
Morgan Lewis
CYBER INSURANCE:
IS YOUR COMPANY COVERED?
Mark L. Krotoski and Jeffrey S. Raskin
March 12, 2019
© 2019 Morgan, Lewis & Bockius LLP

Overview

- Current Threat Environment
  - Increasing Cyber Threats
  - Significant Costs and Consequences
  - Heightened Regulatory Enforcement
- Notification Issues
- When a Data Breach Occurs
- Cyber Insurance Coverage Issues

INCREASING CYBER THREATS

Cyber Threat Environment

Many Actors

- Organized cyber crime
  - Division of labor
  - International hacking groups
  - Hackers for hire
- State-sponsored actors
- Cyber terrorists
- Hacktivists
- Insider threat
- Third-party vendor attacks
- Inadvertence

Cyber Threat Environment

Many Actors

- Organized cyber crime
  - Division of labor
  - International hacking groups
  - Hackers for hire
- State-sponsored actors
- Cyber terrorists
- Hacktivists
- Insider threat
- Third-party vendor attacks
- Inadvertence

Variety of Methods

- More targeted attacks
- Greater sophistication
- Exploiting vulnerabilities
- Zero-day exploits
- Malware variations
  - Destructive
  - Capture credentials
  - Data exfiltration

Business Email Compromise

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number
I-071218-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

DEFINITION

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018:**

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	$12,536,948,299

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the IC3 from **October 2013 to May 2018:**

Total U.S. victims:	41,058
Total U.S. victims:	$2,935,161,457
Total non-U.S. victims:	2,565
Total non-U.S. exposed dollar loss:	$671,915,009

The following BEC/EAC statistics were reported by victims via the financial transaction component of the IC3 complaint form, which became available in June 2016[3]. The following statistics were reported in victim complaints to the IC3 from **June 2016 to May 2018:**

Total U.S. financial recipients:	19,335
Total U.S. financial recipients:	$1,629,975,562
Total non-U.S. financial recipients:	11,452
Total non-U.S. financial recipients exposed dollar loss:	$1,690,788,278

https://www.ic3.gov/media/2018/180712.aspx

Spear Phishing Attacks

- Target particular users to entice them into opening an attachment or clicking on a link that launches malware on the system

- Nearly "80% of all espionage-motivated attacks used either a link or attachment in a phishing email to gain access to their victim's environment"

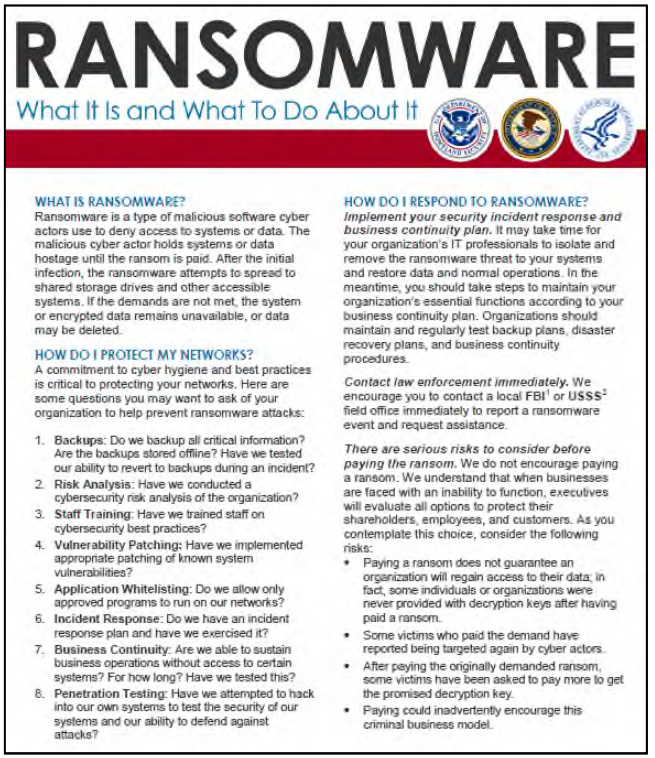
http://www.verizonenterprise.com/DBIR/2014/
http://www.mcafee.com/us/resources/reports/rp-phishing-quiz-assessment.pdf?snspd-0115

Payment?

"We do not encourage paying a ransom.

As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model."



RANSOMWARE

What It Is and What To Do About It

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

HOW DO I RESPOND TO RANSOMWARE?

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact a local FBI[1] or USSS[2] field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

Second Ransomware Demand

- Hackers "locked up the files, refusing to give back access unless the hospital paid up."
- "I'm not at liberty because it's an ongoing investigation, to say the actual exact amount. A small amount was made," the hospital president said.
- After payment, "the hackers didn't return full access to the files" and "**demanded another ransom**."
- "The hospital says, it will not pay again."

KWCH12 expect more

Weather | Sports | Station Info | Catch it Kansas | Livestream

Home / Crime / Article

Hackers demand ransom payment from Kansas Heart Hospital for files

By Deedee Sun | Posted: Fri 10:04 PM, May 20, 2016 | Updated: Fri 10:37 PM, May 20, 2016

WICHITA, Kan. A hospital held hostage by hackers and denied access to its files until it pays a ransom. It's a crime that's been reported across the country, and now it's happened in Wichita.

It's called "ransomware" - hackers hijack your computer and hold the data until you pay up.

The Kansas Heart Hospital is the latest victim of this attack.

The hospital's president, Dr. Greg Duick, says the hackers never got access to patient information, but the attack did cause problems.

"Kansas Heart Hospital had a cyber attack occur late Wednesday evening," Duick said. "We suspect, as attacks other parts of the country, this was an offshore operation," he said.

Duick says hackers holding hospital files hostage is very common.

"Upwards of 45% of hospitals have received some kind of cyber attack. And multiple hospitals had additional attacks," he said.

About 9pm Wednesday, a hospital employee lost access to files.

http://www.kwch.com/content/news/Hackers-demand-ransom-payment-from-Kansas-Heart-Hospital-380342701.html

Passwords

1. **123456 [Unchanged]**
2. **password [Unchanged]**
3. **123456789 [Up 3]**
4. **12345678 [Down 1]**
5. **12345 [Unchanged]**
6. **111111 [New]**
7. **1234567 [Up 1]**
8. **sunshine [New]**
9. **qwerty [Down 5]**
10. **iloveyou [Unchanged]**
11. **princess [New]**
12. **admin [Down 1]**
13. **welcome [Down 1]**
14. **666666 [New]**
15. **abc123 [Unchanged]**

SplashData's Top 100 Worst Passwords of 2018

by JOHN HALL

LOS GATOS, CA (DECEMBER 13, 2018) – Bad habits die hard, according to SplashData's eighth annual list of Worst Passwords of the Year. After evaluating more than 5 million passwords leaked on the Internet, the company found that computer users continue using the same predictable, easily guessable passwords. Using these passwords will put anyone at substantial risk of being hacked and having their identities stolen.

Type he

RECENT POSTS

https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/

Protecting Passwords

- **Brute Force Attack**
  - Computer program using password combinations
  - "123456"
- **Dictionary Attack**
  - Computer program using common words
- **Key Logger Attack**
  - Computer program to track keystrokes
- **Same Password Multiple Accounts**
  - Providing access to secure areas
- **Inadvertence**
  - Post-it or written down

Password Access

"qwerty"

North Korean Government

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS

National Press Releases

Home • News • Press Room • Press Releases • Update on Sony Investigation

Twitter (3,816) Facebook (3,008) Share

Update on Sony Investigation

Washington, D.C.
December 19, 2014

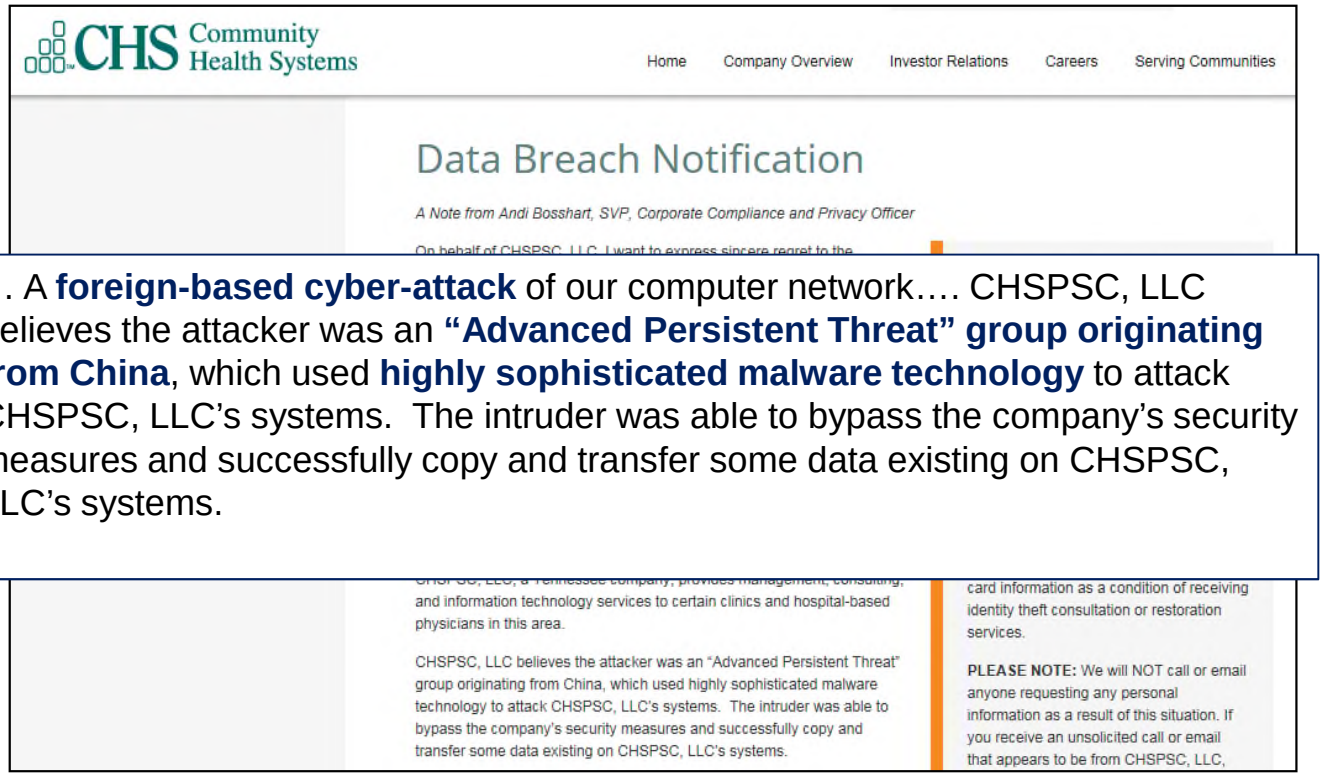
FBI National Press Office
(202) 324-3691

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the "Guardians of Peace" claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE's network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations.

http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

Foreign-Based Cyber Attacks

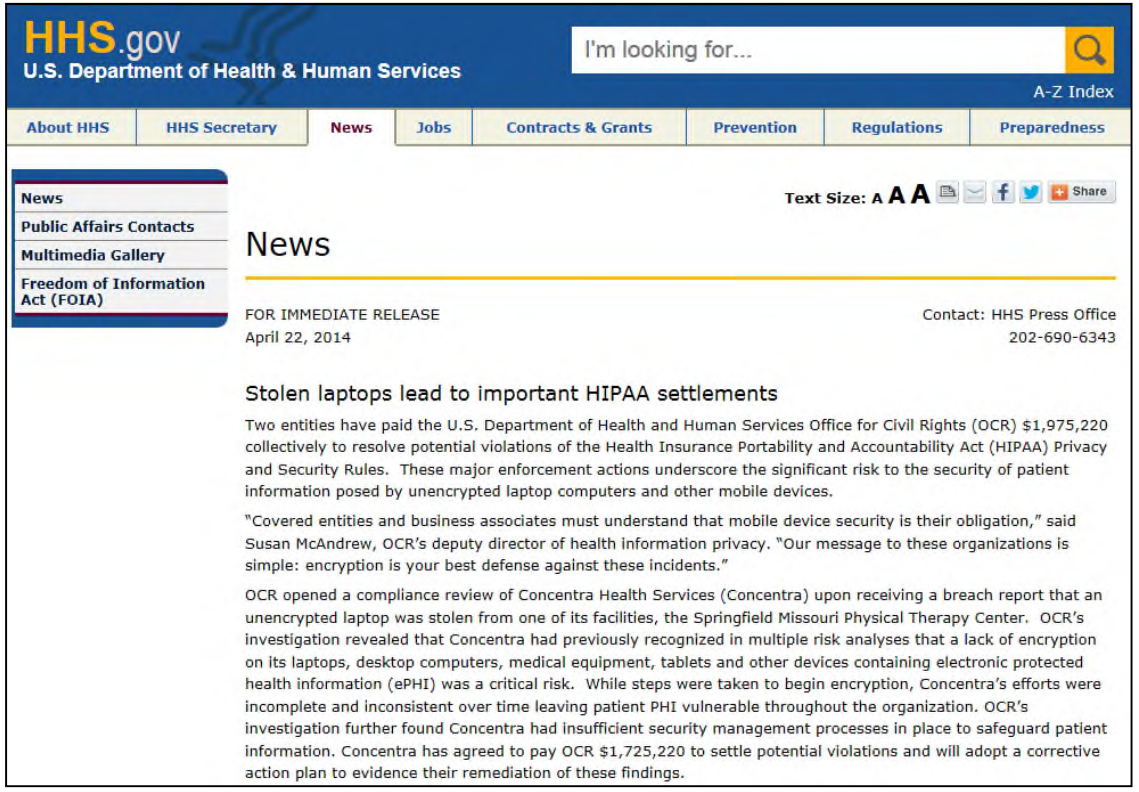


… A **foreign-based cyber-attack** of our computer network…. CHSPSC, LLC believes the attacker was an **"Advanced Persistent Threat" group originating from China**, which used **highly sophisticated malware technology** to attack CHSPSC, LLC's systems. The intruder was able to bypass the company's security measures and successfully copy and transfer some data existing on CHSPSC, LLC's systems.

Third Party Service Provider Security Policy

- **Written Policies and Procedures**
  - Based upon the overall Risk Assessment
- **Policies and Procedures Addressing**:
  - The identification and risk assessment of TPSPs
  - Minimum cybersecurity practices
  - Due diligence processes used to evaluate the adequacy of cybersecurity practices of TPSPs
  - Periodic assessment of TPSPs based on risk they present and the continued adequacies of their cybersecurity policies
- **Outline Contractual Protections**:
  - Policies regarding access controls, including its use of Multi-Factor Authentication
  - Use of encryption (both in transit and at rest)
  - Incident response and notice policies in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or its Nonpublic Information
  - Representations and warranties addressing cybersecurity policies and procedures relating to security controls

Unencrypted Data



HHS.gov
U.S. Department of Health & Human Services

I'm looking for...

A-Z Index

About HHS | HHS Secretary | News | Jobs | Contracts & Grants | Prevention | Regulations | Preparedness

- News
- Public Affairs Contacts
- Multimedia Gallery
- Freedom of Information Act (FOIA)

Text Size: A A A Share

News

FOR IMMEDIATE RELEASE
April 22, 2014

Contact: HHS Press Office
202-690-6343

Stolen laptops lead to important HIPAA settlements

Two entities have paid the U.S. Department of Health and Human Services Office for Civil Rights (OCR) $1,975,220 collectively to resolve potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. These major enforcement actions underscore the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

"Covered entities and business associates must understand that mobile device security is their obligation," said Susan McAndrew, OCR's deputy director of health information privacy. "Our message to these organizations is simple: encryption is your best defense against these incidents."

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.

http://www.hhs.gov/news/press/2014pres/04/20140422b.html

SIGNIFICANT COSTS AND CONSEQUENCES

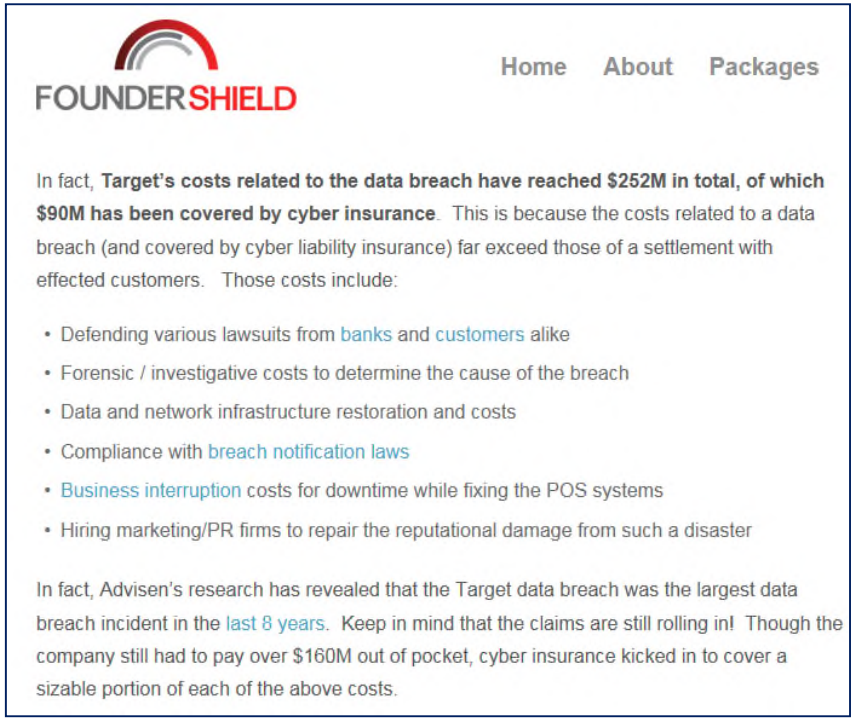
Cost of Data Breaches Continue to Increase

IBM Security and Ponemon Institute 2018 Cost of Data Breach Study: Global Overview

- 2,200 IT, data protection, and compliance professionals
- 477 companies with data breach over the last 12 months
- "[D]ata breaches continue to be costlier and result in more consumer records being lost or stolen, year after year."

https://www.ibm.com/downloads/cas/861MNWN2

Coverage Issues



FOUNDERSHIELD

Home About Packages

In fact, **Target's costs related to the data breach have reached $252M in total, of which $90M has been covered by cyber insurance**. This is because the costs related to a data breach (and covered by cyber liability insurance) far exceed those of a settlement with effected customers. Those costs include:

- Defending various lawsuits from banks and customers alike
- Forensic / investigative costs to determine the cause of the breach
- Data and network infrastructure restoration and costs
- Compliance with breach notification laws
- Business interruption costs for downtime while fixing the POS systems
- Hiring marketing/PR firms to repair the reputational damage from such a disaster

In fact, Advisen's research has revealed that the Target data breach was the largest data breach incident in the last 8 years. Keep in mind that the claims are still rolling in! Though the company still had to pay over $160M out of pocket, cyber insurance kicked in to cover a sizable portion of each of the above costs.

April 9, 2015

http://foundershield.com/the-2013-target-data-breach-insurance-coverage-recap/

HEIGHTENED REGULATORY ENFORCEMENT

Regulatory Landscape

Cybersecurity Landscape
Growing Patchwork of Laws

Data Breach Notification Statutes • First: California Data Breach Notification Statute (2002) • Now: 54 US Jurisdictions (DC, Puerto Rico, Guam, and Virgin Islands)
California Consumer Privacy Act of 2018
Special Focus Statutes: South Carolina Insurance Data Security Act (H. 4655)
New York Department of Financial Services (NYDFS) Cybersecurity Rule (March 2017)
Federal Trade Commission • Section 5: "unfair or deceptive acts or practices in or affecting commerce"
Securities and Exchange Commission (SEC) Statement and Guidance on Public Company Cybersecurity Disclosures
Health Insurance Portability and Accountability Act (HIPAA) of 1996
European Union (EU) **General Data Protection Regulation (GDPR)** (May 2018)

Statutory Reasonableness Standard

- Cal. Civ. Code § 1798.81 businesses must take "**reasonable steps** to dispose, or arrange for the destruction of, customer records within its custody or control containing personal information."

- Cal. Civ. Code § 1798.81.5 businesses that "own" or "license" personal information about a California resident must "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."

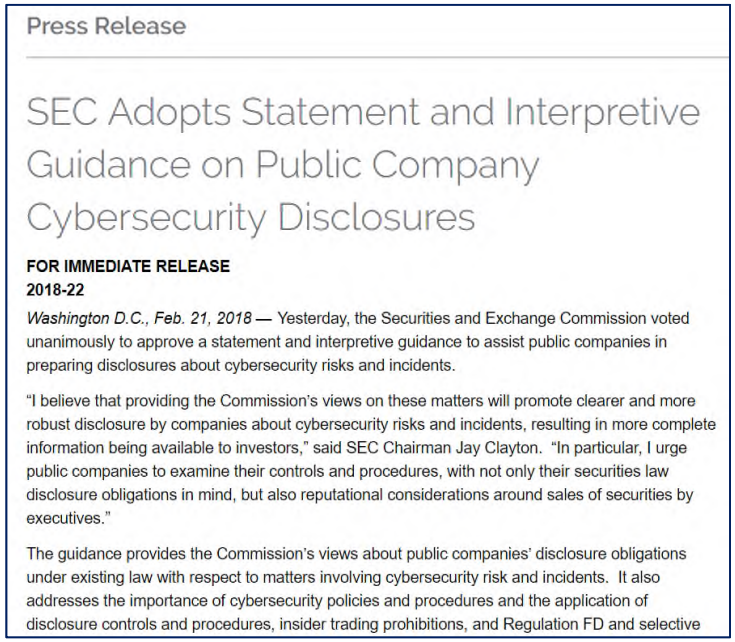
FTC v. Wyndham Worldwide Corp.

"Today's Third Circuit Court of Appeals decision reaffirms the **FTC's authority to hold companies accountable for failing to safeguard consumer data**. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers **when companies fail to take reasonable steps to secure sensitive consumer information**."

https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect

SEC Guidance on Cybersecurity Disclosures

- **Feb. 21, 2018**
- Disclosures Based on Reporting Obligations
  - Management's Discussion and Analysis of Financial Condition and Results of Operations
  - Cybersecurity Risk Factors
- Materiality Standard
- Timing of Disclosures
- Board Role
  - Managing cyber risk
- Cybersecurity Policies and Procedures
- Insider Trading Policies and Procedures Related to Cyber Risks and Incidents



Press Release

SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures

FOR IMMEDIATE RELEASE
2018-22

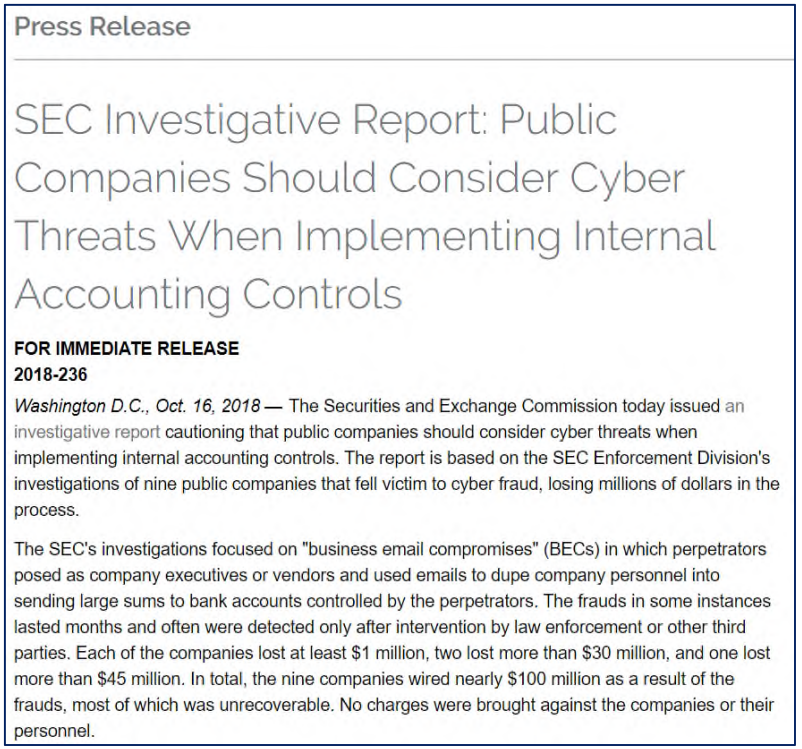
Washington D.C., Feb. 21, 2018 — Yesterday, the Securities and Exchange Commission voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

"I believe that providing the Commission's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors," said SEC Chairman Jay Clayton. "In particular, I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."

The guidance provides the Commission's views about public companies' disclosure obligations under existing law with respect to matters involving cybersecurity risk and incidents. It also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective

SEC Investigative Report (Oct. 16, 2018)

- SEC Investigative Report
  - Nine public companies victims of cyber-related frauds
  - Issue: Whether these companies violated federal securities laws by failing to have a sufficient system of internal accounting controls.
  - Public companies could still be liable for federal securities violations if they do not have sufficient internal accounting controls that specifically take into account these new threats.
  - Focus on internal accounting controls that reasonably safeguard company and investor assets from cyber-related frauds.
    - "Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management's general or specific authorization" and that "(iii) access to assets is permitted only in accordance with management's general or specific authorization." Section 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act.



Press Release

SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls

FOR IMMEDIATE RELEASE
2018-236

Washington D.C., Oct. 16, 2018 — The Securities and Exchange Commission today issued an investigative report cautioning that public companies should consider cyber threats when implementing internal accounting controls. The report is based on the SEC Enforcement Division's investigations of nine public companies that fell victim to cyber fraud, losing millions of dollars in the process.

The SEC's investigations focused on "business email compromises" (BECs) in which perpetrators posed as company executives or vendors and used emails to dupe company personnel into sending large sums to bank accounts controlled by the perpetrators. The frauds in some instances lasted months and often were detected only after intervention by law enforcement or other third parties. Each of the companies lost at least $1 million, two lost more than $30 million, and one lost more than $45 million. In total, the nine companies wired nearly $100 million as a result of the frauds, most of which was unrecoverable. No charges were brought against the companies or their personnel.

https://www.sec.gov/litigation/investreport/34-84429.pdf

Rule 30 of Regulation S-P (the Safeguard Rule)

- Requires registered broker-dealers, investment advisers and investment companies to establish **written policies and procedures** that are reasonably designed to **safeguard customer information**.
- The Safeguard Rule requires firms to:
  - address the administrative, technical, and physical safeguards for the protection of nonpublic personal information;
  - insure the security and confidentiality of customer records and information;
  - protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
  - protect against any unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Regulation S-P, Privacy of Consumer Financial Information. 17 C.F.R. Part 248; SEC Release No. IC-24543 (Jun. 22, 2000)

HIPAA

- Health Insurance Portability and Accountability Act ("HIPAA")
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Applies to covered entities and business associates
  - "Covered entities" are defined under HIPAA as (1) health plans, (2) healthcare clearinghouses, and (3) healthcare providers that electronically transmit any health information in connection with transactions for which the Department of Health and Human Services has adopted standards.
  - A "business associate" is defined as a person who creates, receives, maintains, or transmits protected health information on behalf of a covered entity (e.g., claims processing or administration, billing, practice management, etc.), or who provides legal, actuarial, administrative, financial, and similar services to or for a covered entity.

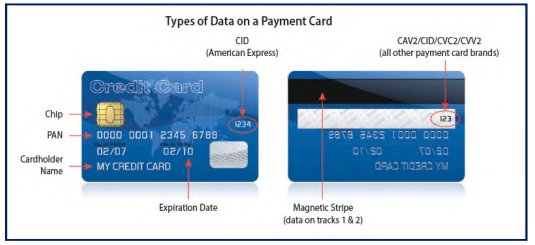
45 C.F.R. § 160.103.

Data Security & Controls

- Some industry or propriety standards may apply

- Payment Card Industry Data Security Standard (PCI DSS)

- Separate card compliance programs
  - American Express: www.americanexpress.com/datasecurity
  - Discover: www.discovernetwork.com/fraudsecurity/disc.html
  - JCB International: http://partner.jcbcard.com/security/jcbprogram/
  - MasterCard: www.mastercard.com/sdp
  - Visa Inc: www.visa.com/cisp
  - Visa Europe: www.visaeurope.com/ais



https://www.pcisecuritystandards.org/documents/PCISSC%20QRG%20August%202014%20-print.pdf


Washington
Oregon
California
Nevada
Idaho
Montana
Wyoming
Utah
Arizona
Colorado
New Mexico
North Dakota
South Dakota
Nebraska
Kansas
Oklahoma
Texas
Minnesota
Iowa
Missouri
Arkansas
Louisiana
Wisconsin
Illinois
Michigan
Indiana
Ohio
Kentucky
Tennessee
Mississippi
Alabama
Georgia
Florida
South Carolina
North Carolina
Virginia
West Virginia
Pennsylvania
New York
Maine
Vt.
N.H.
Mass.
R.I.
Conn.
New Jersey
Delaware
Md.
Alaska
Hawaii

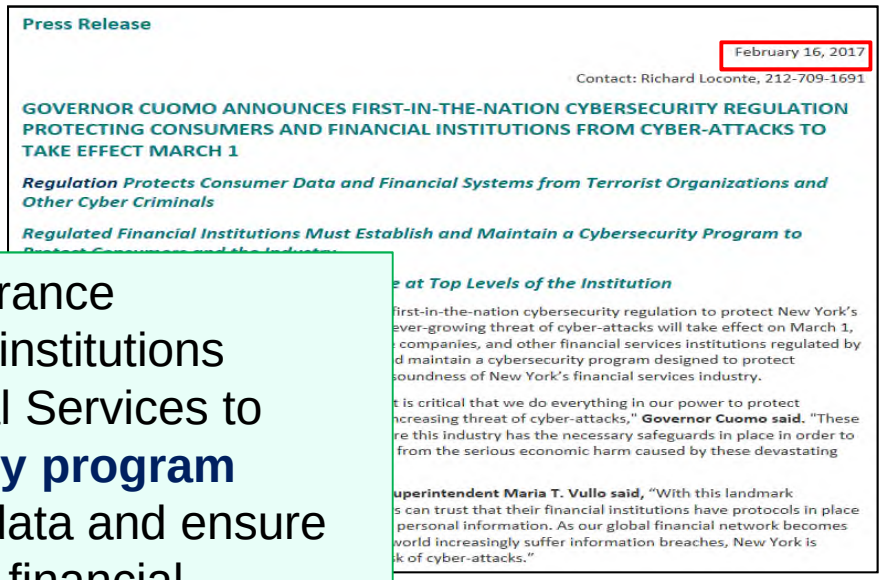
States Cybersecurity Landscape

- California Data Breach Notification Statute (2002)

- Recent States
  - March 21, South Dakota data breach statute (SB 62), effective July 1, 2018
  - March 28, "Alabama Data Breach Notification Act of 2018" (SB 318), effective June 1, 2018

- 54 US Jurisdictions
  - 50 states plus DC, Puerto Rico, Guam, and Virgin Islands

NY DFS Cybersecurity Regulation



Press Release

February 16, 2017

Contact: Richard Loconte, 212-709-1691

GOVERNOR CUOMO ANNOUNCES FIRST-IN-THE-NATION CYBERSECURITY REGULATION PROTECTING CONSUMERS AND FINANCIAL INSTITUTIONS FROM CYBER-ATTACKS TO TAKE EFFECT MARCH 1

***Regulation** Protects Consumer Data and Financial Systems from Terrorist Organizations and Other Cyber Criminals*

Regulated Financial Institutions Must Establish and Maintain a Cybersecurity Program to

at Top Levels of the Institution

first-in-the-nation cybersecurity regulation to protect New York's
ever-growing threat of cyber-attacks will take effect on March 1,
companies, and other financial services institutions regulated by
d maintain a cybersecurity program designed to protect
soundness of New York's financial services industry.

t is critical that we do everything in our power to protect
ncreasing threat of cyber-attacks," **Governor Cuomo said.** "These
re this industry has the necessary safeguards in place in order to
from the serious economic harm caused by these devastating

uperintendent Maria T. Vullo said, "With this landmark
s can trust that their financial institutions have protocols in place
personal information. As our global financial network becomes
world increasingly suffer information breaches, New York is
k of cyber-attacks."

The final regulation requires banks, insurance companies, and other financial services institutions regulated by the Department of Financial Services to **establish and maintain a cybersecurity program** designed to protect consumers' private data and ensure the safety and soundness of New York's financial services industry.

http://www.dfs.ny.gov/about/press/pr1702161.htm

NOTIFICATION ISSUES

Notification Questions

- Who must be notified?
  - Customers
  - Government
- When must they be notified?
  - Reasonable notice
  - Delayed notification
- What data (PII) triggers notification?
- What constitutes a "data breach"?
  - What exemptions?
  - Any reasonable likelihood of harm?
- What form of notice is required?
  - Email notification
  - Substitute notice
- What consequences and penalties?
  - Private right of action
- Any there any industry-specific requirements?
  - Insurance (GA, KS, ME, MT)
  - Medical records (CA, LA)
  - Financial institutions (MN)
  - Public utilities (MI)

Compare Notification Standards

California	Texas
• "The disclosure shall be made in the most expedient time possible and **without unreasonable delay**, consistent with the legitimate needs of law enforcement . . . or any measures necessary to **determine the scope of the breach** and restore the reasonable integrity of the data system." Cal. Civ. Code §1798.82(a).	• "The disclosure shall be made **as quickly as possible**, except as provided by Subsection (d) [for law enforcement] or as necessary to **determine the scope of the breach** and restore the reasonable integrity of the data system." Tex. Bus. & Com. Code Ann. § 521.053(b).

Notification Periods

Jurisdiction	Notification
California	"most expedient time possible and **without unreasonable delay**…"
New York Department of Financial Services	72 hours
Colorado	30 days
Florida	30 days
Ohio	45 days
Oregon	45 days
Washington	45 days
Connecticut	90 days

Public Agency Notifications

Jurisdiction	Trigger
New York	Attorney General State Police Division of Consumer Protection For **any data breach notification**
Vermont	Attorney General or the Department of Financial Regulation "provide a preliminary description of the breach within **14 business days** … of the data collector's discovery of the security breach or when the data collector provides notice to consumers"
California	Attorney General "more than **500 CA residents** as a result of a single breach of the security systems"
Colorado	Attorney General **500 or more CO residents**
Oregon	Attorney General More than **250 OR consumers**
Washington	Attorney General More than **500 WA residents**

SEC (April 24, 2018)

- **Fine**: $35 million; SEC Order
- **Failure to Disclose**: "Despite its knowledge of the 2014 data breach, Yahoo **did not disclose the data breach in its public filings for nearly two years**."
  - 2014 data breach disclosed in September 2016 in a press release attachment to a Form 8-K.

Press Release

Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million

FOR IMMEDIATE RELEASE
2018-71

Washington D.C., April 24, 2018 — The Securities and Exchange Commission today announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts.

According to the SEC's order, within days of the December 2014 intrusion, Yahoo's information security team learned that Russian hackers had stolen what the security team referred to internally as the company's "crown jewels": usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts. Although information relating to the breach was reported to members of Yahoo's senior management and legal department, Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors. The fact of the breach was not disclosed to the investing public until more than two years later, when in 2016 Yahoo was in the process of closing the acquisition of its operating business by Verizon

https://www.sec.gov/news/press-release/2018-71

CA Data Breach Notification

https://oag.ca.gov/privacy/databreach/list

CALIFORNIA CONSUMER PRIVACY ACT

Businesses Subject to the CCPA

- For-profit organization or legal entity that:
  - Does business in California
  - Collects consumers' personal information, either directly or through a third party on its behalf
    - "Collects" is broadly defined to include "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means."
  - Either alone, or jointly with others, determines the purposes and means of processing of consumers' personal information
    - Resembles GDPR's "data controller" concept
- Also satisfies one of three thresholds:
  1) The annual gross revenue in excess of $25 million
  2) Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone or in combination
  3) Derives 50% or more of its annual revenue from selling consumers' personal information
- Applies to brick-and-mortar businesses, not just collection of personal information electronically or over the internet
- Does not apply to nonprofits

CCPA Does Not Apply To …

- "Protected health information" (PHI) collected by **covered entities** governed by HIPAA or the California Confidentiality of Medical Information Act (CMIA)
  - Appears to apply to HIPAA business associates because PHI received by a BA could be said to be "collected by" a CE (and SB 1121 clarifies that point)
- Personal information subject to the Gramm-Leach-Bliley Act (GLBA) "if the CCPA conflicts with that law"
  - Suggests that a financial institution must comply with both CCPA and GLBA, performing a preemption analysis
  - SB 1121 clarifies this issue and creates a blanket exception for entities subject to GLBA and the California Financial Privacy Act
- SB 1121 adds an exception for clinical trials data

New Statutory Rights

- Right to know the categories of information
- Right of access and data portability
- Right to be forgotten
- Right to opt out of the sale of personal information to third parties
- Right to equal service and price

Very Broad Definition of "Personal Information"

- Personal information includes any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"
  - Much broader than the definition of "personal information" under CA's security breach notification law

- Extremely broad definition intended to include the sort of robust consumer profile and preference data collected by social media companies and online advertisers

Compare California Data Breach Notification Statute

"Personal Information" includes:

(1) An individual's first name or first initial and last name in combination with:

(A) Social Security number.

(B) Driver's license number or California identification card number.

(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

CCPA Definition of "Personal Information"

1) Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, or passport number
2) Categories of PI described in California's customer records destruction law
3) Characteristics of protected classifications under CA or federal law
4) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
5) Biometric information
6) Geolocation data
7) Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
8) Audio, electronic, visual, thermal, olfactory, or similar information
9) Professional or employment-related information
10) Education information that is subject to the Family Educational Rights and Privacy Act
11) Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

CCPA Enforcement

- **Private Right of Action**
  - Consumer action for business's alleged failure to "implement and maintain reasonable security procedures and practices" that results in a data breach. (CCPA § 1798.150(c).)
  - Eliminated requirement that a consumer notify the AG upon bringing a CCPA action against a business and AG authority to instruct consumer to not proceed. (CCPA § 1798.150(b).)

- **Enforcement**
  - AG civil penalties limited to $2,500 for each CCPA violation or up to $7,500 per each **intentional** violation
  - Injunction remedies. (CCPA § 1798.155(b).)
  - Delays AG CCPA enforcement actions until six months after publication of the implementing regulations or July 1, 2020, whichever comes first. (CCPA § 1798.185(c).)

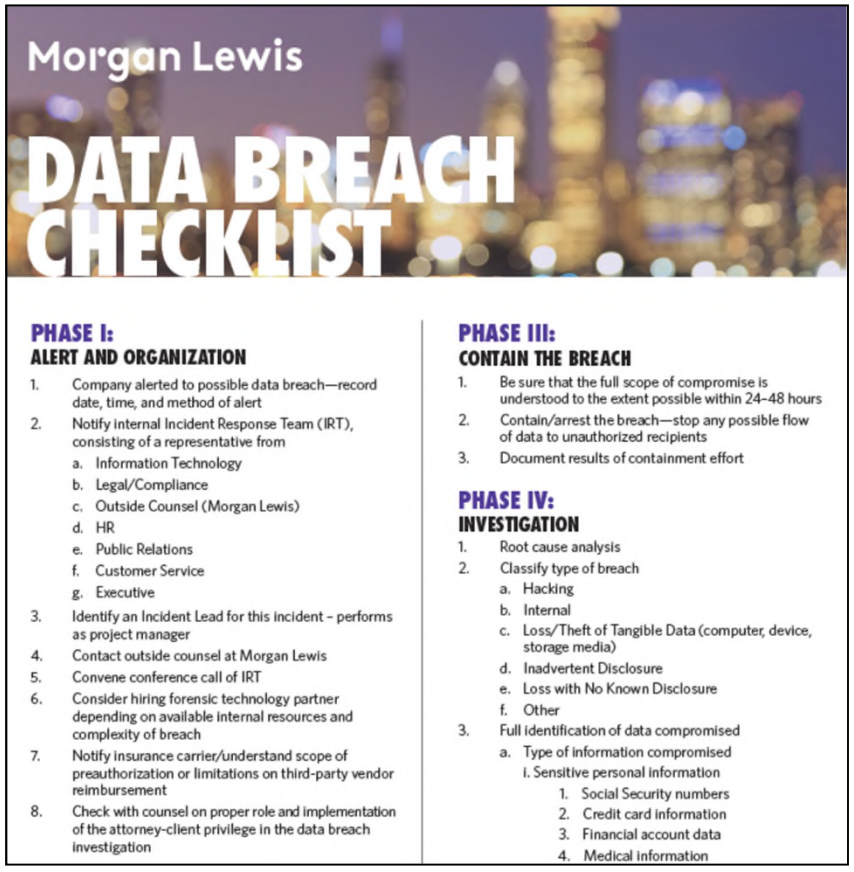
Attorney General Regulation Areas

- Personal information categories
  - "in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns"
- Definition of "unique identifiers"
- Rules and procedures for consumer opt-out of the sale of personal information
- Business notices and information
- Exceptions necessary to comply with state or federal law
  - including, but not limited to, those relating to trade secrets and intellectual property rights
- "[A]dditional regulations as necessary to further the purposes of this title"

Cal. Civil Code § 1798.185(a), (b)

WHEN A DATA BREACH OCCURS

Data Breach Checklist



Morgan Lewis

DATA BREACH CHECKLIST

PHASE I:
ALERT AND ORGANIZATION

1. Company alerted to possible data breach—record date, time, and method of alert
2. Notify internal Incident Response Team (IRT), consisting of a representative from
   a. Information Technology
   b. Legal/Compliance
   c. Outside Counsel (Morgan Lewis)
   d. HR
   e. Public Relations
   f. Customer Service
   g. Executive
3. Identify an Incident Lead for this incident – performs as project manager
4. Contact outside counsel at Morgan Lewis
5. Convene conference call of IRT
6. Consider hiring forensic technology partner depending on available internal resources and complexity of breach
7. Notify insurance carrier/understand scope of preauthorization or limitations on third-party vendor reimbursement
8. Check with counsel on proper role and implementation of the attorney-client privilege in the data breach investigation

PHASE III:
CONTAIN THE BREACH

1. Be sure that the full scope of compromise is understood to the extent possible within 24–48 hours
2. Contain/arrest the breach—stop any possible flow of data to unauthorized recipients
3. Document results of containment effort

PHASE IV:
INVESTIGATION

1. Root cause analysis
2. Classify type of breach
   a. Hacking
   b. Internal
   c. Loss/Theft of Tangible Data (computer, device, storage media)
   d. Inadvertent Disclosure
   e. Loss with No Known Disclosure
   f. Other
3. Full identification of data compromised
   a. Type of information compromised
      i. Sensitive personal information
         1. Social Security numbers
         2. Credit card information
         3. Financial account data
         4. Medical information

Overseeing Internal Cyber Investigation

Initial call
- How was the cyber compromise/incident discovered?
- Launch Incident Response Plan

Determine Scope and Nature of Breach
- Did a "data breach" occur?

Attorney Client Privilege
- Is the privilege effectively in place?

Assess Legal Consequences
- What notification obligations?
- What regulatory agencies?
- Was information accessed, acquired or exfiltrated?
- Which customers?
- What legal standards apply?

Coordination Issues/Coverage Obligations

CYBER INSURANCE COVERAGE ISSUES

Businesses and Other Entities Are Massively "Under-Covered" for Cyber-Related Losses

- Cyber Risk Management, whose members include Lloyd's of London, Aon and TransRe, conducted a simulated "stress test" of the effect of a single replicating ransomware attack with a single email origin and found the following:
  - If the single email recipient automatically forwarded the message upon opening to each of its contacts, and this was replicated continually, the attack could encrypt data on 30 million devices worldwide within 24 hours.
  - The attack would force the affected companies to decrypt their data, replace devices, and address supply chain disruptions.
  - Estimated costs: Up to $193 billion
  - Estimated responsive insurance coverage: No more than $27 billion
  - Coverage gap: Up to 86%[1]

[1] The full report can be downloaded here: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack

Businesses and Other Entities are Massively "Under-Covered" for Cyber-Related Losses (continued)

- "WannaCry" attack (2017) left the National Health Service with uncovered losses of $121 million after the attack affected up to 70,000 computers, MRI scanners, blood-storage refrigerators, and theater equipment. More than $90 million related to IT support and restoring data and systems.
- Equifax data breach (2017): Cost approximately $439 million to address, of which only $125 million was covered by insurance (71% underinsurance rate).

Businesses and Other Entities are Massively "Under-Covered" for Cyber-Related Losses (continued)

- "Under-coverage" is a supply and demand problem
  - Insurance market does not presently have enough products to cover all risks. New types of "ransomware" attacks are constantly being hatched. "Cryptojacking" (the unauthorized use of someone's computer to mine cyptocurrency) is on the rise.
  - Small and mid-sized companies, and those that do not perceive themselves as being in "tech," often do not see the need for cyber coverage. Large companies are often under-insured.
  - Midsized companies (revenues below $1 billion) are often prime targets of attacks because they often lack resources and protocols to defend themselves.

Businesses and Other Entities are Massively "Under-Covered" for Cyber-Related Losses (continued)

- Elizabeth Geary, global head of cyber coverage at TransRe: "As companies increase their reliance on technology, it is essential they increase their defenses against challenges such as malware, and effective cyber insurance is a component of that defense. Similarly, the insurance industry must also acknowledge and appreciate the potential for systemic risk, in addition to monitoring loss frequency and severity."

Types of Cyber Coverage

- Protection of digital assets
  - Data breach
  - Cyber crime, fraud, and extortion
  - Data and software loss and restoration
- Protection of the enterprise
  - Business interruption[2]
  - Network and service liability
  - Damage to physical assets

[2] Approximately 60% of businesses have reported some business interruption loss following a cyber incident.

Types of Cyber Coverage (continued)

- "Response" costs
  - Crisis management and public relations
  - Forensic investigation
  - Regulatory response, notification of affected persons, credit and identity theft monitoring

Types of Cyber Coverage (continued)

- "Loss Prevention" – The Stick and the Carrot
  - Policies frequently require reporting of cybersecurity efforts, with the potential loss of coverage for noncompliance
  - Suggestions have been made to insurers to broadly offer premium discounts as a loss prevention incentive on the theory that preventive measures will reduce incidence of loss
  - In all respects, companies with comprehensive, cyber-risk management plans with demonstrated levels of security and internal controls will be more attractive risks and will likely obtain more favorable premiums.

One Size Does Not Fit All

- A company in the business of handling and maintaining personal data will need different coverage than a retailer that handles and maintains personal data incidentally as part of its business.
- Companies will be subject to differing regulations depending on the industries in which they operate. For example, financial institutions and healthcare companies handle different types of private information, are subject to different privacy statutes, and need policies tailored to their particular situations.
- The unregulated and nonstandardized nature of cyber insurance means that substantial opportunities exist to design policies for particular risks and to negotiate favorable coverage terms and appropriate limits of liability.

Policy Wordings Can Vary Substantially

- Although typically written on a "claims made" basis – claims must be "made" and usually also "reported" during the period of the policy for coverage potentially to exist – some policies may also limit coverage to "breaches" that happen during the policy period.
- Some policies confine coverage to situations where data has been leaked to, or stolen by, third-parties, while others may also cover situations where data has been destroyed by an intrusion and rendered useless.

Policy Wordings Can Vary Substantially (continued)

- Some policies limit coverage to "personal" data; others might also include confidential corporate data within coverage.
- Some policies may limit coverage to company-owned mobile devices; others may also cover employee-owned devices used for company purposes.
- Some policies provide coverage for the costs of responding to governmental inquiries, subpoenas, audits, and investigations; others do not.

Recent Cyber Crime Coverage Cases

- *Medidata Solutions v. Federal Insurance Co.*, 729 Fed.Appx. 117 (2d. Cir. 2018): Second Circuit affirmed a district court's finding that a nearly $4.8 million loss sustained by Medidata was covered under a computer fraud provision in a crime policy after its employees were fraudulently tricked via a spoofed e-mail into wiring funds to an offshore account.[3]
- *American Tooling Center, Inc. v. Travelers Casualty and Surety Co.*, 895 F.3d 455 (6th Cir. 2018): Sixth Circuit reversed a district court's grant of summary judgment in favor of the insurer where American Tooling sustained a loss of nearly $834,000 when its employees were fraudulently tricked via spoofed e-mail into wiring money to an impersonator of one of the company's vendors.[4]

[3] The District Court decision can be found at 268 F.Supp.3d 471
[4] The District Court decision can be found at 2017 WL 3263356

Recent Cyber Crime Coverage Cases (continued)

- *Ad Advertising Design, Inc. v. Sentinel Insurance*, 344 F. Supp. 3d 1175 (D. Mont. 2018): The insured's employee transferred $115,595 to a designated bank account after receiving four fraudulent emails purportedly from the insured's President. The court held that a "false pretense" exclusion in a policy covering forgery and computer fraud was ambiguous and did not bar coverage because it applied only to "physical loss" or "physical damage." The Ninth Circuit has held that "physical loss" means a loss of tangible property, and the court has held that money in a bank account is not "tangible" property because it lacks a "physical presence."

Recent Cyber Crime Coverage Cases (continued)

- *Rainforest Chocolate, LLC v. Sentinel Insurance Company*, 2018 WL 6817065 (Vt. Supreme Court, Dec. 28, 2018): Vermont Supreme Court reversed summary judgment for the insurer where the insured's employee transferred $19,875 to a specified outside bank account after receiving a fraudulent e-mail purportedly from his manager. The court held that a "false pretense" exclusion in the same policy at issue in Ad Design – covering forgery and computer fraud – did nor bar coverage because it only applied to "physical loss" or "physical damage" and the loss of money was not "physical."

Recent Cyber Crime Coverage Cases (continued)

- *Interactive Communications International v. Great American Insurance Company,* 731 Fed. Appx. 929 (11th Cir. 2018): Eleventh Circuit affirmed a grant of summary judgment for the insurer denying coverage for an $11.4 million loss after fraudsters exploited a glitch in the insured's computerized interactive telephone system permitting them to improperly redeem more than 25,000 "chits" of specific monetary value to various debit cards. Although the court agreed that the scheme was accomplished via the use of a "computer," as required under a computer fraud policy, the loss did not "directly result" from the fraudulent use of the interactive system, but instead happened only after the bank that issued the debit cards disbursed the funds.[5]

[5] The District Court decision can be found at 2017 WL 1021749

Recent Cyber Crime Coverage Cases (continued)

- *Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co.*, 719 Fed.Appx. 701 (9th Cir. 2018): Ninth Circuit affirmed the district court's judgment in favor of the insurer where Aqua Star sustained $700,000 in losses after fraudsters posing as employees directed other employees to change customer account information and send four separate payments to the fraudster's account. The policy had an exclusion for "loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System..."[6]

[6] The District Court decision can be found at 2016 WL 3655265

Recent Cyber Crime Coverage Cases (continued)

- The trial court in *Rainforest Chocolate:*

> The complicated nature of this policy, with its layers of coverages and exclusions, is almost impossible to follow without a compass and a guide. It took the court many hours of reading and rereading the policy and the briefs to reach a clear understanding of how the various provisions fit together. How any insured, however sophisticated, is supposed to determine that it is getting what it paid for with a policy like this is a mystery to the court. Nonetheless, the court concludes that the terms of the policy, while confusing, are not ambiguous and must be enforced as written.

Coverage For Regulatory Compliance, Fines And Penalties

- Insurance policies historically have responded to claims of damage, injury, and loss. Costs incurred preventing potential injury or safeguarding property have not been insurable.
- Regulatory efforts in the cyber sphere have focused on actions businesses must take after a cyber incident, including notifying law enforcement and notifying customers.

Coverage For Regulatory Compliance, Fines And Penalties (Continued)

- Enactments such as the EU's General Data Protection Regulation, the California Consumer Privacy Act (effective in 2020) and the New York State Department of Financial Services Cybersecurity Regulation (effective as of August 2017) seek to prevent cyber incidents from happening by imposing new obligations on organizations to (i) protect the information they collect, (ii) ensure they are permitted collect such information, (iii) ensure they are using the information legally, and (iv) ensure they remain responsible for information shared with third-parties.
- Enactments carry the potential imposition of fines and penalties for non-compliance. Some "cyber" policies indemnify for fines and penalties, but also say they do not cover **anything** that is not "insurable" by law.

Coverage For Regulatory Compliance, Fines And Penalties (Continued)

- Fines and penalties are often considered to be legally noninsurable because they typically are associated with intentional wrongdoing.
- The new preventative harm regulatory regimes, however, impose fines and penalties without fault, simply for failing to comply. Indemnification might not be "illegal" under the circumstances.
- Indemnification of defense costs and response costs should be permissible in any event.

Cyber Coverage Trends

- Pricing will be stable, and capacity will keep pace with demand.
- Renewal premium increases will generally be in the low single digits.
- Premium decreases may be offered at renewal for companies with increased levels of security, internal controls, and favorable claim experiences.
- Growth will be driven by companies with annual revenues, below $1 billion.

Cyber Coverage Trends (continued)

- Coverage will be written specifically for increasing regulatory focus on preventing data losses before they happen.
- Workforce issues: Up to two-thirds of cyber incidents are the result of employee behavior, including claims of trickery (as we saw in the cases discussed above) and the negligent handling of data. "As organizations continue to make substantial investments to strengthen their security and privacy protections through technology and become more vigilant about tackling the human element of cyber risk, they will have further leverage to press on pricing and coverage improvements."

Source: Willis Towers Watson

Mark L. Krotoski

Mark L. Krotoski
Silicon Valley
+1.650.843.7212
mark.krotoski@morganlewis.com

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues.
- Advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Experience handling complex and novel cyber investigations and high-profile cases
  - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
  - Served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, in addition to other DOJ leadership positions.

Jeffrey S. Raskin

Jeffrey S. Raskin
San Francisco
+1.415.442.1219
jeffrey.raskin@morganlewis.com

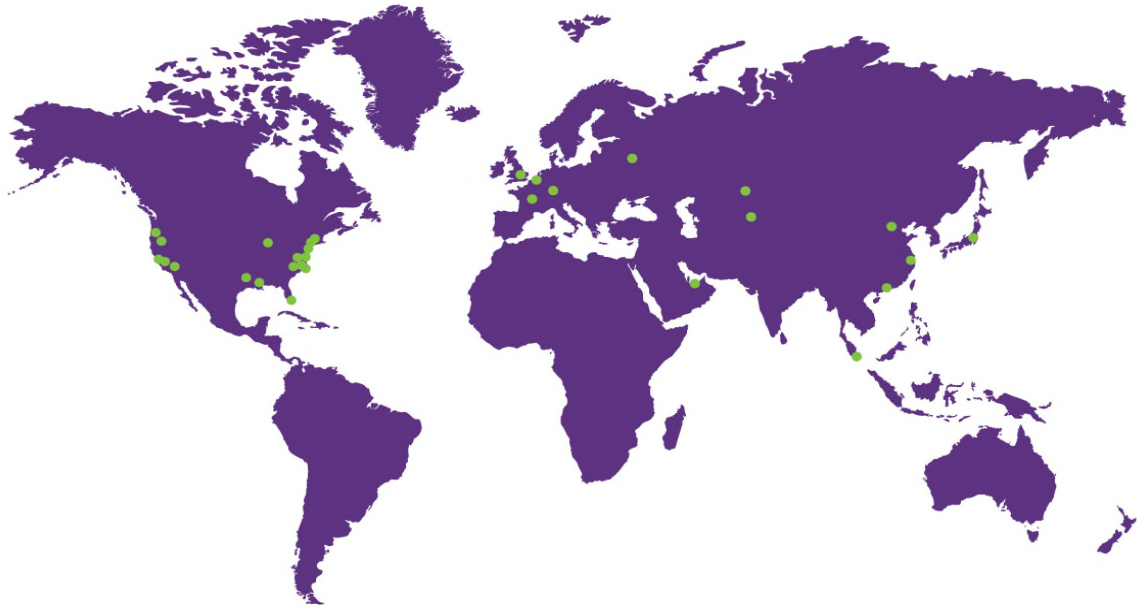
- Jeffrey is the head of Morgan Lewis's Insurance Recovery Practice in the San Francisco office. He advises clients in litigation, mediation, and arbitration around insurance coverage matters, and intellectual property, commercial, real estate, and environmental disputes. Head of Morgan Lewis's Insurance Recovery Practice in the San Francisco office, Jeffrey counsels clients seeking recovery for catastrophic losses in securities, environmental, asbestos, silica, toxic tort, product liability, intellectual property, and employment practices cases.
- Jeffrey has written on a variety of topics about insurance, as well as discovery of email in civil litigation. His most recent writings discuss the emerging fields of "cyber" insurance, with a particular focus on the types of first- and third-party coverages available to companies to protect themselves against the financial consequences resulting from various types of data breaches.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.