INFORMATION SECURITY:
Cyber Breach & Coverage Issues

Presented By:
David J. Walton
Cozen O'Connor
Philadelphia, PA
dwalton@cozen.com

COZEN O'CONNOR

OVERVIEW

- Cybersecurity Risks and Exposures
  - Risk Profiles -- Why? Who? What? Where? How?
- Regulatory Frameworks for Data Protection
  - Comprehensive Model -- EU Data Protection Directive
  - Sectorial Model -- US Federal and State Laws
  - Co-Regulatory/Self-Regulation Model -- PCI/DSS
  - Technology-Based Models -- Google/Yahoo encryption
- Data Breach Case Studies
  - AVMed, Sony, Heartland, Target
- Insurance
  - CGL and Cyber/Technology Coverage
- Best Practices
  - Underwriting and Incident Response

COZEN O'CONNOR

WHY?

The Gravity of Cybersecurity

- "The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas through cyber intrusions. This threatens innovation and, as citizens, we are also increasingly vulnerable to losing our personal information. That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats."

  - FBI Director James Comey

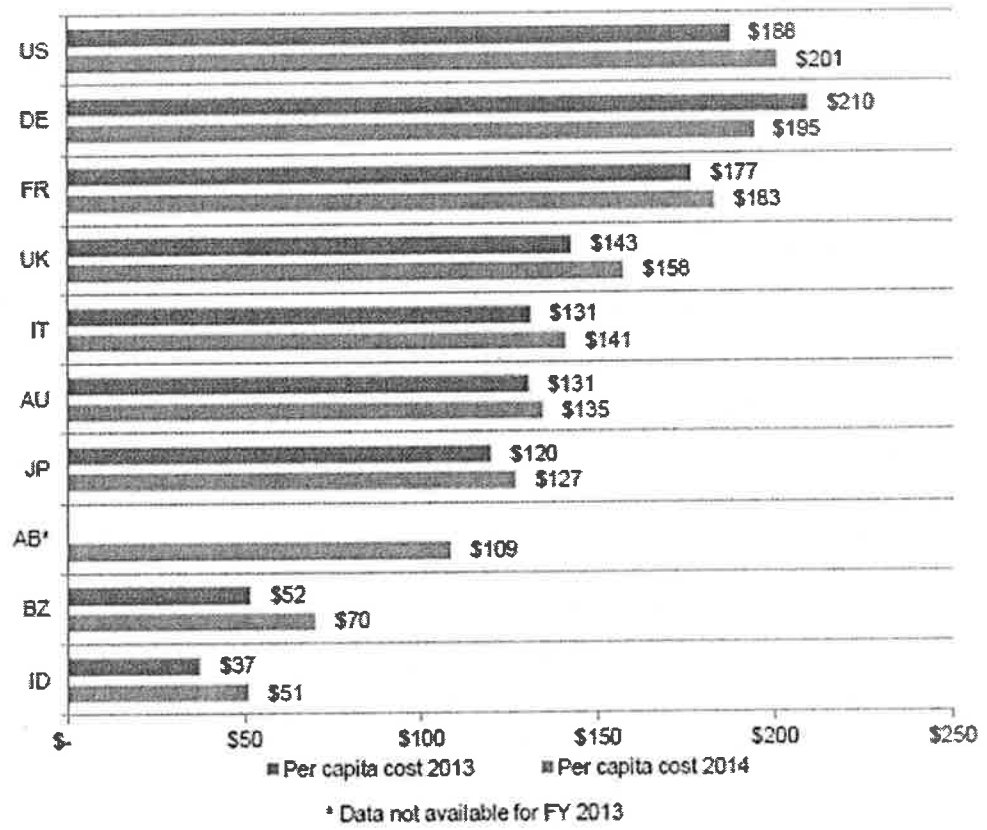
- "The cyber threat is one of the most serious economic and national security challenges we face as a nation… America's economic prosperity in the 21st century will depend on cybersecurity."

  - President Obama

COZEN O'CONNOR

Per Record Costs of Data Breach

Figure 2. The average per capita cost of data breach over two years
Measured in US$

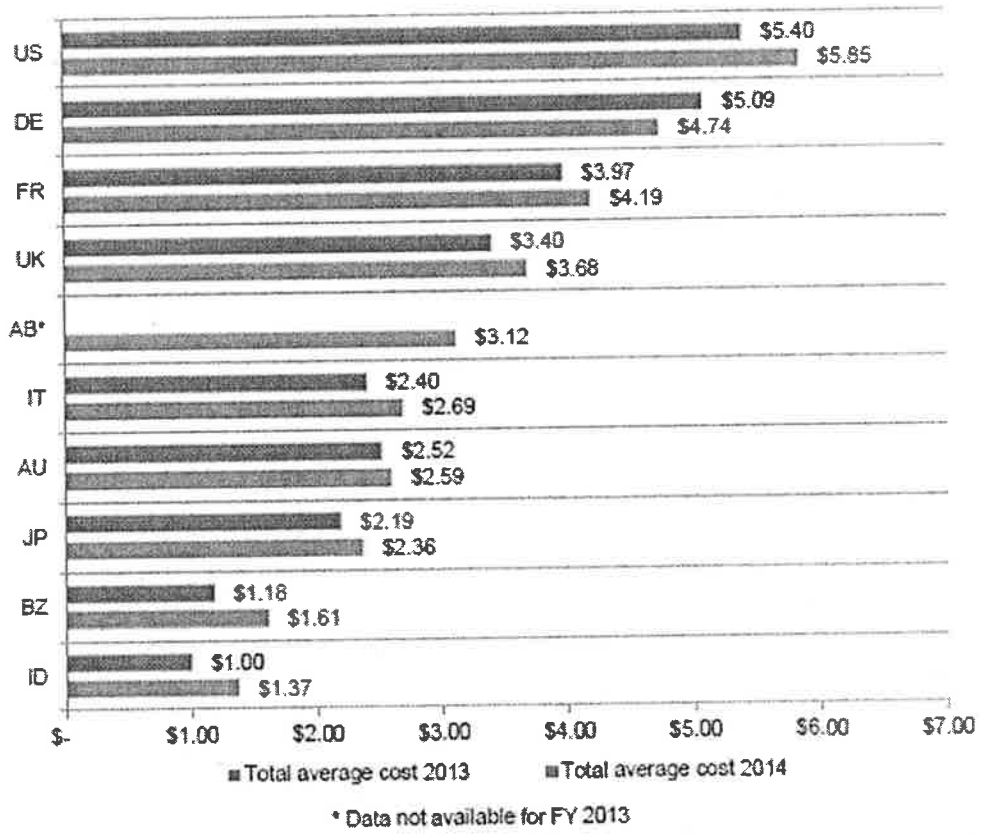


Source: Ponemon Institute LLC
2014 Cost of Data Breach Study: Global Analysis (IBM sponsored)
http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

COZEN O'CONNOR

Total Costs of Data Breach

Figure 3. The average total organizational cost of data breach over two years
Measured in US$ ($000,000 omitted)



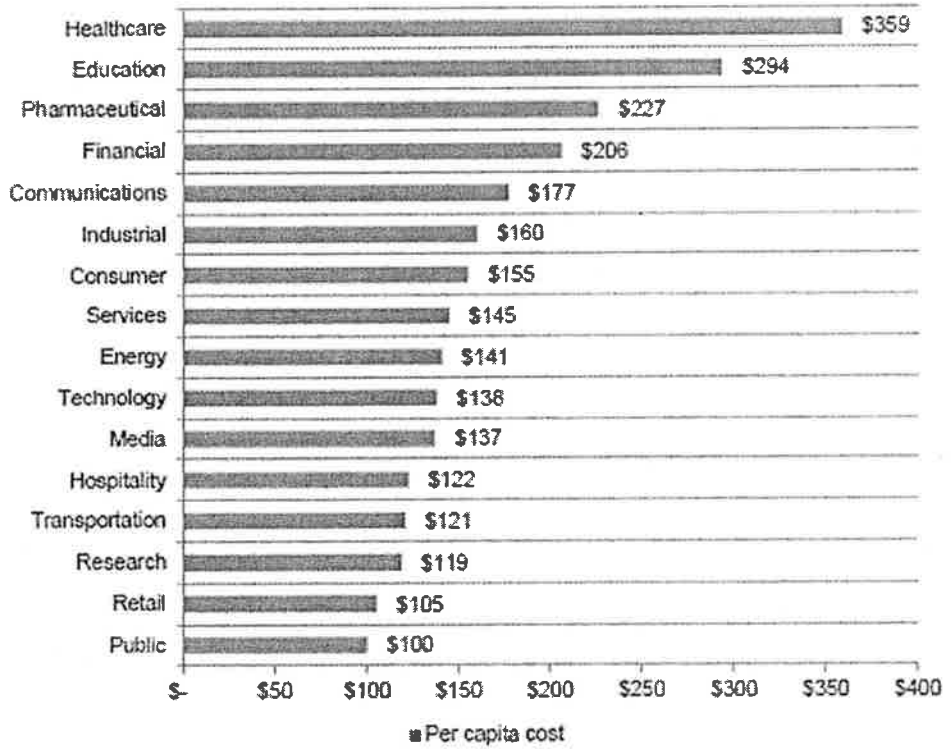
* Data not available for FY 2013

Source: Ponemon Institute LLC
2014 Cost of Data Breach Study: Global Analysis (IBM sponsored)
http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

COZEN O'CONNOR

Costs of Data Breach by Industry

Figure 4. Per capita cost by industry classification
Consolidated view (n=314)

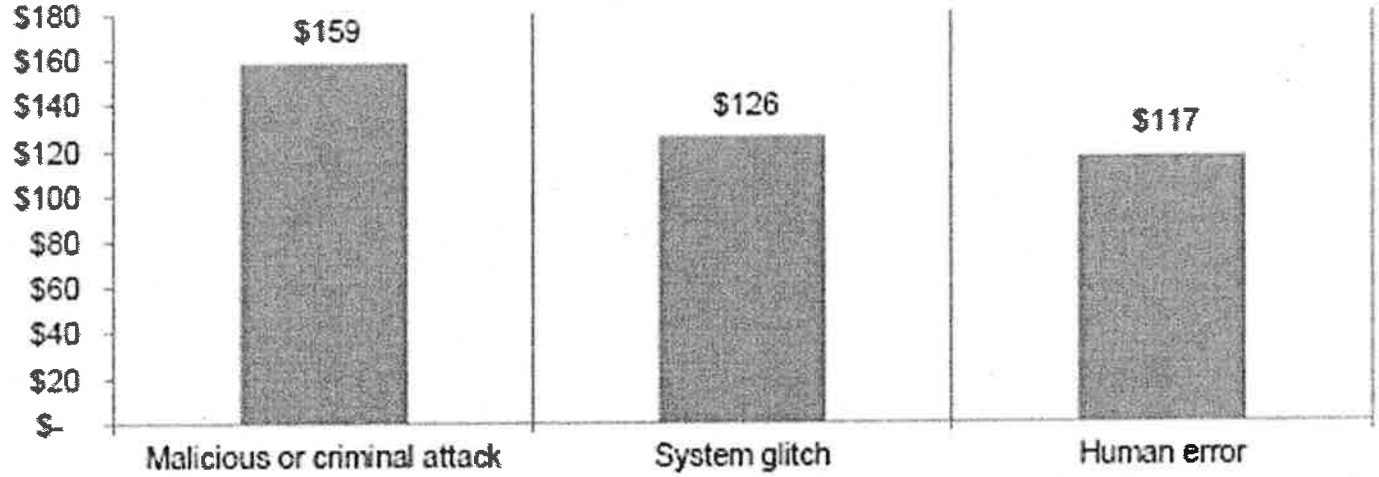


Source: Ponemon Institute LLC
2014 Cost of Data Breach Study: Global Analysis (IBM sponsored)
http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

COZEN O'CONNOR

Costs of Data Breach By Source

Figure 6. Per capita cost for three root causes of the data breach
Consolidated view (n=314)
Measured in US$

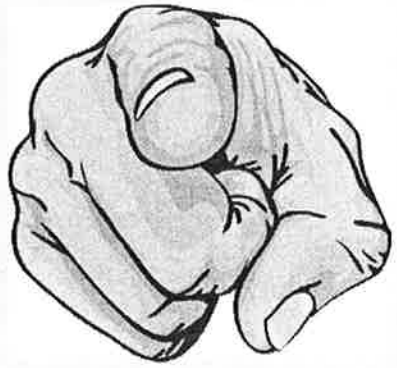


Source: Ponemon Institute LLC
2014 Cost of Data Breach Study: Global Analysis (IBM sponsored)
http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

COZEN O'CONNOR

Who?
Is At Risk

- Data Subjects, Data Controllers, and Data Processors
- Risk Is Not Industry Specific:
  - Financial Institutions
  - Merchants
  - Healthcare Providers
  - Critical Infrastructure Providers
  - Governmental Entities
  - Sole Proprietorships and Individuals



- 40% of breaches in companies under 1000 employees
- 31% of breaches in companies with under 100 employees

COZEN O'CONNOR

What?

Types of Information At Risk?

- Personal Identifiable Information (PII)
- Protected Health Information (PHI/ePHI)
- Customer Information
- Proprietary Business Information

COZEN O'CONNOR

Personal Identifiable Information (PII)

- Name; address; telephone number; electronic mail address; fingerprints; photographs or computerize images; a password; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; date of birth; financial information

- Vastly different definitions of PII

COZEN O'CONNOR

Protected Health Information (PHI)-

- Any individually identifiable health information that is transmitted or maintained in any form or medium held by a covered entity, employer, or Business Associate

Electronic Protected Health Information (ePHI)

- Any PHI that is transmitted or maintained in electronic media (hard drives, tapes, CDs, memory cards

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

COZEN O'CONNOR

Customer Information

- Accounts Receivable
- Bank/Wire Instructions
- Pricing Information

Proprietary Information

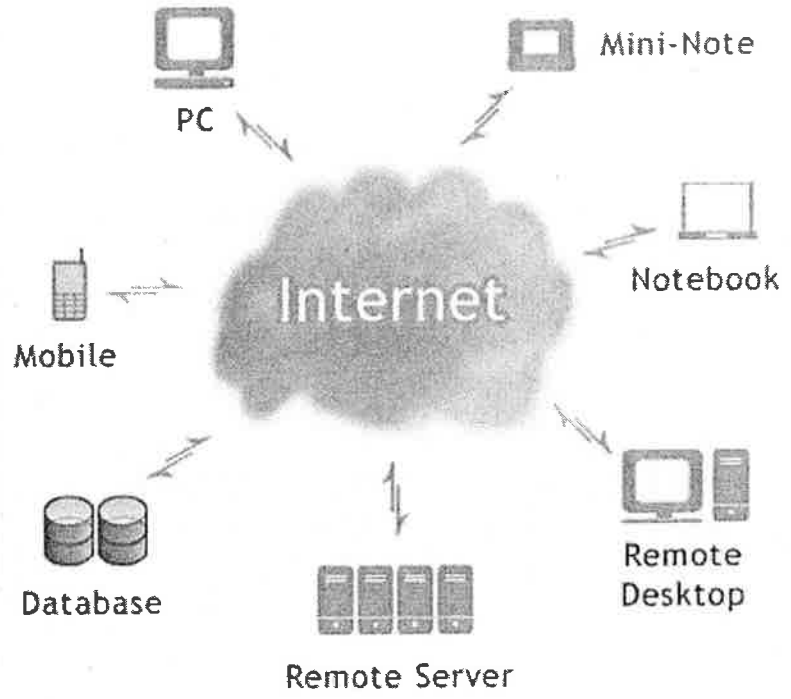
- Competitive Information
- Trade Secrets
- Test Results

COZEN O'CONNOR

Where?
Location And Risk

- Hand-Held Devices
- Laptops
- Desktops
- Servers/Databases
- Web Applications
- POS Equipment
- Thumb Drives

- The Cloud - aaS



COZEN O'CONNOR

Where?
Location And Risk

- Exponential Growth of Mobile Electronics
  - 5 billion mobile phones
  - Apple Store: 1M apps and 50 billion app downloads in 2013
- Cheaper, Faster, More Powerful Memory
  - $60 for enough memory to store all of the music ever created in the world
  - Data warehouse and cloud computing boom
- Data, Data, and More Data
- By 2016, gigabyte equivalent of all movies ever made will cross global IP networks every 3 minutes

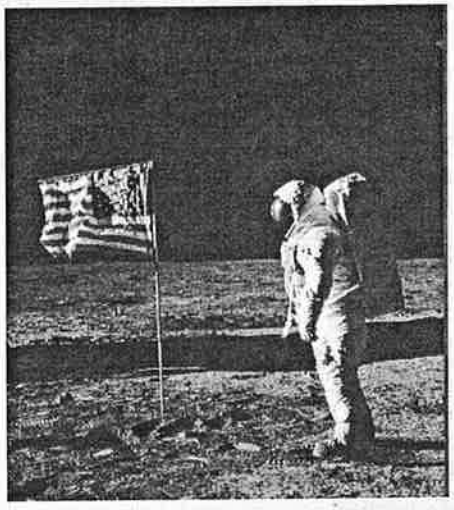
COZEN O'CONNOR

Where?

Location And Risk

New York City Taxi Association reported 73,000 lost cellphones in 2013

Average smartphone has more computer power than all of NASA in 1969



COZEN O'CONNOR

Social Media

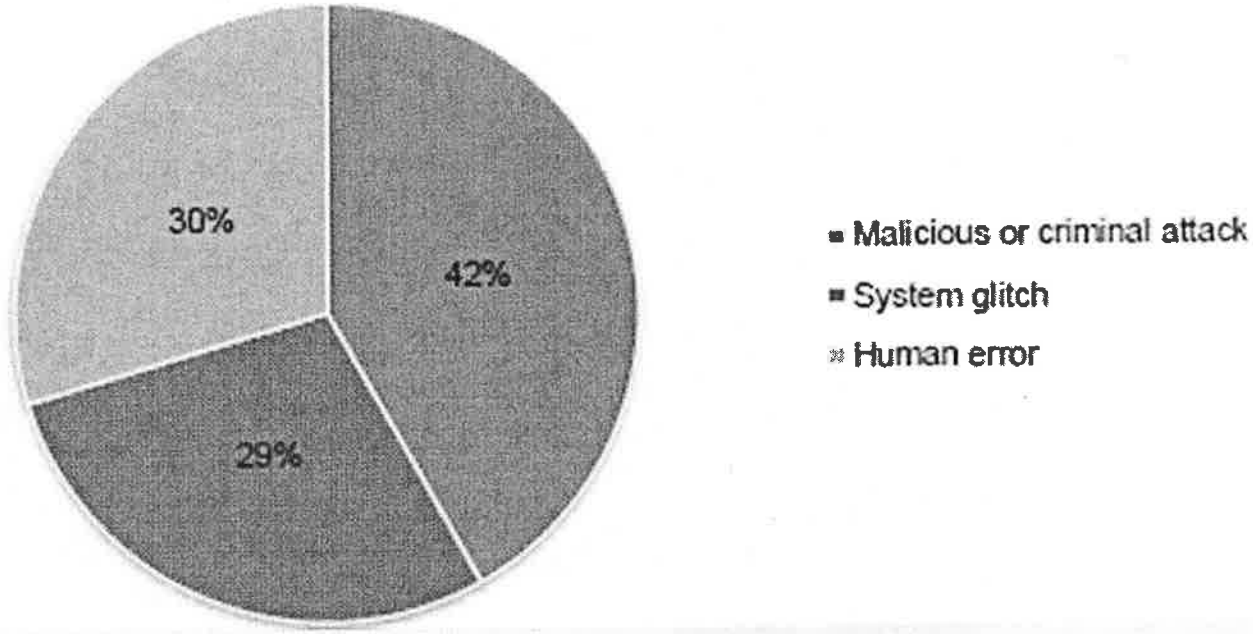
- Facebook
  - Over 1.28 billion users
  - 2.5 billion "likes" per day
- LinkedIn
  - Over 225 million users
- Twitter
  - 255 million users
  - 500 million Tweets per day

COZEN O'CONNOR

How?

Sources of Data Breach

Figure 5. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=314)



Source: Ponemon Institute LLC
2014 Cost of Data Breach Study: Global Analysis (IBM sponsored)
http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

COZEN O'CONNOR

How?
Sources of Data Breach

- Malicious Attack:
  - Social engineering – phishing/spam
  - Malware
  - Physical attacks – stolen hardware/infected memory cards
  - Weak/stolen credentials (passwords)
- Human Error:
  - Lost Device
- System Glitch
  - Application vulnerabilities
  - Improper configuration/user error

COZEN O'CONNOR

How?

The Perpetrators

- Insiders
  - Malicious: anger or frustration with the company, coercion, greed, etc.
  - Unintentional: configuration mistakes, lost equipment, etc.

- Outsiders
  - "Hacktivists"
  - Organized crime
  - State-affiliated entities ("cyber-espionage")
  - Trade secret theft
  - Ex-employees

COZEN O'CONNOR

Models of Data Protection

More than 80 countries have data protection laws and 50% had enacted privacy laws as of 2000

- Comprehensive Model
  - European Union: Data Protection Directive 95/46/EC
- Sectorial Model
  - US Federal and State Regulations
- Co/Self-Regulatory Model
  - Payment Card Industry Data Security Standard (PCI/DSS)
- Technology Model
  - Google and Yahoo: website and mail encryption

COZEN O'CONNOR

EU Data Protection Directive

- Comprehensive legal structure to protect fundamental rights for individuals in Processing of Personal Data
- Based on Fair Information Practice first developed in United States in 1970s
  - "Personal Data" is broadly defined as data that relates to an identified or identifiable individual acting in business or professional capacity
  - "Processing" is designed to cover all possible operations: collection, storage, handling, use, and deletion
- International Data Transfers: Adequate Protections, Model Contracts, Binding Corporate Rules, US Safe Harbor (under FTC and DOT)
  - Information Commissioner for UK

COZEN O'CONNOR

Federal Information Security/Privacy Laws of the United States

- There is no single, comprehensive US federal law that governs privacy issues, particularly data privacy issues; rather, many disparate regulations
  - Executive Order 13636 (February 12, 2013)
    - "Improving Critical Infrastructure Cybersecurity"
  - Health Information Privacy: HIPAA/HITECH, GINA
  - Financial Privacy: FCRA, FACTA (Red Flag Rules), GLBA
  - Education Records: FERPA, PPRA
  - Telecommunications, Marketing, and Online Activities: TSR/TCPA, CAN-SPAM, COPPA

COZEN O'CONNOR

Executive Order 13636 Cybersecurity Framework

- Voluntary risk-based set of industry standards and best practices to help organizations manage cybersecurity risks

- Critical infrastructure:
  - "[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

- Department of Homeland Security and National Institute of Standards and Technology (NIST)

COZEN O'CONNOR

US Health Information Privacy Laws

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Privacy Rule, Security Rule, Enforcement Rule: most detailed implementation of Fair Information Privacy Practices
    - » Requirements: Privacy Notices, Authorizations, Minimum Use/Disclosure, Access and Safeguards
      - » Administrative Safeguards
      - » Physical Safeguards
      - » Technical Safeguards

- Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
  - Business Associates of Covered Entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.
  - Notify HHS-OCR of breaches of unsecured PHI affecting fewer than 500 individuals not later than 60 days after the end of the calendar year
  - Civil Money Penalties: $100 - $50,000 - $1,500,000 per occurrence

- Genetic Information Nondiscrimination Act of 2008 (GINA)
  - Prohibits health insurance companies from discriminating on basis of genetic predispositions without manifest symptoms, requesting testing or employers from using in employment decisions

COZEN O'CONNOR

US Financial Privacy Laws

- Fair Credit Reporting Act of 1970 (FCRA)
  - Privacy Rights in use of consumer reports by Consumer Reporting Agencies, Users (banks, insurers, employers), and furnishers (reporting to CRAs)
  - Enforced by FTC, CFPB, State Attorney Generals, and individual private right of action
  - Civil and Criminal Penalties - $1,000 per violation ($2,500 willful)
  - Notice, Permissible Purpose, Certifications, Adverse Action Correction
- Fair and Accurate Credit Transactions Act of 2003 (FACTA)
  - Credit Card Number (--XXX) on receipts, free annual credit report, Disposal Rule
  - Enforced by FTC, CFPB, Banking Regulators,
  - Red Flags Rule: Implement written identity theft detection programs for creditors
- Gramm-Leach-Bliley Act of 1999 (GLBA)
  - Enforced by CFPB, SEC, and CFTB
  - Applies to Financial Institutions (banks, insurers, even brokers as defined under Bank Holding Company Act – engaging in financial activities)
  - Requirements: Privacy Notices and development of Comprehensive Information Security Program (Administrative, Technical, Physical Safeguards), designate information security officer
- Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
  - Created CFPB with power to bring enforcement actions for unfair and deceptive practices
- Anti-Money Laundering Laws
  - Bank Secrecy Act, Patriot Act

COZEN O'CONNOR

US Educational Record Privacy Laws

- Family Educational Rights and Privacy Act of 1974 (FERPA)
  - Applies to all Education Institutions that receive federal funding
  - Enforced by Department of Education
  - Forbids disclosure of PII other than for directory purposes without student consent
    - » Academic Records, Financial Aid, Disciplinary, Applications
    - » Not apply to police records, employment records, alumni records
- Protection of Pupils Rights Amendment of 1978
  - limits use of surveys to minors for collection of sensitive information

COZEN O'CONNOR

US Marketing and Internet Laws

- Telephone Consumer Protection Act and Telemarketing Sales Rule of 1991 and 2010 (TCPA/TSR)
  - Enforced by FTC, FCC, and state attorney generals
  - Privacy Rights for telemarketing and consumer database lists
    - » Do Not Call Registry, Timing (8am – 9pm), Caller ID, Disclosures, Misrepresentations and Material Omissions, Robo-call Abandonment, Record-Keeping
  - Aggressively enforced and $16,000 per call civil penalties
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
  - Enforced by FTC and state attorney generals
  - Applies to advertisement of products or services via email within the US
  - Penalties of $250 per violation (up to $6M) and 5 years in prison
- Children's Online Privacy Protection Act of 1998 (COPPA)
  - Enforced by FTC
  - Applies to commercial websites and online services directed at children under age of 13
  - Application Developers and website operators
  - Strict privacy and parental consent requirements

COZEN O'CONNOR

State Privacy Laws of the United States

- State laws offer more comprehensive protection in many instances, but are limited in application to state consumer data
  - Private or government entities to notify individuals of security breaches of information involving personally identifiable information
  - Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information)

COZEN O'CONNOR

State Privacy Laws of the United States

- In the event of a breach of security, generally require written notification to individual(s) Often what matters is where the individual resides, not where the information is stored or outsourced for storage
- States vary in:
  - the definition of what constitutes a breach
  - the definition of personal information (only a few include personal health information)
  - inclusion of a risk of harm standard
  - content requirements for notice
  - authorities that must be notified (and timing)
  - available penalties and private right of action

Note: Federal breach law proposed – might simplify notification, but only if it preempts all state laws

COZEN O'CONNOR

State Privacy Laws of the United States

Fines for Data Breaches

- State statutes contain a wide variety of enforcement mechanisms, some of which have express limits per violation or per series of similar violations.
- New York statute allows for the state Attorney General to seek injunctive relief and damages to consumers for actual costs or losses incurred, including financial losses. Further, if a court determines a business violated their data breach notification law knowingly or recklessly, the court can impose a civil penalty of up to $150,000.
- Florida caps the amount of a breach-related state-issued fine at $500,000. These are just a couple of examples of states that issue fines.
- Additionally, in many states, an attorney general's avenue of recovery is via trade or business practices laws

COZEN O'CONNOR

Co/Self-Regulatory Models

- Payment Card Industry Data Security Standard (PCI-DSS)
  - Comprehensive standards for securing cardholder data throughout transaction cycle
  - Created by major card brands and compliance is requirement through Security Standards Council
  - Issuing Banks, Merchant Bank, Processors, Merchants required to undergo periodic scans and file Reports of Compliance
  - Not a guarantee of security

- Minnesota Plastic Card Security Act
  - First state to codify the PCI standards

COZEN O'CONNOR

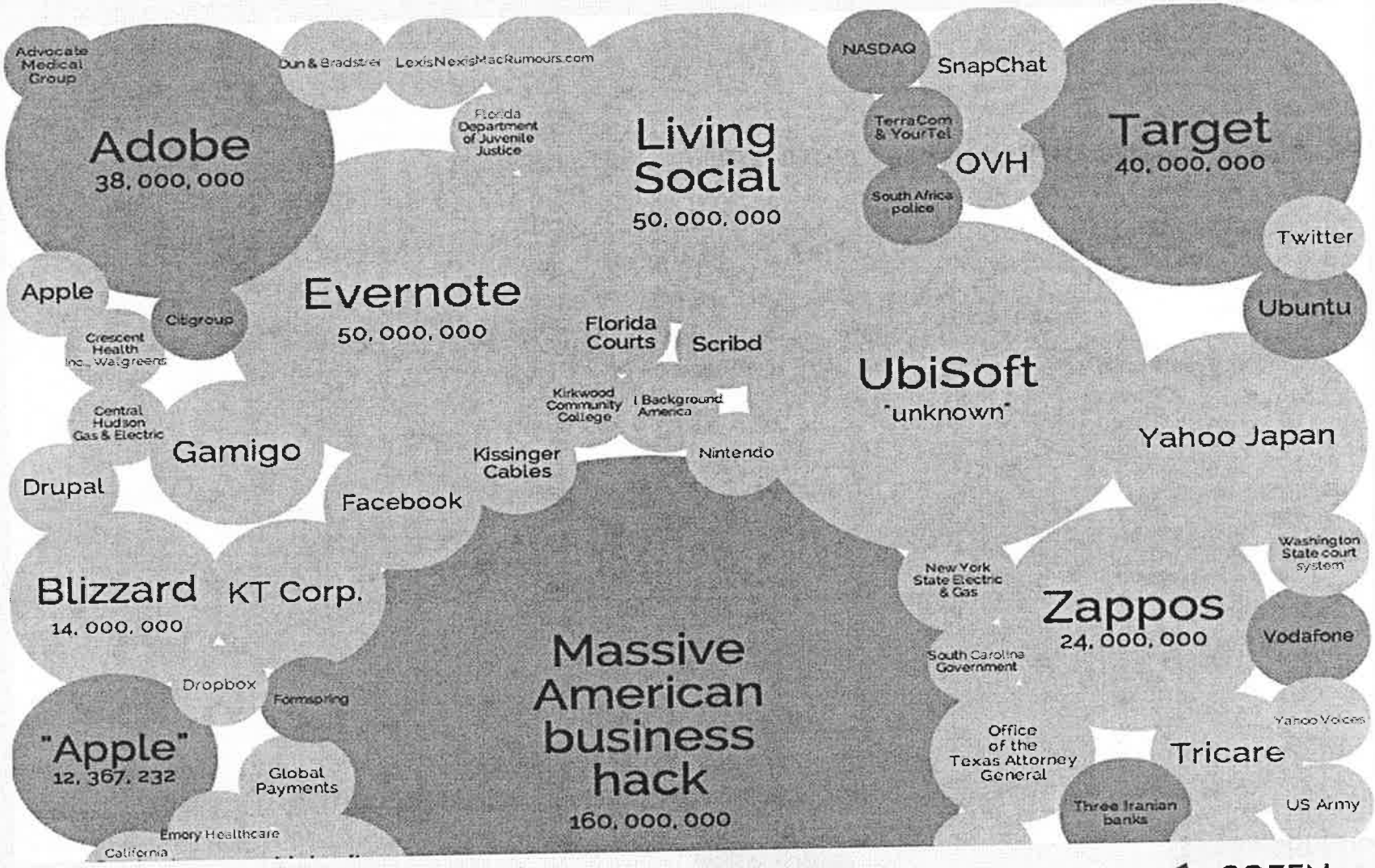
Technology Model

- Designed to reduce need for administrative measures by building safeguards into IT system

- Privacy by Design
  - Google, Yahoo, Microsoft increased automated encryption of websites and email

COZEN O'CONNOR

Data Breach Case Studies



COZEN O'CONNOR

Data Breach Case Studies

AvMed Health Plans

2009: theft of two AvMed laptops, one contained unencrypted PII and PHI for 1.2 million individuals, resulted in $3 millions in settlements and $750,000 in legal fees, was facing $1.5 million OCR fine

Playstation.

- 2011: Hackers compromised the personal data of around 77 million PlayStation users, 2.2 million credit card records - Sony estimated cost of breach at $171M
  - $15M Class Action Settlement proposed in MDL

Heartland PAYMENT SYSTEMS™

- 2008: breach exposed 130 million U.S. debit and credit cards - accrued over $140 million in breach-related expenses, including $63M in settlements with VISA and AmEx, $26M in legal fees, but less than half reportedly covered by insurance

COZEN O'CONNOR

TARGET

2013:

Potentially up to 110 million total customers affected (41 million customers' credit cards and 70 million customers' "guest" information (names, addresses, phone numbers, emails)

Timeline

- September 2013 – certified PCI DSS Compliant
- Hackers steal Fazio (HVAC vendor) credentials
- November 12, 2013 – hackers breach Target network; continue to test malware through Nov. 28
- November 30, 2013 – malware fully installed; Symantec and FireEye pick up unusual activity on Target's system

COZEN O'CONNOR

Timeline

- December 12, 2013 – DOJ alerts Target of unusual activity
- December 15, 2013 – Target confirms breach and removes malware
- December 18, 2013 – story breaks; Target notifies Aon
- December 19, 2013 – Aon notifies insurers; Target notifies public of 40 million
- January 10, 2014 – Target announces additional breach of 70 million

COZEN O'CONNOR

Cause of the Breach

- Hackers allegedly sent "phishing" email to employees of Fazio Mechanical, HVAC vendor
- Fazio uses free version of antivirus software – did not detect the intrusion
- Fazio's data connection is only for electronic billing, contract submission, and project management; gives access to Target's external billing system, Ariba
- Speculation is that access to Ariba gave hackers access to Target's internal server. Still unclear how they progressed further, but might have been a default password

COZEN O'CONNOR

JP MORGAN BREACH

- Information about 76 million households was compromised.
  - Included names, addresses, phone numbers, and e-mail of account holders.
- Breach also affected approximately 7 million small business customers.
- Attack went unnoticed for approx. two months.
- Shows how hackers can easily wreak havoc on the nations financial infrastructure.

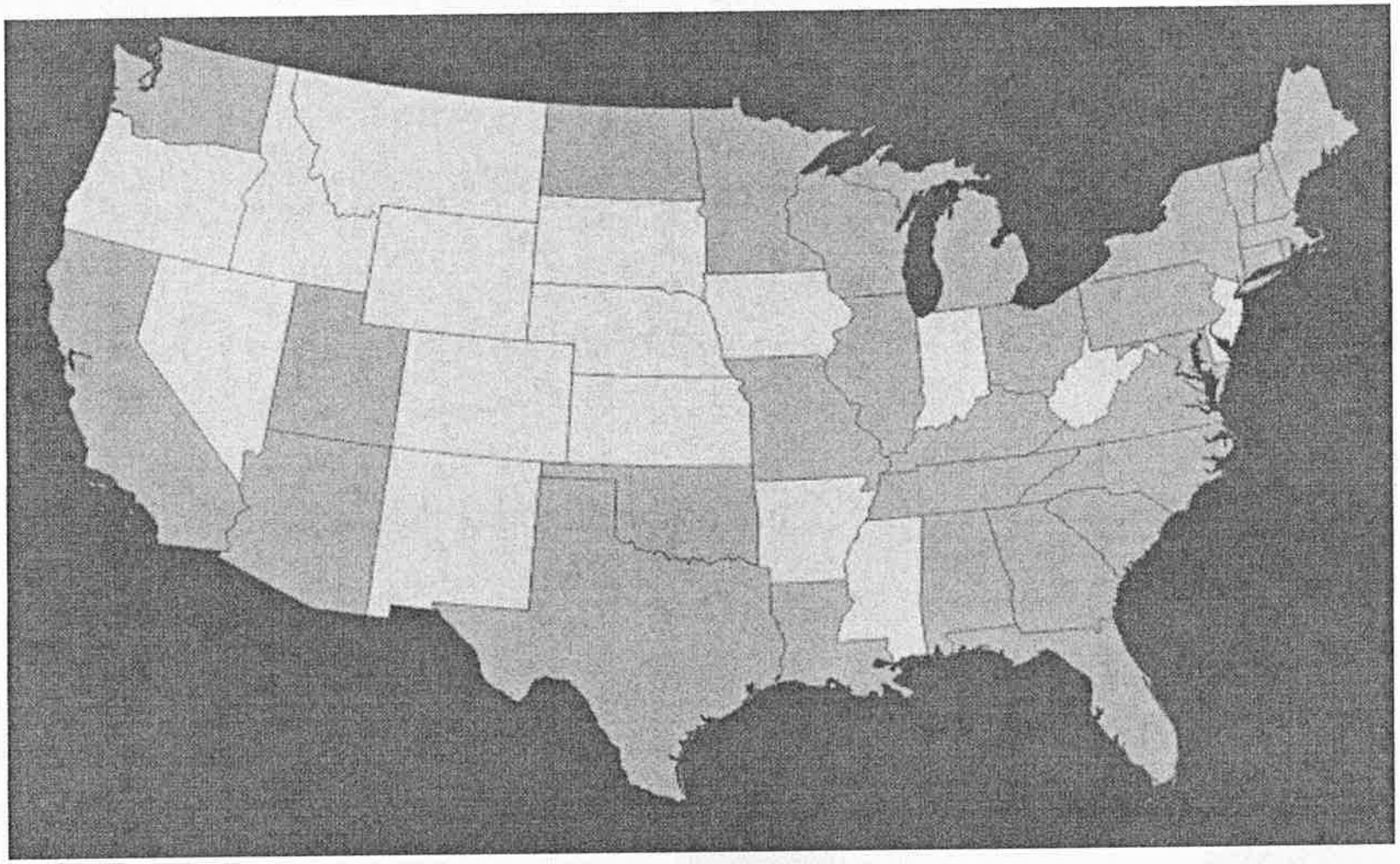
COZEN O'CONNOR

Anthem Inc. Data Breach

- Earlier this month, hackers stole databases dating back as far as 2004 from this health insurance provider.
  - Included social security numbers, addresses, e-mail addresses, health care ID numbers and birthdates of approximately 80 million consumers nationwide.
- Anthem is sending letters to all consumers who may have been affected.
  - They are also working with AllClear ID to provide identity protection and credit monitoring services to affected consumers.

COZEN O'CONNOR

Actions in 32 States



COZEN O'CONNOR

Claims and Litigation

- MDL in Minnesota – 62 Consumer Class Actions
- 10 Consumer Non-Class Actions (Small Claims or Actions Not Seeking Class Relief)
- 8 Consumer Demand Letters
- 10 Bank Class Actions
- FTC and SEC Investigation
- 41 Attorneys General Investigations
- 2.2 million have signed up for credit monitoring in U.S.; 5,000 in Canada

COZEN O'CONNOR

Legal Theories in Consumer Class Actions

- Actual losses from fraud
- State Causes of Action
  - Plastic Card Security Act, Minn. Stat. § 325E.64
  - Consumer Protections Laws of Various States
  - Data Breach Notification Laws of Various States
- Federal Causes of Action
  - Stored Communications Act, 18 U.S.C. § 2702
  - Gramm-Leach-Bliley Act, 15 U.S.C. § 6801
- Breach of Industry Standards, *i.e.*, PCI DSS
- Negligence - Common Law, Per Se, Misrepresentation, Performance of Services
- Contractual
- Unjust Enrichment
- Breach of Fiduciary Duty
- Breach of Warranty (express/implied)
- Bailment
- Conversion
- Concealment
- Invasion of Privacy

COZEN O'CONNOR

Damages Claimed in Consumer Class Actions

- Actual Loss Due to Fraud
- Consequential and Incidental Damages to Compromised Security
- Equitable, Injunctive, and Declaratory Relief
- Actual, Compensatory, and Consequential Damages
- Statutory Damages
- Restitution and Disgorgement
- Credit Monitoring Services
- Punitive
- Exemplary
- Mental Anguish
- Interest
- Attorney's Fees and Costs
- Lost Wages in Remedying Breach and Fraud
- Cost to Notarize Affidavits of Fraud

COZEN O'CONNOR

Damages Sought in Bank Actions

- Greater Proportion Allege Specific Damages
  - *E.g.*, $12/card reissued and $1,000 in known fraud losses
  - *E.g.*, the *International Bank* demand letter includes an itemized invoice totaling $549,622.49 for costs related to communications, analysis, the reissuance of debit cards, and fraud.
- Increased Communications with Customers
- Closing and/or Opening Customer Accounts
- Reissuing Credit and Debit Cards
- Absorbing Unauthorized Charges
- Lost Interest
- Lost Transaction Fees
- Administrative Expenses Associated with Monitoring and Preventing Fraud
- Statutory Damages
- Punitive or Exemplary Damages
- Attorneys Fees and Costs

COZEN O'CONNOR

Insurance Coverage

- Coverage under CGL policies remains unsettled

  ISO Form CG 00 01 04 13 (2012)) states:

  > the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury,'" which is defined to include the "offense" of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."

  - *Hartford Casualty v. Corcino & Associates*
    - Central District of California 2013
  - *Recall Total Information Management, Inc., v. Federal Insurance Company*
    - Connecticut Appellate Court 2014
  - *Zurich American Insurance Co. v. Sony Corp. of America*
    - N.Y. Sup. Ct. 2014

COZEN O'CONNOR

Insurance Coverage

ISO – CG 21 06 05 14 Exclusion May 2014

Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Limited Bodily Injury Exclusion

2. Exclusions

This insurance does not apply to:

(1) Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or

(2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

. . . . .

This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.

COZEN O'CONNOR

Insurance Coverage

- Data Breach Cyber Liability Coverage:
  - Difficulties in Underwriting due to:
    - Complexity in assessing scope of company's data assets and IT operations as sub-set of business operations
    - Varied exposures to civil suits under consumer protection laws and regulatory penalties
    - Evolving business models for IT operations and data retention/processing combined with evolving threat mechanisms
  - Difficulties in Claim adjustment due to:
    - Varied and undefined loss claims: hard costs (replacement of credit card and credit monitoring) verses (impact on consumer credit rating, loss of business continuity/reputation)

COZEN O'CONNOR

Information Security Best Practices

- Assess the IT Infrastructure, inventory data assets, address information asset management – CIO/CTO
- Risk Profile of the Safeguards:
  - Administrative Controls
    - Security Policies and Standards, Incident Response Procedures and IT Contracts
  - Technical Controls
    - Firewalls, Authentication, Encryption, Access Logs
  - Physical Controls
    - Locks, Security Cameras, Access Cards

ISO 27001 and 27002

Ultimately information security is about PEOPLE

COZEN O'CONNOR

Information Security Best Practices

Risk Assessment and Underwriting

- Collect, store or transact any personal information, or financial or health data?
- Experienced a data breach or system attack event?
- Outsource any part of computer network operations to a third-party service provider?
- Outside contractors to manage your data or network in any way?
- Partner with entities and does this alliance involve the sharing or handling of their data (or your data) or do your systems connect/touch their systems?
- Recent cyber risk assessment of security/privacy practices to ensure that they are prudent and measure up with your peers?

COZEN O'CONNOR

Information Security Best Practices

Breach Prevention

- Security measures are only as strong as the people that follow them.
- Conduct annual Risk Assessments and develop and Incident Response Plan.
- Hold an internal "Privacy Summit" to identify vulnerabilities
  - Risk, Compliance and Privacy, HR, Legal, IT, and executive management
  - Physical Security / Facilities
- Monitoring and Compliance
  - Self Assessment and Third-Party Audits
  - Follow Regulatory Updates

COZEN O'CONNOR

Information Security Best Practices

Incident Management and Data Breach Notification

- Detection and Discovery
  - Unauthorized Access, Failed-Log In, DNS, System Log Gaps, System Scans
- Containment and Analysis
  - Quarantine and partition compromised systems, Preserve for forensic assessment, maintain business continuity
- Notification
  - Determine applicable laws and manner/extent to which regulators, law enforcement, individuals, media and shareholders must be notified
- Eradication and Prevention
  - Remediate gaps in security, processes, or training

COZEN O'CONNOR

Information Security Best Practices

Incident Management and Data Breach Notification

Key Contacts and Protocols:

- Chief Privacy Officer
- Comprehensive Information Security Program
- Training, Training, Training
- Breach Service Provider, Outside Legal Counsel, and Reputational Risk Advisor
  - Specializing in Privacy Law and Breach Crisis Management

COZEN O'CONNOR

White House Guidelines for US Infrastructure Providers

Cyber Security Framework

- The Framework for Improving Critical Infrastructure Cybersecurity "enables organizations– regardless of size, degree of cybersecurity risk, or cybersecurity sophistication– to apply the principles and best-practices of risk management to improving the security and resilience of critical infrastructure" –*White House Statement*
- Gathers existing global standards and practices to help organizations manage their cyber risks, and it provides a roadmap for organizations that don't know where to start.
- Components:
  - Framework Core
    - A set of common activities that should be used in all programs, providing a high-level view of risk management.
  - Framework Implementation Tiers
    - Tiers allow users to evaluate cybersecurity implementations and manage risk. Four tiers describe the rigor of risk management and how closely it is aligned with business requirements.
  - Framework Profile
    - Help each organization align cybersecurity activities with its own business requirements, and to evaluate current risk management activities and prioritize improvements.
- Although the Framework is voluntary, regulatory agencies are working to harmonize existing regulations with the document.

COZEN O'CONNOR

White House Guidelines for US Infrastructure Providers

- **Framework Core:**
  - Set of activities to achieve specific cybersecurity outcomes.
  - The Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.
    - Identify: cybersecurity risk to systems, assets, data, and capabilities
    - Protect: develop/implement appropriate safeguards to ensure delivery of critical infrastructure services.
    - Detect: develop/implement activities to identify the occurrence of a cybersecurity event.
    - Respond: develop/implement activities to take action when an event is detected.
    - Recover: develop/implement activities to maintain plans for resilience and restore capabilities/services that were impaired as a result of an event.
  - The Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

COZEN O'CONNOR

White House Guidelines for US Infrastructure Providers

- **Framework Implementation Tiers:**
  - Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.
  - The Tiers identify the degree to which an organizations cybersecurity risk management practices comply with the Framework.
  - There are four Tiers from Partial (Tier 1) to Adaptive (Tier 4).
  - These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

COZEN O'CONNOR

White House Guidelines for US Infrastructure Providers

Framework Implementation Tiers (continued):

- **Tier 1: Partial-**
  - Risk Management- practices are not formalized, and risk is managed in an *ad hoc* or reactive manner.
  - Integrated program- limited awareness of risk and a standard approach has not been established.
  - External Participation- The organization does not have the processes in place to participate in collaboration with other entities.
- **Tier 2: Risk Informed-**
  - Risk Management- practices are approved by management but may not be established as policy.
  - Integrated Program- there is an awareness of risk at the organizational level, but as standard approach has not been established.
  - External Participation- no formalized capabilities to interact and share info externally.
- **Tier 3: Repeatable-**
  - Risk Management- practices are formally approved and expressed as policy.
  - Integrated Program- There is an organization-wide approach to manage cybersecurity risk.
  - External Participation- receives info from partners that enables collaboration and risk based management decisions within the organization.
- **Tier 4: Adaptive-**
  - Risk Management- practices actively adapt based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.
  - Integrated Program- there is an organization-wide approach to manage cybersecurity risk. That uses risk-informed policies, processes and procedures to address potential events.
  - External Participation- manages risk and actively shares info with partners to ensure accurate/current info is being distributed to improve security before an event occurs.

COZEN O'CONNOR

White House Guidelines for US Infrastructure Providers

- **Framework Profile:**
  - The alignment of standards, guidelines and practices with the Framework Core in a particular implementation scenario.
  - Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities.
  - Profiles can be used to identify opportunity for improving cybersecurity by comparing a current profile (the "as is" state of security) with a target profile (the "to be" state of security).
  - Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

COZEN O'CONNOR

White House Guidelines for US Infrastructure Providers

- The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement.

- The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program.

COZEN O'CONNOR

Contact Information

David J. Walton
1900 Market Street
Philadelphia, PA 19103
dwalton@cozen.com
215.665.5547

COZEN O'CONNOR