



Data Privacy Compliance

Corporate & Regulatory Compliance Boot Camp

Lauren Silvestri Burke
Daniel Cotter
Kyle Miller

Meet the Faculty

Panelists

[Lauren Silvestri Burke](#) - Morgan, Lewis & Bockius LLP

[Kyle Miller](#) – Dentons

Moderator

[Daniel Cotter](#) - Dickinson Wright



Practical & Entertaining Education for:

- Attorneys • Accountants
- Business Owners
- Executives • Investors

Thank you to our co-producer

THE NATIONAL LAW REVIEW

The National Law Review (NLR) is a premier legal news website offering in-depth analysis on a wide range of legal and business topics. Established in 1888, NLR has evolved into a **trusted resource** for legal professionals, business leaders, and the general public, providing timely and relevant information on legislative changes, court decisions, and regulatory developments

Visit *The National Law Review* to learn more
- <https://natlawreview.com/>

Comprehensive Coverage: NLR covers nearly every legal topic, including litigation, AI & the Law, employment law, IP Law, real estate, energy, health care, bankruptcy and much more.

Expert Analysis: Articles are authored by experienced attorneys and legal professionals, ensuring accurate and insightful commentary.

Daily Updates: NLR provides hourly legal news updates, keeping readers informed about the latest developments in the legal world.

Disclaimer

- The material in this webinar is for informational purposes only. It should not be considered legal, financial, or other professional advice.
 - You should consult with an attorney & another appropriate professional to determine what may be best for the needs of your specific situation.
 - While the webinar producers & speakers take reasonable steps to ensure that the information presented is accurate, they make no guarantee in this (or any) regard.

*** These slides were produced in connection with a video webinar that premiered on 7/02/2025. Take note, we make the PDF available for free download because the real benefit of a Financial Poise webinar is the conversation that the faculty has around the slide deck. You can access the webinar on-demand at Cerfi's LegalEdge (f/k/a [West Legal Ed Center](#)) (for attorneys or accountants seeking CLE or CPE) or [Financial Poise](#) (for everyone else).

About This Webinar

Data Privacy Compliance

All levels of society rely upon information technology systems. Network operations are pervasive and impact nearly every aspect of our society. The desire of companies to collect, use, store, and secure information about customers, employees, and other individuals is a requirement of the new economy. It is no wonder that the prevalence of electronic communications and a growing dependency on cyber structures and operations also create potential vulnerabilities to cyberattacks. It is critical to preserve information systems and address and prevent weaknesses in cyber protection efforts.

This webinar examines the means for companies to reach data goals ethically, efficiently, and legally. The panel will also discuss the evolving regulatory approaches of the European Union, United States Federal government, and significant developments in U.S. state regimes, including California. The best practices and models of comprehensive privacy and cybersecurity policies will also be discussed. And, data breach response and related litigation, including class action litigation issues, and fiduciary duty violations under corporate law, are discussed.

About This Series

Corporate & Regulatory Compliance Bootcamp

This webinar series covers corporate and regulatory compliance as it relates to procurement, government contracting, the Foreign Corrupt Practices Act, data privacy, and social media. The various episodes examine these topics from a company's perspective, delving into compliance issues that pertain to specific company practices across industries and borders and impact companies of all sizes and types.

As with every Financial Poise Webinar, each episode is delivered in plain English so that you do not have to be a Business Law specialist to understand and benefit from them. And, as with every Financial Poise Webinar, each episode brings you into engaging, sometimes humorous, conversations designed to entertain as it teaches. Each episode in the series is designed to be viewed independently of the other episodes so that participants will enhance their knowledge of this area whether they attend one, some, or all episodes.

Episodes In This Series

#1 Overview of General Corporate Law Compliance

Premiere Date: 3/26/2025

#2 Procurement & Government Contracting Compliance

Premiere Date: 5/28/2025

#3 Foreign Corrupt Practices Act Compliance

Premiere Date: 6/11/2025

#4 Data Privacy Compliance

Premiere Date: 7/2/2025

#5 Internal Investigations - 101

Premiere Date: 8/6/2025

#6 Securities Law Compliance

Premiere Date: 9/10/2025

#7 Executive Compensation

Premiere Date: 10/8/2025

Episode #4

Data Privacy Compliance

Each Financial Poise Webinar is delivered in Plain English, understandable to investors, business owners, & executives without much background in these areas, yet is of primary value to attorneys, accountants, & other seasoned professionals. Each episode brings you into engaging, sometimes humorous, conversations designed to entertain as it teaches. Each episode in the series is designed to be viewed independently of the other episodes so that participants will enhance their knowledge of this area whether they attend one, some, or all episodes.

What Data Should We Be Concerned About?

- Challenge = Identifying Information That Is Held To A Higher Standard Of Care
- Information protected by law (i.e. personally identifiable or protected health information)
 - Example statutes: State privacy laws, Federal Trade Commission Act, HIPAA/HITECH, Gramm-Leach Bliley, etc.
- Information required to be kept confidential by contract
 - Examples: Information subject to non-disclosure agreements including Merchant Service Agreements (Payment Card Information)
- Corporate confidential information
 - Examples: trade secrets, confidential customer lists, etc.

Legal Landscape

- 48 out of 50 states have breach notification laws, no two are the same
- Each has a different definition of Personally Identifiable Information (PII) can vary from state to state (what is considered a breach in one state is not always one in another)
- Transfer of data to a third party does not constitute a shift in responsibility
- The laws that apply are by residency of the affected persons, not the residency of the affected organization
- Federal Laws (i.e. HIPAA, FCRA, Gramm Leach Bliley, etc.) impose data security requirements and allow for regulatory action to be brought
- Contracts also pose exposure problems (Merchant Service and Non-Disclosure Agreements – patents are not covered)

What are the Threats?

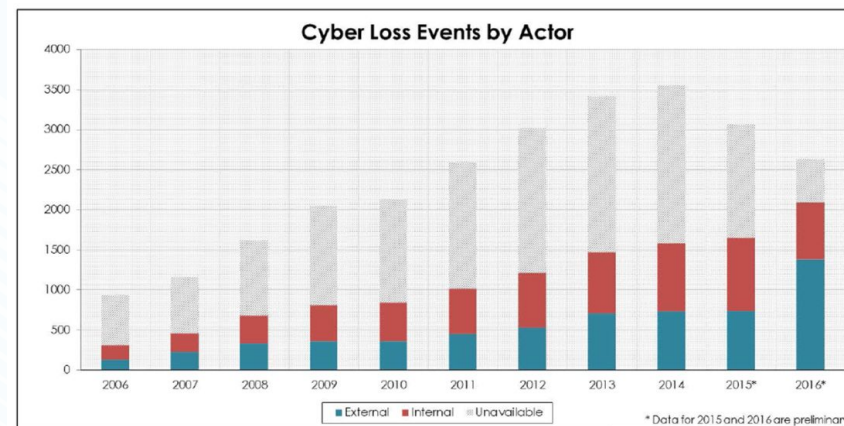
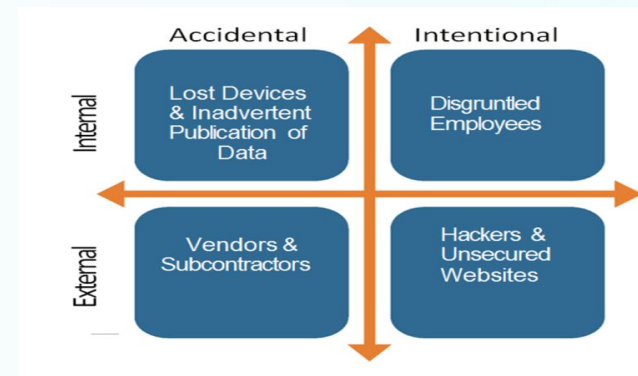
- Challenge = Maintaining Policies That Tackle Both Internal and External Threats

- External Causes of Loss

- Hackers
- Viruses
- Social Media
- Third Party Vendors
- A Changing Regulatory Environment

- Internal Causes of Loss

- Rogue/Disgruntled Employees
- Human Error
- Mobile Devices
- Insufficient Physical Security



What Types of Information and Data do All Companies Need to Protect?

- Personally identifiable information (PII): information that can be linked to a specific individual
 - Includes name, birthdate, social security number, driver's license number, account numbers
- Non-personally identifiable information: cannot by itself be used to identify a specific individual
 - Aggregate data, zip code, area code, city, state, gender, age
- Gray area – “anonymized data”
 - Non-PII that, when linked with other data, can effectively identify a person
 - Includes geolocation data, site history, and viewing patterns from IP addresses

What Data Must be Protected?

- Personally Identifiable Information (PII)
 - Social Security number
 - Drivers license number
 - Credit/debit card numbers
 - Passport number
 - Bank Account Information
 - Date of Birth
 - Medical Information
 - Mother's maiden name
 - Biometric data (i.e., fingerprint)
 - E-mail/username in combination with password/security question & answer

What Data Must be Protected?

(cont'd)

- Payment Card Information (PCI)
 - Primary Account Number (PAN)
 - Cardholder Name
 - Expiration Date
 - Service Code (3 or 4 digit code)
 - PIN

What Data Must be Protected?

(cont'd)

- Business Information:
 - Customer lists
 - Prospect lists
 - Trade secrets
 - Pricing information
 - Business plans and strategies
 - Employee lists

Global Regulatory Environment Changes

NYDFS 23 NYCCR500

The New York State Department of Financial Services established a set of cybersecurity requirements for financial services companies who are supervised by the NYDFS to address the heightened risk of cyber attacks by nation-states, terrorist organizations, and independent criminal actors.

FFIEC CAT

The FFIEC updated the Cyber Assessment Tool and IT Examination Handbook was on May 31st of 2017. Changes to the assessment and maturity scoring will affect any organization utilizing the methodology.

GLBA

There are multiple pending changes to GLBA from multiple government agencies and the NAIC. As well, the current administration has identified this regulation as an area of interest.

PCI DSS 3.2

PCI DSS 3.1 was retired in October of 2016 with the 3.2 version, introduced in May of 2017, officially taking over as best practices. Version 3.2 will become required in February of 2018.

CCPA

The **California Consumer Privacy Act of 2018** (CCPA) gives consumers more control over the personal information that businesses collect about them. This landmark law secures new privacy rights for California consumers, including: The **right to know** about the personal information a business collects about them and how it is used and shared; The **right to delete** personal information collected from them (with some exceptions); The **right to opt-out** of the sale of their personal information; and **The right to non-discrimination** for exercising their CCPA rights.

GDPR

EU General Data Protection Regulation - The EU is updating their 1995 Data Protection Directive with the GDPR who's final form will be enforceable May 25th 2018. This regulation will require an review of how information is collection and stored for any company doing business in the EU.

- **NAIC Cybersecurity Model Law**
- **FED, FDIC, OCC Enhanced Cyber Risk Management Standards**
- **FFIEC Additional Rules**

What's next?

How is Privacy Protected?

Two Predominant Approaches: Europe versus United States

U.S. Conflict, Security, and Civil Liberties

- Pew Research Center surveys since the 9/11 terrorist attacks have generally shown that in the periods when high-profile cases related to privacy vs. security first arise, majorities of adults favor a “security first” approach to these issues, while at the same time urging that dramatic sacrifices on civil liberties be avoided. New incidents often result in Americans backing at least some extra steps by the law enforcement and intelligence communities to investigate terrorist suspects, even if that might infringe on the privacy of citizens. But many draw the line at deep interventions into their personal lives.
- Lee Rainie and Shiva Maniam, Americans feel the tensions between privacy and security concerns, Pew Research Center Fact Tank, February 19, 2016

<http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/>

U.S. Consumer Privacy Concerns

- As businesses increasingly mine data about consumers, Americans are concerned about preserving their privacy when it comes to their personal information and behaviors. Those views have intensified in recent years, especially after big data breaches at companies such as Target, eBay and Anthem as well as of federal employee personnel files. Our surveys show that people now are more anxious about the security of their personal data and are more aware that greater and greater volumes of data are being collected about them. The vast majority feel they have lost control of their personal data, and this has spawned considerable anxiety. They are not very confident that companies collecting their information will keep it secure.
- Lee Rainie and Shiva Maniam, Americans feel the tensions between privacy and security concerns, Pew Research Center Fact Tank, February 19, 2016

<http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/>

"The privacy protections we see reflected in modern European law are a response to the Gestapo and the Stasi," Professor Cate said, referring to the reviled Nazi and East German secret police — totalitarian regimes that used informers, surveillance and blackmail to maintain their power, creating a web of anxiety and betrayal that permeated those societies. "We haven't really lived through that in the United States," he said.

Adam Liptak, When American and European Ideas of Privacy Collide,
New York Times
(Feb. 20, 2010).

What Laws Apply to your Company?

- Companies can have multiple privacy laws and regulations apply to them based on industry and the type of information sought to be protected.
- Information must also be protected because it has value to the company either because it is proprietary or because it is confidential information.
- Some information must be protected because it implicates the antitrust laws, such as pricing.

Privacy and Data Protection Laws

- EU Data Protection Directive,
- HIPAA or the Health Insurance Portability and Accountability Act,
- The Sarbanes Oxley Act,
- Federal Information Security Management Act of 2002 (FISMA),
- Family Educational Rights and Privacy Act (FERPA),
- Gramm Leach Bliley Act (GLBA),
- Payment Card Industry Data Security Standard (PCI-DSS),
- Proposed State Laws (NY).

U.S. Legal Framework

- Variety of industry specific laws, usually Federal laws
- State laws (newer development)
- Self-regulation



Federal Privacy and Data Protection Laws

- HIPAA or the Health Insurance Portability and Accountability Act,
- The Sarbanes Oxley Act,
- Federal Information Security Management Act of 2002 (FISMA),
- Family Educational Rights and Privacy Act (FERPA),
- Gramm Leach Bliley Act (GLBA), and
- Payment Card Industry Data Security Standard (PCI-DSS).

Financial

Sarbanes Oxley SOX

- Sarbanes Oxley was established in the wake of the ENRON collapse to prevent corporate fraud.
- SOX only applies to public companies, but there are many private companies which incorporate SOX principles as best practices and many states which have incorporated SOX principles into state law.
- As far as privacy is concerned, there is a requirement to preserve and maintain financial records for seven years.

Gramm Leach Bliley Act

- GLBA allowed insurance companies, commercial banks, and investment banks to be within the same company.
- Financial Institutions have to secure the private information of clients and customers.
- Financial Institutions are defined as companies that offer financial products or services to individuals. Products or services include loans, financial or investment advice, or insurance.

Cybersecurity Requirements for Financial Services Companies

NEW YORK STATE

DEPARTMENT OF FINANCIAL SERVICES
PROPOSED 23 NYCRR 500

New York State Department of Financial Services

What is Proposed 23 NYCRR 500?

- The regulation requires banks, insurance companies, and other financial services institutions regulated by the State Department of Financial Services to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State's financial services industry.
- Designed by New York State Department of Financial Services ("DFS") to promote the protection of customer information as well as the information technology systems of entities regulated by the DFS in light of ever-increasing threat of cyber attacks.

The Cybersecurity Requirements for Financial Services Companies

- Requires assessment of specific risk profile and design of program addressing risks, for which senior management is responsible including annual certification of compliance.
- All covered entities must move quickly – effective date 1/1/17, with 180 day transition period.



Who Does it Apply to?

- Contains a very broad definition of “Covered Entity”:
 - “Any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law.”
- Limited exception to total compliance applies only where:
 1. Fewer than 1000 customers in each of the last three calendar years, and
 2. Less than \$5,000,000 in gross annual revenue in each of the last three fiscal years, and
 3. Less than \$10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, shall be exempt from the requirements of this Part other than the requirements set forth in this section, Sections 500.02, 500.03, 500.07, 500.09, 500.11, 500.13, 500.17, 500.19, 500.20 and 500.21.

What do the Regulations Require? A Lot

1. Establishment of a cybersecurity program
2. Creation and implementation of written cybersecurity policy
3. Designation of a Chief Information Security Officer (“CISO”), Retention of cybersecurity personnel and internal training of all personnel
4. Penetration testing, vulnerability assessments, audit trail, and annual risk assessments
5. Access privileges, application security, multi-factor authentication and encryption
6. Written policies regarding third party information security guidelines
7. Creation of written incident response plan
8. Various notices to the Superintendent regarding cybersecurity events and compliance

The Cybersecurity Program

- Covered Entities shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of its information systems by performing the following functions:
 - Identify internal and external cyber risks by, at a minimum, identifying the Nonpublic Information stored on the Covered Entity's Information Systems, the sensitivity of such Nonpublic Information, and how and by whom such Nonpublic Information may be accessed;
 - Use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;
 - Detect Cybersecurity Events;
 - Respond to identified or detected Cybersecurity Events to mitigate any negative effects;
 - Recover from Cybersecurity Events and restore normal operations and services; and
 - Fulfill all regulatory reporting obligations.

The Cybersecurity Policy

- There must be a written cybersecurity policy setting forth policies and procedures for the protection nonpublic information addressing, at a minimum, the following:
 - Information security;
 - Data governance and classification;
 - Access controls and identity management;
 - Business continuity and disaster recovery planning and resources;
 - Capacity and performance planning;
 - Systems operations and availability concerns;
 - Systems and network security;

The Cybersecurity Policy (cont'd)

- Systems and network monitoring;
- Systems and application development and quality assurance;
- Physical security and environmental controls;
- Customer data privacy;
- Vendor and third-party service provider management;
- Risk assessment; and
- Incident response.

The cybersecurity policy must be reviewed by the Covered Entity's board of directors and approved by a senior officer of the Covered Entity, on at least an annual basis.

Chief Information Security Officer

- Each Covered Entity must designate a qualified individual to serve as the Chief Information Security Officer (“CISO”) responsible for overseeing and implementing the cybersecurity program and enforcing its cybersecurity policy.
- The CISO of each Covered Entity shall develop a report, at least bi-annually, for presentation to the board of directors or equivalent governing body, or, if none, to the senior officer responsible for the cybersecurity program:
 - Assess the confidentiality, integrity and availability of the Covered Entity’s Information Systems;
 - Detail exceptions to the Covered Entity’s cybersecurity policies and procedures;
 - Identify cyber risks to the Covered Entity;
 - Assess the effectiveness of the Covered Entity’s cybersecurity program;
 - Propose steps to remediate any inadequacies identified therein; and
 - Include a summary of all material Cybersecurity Events that affected the Covered Entity during the time period addressed by the report.

Cybersecurity Personnel and Intelligence

- In addition to a CISO, a covered entity must:
 1. Employ cybersecurity personnel (who may be qualified third party) sufficient to manage cybersecurity risks and perform core cybersecurity functions specified in the regulation;
 2. Provide for and require all cybersecurity personnel to attend regular cybersecurity update and training sessions; and
 3. Require key cybersecurity personnel to take steps to stay abreast of changing cybersecurity threats and countermeasures.

- Training and Monitoring:
 1. Implement risk-based policies, procedures and controls to monitor activity of Authorized Users and detect unauthorized access or use of, or tampering with, nonpublic information by such users; and
 2. Provide for and require all personnel to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified annual assessment of risks.

Penetration Testing and Vulnerability Assessments

- The cybersecurity program for each Covered Entity shall, at a minimum, include:
 - Penetration testing of the Covered Entity's Information Systems at least annually; and
 - Vulnerability assessment of the Covered Entity's Information Systems at least quarterly.
- Application Security
 - Cybersecurity program shall, at a minimum, include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications, as well as procedures for assessing and testing the security of all externally developed applications utilized by the Covered Entity.
 - These procedures, guidelines and standards shall be reviewed, assessed and updated by the CISO of the Covered Entity at least annually.

Audit Trail

- The cybersecurity program must implement and maintain audit trail systems that:
 - Track and maintain data for reconstruction of all financial transactions and accounting necessary to detect and respond to a Cybersecurity Event;
 - Track and maintain data logging of all access to critical systems;
 - Protect integrity of data stored and maintained as part of any audit trail from alteration or tampering;
 - Protect integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware;
 - Log system events including access and alterations made to audit trail systems, and all system administrator functions performed on the systems; and
 - Maintain records produced as part of the audit trail for not fewer than six years.

Audit Trail *(cont'd)*

Risk Assessment.

- At least annually, each Covered Entity shall conduct a risk assessment of information systems, which must be documented in writing:
 - Criteria for the evaluation and categorization of identified risks;
 - Criteria for the assessment of the confidentiality, integrity and availability of the Covered Entity's Information Systems, including the adequacy of existing controls in the context of identified risks; and
 - Requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks.

Multi-Factor Authentication and Encryption of Nonpublic Information

- Multiple-factor authentication will be required for:
 - Any individual accessing the Covered Entity's internal systems or data from an external network;
 - Privileged access to database servers that allow access to Nonpublic Information; and
 - Access to web applications that capture, display or interface with Nonpublic Information.
- Encryption of all nonpublic information, whether held or transmitted, and both in transit and at rest.
- There are grace periods to the extent that encryption is currently infeasible for a covered entity:
 - For information in transit, alternative controls are permissible for one year after the effective date; and
 - For information at rest, alternative controls are permissible for five years after the effective date.

Third Party Information Security Policy

- The proposed regulation also affects dealings with third parties, requiring implementation of written policies and procedures designed to ensure the security of systems and nonpublic information that are accessible to, or held by, third parties that address:
 - Identification and risk assessment of third parties with access to such systems or information;
 - Minimum cybersecurity practices required to be met by such third parties in order for them to do business with the covered entity;
 - Due diligence processes used to evaluate the adequacy of cybersecurity practices of such third parties; and
 - Periodic assessment, at least annually, of such third parties and the continued adequacy of their cybersecurity practices.
 - These policies and procedures must also establish preferred provisions to be included in contracts with third party service providers.

Incident Response Plan

- A cybersecurity program requires the creation of a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event affecting the confidentiality, integrity, or availability of the covered entity's information systems or the continuing functionality of any aspect of the business, and must address:
 - Internal processes for responding to a cybersecurity event;
 - Goals of the incident response plan;
 - Definition of clear roles, responsibilities and levels of decision-making authority;
 - External and internal communications and information sharing;
 - Remediation of any identified weaknesses in information systems and associated controls;
 - Documentation and reporting regarding cybersecurity events and related incident response activities; and
 - The evaluation and revision of the incident response plan following a cybersecurity event.

Written Information Security Program

- Some state and federal laws already have broad requirements in place for protection of personal and other sensitive information (i.e., Massachusetts's Data Security Regulation, Oregon's Identity Theft Protection Act, GLBA Safeguards Rule).
- Companies must draft and implement a written information security program in compliance with these laws, taking into consideration:
 - The size, scope, and type of its business or other activities;
 - Its information collection and use practices, including the amount and types of personal and other sensitive information it maintains; and
 - The need to secure both customer and employee personal information.

Written Information Security Program *(cont'd)*

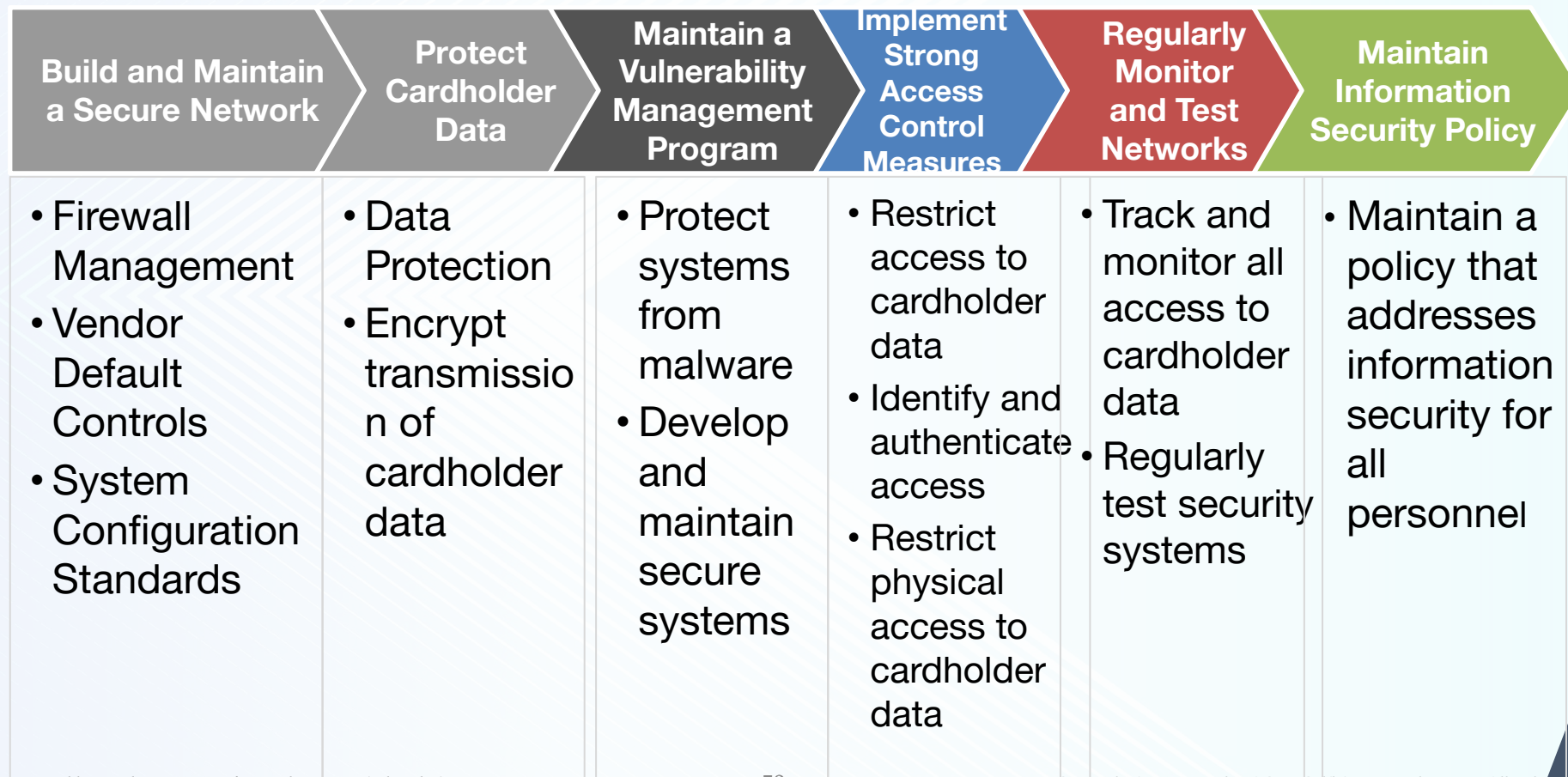
- Specific applicable legal requirements, which may depend on, among other things:
 - the nature and industry of the business or organization;
 - the type of information collected and maintained;
 - the geographic footprint of the business, including the states where the organization's customers and employees reside; and
 - the resources available to implement and maintain an information security program.

Retail

Payment Card Industry Data Security Standard PCI-DSS, “Self-Regulation Industry”

Introduction to PCI

PCI Data Security Standard



Payment Card Industry Data Security Standard PCI-DSS

- 17 standards (industry self regulation).
 - Designed to reduce fraud and
 - Protect customer credit card information.

- Applies to all companies that handle credit card information.



History

- The credit card industry has taken steps to protect personal information and the credit card process.
- In 2004, VISA and MasterCard created the PCI-DSS industry security requirements.
- In 2006, American Express, Discover, JCB, MasterCard and VISA formed the Payment Card Industry Security Standards Council to manage the PCI-DSS.

Parties Involved

- Payment Brands: Processing Organizations (MasterCard, VISA, American Express, etc.) that license members and merchants to accept and issue credit cards.
- Issuers: Financial institutions that credit cards to cardholders (Chase, CitiBank, Bank of America).
- Acquirers: Financial institutions that provide services for processing payment card transactions, accepts credit card transactions from the merchant.
- Merchants: Business owners, agencies, governments, authorized to accept credit card payments.
- Service Providers: Organizations that process, transmit, or STORE cardholder data for merchants, members, or service providers. (PayPal).

PCI-SCC Standards

- The PCI Data Security Standard (PCI-DSS) - A set of twelve requirements designed to build a strong payment security foundation.
- The Payment Application Data Security Standard (PA-DSS) which establishes protocols and a testing procedure for software running on point of sale devices and electronic shopping carts.
- The PIN Transaction Security Standard (PTS) which defines the physical and logical security of devices involved in credit card transactions through swiping, pin entry devices, and payment terminals (unattended terminals like gas stations and parking facilities).

PCI-SCC Standards *cont'd*

- Does not oversee compliance. Each credit card company has its own internal compliance requirements.
- Trains and organizes PCI data assessors (PCI data security assessments or scanning).
- Tests and approves Scanning Vendors that are part of the compliance requirements for some merchants,
- Tests and maintains approved software and hardware for securely conducting payment transactions.
- Maintains PCI-SCC issued documents which are updated frequently on their website. <https://www.pcisecuritystandards.org/>

Payment Card Industry Data Security Standard PCI-DSS

- PCI-DSS - Global data security standard that governs any business that accepts payment cards and stores, processes, or transmits cardholder data.
- Priorities:
 - Protects cardholder payment data and increases consumer confidence
 - Mirrors best security practices for the protection of sensitive information
 - Twelve basic steps for protecting credit card information
 - Applies to internally developed applications that are not sold to a third party.

Payment Application Data Security Standard PA-DSS

- Standard for vendors (software and others) to reduce vulnerabilities.
- Standards for point of sale software, e-commerce, and kiosks.
- Applies to payment applications that are sold, distributed, or licensed to third parties.
- Certified payment applications can be found at:
www.pcisecuritystandards.org/assessors

Pin Transaction Security/Pin Entry Device Security PED PCI-PED



Financial Poise
Webinars

- Applies to companies that make devices that accept personal identification numbers (PINs) or swipe machines.
- Sets the standard for acceptable devices.
- Approved devices can be found at:
<https://www.pcisecuritystandards.org/assessors>

Best Practices

- Understand where payment data goes during the entire transaction.
- Verify that payment card terminals comply with the PCI PIN standards.
- Verify payment applications comply with the PA-DSS standards.
- If you retain cardholder data for legitimate business needs ensure:
 - The retention is authorized, and,
 - The data is protected (use appropriate cryptography and layered security technologies).
- Ensure that third parties who process payments comply with PCI-DSS, PA-DSS, or PCI-PED.
- Create access and password protection policies.

Best Practices *(cont'd)*

- DO NOT, store cardholder data unless absolutely necessary and never store authentication data from the payment card's storage chip or magnetic stripe or the validation code.
- Personally identifiable information should not be printed by PED terminals and printouts should be truncated or masked.
- Secure access to stored cardholder data:
- Payment card information cannot be stored on PCs, laptops, smart phones or other unprotected endpoint devices.
- Secure servers or other card system storage devices in locked, fully secured and access controlled rooms.
- More detailed information can be found at:
https://www.pcisecuritystandards.org/document_library?association=PCI-DSS

Restrictions on PCI Data Storage

- Cardholder Data CAN be stored IF the following are protected:
 - Primary Account Number
 - Cardholder Name
 - Service Code
 - Expiration Date
- Any data stored in conjunction with a primary account number might also implicate a variety of laws related to consumer personal data, privacy, identity theft and data protection.

Restrictions on PCI Data Storage *(cont'd)*

- Sensitive Authentication Data CANNOT be stored even if encrypted.
- Sensitive Authentication Data includes:
 - Full magnetic stripe data
 - CAV2/CVC2/CVV2/CID
 - PIN/PIN Block
- More specifics on data storage can be found at:
https://www.pcisecuritystandards.org/pdfs/pci_fs

Consequences of a Credit Card Breach

- Lose the ability to process cards
- Increase in compliance measures such as scanning your system
- Damage to other stakeholders
- Extreme damage to public reputation.
- Fines and fees.

PCI-SSC Fines and Fees

- Fines and fees increase based on:
 - Number of stolen credit card numbers;
 - if magnetic stripe data was stored;
 - Whether the incident was immediately reported ; and
 - Other circumstances regarding the incident.

- Fines can also come from each credit card company.
- Breach mitigation costs can be imposed on the company.
- Forensic investigations can be charged to the company.
- Annual on-site security audits can be imposed.

EMV Chip

- 2015 migration from magstripe or swipe to EMV/Chip payments
- Main fraud protection comes from the point of sale.
- Changes the way card fraud is detected and prevented but DOES NOT replace PCI complaisance.
- EMV helps to prevent counterfeit cards.
- EMV makes it more difficult to use stolen card data.

EMV Chip *(cont'd)*

- EMV IS NOT ENCRYPTION so the Primary Account Number is still subject to PCI guidelines.
- EMV does not help with e-commerce.
- One rather unfortunate circumstance is that once EMV takes hold there will be a shift of activity in fraud to e-commerce.
- Exactly that type of shift occurred in Europe when the transition occurred.
- THIS MEANS EVERYONE SHOULD TAKE EXTRA PRECAUTIONS
 - Review your payment acceptance methods.
 - Review the security of any web applications.

Healthcare

Health Insurance Portability and Accountability Act HIPAA

- HIPAA has two parts:
 - Title I protects people who are transitioning between jobs or are laid off.
 - Title II both shifts healthcare from paper to electronic data and protects the privacy of patients
- Companies affected by HIPAA include those in the healthcare industry as well as all employers.

Background

- Security Rule General Requirements:
 - Ensure confidentiality, integrity, and availability of all electronic protected health information (PHI) the covered entity creates, receives, maintains, or transmits
 - Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
 - Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
 - Ensure compliance by its workforce
- Compliance Date – The Final Rule was published on February 20, 2003 and became enforceable on April 21, 2005.

Latest Developments

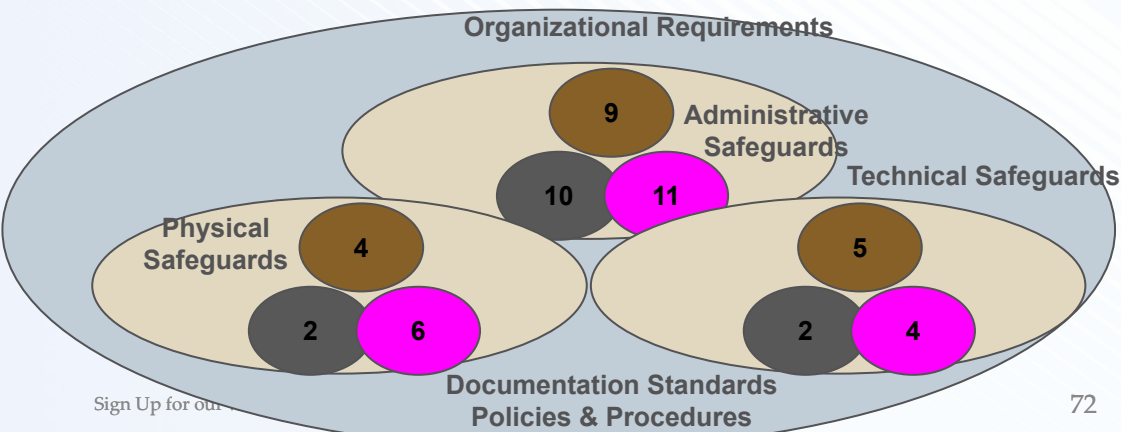
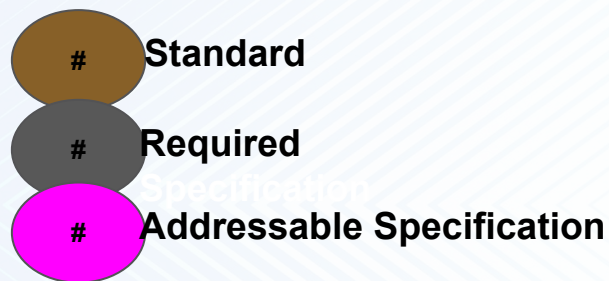
- NIST has updated SP 800-66 – this is a core implementation guidance document which may provide deeper insight for emerging security issues – and released this as 800-66 Rev1 in October 2008
- CMS continues to issues guidance documents (e.g. remote access guidance) – these should be considered for compliance as they may become part/parcel of future audits
- The landscape will continue to evolve, especially with emerging issues and State Laws regarding data breaches (e.g. expansion of CA SB 1386) and encryption of customer non-public information (MA, NV, etc) – this places even more emphasis on the risk assessment process and overall security program integration.

Regulation Components

- Standards: what must be met
- Implementation specifications: how to meet it
 - Required: **must be implemented**
 - Addressable:
 - Assess if reasonable
 - If reasonable – implement
 - If not reasonable –
 - ✓ Document
 - ✓ Implement alternate that meets standard

Required vs. Addressable Specifications

Count & Regulation Type



HIPAA Security Standards Matrix		
Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Recovery Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written contract of Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

HIPAA Solutions

Assess

- **Risk Analysis:** Assess reasonably anticipated threats and vulnerabilities to your ePHI assets, evaluate the sufficiency of current controls, determine the likelihood and impact to help calculate your significant risk areas, determine key areas of strategic focus, and recommend feasible solution alternatives.
- **Gap Evaluation:** Compare current business practices to HIPAA Privacy/Security/Breach regulations in order to identify and prioritize discrepancies, and recommend solution alternatives that are aligned with your strategic goals.
- **Security Management:** Create end-to-end security functions including enterprise security mission, vision, scope, and organizational structure.
- **Policies & Procedures:** Help ensure business risks are effectively documented, managed, and communicated.
- **Penetration Testing and Vulnerability Assessments:** Implement comprehensive security testing methodologies and techniques.

HIPAA Solutions *(cont'd)*

Respond

- **Security Monitoring:** Measure ongoing compliance of the organization through performance metrics, enterprise reporting, and internal audit.
- **Compliance Audit:** Compare revised business practices to HIPAA regulations in order to identify residual gaps.
- **Intrusion Detection:** Design and deployment of knowledge-based or behavior-based IDS.
- **Identity Management:** Coordinate and implement authentication of user accounts.
- **Virus Management:** Define preventative measures to ensure the integrity and availability of data.

Major Areas/Efforts

- Risk Assessment/Analysis
- Develop and Document Policies & Procedures
- Develop and implement security awareness training
- Minimum baseline standards
- Security Testing
- Security patch management
- Monitoring and compliance program
- Audit and Logging of Access
- Managing Business Partner Risks (BA agreements and Due Diligence)

More Information

- CMS HIPAA Website –
<http://www.cms.hhs.gov/HIPAAGenInfo/>
- DHHS OIG Audit of CMS –
<http://oig.hhs.gov/oas/reports/region4/40705064.pdf>
- NIST HIPAA Guidance –
<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>
- HIPAA Compliance Information -
<http://www.hipaacomply.com/>

Consumer Data

Federal Trade Commission

- The Federal Trade Commission (FTC or Commission) is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy.
- The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace.
- The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.

FTC and Privacy

- FTC's principal tool has two parts:
 - Bring enforcement actions to stop law violations and
 - Require companies to take affirmative steps to remediate the unlawful behavior.

Enforcement

- If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations.
- The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule.
- To date, the Commission has brought hundreds of privacy and data security cases protecting billions of consumers.

FTC Enforcement

- The FTC has brought enforcement actions addressing a wide range of privacy issues including:
 - Spam,
 - Social networking,
 - Behavioral advertising,
 - Pretexting,
 - Spyware, peer-to-peer file sharing, and
 - Mobile.
- These matters include over 130 spam and spyware cases and more than 50 general privacy lawsuits.

Remediation

- Remediation can take the form of:
 - Implementation of comprehensive privacy and security programs;
 - Biennial assessments by independent experts;
 - Monetary redress to consumers;
 - Disgorgement of ill-gotten gains;
 - Deletion of illegally obtained consumer information; and
 - Provision of robust notice and choice mechanisms to consumers.

Credit Reporting and Financial Privacy

- The Fair Credit Reporting Act ("FCRA") sets out rules for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants.
- The FTC has brought over 100 FCRA cases against companies for credit-reporting problems and has collected over \$30 million in civil penalties.
- The Gramm-Leach-Bliley ("GLB") Act requires financial institutions to:
- Send consumers annual privacy notices and allow them to opt out of sharing their information with unaffiliated third parties.
- It also requires financial institutions to implement reasonable security policies and procedures.
- Since 2005, the FTC has brought almost 30 cases for violation of the GLB Act of the GLB Act.

Rules and Regulations

- As directed by Congress, the FTC has authority to develop rules that regulate specific areas of consumer privacy and security.
- Since 2000, the FTC has promulgated rules in a number of these areas relevant to the credit industry:
 - The Health Breach Notification Rule requires certain Web-based businesses to notify consumers when the security of their electronic health information is breached.
 - The Red Flags Rule requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

Rules and Regulations *(cont'd)*

- The Red Flags Rule requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.
- The GLB Safeguards Rule requires financial institutions over which the FTC has jurisdiction to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards.
- The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.
- The Prescreen Opt-out Rule under FACTA requires companies that send “prescreened” solicitations of credit or insurance to consumers to provide simple and easy-to-understand notices that explain consumers’ right to opt out of receiving future offers.

Defense

Federal Information Security Management Act of 2002 FIMSA

- This law recognizes information security is a matter of national security and mandates that all federal agencies develop a method of protecting information systems.
- This applies to all Federal agencies.
- Because it is a priority of all Federal agencies, if your company does any work for the government or others who do work for the government there is often a requirement to certify that all vendors have certain minimum cybersecurity protections in place.

Safeguarding Defense Information and Cyber Incident Reporting

- Applies to those doing government contract work.
- Applies to covered defense information that resides or transits through covered contractor information systems .
- Requires specific network security requirements.
- Requires reporting of cyber incidents.

Covered Defense Information

- Covered defense information” means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at (<http://www.archives.gov/cui/registry/category-list.html>) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
 1. Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
 2. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Incident Reporting Policy

- Contractors and subcontractors are required to rapidly report cyber incidents directly to DoD at <http://dibnet.dod.mil>.
- Subcontractors provide the incident report number automatically assigned by DoD to the prime contractor.
- Lower-tier subcontractors likewise report the incident report number automatically assigned by DoD to their higher-tier subcontractor, until the prime contractor is reached.
 - If a cyber incident occurs, contractors and subcontractors submit to DoD:
 - ✓ A cyber incident report;
 - ✓ Malicious software, if detected and isolated; and
 - ✓ Media (or access to covered contractor information systems and equipment) upon request.

DOD Cyber Policy Regulations

- The government regulations require protection of any proprietary information of the company that is reporting to encourage cyber incident reporting. The protection of a reporting company's information extends to any vendors used by the government to assist in cyber security and regulation.
- There is no presumption that because a company has reported a cyber indictment that the company did not provide adequate security on the covered contractor information system.

Mandatory Cybersecurity Requirements

- The Federal Government issued new regulations requiring commercial companies contracting with the Federal government (or have Federal data) to protect data in a specified manner
- Major regulations:
 - DFARS Case 2013-D018 - “Network Penetration and Reporting for Cloud Services”
 - DFARS 252.239-7010 - “Cloud Computing Services”
 - DFARS 252.204-7012 - “Safeguarding Covered Defense Information and Cyber Incident Reporting”
 - 48 CFR 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems

Mandatory Cybersecurity Requirements

- NIST standards:
 - NIST Special Publication 800-53 Revision - 4 Security and Privacy Controls for Federal Information Systems and Organizations
 - NIST Special Publication 800-171 Rev 1 - "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
 - FEDRAMP (Medium) for Government Data stored in Cloud Computing Services
 - NIST 7621 (Small Business Information Security: the Fundamentals)

What are the Key Obligations of DFARS 7012?

- Provide “adequate security”
 - If operating an USG IT service, then use the controls cited in the contract (e.g., NIST SP 800-53)
 - For contractor systems that store, use or transmit CUI, use the controls cited in NIST SP 800-171
 - For cloud computing, use FedRAMP (Medium) as the standard
- Report to DoD OCIO within 30-days of the award of any -171 requirements not met and your plan to meet them

What are the Key Obligations of DFARS 7012? *(cont'd)*

- Investigate and report “cyber incidents”
 - Investigate and Report within 72 hours
 - Submit malicious software to the DoD Cyber Crime Center
 - Protect and preserve images of the affected systems for at least 90 days
 - Provide Government Access if requested
- Flow down the -7012 clause to sub-contractors
- December 2017 deadline to meet -171

DFARS 7012

- Contractors at all tiers must now fully understand what CDI they store, process, or transmit in the course of doing business with DoD and be prepared to provide adequate security using controls in NIST SP 800-171 Revision 1, Security and Privacy Controls for Non-Federal Information Systems.
- All prime and subcontractors must complete the following activities to achieve DFARS 7012 compliance:

Scope

What contracts have the DFARS 7012 clause included?

What data is associated with those contracts?

What Systems store and / or process that data?

Assess

- Perform a security controls assessment against NIST SP 800-171 Rev 1 to determine compliance.

Remediate

- Remediate assessment findings;
- Create a System Security Plan (SSP); and
- Create a Plan of Action and Milestones (POA&M) to achieve compliance on all the items identified as deficient.

Certify

Submit to DoD by December 31, 2017.

Energy

Energy Sector Cybersecurity Regulators

- The Department of Energy is the Sector-Specific Agency (SSA) for electrical infrastructure, DOE ensures unity of effort and serves as the day-to-day federal interface for the prioritization and coordination of activities to strengthen the security and resilience of critical infrastructure in the electricity subsector.
- DOE collaborates with vendors, utility owners, and operators of the electricity and oil and natural gas sectors.
- With 90 percent of the nation's power infrastructure privately held, coordinating and aligning efforts between the government and the private sector is vital.
- The DOE's Office of Electricity Delivery and Energy Reliability (OE) is charged with keeping the nation's electric power grid and oil and natural gas infrastructure resilient to cyber threats.

Energy Sector Cybersecurity OE's Cybersecurity Program

- Strengthening energy sector cybersecurity preparedness
- Coordinating cyber incident response and recovery
- Accelerating research, development and demonstration (RD&D) of game-changing and resilient energy delivery systems

Energy Sector Cybersecurity Preparedness

- Situational Awareness and Information Sharing
 - Cybersecurity Risk Information Sharing Program (CRISP)
 - CRISP) is a public-private partnership, co-funded by DOE and industry and managed by the Electricity Information Sharing and Analysis Center (E-ISAC)
 - Current CRISP participants provide power to over 75 percent of the total number of continental U.S. electricity subsector customers.

Cyber Incident Response and Recovery

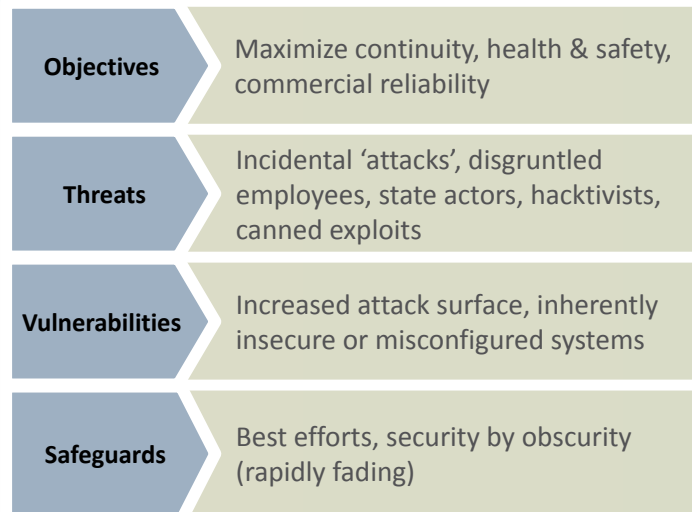
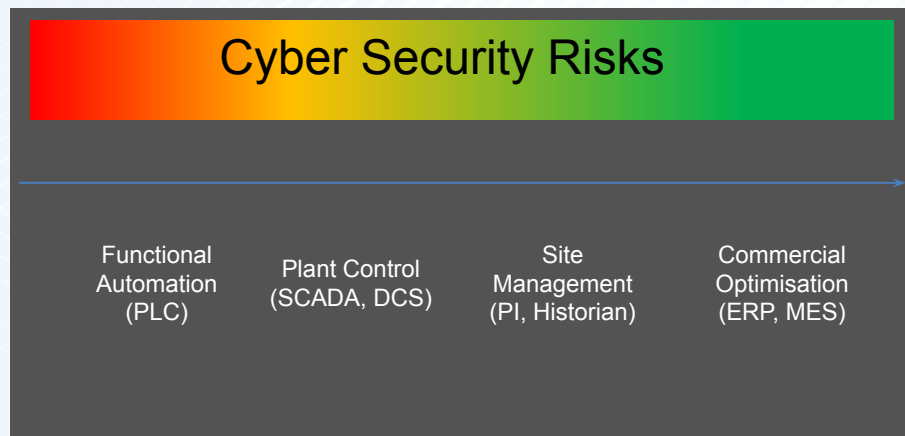
- OE facilitates incident coordination across government and with the private sector to enhance response and recovery efforts and coordinates federal capabilities to mitigate the impact of a cyber attack.
- The OE works within the National Incident Management System (NIMS) and National Response Framework (NRF).

Research Development and Demonstration

- OE works closely with its private and public partners to accelerate the research, development and demonstration (RD&D) of next-generation cyber-resilient energy delivery systems and components.
- Combine the disciplines of information technology with operational technology used in energy delivery functions and operational networks.
- OE's Cybersecurity for Energy Delivery Systems (CEDS) R&D program aligns all activities with Federal priorities as well as the strategy and milestones articulated in the energy sector's Roadmap to Achieve Energy Delivery Systems Cybersecurity that envisions resilient energy delivery control systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

OT (Operational Technology) Cybersecurity

- Owners of modern operational assets cannot ignore the benefits of increasing their OT capabilities. To maximize capabilities, however, connectivity with IT systems and networks becomes necessary and this connectivity exposes traditionally 'air-gapped' OT systems to traditional IT security risks. Protiviti helps process industry organizations overcome organizational and technical differences between OT and IT to effectively define and deliver OT cyber security programs or individual components of it.



OT Transformation

- Assess current state operating model for OT people, process and technology
- Define and implement target operating model
- Incorporate security into, organizational structure, operating processes and OT architecture

OT Continuity

- Intelligent, process-driven asset identification and classification
- Assessment of outage risks
- Capability and requirements analysis
- Remediation planning and project management

OT Security Program Management

- Establish objectives and governance model; Define scope, objectives and milestones; Socialize program with IT and OT personnel
- Identify and classify assets; Deliver program activities

Energy Sector Cybersecurity Regulators

- The Energy Policy Act of 2005 (Energy Policy Act) gave the Federal Energy Regulatory Commission (Commission or FERC) authority to oversee the reliability of the bulk power system, commonly referred to as the bulk electric system or the power grid. This includes authority to approve mandatory cybersecurity reliability standards.
- The North American Electric Reliability Corporation (NERC), which FERC has certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection (CIP) cyber security reliability standards.
- On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns.

Energy Sector Cybersecurity

Regulators *(cont'd)*

- Additionally, the electric industry is incorporating information technology (IT) systems into its operations – commonly referred to as smart grid – as part of nationwide efforts to improve reliability and efficiency.
- There is concern that if these efforts are not implemented securely, the electric grid could become more vulnerable to attacks and loss of service. To address this concern, the Energy Independence and Security Act of 2007 (EISA) gave FERC and the National Institute of Standards and Technology (NIST) responsibilities related to coordinating the development and adoption of smart grid guidelines and standards.

NERC and CIP

- In 2013, the FERC approved changes and additions to Critical Infrastructure Protection (CIP) Reliability Standards, also known as CIP v5, which are a set of requirements for securing the assets responsible for operating the bulk power system.
- CIP is just one of 14 mandatory NERC standards that are subject to enforcement in the U.S.
- This regulation is centered on the physical security and cybersecurity of assets deemed to be critical to the electricity infrastructure.

NERC Cybersecurity

- The stated purpose of mandatory NERC Standards CIP-002 through CIP-009 is to provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system.
- Responsible entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

CIP Compliance Principles

- Standard CIP-002 requires the identification and documentation of the critical cyber assets associated with the critical assets that support the reliable operation of the bulk electric system.
- Responsible entities must have minimum security management controls in place to protect critical cyber assets.
- Information access must be controlled.
- A protocol and controls must be in place to address changes to any cyber asset.
- Electronic security perimeters around assets and at access points to assets must be established and protected.

CIP Compliance Principles *(cont'd)*

- Electronic access must be monitored at all times.
- Vulnerability assessment must be conducted and all compliance must be reviewed and maintained annually, all changes updated within 90 days, and all access logs must be maintained for at least 90 days.
- Personnel must be aware of compliance requirements, trained, and personnel must be subject to individual risk assessment. Access by personnel must be controlled and monitored.

Industrial Control Systems (ISC) SCADA Controls

- The North American Electric Reliability Corporation (NERC) is a nonprofit corporation designed to “ensure that the bulk electric system in North America is reliable, adequate and secure.”
- The Critical Infrastructure Protection (CIP) Cyber Security Standards maintained by NERC are intended to ensure the protection of the Critical Cyber Assets that control or effect the reliability of North America’s bulk electric systems.
- In 2006, the Federal Energy Regulatory Commission (FERC) approved the Security and Reliability standards proposed by NERC, making the CIP Cyber Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system.

Industrial Control Systems (ISC) SCADA Controls *(cont'd)*

- Standard CIP-003-2 — Cyber Security — Security Management Controls
- Adopted by NERC Board of Trustees: May 6, 2009 1
- R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

Industrial Control Systems (ISC) SCADA Controls (cont'd)

- R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
- R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
- R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

Controls (*cont'd*)

- NIST Industrial Control 800-53
- AC-5 SEPARATION OF DUTIES
- Control: The information system enforces separation of duties through assigned access authorizations.
- Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Industrial Control Systems (ISC) SCADA Controls (*cont'd*)

- ICS Supplemental Guidance: In situations where the organization determines it is not feasible or advisable (e.g. adversely impacting performance, safety, reliability) to implement separation of duties (e.g., the organization has a single individual to perform all roles or the ICS does not differentiate roles), the organization documents the rationale for not implementing the control, documents appropriate compensating security controls in the System Security Plan, and implements these compensating controls. Related security control: PL-2.
- Control Enhancements: None.
- LOW Not Selected MOD AC-5 HIGH AC-5

Industrial Control Systems (ISC) SCADA Controls *(cont'd)*

- The Pipeline and Hazardous Materials Safety Administration (PHMSA) is a United States Department of Transportation agency responsible for developing and enforcing regulations for the safe, reliable, and environmentally sound operation of the United States 2.6 million mile pipeline transportation.
- There are industry organizations per domain such as electric, pipeline, NGAS, water, pharmaceutical, chemical, transportation, and others that have specific goals and standards, however many are voluntary within the industry.

Sample SCADA Security Approach

- Typical assessments have the following key steps:
- Ensure that access to the SCADA systems is appropriately restricted from the internal corporate network;
- Ensure that the SCADA network is not accessible from the internet and remote access is secure;
- Review access controls that are protecting the SCADA environment (network and systems);
- Assess the SCADA environment based on applicable NIST, NERC, and PHMSA standards.
- Key controls are selected from industry leading practices for securing SCADA systems such as the following:
- National Institute of Standards and Technology document SP800-82;
- North American Electric Reliability Corporation Critical Infrastructure Protection documents 002 through 011 version 5; and
- U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration security standards. (49 CFR 192.631/195.446 Control Room regulations).

Sample SCADA Security Approach (cont'd)

- Key areas are covered including:
 - Firewall and Networking
 - Ports and Services
 - Account and Password Policies
 - Patch Management
 - Configuration Management
 - Vulnerability Management
 - Logging and Monitoring
 - Modem and Remote Access Controls
 - Anti-Virus
 - Physical Security
 - Policies and Procedures

EU

EU Data Privacy

Data Protection Directive 95/46/EC

- Strong history of privacy protection in Europe.
- All EU Members are part of European Convention on Human Rights a treaty which specifically protects the right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions.
- Incorporates all seven OECD principles.
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA) brings Canadian law into line with EU data protection law.

7 Principles Governing the OECD Recommendations

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data".

7 Principles Governing the OECD Recommendations *(cont'd)*

The seven principles governing the OECD's recommendations for protection of personal data were:

Notice—data subjects should be given notice when their data is being collected;

Purpose—data should only be used for the purpose stated and not for any other purposes;

Consent—data should not be disclosed without the data subject's consent;

Security—collected data should be kept secure from any potential abuses;

Disclosure—data subjects should be informed as to who is collecting their data;

Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and

Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

EU Process

- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was negotiated within the Council of Europe in 1981. This convention requires the signatories to enact legislation concerning the automatic processing of personal data
- The European Commission put forward the Data Protection Directive focused on the issue that diverging data protection legislation amongst EU member states impeded the free flow of data within the EU and accordingly proposed the Data Protection Directive.

U.S. Process

- United States privacy legislation tends to be adopted in response to when certain sectors or circumstances require legislation and employs self-regulation where possible.

U.S. – EU Safe Harbor

- The FTC enforces the U.S. - EU Safe Harbor Framework, which was implemented in 2000 to facilitate the transfer of personal data from Europe to the United States.
- The FTC brought a number of new cases this year against companies that violated Section 5 of the FTC Act by making misrepresentations about their participation in the program.
- It also issued final orders against several companies that had previously violated their Safe Harbor promises.
- In total, the FTC has used Section 5 to bring 39 Safe Harbor cases since 2009.

Framework Elements

- Strong obligations on companies handling Europeans' personal data and robust enforcement.
- Clear safeguards and transparency obligations on U.S. government access.
- Effective protection of EU citizens' rights with several redress possibilities.

Decision 2000/520/EC and the New Framework

- October 6, 2015, the European Court of Justice issued a judgment declaring as invalid the European Commission's Decision 2000/520/EC of 26 July 2000 on the adequacy of the U.S.-EU Safe Harbor Framework.
- In February 2016 the U.S. and EU officials reached an agreement on a new framework to be enforced by the FTC & US Department of Commerce, including cooperation with the European Data Protection Authorities.
- The new arrangement includes commitments by the U.S. that possibilities under U.S. law for public authorities to access personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, preventing generalized access.
- Europeans will have the possibility to raise any enquiry or complaint in this context with a dedicated new Ombudsperson.

Strong Obligations on Companies Handling Europeans' Personal Data and Robust Enforcement

- U.S. companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed.
- The Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under U.S. law by the US. Federal Trade Commission.
- In addition, any company handling human resources data from Europe has to commit to comply with decisions by European DPAs.

Clear Safeguards and Transparency Obligations on U.S. Government Access

- For the first time, the US has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms.
- These exceptions must be used only to the extent necessary and proportionate.
- The U.S. has ruled out indiscriminate mass surveillance on the personal data transferred to the US under the new arrangement.
- To regularly monitor the functioning of the arrangement there will be an annual joint review, which will also include the issue of national security access.
- The European Commission and the U.S. Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European Data Protection Authorities to it.



Effective Protection of EU Citizens' Rights with Several Redress Possibilities

- Any citizen who considers that their data has been misused under the new arrangement will have several redress possibilities.
- Companies have deadlines to reply to complaints. European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission.
- In addition, Alternative Dispute resolution will be free of charge.
- For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.

EU General Data Protection Regulation GDPR

- EU General Data Protection Regulation - The EU is updating their 1995 Data Protection Directive with the GDPR and its final form will be enforceable May 25th 2018.
- This regulation will require an review of how information is collection and stored for any company doing business in the EU.
- Companies that collect data on citizens in European Union (EU) countries will need to comply with strict new rules around protecting customer data
- GDPR takes a wide view of what constitutes personal identification information. Companies will need the same level of protection for things like an individual's IP address or cookie data as they do for name, address and Social Security number.

EU General Data Protection Regulation

GDPR (cont'd)

- EXPANSIVE POTENTIAL INTERPRETATION FOR NEW PROVISIONS. Companies must provide a “reasonable” level of protection for personal data, for example, but GDPR does not define what constitutes “reasonable.”
- This gives the GDPR governing body a lot of leeway when it comes to assessing fines for data breaches and non-compliance.

EU General Data Protection Regulation

GDPR (cont'd)

- Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU.
- Specific criteria for companies required to comply are:
- A presence in an EU country.
- No presence in the EU, but it processes personal data of European residents.
- More than 250 employees.
- Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data. That effectively means almost all companies.
- The GDPR allows for steep penalties of up to €20 million or 4 percent of global annual turnover, whichever is higher, for non-compliance.

What Types of Privacy Data Does the GDPR Protect?

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

- The GDPR requirements will force U.S. companies to change the way they process, store, and protect customers' personal data.
- Companies will be allowed to store and process personal data only when the individual consents and for “no longer than is necessary for the purposes for which the personal data are processed.”
- Personal data must also be portable from one company to another, and companies must erase personal data upon request. This is known as the “right to be forgotten.”
- Exceptions: GDPR does not supersede any legal requirement that an organization maintain certain data such as HIPAA health record requirements.
- Estimates on typical GDPR compliance are high.

GDPR

COMMON TRENDS EMERGING FROM OUR GDPR READINESS ASSESSMENTS

DATA PRIVACY BY DESIGN AND BY DEFAULT	Organisations are not able to demonstrate any privacy by design and by default approach. Privacy is not yet a primary consideration when organisational processes are designed.
WRITTEN RECORDS OF PROCESSING ACTIVITIES	Organisations have not been able to document all of their personal data processing activities, to the level of detail mandated by the GDPR.
DATA BREACH REPORTING AND COMMUNICATION	Data breach management processes do not yet acknowledge all of the obligations defined by the GDPR. Many organisations even have difficulties identifying which data subjects must be notified of a breach.
SECURITY OF PROCESSING (TECHNICAL AND ORGANISATIONAL MEASURES)	Encryption and Pseudonomysation (formerly known as “anonymization”) is seldom used to protect data at rest and sometimes even in transfer. Encryption, while not unequivocally mandated by the GDPR, is always recommendable as the data breach reporting and communication obligations are waived when the compromised data is in a format unusable by the unauthorised users.
RIGHTS OF DATA SUBJECTS	The ability to cope and comply with all the rights granted to data subjects by the GDPR can only be achieved with a high level of automation which allows data subject to operate on a self serve mode. Organisations often do not have CRM systems capable of providing data subject with self service functionality.
CONDITIONS FOR CONSENT	Organisations have not yet realised the effort it will take them to re-obtain consent in those cases where they are unable to prove that such consent was explicitly obtained in compliance with Art. 7 of the GDPR. All verbally-obtained consent must be re-obtained as it will not longer be valid under the GDPR.
DATA PROTECTION IMPACT ASSESSMENTS	Never been used previously in most organisations and are often not yet operational and embedded processes.
RE-NEGOTIATION SERVICE CONTRACTS	The effort necessary to re-negotiate contracts with service providers with new data protection clauses and the distinction of controller and processor roles is often substantially underestimated.

Questions or Comments?

If you have any questions about this webinar that you did not get to ask during the live premiere, or if you are watching this webinar [On Demand](#), please do not hesitate to email us at info@financialpoise.com with any questions or comments you may have. Please include the name of the webinar in your email & we will do our best to provide a timely response.

IMPORTANT NOTE: The material in this presentation is for general educational purposes only. It has been prepared primarily for attorneys & accountants for use in the pursuit of their continuing legal education & continuing professional education.

*** This PowerPoint was produced in connection with a video webinar that premiered on 7/2/2025. If you are reading this without the benefit of having attended, then you are missing its real value. You can access the webinar on-demand at [West Legal Ed Center](#) (for attorneys or accountants seeking CLE or CPE) or [Financial Poise](#) (for everyone else).

Meet The Faculty

Lauren Silvestri Burke - lauren.burke@morganlewis.com



Lauren S. Burke is an associate in Morgan Lewis's Litigation Practice. Lauren's practice focuses on product liability, complex commercial, and class action litigation. She has represented clients in complex commercial disputes, mass torts, consumer fraud actions, and government investigations. She handles all aspects of litigation from inception through trial and post-trial appeals in actions throughout the United States.

Lauren's significant representations include:

- Representation of a manufacturer of construction products in successful defense of a nationwide class action and subsequent statewide class action.
- Representation of a multinational pharmaceutical company in consumer fraud class actions and attorney general litigation in state and federal trial courts and a number of appeals.
- Representation of a major financial services company in a breach of contract action.
- Representation of a multinational pharmaceutical company in more than one investigation by the Department of Justice regarding off-label promotion and fraud allegations. [Read More](#)

Daniel Cotter - DCotter@dickinson-wright.com



A member in the firm's Chicago office, Daniel Cotter's practice encompasses a range of roles, including a pivotal tenure as general counsel for a major life insurance company and extensive private practice experience. His clientele spans insurance firms, financial institutions, IT/consulting enterprises, and nonprofits.

Since 1996, Dan has been deeply involved in privacy and cybersecurity matters, notably contributing to the formulation of terms and conditions as well as disclaimers for Fortune 500 websites in the late 1990s. His roles as a chief privacy officer across various companies and law firms underscore his depth in these evolving domains.

Dan's proficiency extends to navigating intricate insurance regulatory matters, overseeing substantial reorganizations within holding company systems, and negotiating a myriad of contracts, ranging from simple to elaborate, including outsourcing agreements. [Read More.](#)

Kyle Miller - Kyle.miller@dentons.com



Kyle is a lawyer in the Dentons global Data Privacy and Cybersecurity group. Kyle's practice builds on his career as a cybersecurity professional in bringing value to clients with needs related to cybersecurity, data privacy, intellectual property, and technology.

Kyle counsels clients across all phases of their systems development lifecycle. He drafts and assesses organizations' cybersecurity programs, performing gap and risk assessments under applicable information security frameworks and standards. He also crafts and leads cybersecurity tabletop exercises to test and practice organizations' cybersecurity programs. He drafts and implements data privacy programs compliant with domestic and global legal regimes. Kyle has significant experience reviewing and negotiating technology contracts including data rights and transfer agreements. Kyle also handles trade secret, trademark, and other intellectual property disputes. [Read More](#)

Thank you to our co-producer

THE NATIONAL LAW REVIEW

The National Law Review (NLR) is a premier legal news website offering in-depth analysis on a wide range of legal and business topics. Established in 1888, NLR has evolved into a **trusted resource** for legal professionals, business leaders, and the general public, providing timely and relevant information on legislative changes, court decisions, and regulatory developments

Visit *The National Law Review* to learn more
- <https://natlawreview.com/>

Comprehensive Coverage: NLR covers nearly every legal topic, including litigation, AI & the Law, employment law, IP Law, real estate, energy, health care, bankruptcy and much more.

Expert Analysis: Articles are authored by experienced attorneys and legal professionals, ensuring accurate and insightful commentary.

Daily Updates: NLR provides hourly legal news updates, keeping readers informed about the latest developments in the legal world.

About Financial Poise



The primary mission of Financial Poise™ is to provide reliable plain English business, financial, & legal education to individual investors, entrepreneurs, business owners, & executives, & to help trusted advisors do the same.

*Newsletter subscribers are occasionally offered free webinars. Subscribers never receive more than one email per week & their information is never shared.

Sign up for our free weekly e-newsletter [here](#).*

Learn how to write or speak for Financial Poise [here](#).
The antithesis of “pay-to-play.”

Check out our other webinars [here](#).

Send any other inquiry to info@financialpoise.com