How Data Privacy Laws Will Change the Way You and Your Clients Do Business

September 20, 2018

9:00 a.m. – 12:00 p.m.

CBA Law Center

New Britain, CT

CT Bar Institute Inc.

CT: 2.75 CLE Credits (General)
NY: 3.0 CLE Credits (AOP)

.

Table of Contents

Lawyers' Principles of Professionalism

As a lawyer I must strive to make our system of justice work fairly and efficiently. In order to carry out that responsibility, not only will I comply with the letter and spirit of the disciplinary standards applicable to all lawyers, but I will also conduct myself in accordance with the following Principles of Professionalism when dealing with my client, opposing parties, their counsel, the courts and the general public.

Civility and courtesy are the hallmarks of professionalism and should not be equated with weakness;

I will endeavor to be courteous and civil, both in oral and in written communications;

I will not knowingly make statements of fact or of law that are untrue;

I will agree to reasonable requests for extensions of time or for waiver of procedural formalities when the legitimate interests of my client will not be adversely affected;

I will refrain from causing unreasonable delays;

I will endeavor to consult with opposing counsel before scheduling depositions and meetings and before rescheduling hearings, and I will cooperate with opposing counsel when scheduling changes are requested;

When scheduled hearings or depositions have to be canceled, I will notify opposing counsel, and if appropriate, the court (or other tribunal) as early as possible;

Before dates for hearings or trials are set, or if that is not feasible, immediately after such dates have been set, I will attempt to verify the availability of key participants and witnesses so that I can promptly notify the court (or other tribunal) and opposing counsel of any likely problem in that regard;

I will refrain from utilizing litigation or any other course of conduct to harass the opposing party;

I will refrain from engaging in excessive and abusive discovery, and I will comply with all reasonable discovery requests;

In depositions and other proceedings, and in negotiations, I will conduct myself with dignity, avoid making groundless objections and refrain from engaging I acts of rudeness or disrespect;

I will not serve motions and pleadings on the other party or counsel at such time or in such manner as will unfairly limit the other party's opportunity to respond;

In business transactions I will not quarrel over matters of form or style, but will concentrate on matters of substance and content;

I will be a vigorous and zealous advocate on behalf of my client, while recognizing, as an officer of the court, that excessive zeal may be detrimental to my client's interests as well as to the proper functioning of our system of justice;

While I must consider my client's decision concerning the objectives of the representation, I nevertheless will counsel my client that a willingness to initiate or engage in settlement discussions is consistent with zealous and effective representation;

Where consistent with my client's interests, I will communicate with opposing counsel in an effort to avoid litigation and to resolve litigation that has actually commenced;

I will withdraw voluntarily claims or defense when it becomes apparent that they do not have merit or are superfluous;

I will not file frivolous motions;

I will make every effort to agree with other counsel, as early as possible, on a voluntary exchange of information and on a plan for discovery;

I will attempt to resolve, by agreement, my objections to matters contained in my opponent's pleadings and discovery requests;

In civil matters, I will stipulate to facts as to which there is no genuine dispute;

I will endeavor to be punctual in attending court hearings, conferences, meetings and depositions;

I will at all times be candid with the court and its personnel;

I will remember that, in addition to commitment to my client's cause, my responsibilities as a lawyer include a devotion to the public good;

I will endeavor to keep myself current in the areas in which I practice and when necessary, will associate with, or refer my client to, counsel knowledgeable in another field of practice;

I will be mindful of the fact that, as a member of a self-regulating profession, it is incumbent on me to report violations by fellow lawyers as required by the Rules of Professional Conduct;

I will be mindful of the need to protect the image of the legal profession in the eyes of the public and will be so guided when considering methods and content of advertising;

I will be mindful that the law is a learned profession and that among its desirable goals are devotion to public service, improvement of administration of justice, and the contribution of uncompensated time and civic influence on behalf of those persons who cannot afford adequate legal assistance;

I will endeavor to ensure that all persons, regardless of race, age, gender, disability, national origin, religion, sexual orientation, color, or creed receive fair and equal treatment under the law, and will always conduct myself in such a way as to promote equality and justice for all.

It is understood that nothing in these Principles shall be deemed to supersede, supplement or in any way amend the Rules of Professional Conduct, alter existing standards of conduct against which lawyer conduct might be judged or become a basis for the imposition of civil liability of any kind.

--Adopted by the Connecticut Bar Association House of Delegates on June 6, 1994

How Data Privacy Laws Will Change the Way You and Your Clients Do Business

September 20, 2018

Program Agenda

9:00 a.m. – 9:15 a.m.	Introductions
9:15 a.m. – 9:50 a.m.	The European Union General Data Protection Regulation Presenter: **Dena M. Castricone**, Murtha Cullina LLP
9:50 a.m. – 10:00 a.m.	Break
10:00 a.m. – 10:50 a.m.	New and Amended State Data Breach and Consumer Privacy Laws and Regulations Presenters: **Monique Ferraro**, Munich Re/Hartford Steam Boiler Inspection and Insurance Company **Dena M. Castricone**, Murtha Cullina LLP
10:50 a.m. – 11:00 a.m.	Break
11:00 a.m. – 12:00 p.m.	What's on the Horizon Presenter: **Monique Ferraro**, Munich Re/Hartford Steam Boiler Inspection and Insurance Company
12:00 p.m.	Program Concludes

Faculty Biographies

Dena M. Castricone, Partner, Murtha Cullina
Dena M. Castricone is a Partner at the law firm of Murtha Cullina LLP. She is the Chair of the Privacy and Cybersecurity group and is a member of the Health Care and Long Term Care groups. Prior to joining Murtha Cullina, Dena served as a law clerk to the Chief Justice of the Rhode Island Supreme Court, Frank J. Williams. Dena is a Certified Information Privacy Professional (CIPP/US) and assists businesses and health care organizations with a broad range of privacy and information security matters.

Monique Ferraro, Cyber Counsel, Munich Re/Hartford Steam Boiler Inspection and Insurance Co.
Monique Ferraro provides legal and technical expertise in support of cyber efforts undertaken by Munich Re's U.S. Property & Casualty Operations. She is Counsel in the Cyber & Privacy Practice at Harford Steam Boiler Inspection and Insurance Company. Ms. Ferraro's cybersecurity and privacy experience spans more than twenty-five years in digital forensics, ediscovery, information security and privacy. Ms. Ferraro holds a master’s degree, and a JD. She is a Certified Information Systems Security Professional (CISSP), a Fellow of Information Privacy, Certified Information Privacy Professional/US (CIPP/US), and Certified Information Privacy Manager (CIPM).

MURTHA CULLINA

EU's GDPR: What Does it Mean for My Clients?

Dena M. Castricone, CIPP/US, CIPM
203-772-7767| dcastricone@murthalaw.com

September 20, 2018

GDPR

- General Data Protection Regulation

- Effective May 25, 2018

MURTHA CULLINA

History of EU Privacy Protections

- Privacy of personal data is a fundamental right in EU
  - No comparable right in the US
  - Privacy of personal information has been at the core of EU citizen's fundamental rights for more than 50 years
- EU determined that the US does not have adequate protections for personal information

MURTHA CULLINA

GDPR: What is Protected?

- Personal Data - any information that could directly or indirectly identify an individual
  - Examples
    - Name
    - Email address
    - IP address
- GDPR Art. 4(1)

MURTHA CULLINA

GDPR Scope: Within EU

- Any organization established in the EU that is processing personal data within the EU
  - Processing is defined broadly
    - Includes collecting, using, destroying or storing data

MURTHA CULLINA

GDPR Scope: Extraterritorial

- Any organization, anywhere in the world
  - Offering goods or services to anyone in the EU, regardless of cost; or
  - Monitoring behavior of someone in the EU

GDPR Scope: Extraterritorial

- Basic inquiry: are people within EU being targeted?
  - E.g. EU member state site, EU member state languages, acceptance of EU currency

MURTHA CULLINA

Examples

- A local hospital near a college campus sees a large number of exchange students in its ED each year. Some of those students are from the EU.
  - GDPR does not apply. Nothing is happening within the EU.
- The same hospital launches a campaign to be an international destination hospital for a specific surgery. It offers its website in several different languages, including those of EU member states.
  - GDPR likely applies as the hospital is now offering services to EU.

Examples

- Connecticut-based company with only local employees makes ball bearings and sells them exclusively to other businesses for use in other products that are then sold to consumers world-wide.
  - GDPR does not apply. No activities connected to the EU.
- The same company also manufactures umbrellas and makes them available for sale through its website. It advertises to EU audiences on-line and also accepts payment in a number of foreign currencies.
  - GDPR applies.

MURTHA CULLINA

Examples

- An international, non-profit membership organization promoting human rights is based in CT with a small number of employees scattered around the US. The organization generates a newsletter and holds conferences at various locations world-wide. It does not charge for membership but it does accept donations. Members who sign up provide name, address, and email address and receive regular emails about current human rights topics, a monthly newsletter and information about other organizations that share a similar mission.
- GDPR likely applies.

MURTHA CULLINA

Data Processor v. Data Controllers

- A Data Controller
  - determines the purpose and the means of processing personal data
  - There can be joint controllers
- A Data Processor
  - Processes the personal data on behalf of the controller (e.g. cloud storage company)

MURTHA CULLINA

7 Data Processing Principles

- Lawful, fair and transparent
  - Processed in accordance with law and for a legitimate reason; privacy notice provided
- Limited purpose
  - Collected for a specified, explicit and legitimate purpose and not further processed in an inconsistent manner
- Data minimization
  - Collect/use only the data necessary to carry out the purpose

MURTHA CULLINA

7 Data Processing Principles

- Accurate
- Data retention/destruction
  - Kept no longer than necessary
- Integrity
  - Ensure security, protect against unauthorized processing, loss, damage or alteration
- Accountability
  - Data controller is ultimately responsible

MURTHA CULLINA

Legitimate Bases for Processing

- Consent of the data subject
- Necessary for the performance of a contract
- Necessary to comply with a legal obligation in the EU
- Protection of vital interests of a person
- Public Interest/Official Authority
- Legitimate Interest of the controller/third party

MURTHA CULLINA

Consent

- Must be clear, unambiguous and freely given
  - Use clear and plain language
  - Opt-out or inactivity cannot be consent
  - Service cannot be conditioned on consent
  - No pre-ticked “I agree” boxes
- Data controller must be able to prove consent
- Data subject can withdraw consent at any time

MURTHA CULLINA

Data Subject Rights

- Informed
- Access
- Rectification
- Erasure
- Restrict Processing
- Portability
- Object
- Automated decision making and profiling

MURTHA CULLINA

Elements of Compliance

- Record of processing activities
- Transparent processing activities
  - Privacy notice
  - Disclose lawful bases for processing
- Process for honoring data subject rights

MURTHA CULLINA

Elements of Compliance

- Process for responding to breaches and reporting with 72 hours when required
- Privacy by Design
- Appointment of Data Protection Officer
- Requirements for international data transfers
  - Adequacy considerations
  - Binding Corporate Rules, Model Contract Clauses and E.U.- U.S. Privacy Shield

MURTHA CULLINA

Elements of Compliance

- Explicit Consent for Special Categories of Data
  - Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

MURTHA CULLINA

Penalties and Risks for Noncompliance

- Up to 10 million € or 2% of annual revenues, whichever is greater, for violation of data controller duties (accountability)
- Up to 20 million € or 4% of annual revenues, whichever is greater, for infringement on a data subject's rights, basic data protection principles, unlawful international transfers and non-compliance with DPA orders

MURTHA CULLINA

Questions?

MURTHA CULLINA

State Data Breach Laws

Monique Ferraro
Counsel Cyber Practice
The Hartford Steam Boiler Inspection and Insurance Co.

Dena M. Castricone, CIPP/US, CIPM
Chair, Privacy & Cybersecurity Group

September 20, 2018

State Data Breach Laws

- State Data Breach Laws
  - 50 different state laws
  - Varying notification timeframes and reporting obligations
  - Different definitions of personal information
  - Residency dictates applicable state law

Connecticut Law

- § 36a-701b - Breach of Computerized Data Containing Personal Information
  - Applies to electronic files, media, databases or computerized data
  - Unauthorized access to or acquisition of data containing personal information
  - Not encrypted or otherwise protected

MURTHA CULLINA

Connecticut Law

- "Personal information" means first name or first initial and last name and:
  - Social security number
  - Driver's license or state ID number
  - Account number, credit or debit card number, with security code, access code or password
  - But not publicly available info (i.e. phone book)

Connecticut Law

- Notice to consumer and AG
  - 90 days from the discovery of the breach unless
    - shorter federal timeframe applies (e.g. HIPAA)
    - or if law enforcement determines that notification would impede criminal investigation
- Identity theft prevention services for 2 years as of Oct. 1, 2018 if SSN involved
  - Had been 1 year but AG's office always insisted on 2 years

MURTHA CULLINA

Connecticut Law

- Information Security Policy
  - Policy regarding efforts to protect personal information
    - Details information you collect and efforts to protect it
  - If you follow policy and comply with notification and reporting, you will be deemed in compliance
- Failure to comply data breach statute = violation of Unfair Trade Practices Act

Connecticut Law

- § 42-471 - Safeguarding of Personal Information
  - Must safeguard all personal information in any form from theft or misuse
  - Shall destroy, erase or make unreadable prior to disposal
  - $500 per violation, up to $500,000 for any single event

Connecticut Law

- Personal Information
  - information capable of being associated with a particular individual such as an SSN, a driver's license number, a state ID card number, an account number, a credit or debit card number, a passport number, an alien registration number, a health insurance ID number or any military ID information
  - does not include publicly available information

Connecticut Law

- Safeguards for SSNs:
  - Any person who collects SSNs in the course of business shall create a privacy protection policy which shall be published or publicly displayed (such as posting on website)
  - Policy must address
    - protection of the confidentiality of SSNs
    - prohibition of unlawful disclosure of SSNs
    - limitation of access to SSNs

MURTHA CULLINA

Connecticut Law

- An Act Concerning Computer Extortion by Use of Ransomware – Eff. Oct. 1, 2017
  - the use of ransomware is a class E felony
  - up to three years of imprisonment, a fine of $3,500, or both

MURTHA CULLINA

Notable Legislation in Other States

- California Consumer Privacy Act
- Ohio Affirmative Defense
- Trend Toward Security Requirements

Federal

Economic Growth, Regulatory Relief, and Consumer Protection Act—Enacted—Effective 120 days after signing (5/24/2018)

Public Law 115-174

Part of the roll back of Dodd-Frank, this Act requires a consumer reporting agency to provide a consumer with free credit freezes and to notify a consumer of their availability. A number of states have passed or are considering similar measures and some state laws provide greater consumer protection than that provided in this federal law. At this time, the extent to which the federal law preempts state laws with respect to credit freeze provisions is unsettled. (Available online at: https://www.congress.gov/bill/115th-congress/senate-bill/2155?q=%7B%22search%22%3A%5B%22Economic+Growth%2C+Regulatory+R

Consumer Information Notification Requirement Act

Rep. Luetkemeyer introduced the Consumer Information Notification Requirement Act. The bill would amend GLBA to include data breach notification in the event of unauthorized access to PII "that is reasonably likely to result in identity theft, fraud, or economic loss." (Online at: https://www.congress.gov/bill/115th-congress/house-bill/6743/text?q=%7B%22search%22%3A%5B%22Consumer+Information+Notification+Requirement+Act%22%5D%7D&r=1)

States

Alabama

Data Breach Bill

Alabama became the 50th state to have a data breach notification law that went into effect June 1, 2018. The Act requires notification of a breach within 45 days to affected individuals and includes a safe harbor for encrypted information. Covered entities must designate "an employee or employees to coordinate" data security measures, implement and maintain "reasonable security measures" to protect personal information in the event of a breach, and keep management informed of its security measures. (Online at: http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2018rs/PrintFiles/SB318-enr.pdf)

Arizona

Arizona Enacts Stricter Data Breach and Cybersecurity Law—Enacted—Effective 4/11/2018

Arizona recently enacted provisions relating to data security breaches by expanding the definition of personal information and security breach. Personal information would include biometric data and online account logins when the password or access key is also accessed or acquired. A security breach would

consist of either acquiring personal information or accessing it in such a way as to compromise the security or confidentiality of the data. The new provisions revise notification requirements and relate to enforcement and civil penalties for security system breaches. The new law also establishes notification requirements for a breach involving personal information and for an online account that does not involved personal information.

(Available online at:
https://custom.statenet.com/pciaa_textonly/resources.cgi?id=ID:BILL:AZ2018000H2154&md5=0764ca37db8a1eeae9b8d187a6474955)

California

Consumer Privacy Act- Enacted—Effective 1/1/2019

In order to stave off a ballot initiative that opponents believed would have been successful and would result in a limited ability to modify the law's requirements, California has enacted a law that contains many of the same requirements of the European Union's recently enacted General Data Protection Regulation.

The new law applies to "businesses" that collect or process consumers' personal information, and do business in the State of California, and that satisfy one or more of the following thresholds: Has annual gross revenues in excess of twenty-five million ($25,000,000); Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices, or; Derives 50 percent or more of its annual revenues from selling consumers' personal information.

Beginning January 1, 2020, the state will recognize the rights of consumers to request businesses to disclose the categories and specific pieces of personal information that they collect about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared. The law requires a business to make disclosures about the information and the purposes for which it is used, grants a consumer the right to request deletion of personal information and requires the business to delete upon receipt of a verified request. The new law grants a consumer a right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, to disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed. The law requires a business to provide this information in response to a verifiable consumer request.

Under the new law, a consumer must be provided with the option to opt out of the sale of personal information by a business and prohibits the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data. The law authorizes businesses to offer financial incentives for collection of personal information. Business are prohibited from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized, to be referred to as the right to opt in.

The law will be enforced by the Attorney General, and provides for a private right of action in connection with specified security breaches, certain unauthorized access, destruction, use, modification, or disclosure of a consumer's personal information. (Online at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375)

Colorado

Amended Data Breach Law- Enacted, Effective 9/1/2018

Colorado amended its data breach notification law. The new law requires covered and governmental entities in Colorado that maintain paper or electronic records that contain personal identifying information to develop and maintain a written policy for the destruction and proper disposal of those documents. Entities that maintain, own, or license personal information, including those that use a nonaffiliated third party as a service provider, must implement and maintain reasonable security procedures for the personal information. The notification laws governing disclosure of unauthorized acquisitions of unencrypted and encrypted computerized data are expanded to specify who must be notified following such unauthorized acquisition and what must be included in such notification. (Available online at: https://custom.statenet.com/pciaa_textonly/resources.cgi?id=ID:BILL:CO2018000H1128&md5=a5ee890205c72d1484a3b1148eb78f84)

Connecticut

24 Months Credit Monitoring Required Following Breach

Connecticut enacted new legislation to extend the period entities must provide identity restoration services to individuals affected by a breach involving social security numbers. (Online at: https://www.cga.ct.gov/2018/SUM/pdf/2018SUM00090-R02SB-00472-SUM.pdf)

Louisiana

Data Breach Law Amended, Reasonable Security Required, Reduces Costs of Substitute Notice- Enacted, Effective 8/1/2018

This Act requires any person that conducts business in Louisiana or owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, as defined, to (i) implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure; and, (ii) take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means. Notifications of security breaches must be made within 60 days. (Available online here: https://custom.statenet.com/pciaa_textonly/resources.cgi?id=ID:BILL:LA2018000S361&md5=7ca805e48dd70c6c0b790932177e2410)

Nebraska

Reasonable Security Required

Nebraska's governor signed an amendment to the state's data breach law requiring that individuals and commercial entities that conduct business in the state and that owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska is required to implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information. Covered entities that comply with Gramm-Leach-Bliley or similar data protection law are considered to be in compliance with the security requirement. (Available online at: https://custom.statenet.com/pciaa_textonly/resources.cgi?mode=show_text&id=ID:BILL:NE2017000L757&verid=NE2017000L757_20180228_0_ESL&md5=d015152915c6398c0c0e3e9266335486)

Ohio- Enacted

Data Security Safe Harbor

Ohio enacted the Safe Harbor for Companies that Implement Cybersecurity Framework. The Act provides an affirmative defense in civil law suits for data breach if the company implements one of the cybersecurity frameworks, such as NIST or CSC. (Available online here: https://www.huntonprivacyblog.com/wp-_)

Oregon

Tighter Data Breach Notification Requirements—Enacted-- Effective the 91st day after the date on which the 2018 regular session of the Seventy-ninth Legislative Assembly adjourns sine die

This Act modifies the Oregon Consumer Identity Theft Protection Act. A consumer reporting agency may not charge consumers a fee to place, remove, or temporarily lift a security freeze. The person with the duty to give notice of a breach is the person who owns, licenses, or otherwise possesses personal information that was breached. Notice of a breach must be given in most expeditious manner, but no later than 45 days of discovery or notification of breach. No person giving notice of breach may require a consumer to provide credit or debit card information or accept other for-fee services as a condition of accepting free credit monitoring or identity theft prevention and mitigation services. Additional services may be offered for a fee if the person notifies consumer separately, distinctly, clearly, and conspicuously that the offer is for paid services. (Available online at: https://olis.leg.state.or.us/liz/2018R1/Downloads/MeasureDocument/SB1551)

South Carolina

NAIC Cybersecurity Model Law—Enacted—Effective 1/1/2019-- Vendor Due Process and Security Requirements Delayed Implementation to 7/1/2019 & 7/1/2020

South Carolina's legislature passed a bill adopting the NAIC Cybersecurity Model Law. (Available online at: https://custom.statenet.com/pciaa_textonly/resources.cgi?mode=show_text&id=ID:BILL:SC2017000H4655&verid=SC2017000H4655_20180503_0_EF&md5=0461a3550d5cceacf8e4bb7b2ae1394d)

South Dakota

Data Breach Bill

South Dakota enacted a data breach notification law, becoming the forty-ninth state to have one. (Available online at:

https://custom.statenet.com/pciaa_textonly/resources.cgi?id=ID:BILL:SD2018000S62&md5=5b12824282c668cd38eb82ba2ecea564)

Vermont

Data Brokers and Personal Consumer Information- Enacted, Effective 1/1/2019

The new law requires data brokers to adopt an information security program with administrative, technical, and physical safeguards to protect sensitive personal information. The measure amends provisions of the Vermont statutes by adding new definitions, requiring an annual registration of data brokers, prohibiting the acquisition of personal information with intent to commit wrongful acts, and requiring a report studying these issues by the Attorney General. Finally, the new law prohibits credit reporting companies from charging fees for placing or removing a security freeze. (https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf)

What Insurance Executives and Board Members Need to Know About Developing a Cybersecurity Program

Hartford Steam Boiler

September 20, 2018

Risk Solutions

Munich RE

Agenda

Hartford Steam Boiler

Munich RE

- What's my motivation?
- Elements of an insurer's cybersecurity program

Cyber Compliance – Your Motivation

Hartford Steam Boiler

Munich RE

- NY DFS CRR500
- NAIC
- State laws
- Supply chain pressure
- Public pressure
- It’s the right thing to do

Elements of a Cybersecurity Program

Hartford Steam Boiler

Munich RE

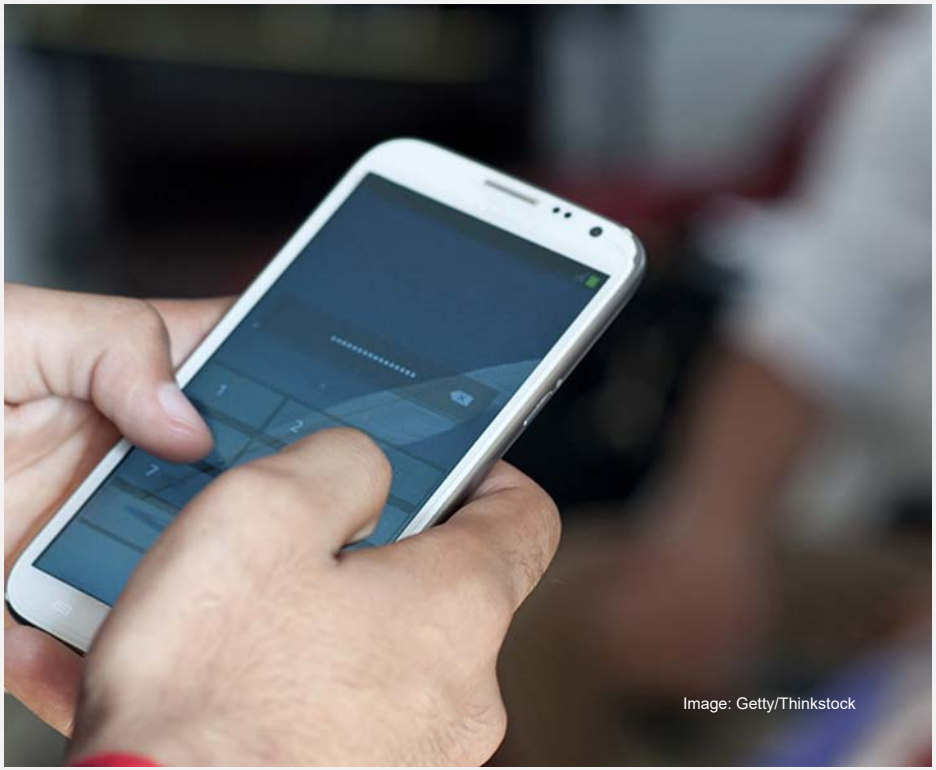
Two components:

- Executive Commitment
- Relevant Capabilities

Executive Commitment- Executive Committee

- Needs to understand the threat/risks
  - Designate primary
  - Regular briefings by CISO/CPO
- Act with a sense of urgency and take cybersecurity seriously
  - Attend training
  - Commit to investment in cybersecurity
- Act as an example

Relevant Capabilities



- Policies
- Controls
  - Technical
  - Human Behavior
- Risk Assessment
- Incident Response Plan
- Vendor Management Due Diligence

Policies

Hartford Steam Boiler

Munich RE

- Policies consistent with standards/frameworks
  - NIST, CSC, ISO 27001
- Select one or more standards to try to attain
- Policy templates

Controls

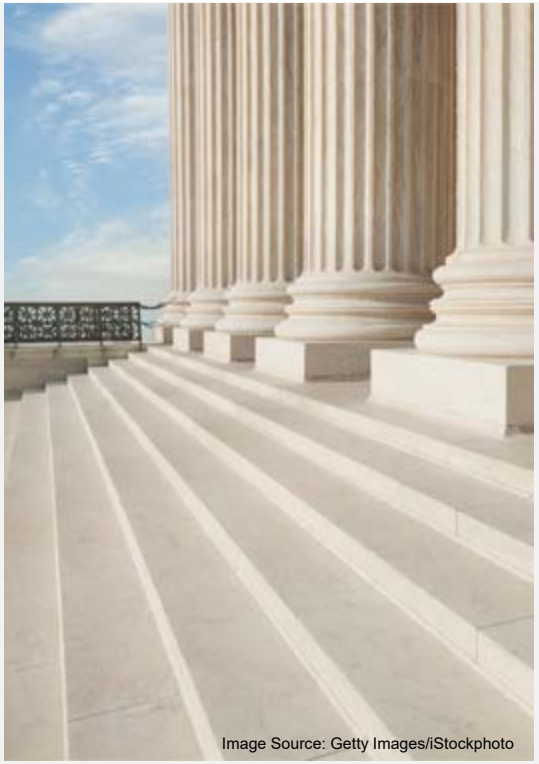


Image Source: Getty Images/iStockphoto

Determine how you will achieve compliance with policies

- Technical-
  - Intrusion Detection Program, Firewall, Behavioral Analytics, how much do you have to spend and what do you want to spend it on?
- Human-
  - So much more than signing off on the employee handbook

The Weakest Link

- Internal risks remain the greatest threat
  - Increased focus on sophisticated social engineering
  - Business email compromise, spear phishing delivery mechanisms for fraudulent funds transfer and ransomware

- Train, reinforce, train, reinforce
  - Classroom, online, newsletters, posters, phish your own people and provide feedback
  - PLENTY of free resources

Training, reinforce, training, reinforce

PLENTY of free resources

Annual Risk Assessments

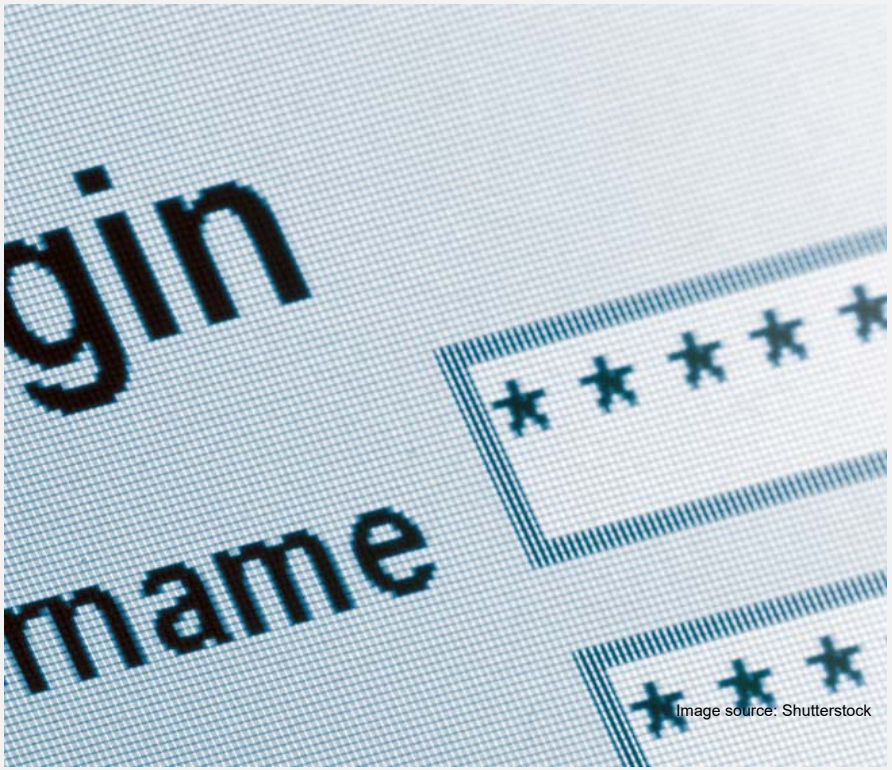


Image source: Shutterstock

- Internal self-assessments
  - Questionnaires
  - Penetration testing
  - Table top exercises
- External penetration testing
- IT security audit

Incident Response Plan

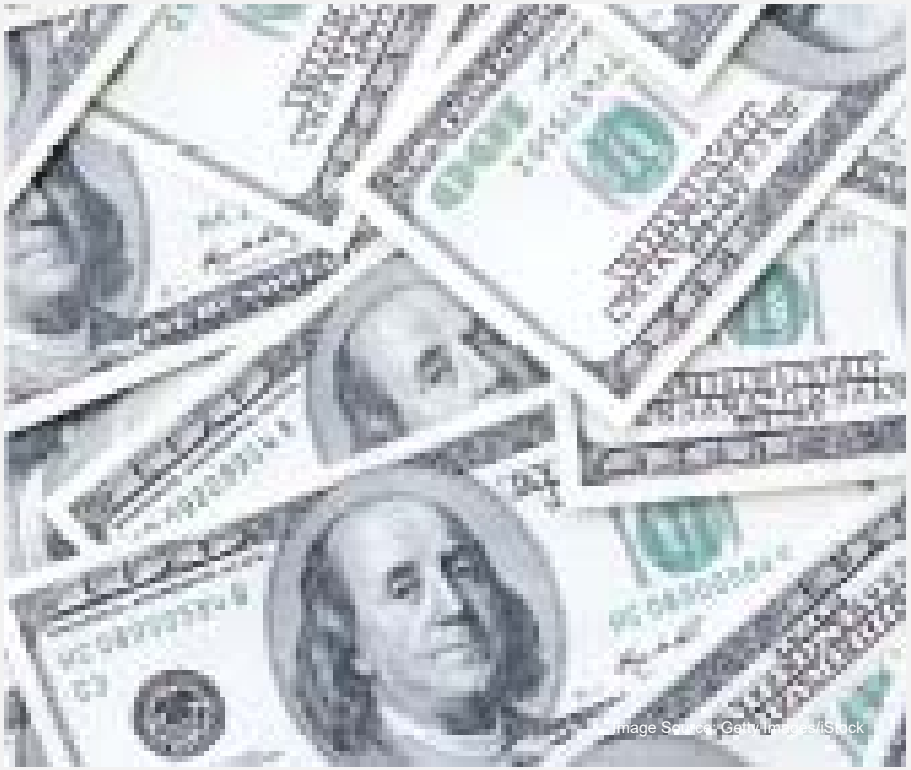
Have a team in place

- Internal team (risk management, human resources, legal, IT)
- Digital forensics investigation and response
- Breach coach
- Cyber insurer
- Public relations, notification provider, credit monitoring (insurer/coach)

Practice, practice, practice your plan

- Table top exercises
- Update policies following exercises and events

Vendor Risk Management



- Due diligence includes assessing cybersecurity and data protection
- May need to review existing contracts to ensure compliance
- Address cybersecurity in vendor contracts moving forward
- Data OWNER (that's YOU) retains responsibility for breach notification and your company's reputation is impacted by breach
- Affirmatively address responsibilities, who pays for what and cyber insurance requirements in contracts

Questions?

Hartford Steam Boiler

Munich RE

Thank you!

Monique_Ferraro@hsb.com 860 493 1056

Hartford Steam Boiler

Munich RE

Questions?