Cybersecurity Compliance – Are You Accidentally Breaking the Law?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Disclaimer

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Learning Objectives

At the end of this session, you will be able to:

- Identify risks of cybersecurity breaches
- Discuss the current state of cybersecurity compliance and oversight
- List common mistakes companies make that create security weaknesses
- Recognize the legal and regulatory implications of a cyber incident
- Identify various cyber security regulations applicable to your company/industry
- Determine what your company needs to do to ensure they comply with any applicable regulations

Introductions

Heather Bearfield, Principal
CLA

Frank Rudewicz, Principal
CLA

David Sun, Principal
CLA

Christopher Luise, Co-CEO
ADNET Technologies

Rob Fitzgerald, Managing Partner
Arcas Risk Management

Current Cyber Threat Landscape

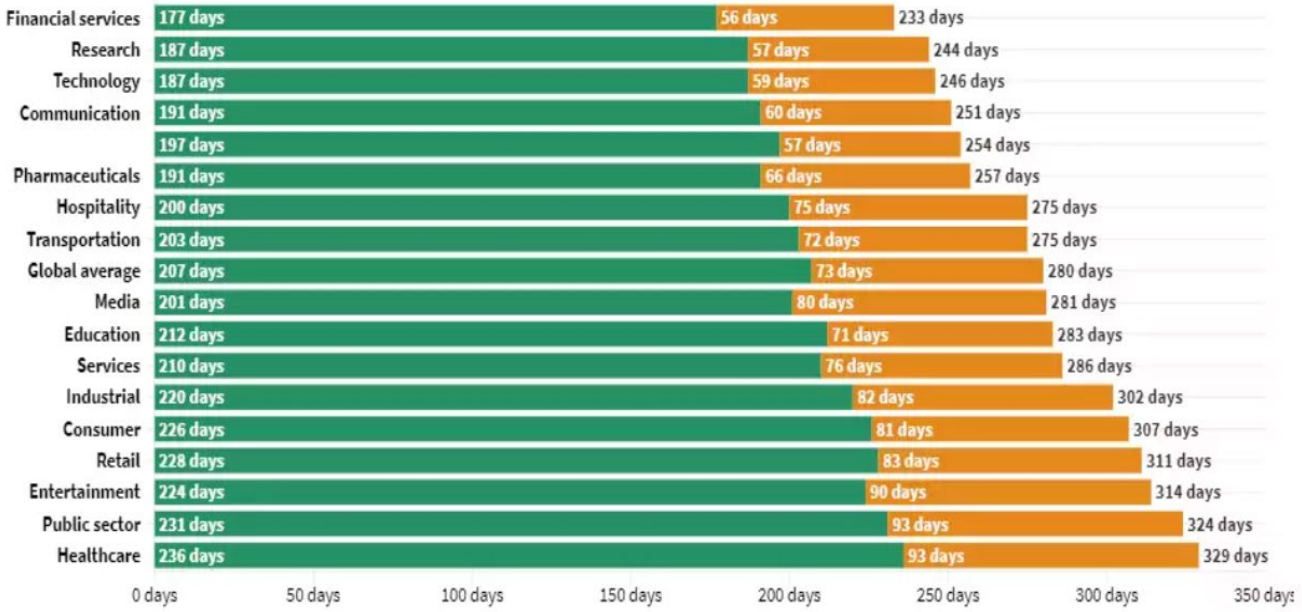
- As a result of the pandemic and the rush to remote work, we have seen a significant increase in security incidents.
- Hackers (both individuals and nation state) recognize continue to exploit weaknesses in cybersecurity systems and practices.
- Supply chain and vendors (Vendor Risk Management) has become a focus.

By the Numbers

A Recent Global study on the Cost of a Data Breach conducted by Ponemon Institute and IBM Security noted:

- $8.64m – Average cost of a data breach in the United States
- 80% - Share of breaches that included records containing customer Personally Identifiable Information (PII), at an average cost of $150 per record
- $2.35m – Average global total cost of a breach for organizations under 500 employees; $5.52m at enterprises over 25K employees

The Number of Days to Identify & Contain Breach



- Average is around 275 days to detect a breach and then contain the attack. 200 days to detect, 75 days to contain.

Behind the Statistics

Hackers can do a lot in and to your network in 191 days

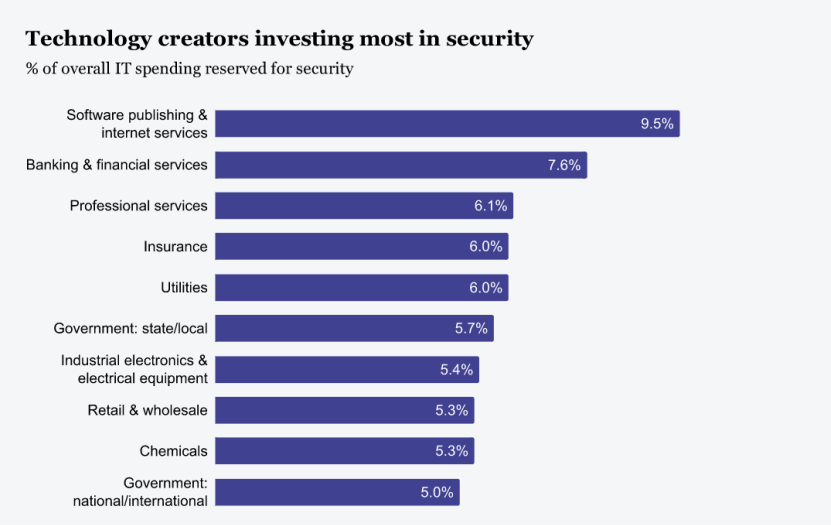
- Learn everything about your business
- Find you crown jewels and take them
- Disable backups and security systems
- Create numerous back doors

Labeling ransomware as the top threat creates a false narrative

- Ransomware is usually coupled with other acts and just the most visible part of the attack
- These days, ransomware coupled with data exfiltration
- Resuming operations is just the first step
- Legal and business ramifications of a data breach can persist

The Problem

- Implementing appropriate cybersecurity measures is costly and inconvenient.
- Businesses want to avoid reputational damage from a data breach leading them to keep things quiet.
- Individuals are kept in the dark that their data has been compromised.



Samantha Ann Schwartz/Cybersecurity Dive, data from Gartner

The Goal for Cyber Regulations

- **Cyber regulations come with two general objectives:**
  - Pre-Breach: Force businesses to spend money to implement protocols to reduce the likelihood of a breach
  - Post-Breach: Require business to notify impacted individuals of potential damages as a result of a breach
  - Some regulations focus on pre-breach, some on post-breach and others cover both
  - Regulations can apply based on geography or industry

Pre-Breach Cyber Regulation Examples

- **California Consumer Privacy Act ("CCPA")**
  - Extended consumer privacy protections to the internet. CCPA is the most comprehensive internet-focused data privacy legislation in the US, and with no equivalent at the federal level.

State Comprehensive-Privacy Law Comparison

Bills introduced 2021

State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Consumer Rights: Right of Access	Right of Rectification	Right of Deletion	Right of Restriction	Right of Portability	Right of Opt-Out	Right Against Automated Decision Making	Private Right of Action (s = security only)	Business Obligations: Opt-in requirement age	Notice/Transparency Requirement	Risk Assessments	Prohibition on Discrimination (exercising rights)	Purpose/Processing Limitation
LAWS PASSED (TO DATE)																
California		CCPA	**California Consumer Privacy Act (2018; effective Jan. 1, 2020)**	x		x			x	x	L	16	x			x
California [1]		Proposition 24	**California Privacy Rights Act (2020; effective Jan. 1, 2023)**	x	x	x	x	x	x	x	L	16	x	x	x	x
Virginia		SB 1392	***Consumer Data Protection Act**	x	x	x			x	x		13	x	x	x	x
ACTIVE BILLS																
Alabama		HB 216	Alabama Consumer Privacy Act	x		x			x	x		18	x		x	x
Alaska		SB 116	Consumer Data Privacy Act	x		x			x	x		18	x		x	x
Colorado		SB 190		x	x	x			x	x		s	x	x	x	x
Connecticut		SB 893		x	x	x			x	x			x	x	x	x
Illinois		HB 3910	Consumer Privacy Act	x		x			x	x		18	x	x	x	x
Massachusetts		SD 1726	Massachusetts Information Privacy Act	x	x	x	x	x	in	x	x	all	x		x	x
Minnesota		HF 1492	Minnesota Consumer Data Privacy Act	x	x	x			x	x	x	s	x	x	x	x
Minnesota		HF 36		x		x			x	x	x	x	x		x	
New Jersey		ab 3283	New Jersey Disclosure and Accountability Transparency Act	x	x	x	x	x	in	x		all	x			x
New Jersey		ab 3255		x		x			x	in		all	x		x	x
New York		A 680	New York Privacy Act	x	x	x	x	x	x	x	x		x			x
New York		A 6042	Digital Fairness Act	x		x			x	in	x	x	all	x	a	x	x
New York		SB 567		x			x		x		x	x	x		x	
Texas		HB 3741		x	x	x			x				x			x

In Session: all above states

Introduced > In Committee > Crossed Chamber > Cross Committee > Passed > Signed

Bold - passed law

~~Strikethrough - bill died in committee or postponed~~

* Continued to 2021 Special Session

L - private right of action for security violations only
in - opt-in consent requirement
p - prohibition without consent
u - unclear
s - opt-in requirement for all sensitive data
a - risk assesment limited to impact of automated decisions

[1] California Privacy Rights Act's right of restriction/limitation is only applicable to sensitive personal data

Legislative Process: Introduced > In Committee > Crossed Chamber > Cross Committee > Passed > Signed

Further information and most recent version of the IAPP's US State Comprehensive Privacy Law Comparison can be found here.

Pre-Breach Cyber Regulation Examples

Depending on your industry, you may be required to implement various protocols, "just as a price of admission".

- Health Insurance Portability and Accountability Act ("HIPAA")
- Department of Defense- Cybersecurity Maturity Model Certification ("CMMC")
- Cybersecurity Requirements for Financial Services Companies ("23 CRR-NY 500.0")

Post-Breach Cyber Regulation Examples

- **All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification**
- **Security breach laws typically have provisions regarding**
  - Who must comply with the law
  - Definitions of “personal information”
  - What constitutes a breach
  - Requirements for notice
  - Exemptions

Post-Breach Cyber Regulation Examples

The most common trends in legislation this year include proposals that would:

- Establish or shorten the time frame within which an entity must report a breach.
- Require state or local government entities to report data breaches.
- Provide an affirmative defense for entities that had reasonable security practices in place at the time of a breach.
- Expand definitions of "personal information“
- Require private sector entities to report breaches to the state attorney general or other state entity.

Post Breach Cyber Regulation Penalties

- Equifax: (At least) $575 Million
- Home Depot: ~$200 million
- Uber: $148 million- (also- Executive Under Federal Indictment)
- Yahoo: $85 million
- Capital One: $80 million
- Morgan Stanley: $60 million
- British Airways: $26.2 million
- Marriott International: $23.7 million
- Target: $18.5 million

Beyond Regulations- What Your Clients are Worried About

- **Clients are requiring vendors to meet standards**
- **Data Integrity**
  - Intellectual Property Protection
- **Regulatory Compliance**
- **Brand Protection**
  - Public Perception
  - Media Awareness
- **Customer Protection**
- **Legal Liability**

How to Determine if You Comply

- 2 Types of Compliance: Regulatory & Contractual
- Lack of Security Program
- Cybersecurity Program is AS important as ERP, HR, Financials
- Desire to “Do it All” in-house
- Expensive tools != Processes
- Topic discussing the common causes/drivers for non-compliance and control gaps that we see in industry that led to the scary scenario in the first place.

SOC 2 vs. ISO 27001

SOC 2 is focused mostly on proving the security controls that protect customer data have been implemented.

Based on AICPA attestation SSAE-18 standard

ISO 27001 (international standard) wants to confirm there are operational Information Security Management System (ISMS) in place to manage your InfoSec program on an ongoing basis.

Primarily focuses on preserving the confidentiality, integrity, and availability of information as part of the risk management process

This adds additional controls around proving the management system is in place and regularly reviewed for conformity to the ISO27001 standard

Trust Service Criteria Mapping

- ISO 27001
- NIST CSF
- COBIT5
- NIST 800-53
- GDPR
- CMMC

AICPA

2017 Trust Services Criteria (TSC)						
TSC Ref.	Criteria	Points of Focus	ISO Ref.	ISO 27001 Requirement	ISO Appendix Ref.	ISO Appendix Title
	CONTROL ENVIRONMENT					
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		5.1	**Leadership and Commitment** Top management shall demonstrate leadership and commitment with respect to the information security management system		
		Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.				
		Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.			A.7.2.2	**Information Security awareness, education and training** All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
		Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.				
		Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.			A.7.2.3	**Disciplinary process** There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
		Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.			A.7.2.1	**Management responsibilities** Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

How to Remediate if you Aren't in Compliance

1	2	3	4
Assess your environment for gaps between current and required state	**Create a plan to address gaps** – recognize it's a journey; most compliance schemes change	**Implement the plan** and remediate gaps	**Re-assess** on a regular basis

Questions

We're Here For You

Find additional resources and learn about upcoming events at CLAconnect.com.

Improving your financial health starts with an honest check-in.

Our guidance can help organizations and individuals stay on the right track.

Learn More

Thank you!

Heather Bearfield
Heather.Bearfield@claconnect.com

Rob Fitzgerald
Rfitzgerald@arcasrisk.com

Frank Rudewicz
Frank.Rudewicz@claconnect.com

Chris Luise
Cluise@thinkadnet.com

David Sun
David.Sun@claconnect.com

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING