.U. citizen's PII
  - Applies to any websites accessible in E.U.

GDPR: €10,000,000 Finable Offenses

Information Security

Article 25: Data Protection by Design and by Default
Article 30: Records of Processing Activities *(security plans)*
Article 32: Security of Processing *(reasonable and appropriate)*
Article 33: Notification of a Personal Data Breach to the Supervisory Authority
Article 34: Communication of a Personal Data Breach to the Data Subject
Article 35: Data Protection Impact Assessment
Article 36: Prior Consultation *(for high risk systems)*
Article 39: Tasks of the Data Protection Officer

GDPR: €10,000,000 Finable Offenses (cont.)

Executive Leadership

- Article 27: Representatives of Controllers or Processors Not Established in the Union
- Article 31: Cooperation with the Supervisory Authority
- Article 37: Designation of the Data Protection Officer
- Article 38: Position of the Data Protection Officer

Legal Department

- Article 26: Joint Controllers *(third-party contracts)*
- Article 28: Processor *(specific contract language)*

Support Staff

- Article 8: Conditions Applicable to Child's Consent in Relation to Information Society Services
- Article 11: Processing Which Does Not Require Identification
- Article 29: Processing Under the Authority of the Controller or Processor

GDPR: €20,000,000 Finable Offenses

Information Security

- Article 44: General Principle for Transfers

Legal Department

- Article 12: Transparent Information, Communications and Modalities for the Exercise of the Rights of Data Subjects *(transparency)*

Support Staff

- Article 6: Lawfulness of Processing *(opt-in)*
- Article 7: Conditions for Consent
- Article 9: Processing of Special Categories of Personal Data *(opt-in)*
- Article 22: Automated Individual Decision-Making, Including Profiling
- Article 49: Derogations for Specific Situations

Federal Laws

- Two basic legal approaches
  - Laws primarily focused on cybersecurity
  - Laws focused on industry regulation with a security component
- Some laws apply to any organization conducting business
  - Discovery laws, trade laws, etc.
- Some apply to only certain categories of businesses
  - Operate across state lines, critical infrastructure, etc.

Federal Laws

Cybersecurity

- 42 CFR Part 2
- CFATS
- CIPA
- CJIS
- COPPA
- FDA 21 CFR Part 11
- FERPA
- FISMA
- HIPAA
- HITECH
- SEC Regulations S-P, S-AM, S-ID

Industry Regulation

- BSA
- CAN-SPAM
- Dodd-Frank
- EFTA
- FAA
- FACTA
- FCRA
- FCUA
- FDCPA
- FDIC
- FTC
- GLBA
- PAMA
- PPRA
- PREA
- SOX
- TCPA
- TILA

Business Regulation

- 4th Amendment to the U.S. Constitution
- ADA
- ADEA
- EPA
- ERISA
- FLSA
- FMLA
- FRCP
- GINA
- IRCA
- OSHA
- Title VII

Health Insurance Portability and Accountability Act

- Code: 45 C.F.R. Part 160
- Regulator: U.S. Department of Health and Human Services
- Scope: Health care providers
- Requirements: Reasonable administrative, technical, and physical safeguards; electronic signatures; policy and procedure; breach notification; privacy policy disclaimer; record access; (specific requirements outlined in law text)
- Penalties: $100 per violation not to exceed $25K; $50K-$250K and up to 10 years imprisonment for wrongful disclosure

Dodd-Frank (for now…)

- Code: Pub.L. 111-203, H.R. 4173
- Regulator: Consumer Financial Protection Bureau and the U.S. Securities and Exchange Commission
- Scope: Mortgage lenders, credit/debit card issuers, investment bankers
- Requirements: Prevent unfair, deceptive, and abusive practices, including misrepresentation of data security practices; develop, implement, and maintain a comprehensive written information security plan; property train employees and fix security flaws; annually obtain an independent data security program audit
- Penalties: Civil penalties not more than the greater of $1M or 3x the monetary gain to such person for each violation

State Breach Notification Laws

- Three basic legal approaches
  - Collecting personal information about citizens of the state
  - Conducting business within the state
  - No breach notification law
- In general, most organizations *probably* collect information about citizens from every state
- In general, most organizations that conduct business online *probably* conduct business within every state

State Breach Notification Laws

Collecting PII about citizens

- Alaska
- Arkansas
- California
- Florida
- Georgia
- Hawaii
- Illinois
- Indiana
- Iowa
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Missouri
- Nebraska
- Nevada
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- District of Columbia
- Guam
- Puerto Rico
- U.S. Virgin Islands

Conducting business in state

- Arizona
- Colorado
- Connecticut
- Delaware
- Idaho
- Kansas
- Minnesota
- Mississippi
- Montana
- New Hampshire
- New Jersey
- South Carolina
- Wyoming

No breach notification law

- Alabama
- South Dakota
- American Samoa
- Northern Mariana Islands

California

- Most progressive state in terms of cybersecurity laws
  - While most states have breach notification, California has at least 30 laws that have cybersecurity requirements
- California Data Breach Report, Feb. 2016
  - "Recommendation 1: The 20 controls in the CIS Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security." *-California Attorney General Kamala D. Harris*

Honorable Mentions

- Massachusetts *"Standards for the Protection of Personal Information of Residents of the Commonwealth"* outlines specific controls to implement
- Nevada *"Security of Personal Information"* requires compliance with PCI-DSS for all payment card transactions
- Rhode Island *"Identity Theft Protection Act of 2015"* requires a risk-based information security program

Industry Regulations

- Mandatory Regulations
  - Required by third-parties and contractual obligation
  - Ex., credit card processors require PCI-DSS compliance
- Voluntary Regulations
  - Provide competitive advantage through assurance
  - Ex., Good Housekeeping Seal of Approval

The Joint Commission Standards

- Regulator: The Joint Commission
- Scope: Accredited health care organizations
- Requirements: Information management; continuity of information management; protect privacy of health information; maintain security and integrity of health information; effectively manage the collection of health information; knowledge-based information resources are available, current, and authoritative
- Penalties: Loss of accreditation

North American Electric Reliability Corporation Standards

- Regulator: North American Electric Reliability Corporation
- Scope: Power production on public grids
- Requirements: Critical cyber asset identification; security management controls; personnel training; electronic security perimeters; physical security; systems security management; incident response; disaster recovery
- Penalties: $1M per violation per day

Payment Card Industry Data Security Standard

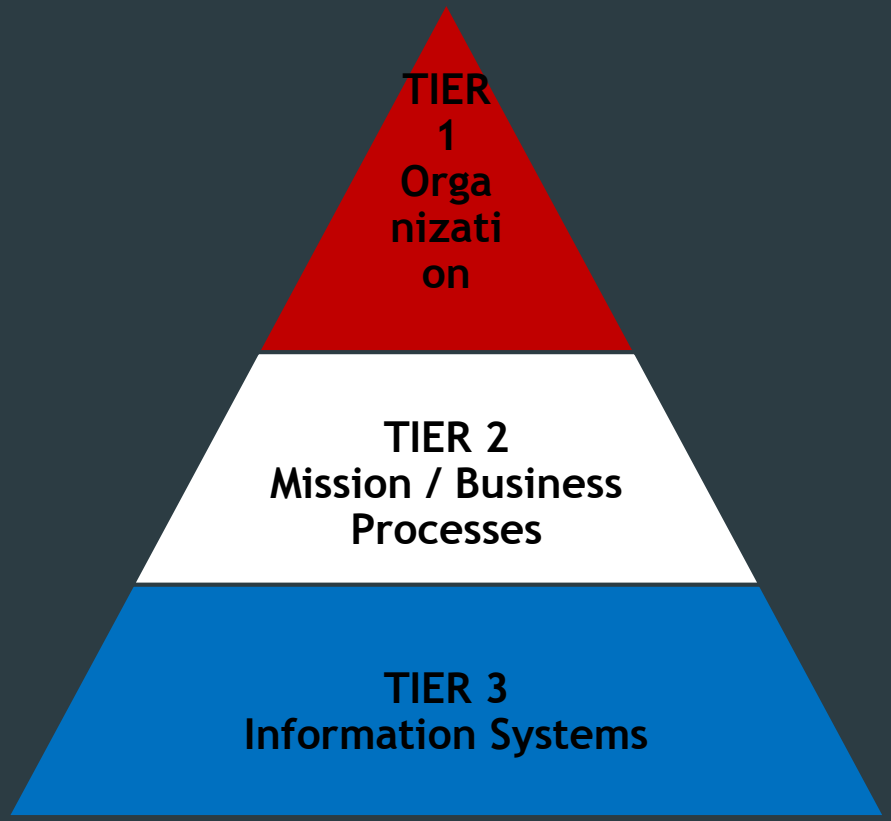
- Regulator: Payment Card Industry Security Standards Council
- Scope: Accepting payment cards from American Express, Discover, JCB, MasterCard, or Visa
- Requirements: Firewall; no default passwords; protect data-at-rest and data-in-transit; antivirus; develop secure systems and applications; access control need-to-know; unique user IDs; restrict physical access; monitor network access; test security systems/processes; maintain information security policy
- Penalties: $50-$90 per cardholder data breached; $5K-$100K per month of breach; loss of ability to accept PCI-sponsored credit cards

Integration with the Risk Management Framework

Risk-Based Security Program

- Risk-based information security program
  - Compliance ≠ Security
  - Reasonable and appropriate
  - Considers cost-benefit but not primary motivation
- Risk Management Framework
  - Mandated by Federal Information Security Management Act (FISMA)
  - Satisfies many federal, state, and industry requirements
  - National standards maintained by NIST under the Department of Commerce

Risk Management Framework



- Cost-effective, risk-based decision making
- Continuous monitoring of information system risk
- Strategic, operational, and tactical risk management
- Standardized process for assessing risk across information systems and operational lines of business
- Tailorable to any industry and regulatory environment

Security Maturity

- No Program
- No Policy
- Unknown Risk

- Reactive

- Federal Law
- State Law
- Industry Regulation

- Proactive

- Awareness
- Participation
- Managed Risk

Questions?