



Morgan Lewis

CYBER INSURANCE: IS YOUR COMPANY COVERED?

Cyber Insurance Webinar Series

Mark L. Krotoski and Jeffrey S. Raskin
December 10, 2019

© 2019 Morgan, Lewis & Bockius LLP


Overview

- Business Email Compromise And Other Types of Cyber Fraud
- Covered Options for a Ransomware Attack
- Insurance coverage issues under the California Consumer Privacy Act (CCPA)

CYBER INSURANCE WEBINAR SERIES

**BUSINESS EMAIL
COMPROMISE AND OTHER
TYPES OF CYBER FRAUD**

Business Email Compromise



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 10, 2019
Alert Number
I-091019-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 EMAIL COMPROMISE THE \$26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.¹

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses². The increase is also due in part to greater awareness of the scam, which encourages reporting to the IC3 and international and financial partners. The scam has been reported in all 50 states and 177 countries. Fraudulent transfers have been sent to at least 140 countries.

The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019**:

| | |
|---|------------------|
| Domestic and international incidents: | 166,349 |
| Domestic and international exposed dollar loss: | \$26,201,775,589 |

The following BEC/EAC statistics were reported in victim complaints to the IC3 between **October 2013 and July 2019**:

| | |
|-------------------------------------|------------------|
| Total U.S. victims: | 69,384 |
| Total U.S. exposed dollar loss: | \$10,135,319,091 |
| Total non-U.S. victims: | 3,624 |
| Total non-U.S. exposed dollar loss: | \$1,053,331,166 |

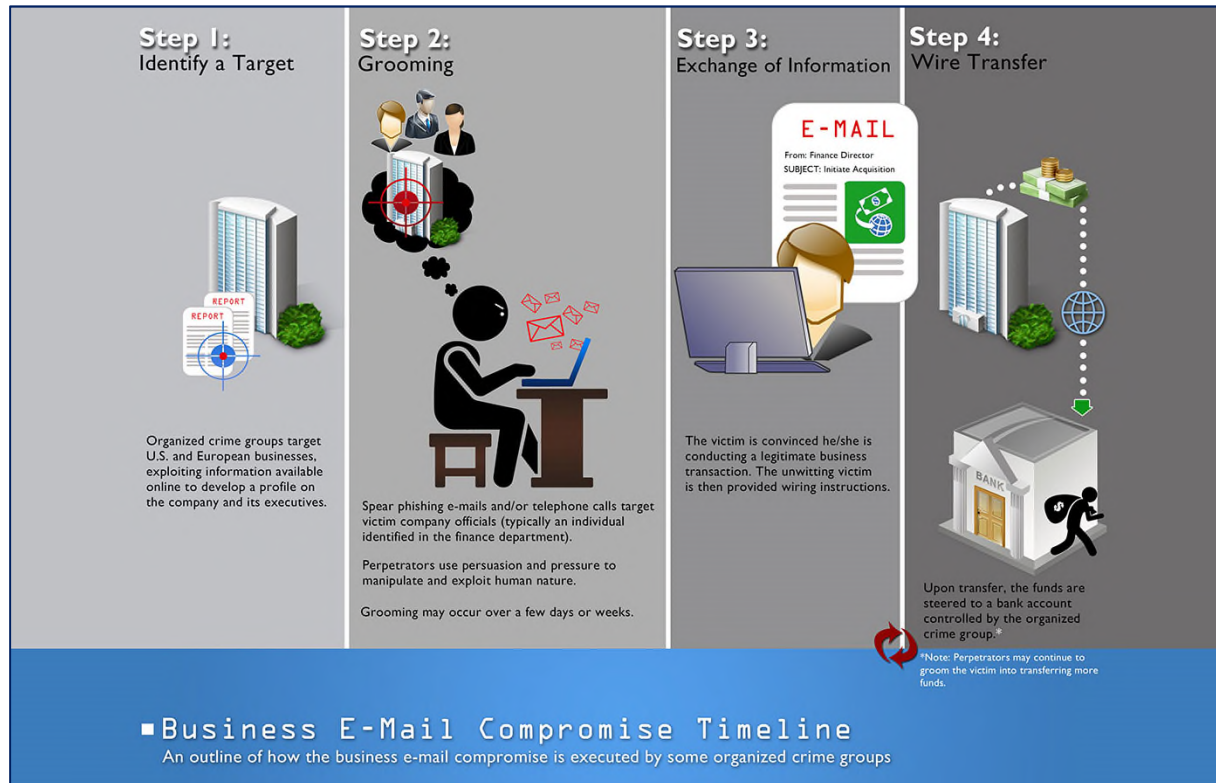
The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019**:

| | |
|---|-----------------|
| Total U.S. financial recipients: | 32,367 |
| Total U.S. financial recipient exposed dollar loss: | \$3,543,308,220 |
| Total non-U.S. financial recipients: | 14,719 |
| Total non-U.S. financial recipient exposed dollar loss: | \$4,843,767,489 |

Business Email Compromise

- Spoofing e-mail accounts and websites:
 - Modified email address (e.g., kellysmith@abc-inc.com to kelleysmith@abc--inc.com)
 - Modified domain (e.g., fullcompany.com to fu11company.com)
- Spear-phishing
 - Fraudulent e-mail requesting confidential information
- Malware
 - Unauthorized access to network to review e-mail communications about billing and invoices
 - May obtain passwords to control and access email accounts
 - Learn financial account information and relationships

Business Email Compromise: Key Steps



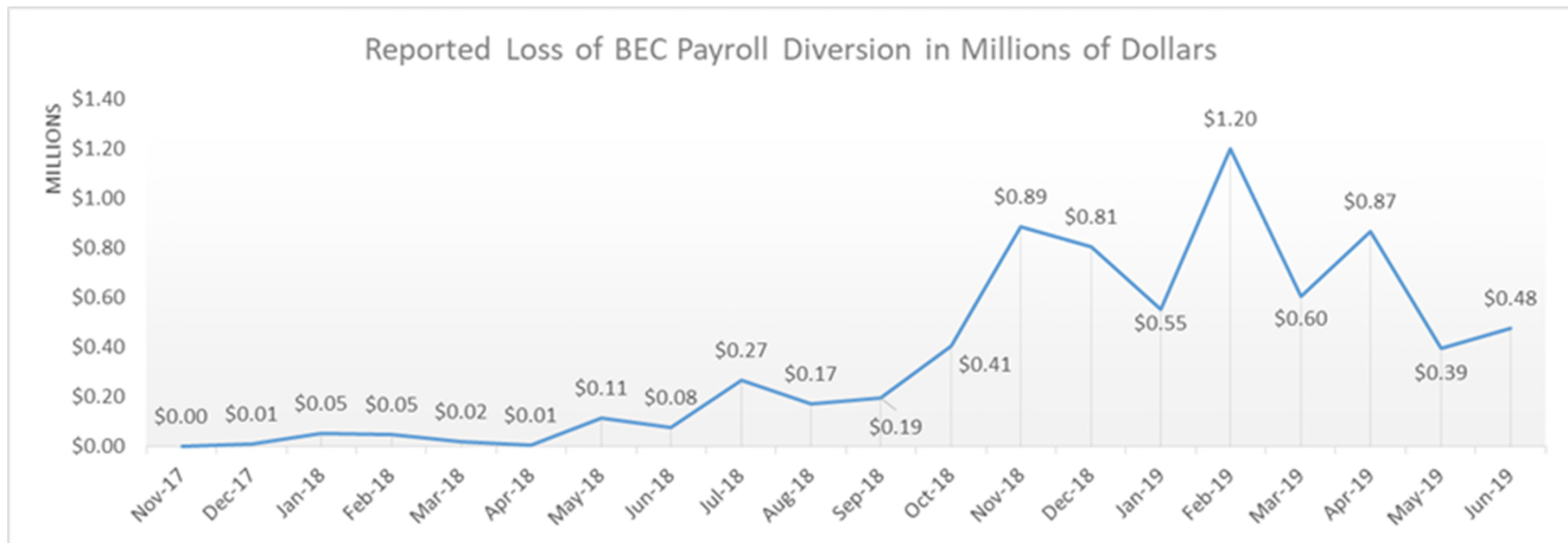
Business Email Compromise:

- Typically redirect funds during pending transaction or invoice
- Identify business relationship, redirect wiring of funds to another account controlled by perpetrators or mule
 - Customer relationships
 - CEO or executive impersonation
- May include other information of value
 - Tax information
 - PII
 - Proprietary information



• Other DOJ Fraud Examples

- **"Employment opportunities scams"** victims are convinced to provide their PII to apply for work-from-home jobs, and, once "hired" and "overpaid" by a bad check, to wire the overpayment to the "employer's" bank before the check bounces;
- **"Real Estate Transactions"** scammer impersonate sellers, realtors, title companies, or law firms during a real estate transaction to ask the home buyer for funds to be sent to a fraudulent account
- **"Rental scams"** scammer agrees to rent a property, sends a bad check in excess of the agreed upon deposit, and requests the overpayment be returned via wire before the check bounces;
- **"Fraudulent online vehicle sales scams"** victims are convinced they are purchasing a nonexistent vehicle and must pay for it by sending the codes of prepaid gift cards in the amount of the agreed upon sale price to the "seller;"
- **"Lottery scams"** victims are convinced they won an international lottery but must pay fees or taxes before receiving the payout;
- **"Romance scams"** victims are lulled into believing they are in a legitimate relationship, and are tricked into sending or laundering money under the guise of assisting the paramour with an international business transaction, a U.S. visit, or some other cover story.

Business Email Compromise



Business Email Compromise: Other Forms



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

February 21, 2018

Alert Number
I-022118-PSA

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

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

INCREASE IN W-2 PHISHING CAMPAIGNS

Beginning in January 2017, IRS's Online Fraud Detection & Prevention (OFDP), which monitors for suspected IRS-related phishing emails, observed an increase in reports of compromised or spoofed emails requesting W-2 information. Sometimes these requests were followed by or combined with a request for an unauthorized wire transfer.

The most popular method remains impersonating an executive, either through a compromised or spoofed email in order to obtain W-2 information from a Human Resource (HR) professional within the same organization.

Individual taxpayers may also be the targeted, but criminals have evolved their tactics to focus on mass data thefts.

This scam is just one of several new variations of IRS and tax-related phishing campaigns targeting W-2 information, indicating an increase in the interest of criminals in sensitive tax information.

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.

Morgan Lewis

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>

Business Email Compromise: DOJ Prosecutions



- **Large Take Downs in US and Abroad**

- **Operation reWired (Sept. 2019)**
 - 281 arrests in US and overseas, including 74 in US, 167 in Nigeria, 18 in Turkey, and 15 in Ghana; also France, Italy, Japan, Kenya, Malaysia, and UK
 - Seizure of nearly \$3.7 million
 - DOJ, DHS, Treasury, Postal Inspection Service, and State
- **Operation Wire Wire (June 2018)**
 - 74 arrests in US and overseas, including 29 in Nigeria, and three in Canada, Mauritius and Poland
 - Seizure of nearly \$2.4 million
 - Recovery of approximately \$14 million in fraudulent wire transfers
 - DOJ, DHS, Treasury, and Postal Inspection Service

Common Criminal Charges

- **Wire fraud**
 - 18 U.S.C. § 1343
- **Mail fraud**
 - 18 U.S.C. § 1341
- **Bank fraud**
 - 18 U.S.C. § 1344
- **Conspiracy**
 - 18 U.S.C. §§ 371, 1349
- **Aggravated identity theft**
 - 18 U.S.C. § 1028A

Business Email Compromise: Key Steps

- Training
 - Alert to targeted financial fraud
 - Fraud scenarios
 - Be alert to other BEC forms that request the transfer of data instead of money
 - Report suspicious activity
- Detection
 - Intercept suspicious emails
 - Email rules
 - Verify URL in emails is associated with the business
 - Allow full email extensions to be viewed by employees
 - Intrusion detection
 - Update software patches
 - Monitor financial transactions
- Verification
 - Limit who can approve the transfer of funds
 - Validate the identity of the requestor
 - Verify changes in vendor payment location or institution
 - Two-factor authentication over threshold amount
 - Review email transfer of fund requests
- Preservation
 - Preserve evidence (including emails and log records) if needed to locate scammers
- Stop funds
 - Alert the company's financial institution promptly concerning suspected fraud to stop the transfer of funds

Types of Cyber Insurance Claims by Incident

- Business E-Mail Compromise: 23%
- Ransomware: 18%
- Data Breach by Hackers: 14%
- Data Breach by Employee Negligence: 14%
- Impersonation Fraud: 8%
- Virus/Malware: 6%
- System Failure/Outage: 5%
- Physical Loss or Theft of Information Assets: 5%
- Denial of Service Attacks/Violation of Data Privacy Regulations: 4%
- Non-Ransomware extortion: 3%

Cyber Claims by Industry

- Professional Services: 22%
- Financial Services: 15%
- Business Services: 12%
- Retail/Wholesale: 9%
- Manufacturing: 8%
- Public Entity/Non-Profit: 8%
- Communications Media and Technology: 7%
- Hospitality & Leisure: 4%
- Transportation and Logistics: 3%
- Energy/Utilities: 3%
- Other Services: 3%
- Healthcare (Hospital and Pharmaceuticals): 3%
- Food, Beverage, Construction, Education: 2%

Morgan Lewis

Source: AIG EMEA (2018)

14

Coverage for Cyber Fraud

- Several different types. We will discuss “Fraudulent Instructions,” “Funds Transfer,” and “Computer Fraud” coverage.
- Usually added to cyber policies by endorsement; limits under these policies are often quite low (\$50,000 - \$250,000).
- Increased limits may be available based on (i) more stringent underwriting and (ii), in the case of business e-mail compromise, where the insured agrees that it will verify the instruction to transfer money by following a pre-arranged “callback” or other established procedural method to authenticate the validity of the request prior to acting upon a transfer instruction.
- Separate “crime” coverages may cover the same types of claims and may provide higher limits. These also can be “all risk” crime policies meaning that any type of “crime” is covered, unless specifically excluded.

Fraudulent Instructions Coverage

- A form of “social engineering fraud” coverage
- Typically requires that money be transferred, paid, or delivered as a “direct result” of specified “fraudulent” activity
 - Specified “fraudulent” activity is typically defined to include:
 - Fraudulent (i) written instructions, (ii) electronic instructions (including e-mail or web-based instructions), or (iii) telephonic instructions
 - Provided by a person purporting to be a vendor, client, or authorized employee, and which are
 - Intended to mislead the insured’s employees through a misrepresentation of a material fact that is relied upon in good faith by the employees.

Fraudulent Instructions Coverage

- The “direct result,” “direct loss,” or “causation,” or “immediate cause” requirement can lead to disputes:
 - Business e-mail compromise usually results from a “chain of events”
 - A fraudulent communication is made to an employee
 - The employee ultimately requests the transfer of funds from a financial institution to the fraudster’s account ¹
- *American Tooling Center, Inc. v. Travelers Casualty and Surety Co.*, 895 F.3d 455 (6th Cir. 2018): A third party pretending to be a vendor sent several fraudulent e-mails to the insured via a computer. The e-mails ultimately caused ATC to send \$834,000 to the fraudster’s account. The court held that the fraud was “the immediate cause” of ATC’s loss, thus satisfying the policy’s “direct loss” requirement, even though a “series of internal actions” (a “chain of events”) occurred between the receipt of the fraudulent e-mails and the transfer of funds to the fraudster’s account.

Fraudulent Instructions Coverage

- Insurer's Petition for Rehearing: "By its very nature, a 'chain of events' is not 'direct' because there is no immediacy between the actual loss and the loss-inducing event . . . Immediacy requires no links, much less a chain of intervening space, time, agencies, and instrumentalities. Even one link is insufficient." Business e-mail compromise usually results from a "chain of events"
 - "After receiving each fraudulent email, ATC verified that [the Alleged Vendor] had completed the tasks required for the next scheduled payment. [ATC's Treasurer] subsequently determined which outstanding invoices to pay, and chose to pay the [Alleged Vendor's] invoice. He then signed into the banking portal and manually entered the fraudulent banking information emailed by the impersonator. Finally, after [ATC's Treasurer] submitted the wire transfer, ATC's Assistant Comptroller approved the payment."

Funds Transfer Fraud Coverage

- A separate type of “social engineering fraud” coverage.
- Typically covers fraudulent instructions issued to a financial institution directing it to transfer, pay or deliver money from the insured’s account without the insured’s knowledge or consent.
- Limited to circumstances where the fraudster induces a financial institution to release funds by posing as the insured and submitting fraudulent instructions. The insured typically needs to prove that the fraudster issued instructions that purport to have been made or authorized by the insured.
- Will not apply when the insured’s employee either initiates or otherwise authorizes the transfer.

Funds Transfer Fraud Coverage

- *Sanderina, LLC v. Great American Insurance Company*, 2019 WL 4307854 (D. Nev. September 11, 2019). A fraudster sent a series of emails to *Sanderina's* controller, Donna Atwood, purporting to be from the company's President. Atwood made six transfers to the fraudster's account totaling \$260,994. Funds transfer coverage, however, was not available:

The funds-transfer fraud provision covers losses "resulting directly from a fraudulent instruction directing a financial institution to transfer, pay or deliver funds from your transfer account." The policy defines "fraudulent instruction" as a "written instruction . . . which purports to have been issued by you and which was sent or transmitted to a financial institution to establish the conditions under which transfers are to be initiated by such financial institution through an electronic funds transfer system and which was issued, forged or altered without your knowledge or consent."

. . .

Sanderina is not a financial institution, so the fraudulent instructions were not "sent or transmitted to a financial institution." Plus, *Sanderina* controller Donna Atwood requested and knew about the transfers, so the fraudulent instructions were not "issued, forged or altered without [*Sanderina's*] knowledge or consent."

Computer Fraud Coverage

- Typically covers losses:
 - “resulting directly” from the use of any computer
 - “to impersonate” the insured, its officers, or employees
 - “to gain direct access” to the insured’s computer system or to the computer system of the insured’s financial institution, and
 - fraudulently cause the transfer of money from the insured’s account.
- Most frequently occurs when a fraudster hacks into a computer system and changes bank routing numbers to transfer funds to his or her account, or to create fake transactions causing funds to be directed to his or her account.

Computer Fraud Coverage

- *Sanderina*: Relied on an earlier Ninth Circuit decision in *Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App'x 627, 628 (9th Cir. 2017):

Losses resulting from similar emails were not covered under a policy requiring “entry into” a computer system without authorization because “there is no support for [plaintiff’s] contention that sending an email, without more, constitutes an unauthorized entry into the recipient’s computer system.” The “direct access” requirement here is substantially similar to the “entry into” requirement in the Taylor & Lieberman policy, and this record does not support a finding that merely sending an email to a *Sanderina* employee constituted direct access to Sanderina’s computer system.

Computer Fraud Coverage

- *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of America*, 719 F. App'x 701, 702 (9th Cir. 2018): The insured received a fraudulent e-mail from requesting that the insured change the vendor's bank account information. The insured manually changed the account information, thus causing future transfers to be sent to the fraudster's account. The Ninth Circuit affirmed the grant of summary judgment to the insurer based on an exclusion stating that the coverage "will not apply to 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"
- *Medidata Solutions, Inc. v. Federal Insurance Co.*, 729 F. App'x 117, 118 (2d Cir. 2018). Computer fraud coverage applied to a business e-mail compromise situation because "the fraudsters . . . crafted a computer-based attack that manipulated [the insured's] email system" that resulted in "a fraudulent entry of data into the computer system" and which altered "the email system's appearance . . . to misleadingly indicate the sender."

Summary of the Three Coverages

- **Fraudulent Instructions Coverage** applies when the insured's employees are "tricked" into instructing a financial institution to transfer funds to the fraudster's account.
- **Funds Transfer Fraud Coverage** applies when a financial institution is tricked into transferring the insured's funds to the fraudster's account.
- **Computer Fraud Coverage** applies when the integrity of the insured's computer system, or the financial institution's computer system, is compromised through unauthorized access, thus resulting in the transfer of the insured's funds to the fraudster's account.

CYBER INSURANCE WEBINAR SERIES

COVERED OPTIONS FOR A RANSOMWARE ATTACK

Ransomware Impact



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

October 02, 2019
Alert Number
I-100219-PSA

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

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

HIGH-IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESSES AND ORGANIZATIONS

This Public Service Announcement (PSA) is an update and companion to [Ransomware PSA I-091516-PSA](#) posted on www.ic3.gov. This PSA contains updated information about the ransomware threat.

WHAT IS RANSOMWARE?

Ransomware is a form of malware that encrypts files on a victim's computer or server, making them unusable. Cyber criminals demand a ransom in exchange for providing a key to decrypt the victim's files.

Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Since early 2018, the incidence of broad, indiscriminant ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information.

Although state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.

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 or USSS 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.

Ransomware Protection and Issues

Protection and Prevention

- Offline, Secure, and Regular Backups
- Training and Awareness
- Avoid Links or Phishing Schemes with Attachments Containing Malware
- Strong Passwords
- Update Operating Systems, Software, and Patches and Use Antivirus Software
- Physical and Logical Segmentation and Separate (e.g., by business units)
- Monitoring and Intrusion Detection
- Tailored Protections
- Incident Response Plan That Is Tested

Ransomware Protection and Issues

Legal Issues

- Initial Cyber Investigation Under Attorney-Client Privilege
- Determining Any Notification Requirements
- Response to Government Inquiries and Enforcement Actions
- Anticipating Potential Civil Litigation
- Contacting Law Enforcement
- Information Sharing in the Private and Public Sectors
- Scope of Cyber-Insurance Coverage

Ransomware Protection and Issues

- Unauthorized access and/or acquisition?
- California data breach notification statute
 - “breach of the security of the system’ means **unauthorized acquisition** of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business” [Cal. Civil Code § 1798.82(g)]

Ransomware Protection and Issues

NY SHIELD Act

- "Breach of the security of the system" shall mean unauthorized **access to or acquisition of . . .** of computerized data that compromises the security, confidentiality, or integrity of [personal] private information maintained by a business.
 - In determining whether information has been **accessed**, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that **the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.**
 - In determining whether information has been **acquired**, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the **following factors, among others:**
 - (1) indications that the information is in the **physical possession and control** of an unauthorized person, such as a lost or stolen computer or other device containing information; or
 - (2) indications that the information has been **downloaded or copied**; or
 - (3) indications that the information was **used by an unauthorized person**, such as fraudulent accounts opened or instances of identity theft reported.

Ransomware/Cyber Extortion Coverage

- Found in the first-party coverage part of a cyber policy. Standalone crime policies may also provide cyber extortion coverage.
- Typical provision:

“The Insurer will pay or reimburse the Insured for cyber-extortion expenses . . . that the Insured incurs directly resulted from and in response to a cyber extortion threat.”
- The details, however, are in the definitions:

“Cyber-Extortion Expenses”

 1. Reasonable and necessary money, *digital currency*, property or other consideration surrendered as payment by or on behalf of the Insured Company, to *which the Insurer has consented*, such consent not to be unreasonably withheld, *in order to prevent, limit or respond to a cyber-extortion threat*
 2. Reasonable and necessary costs charged by:
 - a. breach response providers; or
 - b. qualified third parties *with the consent of the Insurer*, to conduct an investigation and advise the Insured how to respond to and resolve a cyber-extortion threat.

Ransomware/Cyber Extortion Coverage

“Cyber Extortion Threat”

A threat made by a third-party or rogue employee demanding payment in consideration for *the elimination, mitigation or removal of the threat* intended to:

1. Disrupt the network to impair business operations of the Insured.
2. Alter, damage or destroy data stored on the network.
3. Use the network to generate and transmit malware to third parties.
4. Deface the Insured Company’s website.
5. Access or release data, including personally identifiable information, protected health information, confidential business information, stored or previously stored on the network.
6. Refuse to return data stolen from the network; or
7. Prevent access to the network or data by using encryption and withholding the decryption key.

Insurer Consent Requirement

- Potential delay in resolving the extortion incident as consent is sought and obtained. This can result in an increased risk of continued outage resulting from a system failure.

BUT

- Insurers may agree “quickly” to pay to “eliminate,” “mitigate,” “remove,” “limit” or otherwise “respond” to a cyber extortion threat
 - The earlier a threat is addressed and resolved, the less the insurer may ultimately be required to pay under the. This could particularly be true if a system is down, and the cyber policy also provides business interruption coverage.
 - Some of covered resolution costs, particularly the cost of backup restoration, can be greater than the ransom amount.

Insurer Consent Requirement

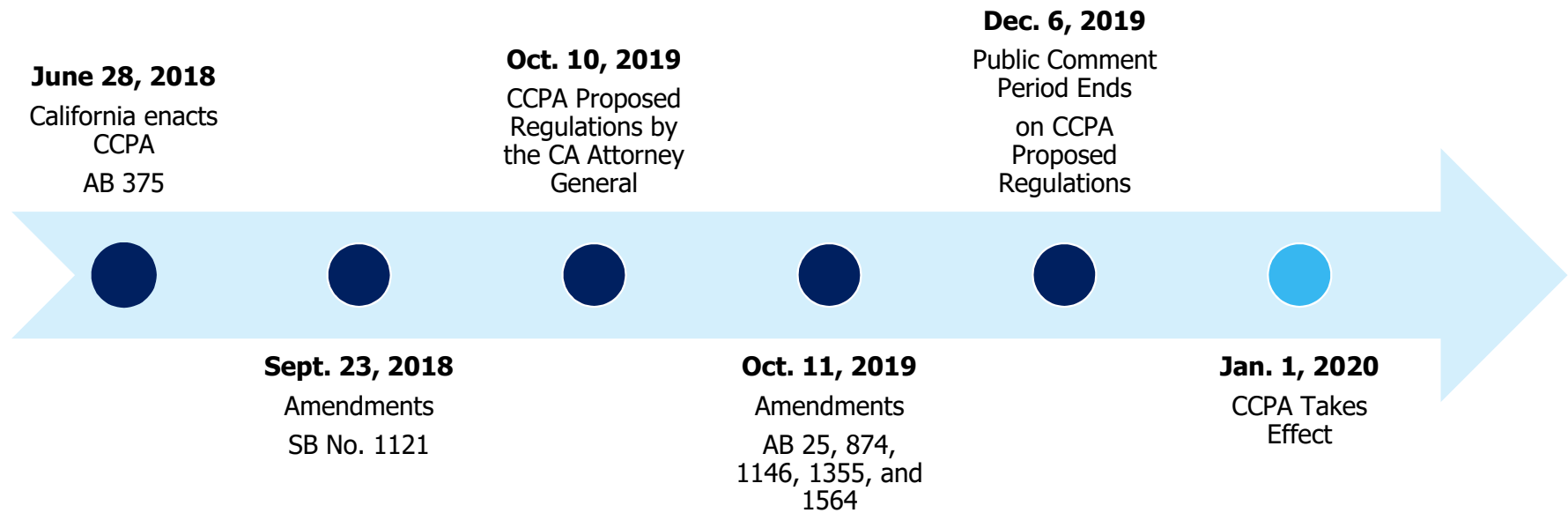
- Coveware, a Connecticut firm that specializes in ransomware response and analytics, reported the following statistics for Q2 of 2019:
 - Average ransom payment was \$36,295.
 - 96% of companies that paid the ransom received a working decryption tool.
 - Victims that paid for a decryptor recovered 92% of their encrypted data. “Data loss is typically a result of a flawed encryption process where files are partially encrypted or wiped. Some clients reduce the expense of running inefficient decryptor tools and simply archive non-essential encrypted data for a rainy day.”

CYBER INSURANCE WEBINAR SERIES

**INSURANCE COVERAGE
ISSUES UNDER THE
CALIFORNIA CONSUMER
PRIVACY ACT (CCPA)**



CCPA Timeline



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 must satisfy 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 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”

- 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

New Statutory Rights



- Right to know the categories of information
- Right of access and data portability
- Right to request data be deleted
- Right to opt out of the sale or sharing of personal information to third parties
 - Businesses prohibited from selling personal information of consumers under the age of 16 without explicit consent
- Right to equal service and price



Morgan Lewis

Enforcement Avenues

- California Attorney General Enforcement
- Limited Private Right of Action



Attorney General Enforcement



- **Scope:** Civil enforcement for **any violation** of CCPA against a “business, service provider, or other person.”
- **Opportunity to Cure:** Applies to violation after business “fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.”
- **Civil Enforcement Damages:**
 - Injunctive relief
 - \$2,500 for each violation
 - \$7,500 for each intentional violation of the CCPA

Attorney General Enforcement



- **Enforcement Delayed:**

- “[U]ntil six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.”

- **New Consumer Privacy Fund:**

- Civil enforcement penalties deposited in the Consumer Privacy Fund
- Intended “to fully offset any costs incurred by the state courts and the Attorney General” in enforcement.

Civil Penalties



- **Limited Consumer Private Right of Action**

- (1) Nonencrypted and nonredacted **personal information**
- (2) "subject to an **unauthorized access** and **exfiltration, theft, or disclosure**"
- (3) "as a result of the business's violation of the duty to implement and maintain **reasonable security** procedures and practices appropriate to the nature of the information to protect the personal information"

- **Recovery**

- Damages
- Injunctive or declaratory relief
- "Any other relief the court deems proper"

- **Opportunity to Cure**

- Statutory Damages

Limited Consumer Private Right of Action



- **“Personal information”**

- Not encrypted or redacted

- (A) First name or first initial and his or her last name plus another data element

- **Social security number**
 - **Driver’s license number or California identification card number**
 - **Account number, 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**
 - **Medical information**
 - **Health insurance information**

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

Reasonable Security Statute



- “A business that owns, licenses, or maintains personal information about a California resident shall 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.”
- Note: Comparable statute in about half the states.

Civil Damages



Statutory or Actual Damages

- **Greater of:**
 - Not less than \$100 and not greater than \$750 per consumer per incident
 - Or actual damages

Statutory Damages Factors

- Nature and seriousness of the misconduct
- Number of violations
- Persistence of the misconduct
- Length of time over which the misconduct occurred
- Willfulness of the defendant's misconduct
- Defendant's assets, liabilities, and net worth
- Other "relevant circumstances presented by any of the parties"

Two Major Insurance Issues Arising from the CCPA

Number 1:

The CCPA permits the filing of actions by the Consumers and the Attorney General as a result of the misuse or improper handling of personal information. ***No actual harm is required. No actual loss of personal information is required:***

- “Any consumer whose nonencrypted or nonredacted personal information . . . ***is subject to an unauthorized access and exfiltration, theft, or disclosure*** as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action” (Civil Code § 1798.150(a)(1))
- “A business shall be in violation of this title ***if it fails to cure any alleged violation*** within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation” (Civil Code § 1798.155(b)) Injunctive relief is also available.

Two Major Insurance Issues Arising from the CCPA

- Traditional view developed under commercial general liability policies: “[C]osts incurred to prevent future harm are generally not covered by insurance. Courts have held that prophylactic costs incurred to prevent future harm are ‘not caused by the happening of an accident, event, or repeated exposure to conditions but rather result from the prevention of such an occurrence.’” *Bellaire Corporation v. American Empire Surplus Lines*, 115 N.E.3d 805, 811, 2018 -Ohio- 2517 (2018).
- Recent experience in seeking enhancements to cyber policies to cover the CCPA:
 - Insurers have developed endorsements that amend the definition of “Claim” to include a “regulatory proceeding” instituted under the CCPA, or that amend the definition of “regulatory proceeding” to include the CCPA and any rules or regulations promulgated thereunder.
 - This would potentially bring an action filed by the Attorney General seeking an imposition of civil penalties within coverage.
 - Insurers have nearly two years of experience with similar issues arising under the EU’s General Data Protection Regulation.
 - There is a slower recognition of the need for coverage enhancements so that policies respond to consumer actions seeking the recovery of statutory damages under the CCPA in the absence of actual harm. This seems to be more of a lack of awareness by some brokers and underwriters of the need for the enhancement than an underwriting intent not to cover these types of claims.

Two Major Insurance Issues Arising from the CCPA

Number 2:

The insurability of penalties

Many cyber policies will indemnify insureds for the imposition of penalties to the extent permitted by law. The insurability of penalties, however, varies from jurisdiction to jurisdiction.

California Insurance Code § 533.5(b):

“No policy of insurance shall provide, or be construed to provide, any coverage or indemnity for the payment of any fine, penalty, or restitution in any criminal action or proceeding or in any action or proceeding brought pursuant to Chapter 5 (commencing with Section 17200) of Part 2 of, or Chapter 1 (*commencing with Section 17500*) of Part 3 of, Division 7 of the Business and Professions Code by the Attorney General, any district attorney, any city prosecutor, or any county counsel, notwithstanding whether the exclusion or exception regarding this type of coverage or indemnity is expressly stated in the policy.”

Two Major Insurance Issues Arising from the CCPA

The CCPA's civil penalties provision is, however, an *independent grant of statutory authority to the Attorney General to seek the imposition of penalties for a failure to comply with the Act*. The Attorney General does not need to prove a violation of the Business and Professions Code to obtain penalties for a violation of the CCPA.²

A cyber policy that indemnifies the insured for the imposition of penalties thus should also contain a "most favorable jurisdiction" choice of law provision. This would provide that the "insurability" of penalties will be determined under the law any jurisdiction that allows the indemnification or penalties with a substantial relationship to the insurer, the insured, the policy or the underlying claim.³

²The prior version of Section 533.5 was not limited to actions filed under the Business and Professions Code but instead applied to "any civil or criminal action or proceeding in which the recovery of a fine, penalty, or restitution is sought by the Attorney General." *Mt. Hawley Ins. Co. v. Lopez*, 215 Cal.App.4th 1385, 1395-96 (2013)

³The CCPA raises a host of cyber policy issues. Further information is contained in the reproduction of two blog posts from the Morgan Lewis Health Scan Blog, which are reproduced on the following two slides.

Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 1

BLOG POST



HEALTH LAW SCAN

LEGAL INSIGHTS AND PERSPECTIVES FOR THE HEALTHCARE INDUSTRY

Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 1

September 24, 2019

AUTHORS

Jeffrey S. Raskin

The California Consumer Privacy Act (CCPA) is a game-changer. Taking effect on January 1, 2020, the data privacy law creates new statutory rights governing the handling, storage, and sale of personal information. It broadens significantly the definition of “personally identifiable information” over prior statutory enactments. It reaches companies inside *and* outside of California based on revenue or the number of consumers whose personal information is bought, sold, shared, or received by a company. It creates private rights of action permitting the potential recovery of statutory or actual damages for consumers, and a new public form of action for the assessment of fines by the state attorney general.

Will typical cyber-related liability insurance policies respond to actions initiated under the CCPA? In their current form, many likely will not. This post suggests enhancements to existing cyberliability policies to maximize their potential responsiveness to CCPA actions.

1. The CCPA permits actions to be filed, and liability imposed, to *prevent* future harm from happening. Actual harm is not required to sue. Liability insurance policies, however, typically indemnify insureds against damages paid on account of injury or damage. Preventive measures usually are not covered because they do not result from the accident, happening, or event to which the policy responds.

A couple of tweaks—in bold—to typical cyberinsurance provisions can address this problem:

Expand the definition of the types of “wrongful acts” to which the policy responds so that it reads: “Loss, theft, **failure to protect** failure to secure, or unauthorized acquisition of personally identifiable information”

Expand the definition of the type of regulatory action to which the policy responds so that it reads: “A written demand for **compliance with data protection law**, a civil investigative demand, a civil investigative proceeding, or civil proceeding brought by or on behalf of a governmental or regulatory entity **alleging a violation of data protection law**.”

2. The CCPA’s expansive definition of “personally identifiable information” may escape the definition of this term in typical cyber-related liability policies. Any attempt to list the many types of information encompassed by the CCPA is fraught with potential exclusions that could doom an insurance coverage

claim from the outset. It is better to be all encompassing, so that the definition of “personally identifiable information” includes the following:

Information concerning an individual or household that would be considered “personal information” or “personally identifiable information” within the meaning of the California Consumer Privacy Act, any amendments thereto, or any associated regulations promulgated by the attorney general of the State of California.

3. The CCPA permits the attorney general to seek to impose penalties on potential violators, with the proceeds remitted to a consumer privacy fund. Many cyber-related liability policies do not indemnify the insured against its payment of penalties. “Penalties” are not seen as “damages” to which a policy should respond, but instead are viewed as imposed punishment for noncompliance with the law.

Some insurers, however, are willing to offer coverage for the imposition of “penalties.” A potential expansion of the liability coverage afforded under a cyber-related policy could read as follows:

The Insurer will pay on behalf of an Insured claims expenses, regulatory damages, **privacy regulatory fines or penalties** . . . that the Insured is legally obligated to pay because of a privacy regulatory action . . . alleging a wrongful act as defined in this policy.

The policy can then define “privacy regulatory fines or penalties” as “a civil monetary **fine or penalty** payable by an Insured to a governmental or regulatory entity or to the **Consumer Privacy Fund** established under the **California Consumer Privacy Act**.”

These suggestions are not revolutionary. Insurers and insureds have been grappling with related issues arising under the European Union’s General Data Protection Regulation (GDPR), which took effect in May 2018. Some insurance policies have been amended to address the GDPR’s unique challenges.

Insureds and their brokers should examine existing cyber-related liability policies in advance of January 1, 2020, and work with their insurers to address the potential shortfalls in coverage discussed in this post, along with those discussed in a forthcoming companion post.

Tags: **California Consumer Privacy Act. Cyberliability Insurance. Personally Identifiable Information**

➤ [Read more from Health Law Scan](#)

Copyright © 2019 Morgan, Lewis & Bockius LLP. All rights reserved.

Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 2

BLOG POST



HEALTH LAW SCAN

LEGAL INSIGHTS AND PERSPECTIVES FOR THE HEALTHCARE INDUSTRY

Consider Enhancing Cyberliability Insurance Policies to Align with CCPA: Part 2

September 26, 2019

AUTHORS

Jeffrey S. Raskin

Our prior post discussed three potential enhancements to cyber-related liability insurance policies designed to maximize their potential responsiveness to actions initiated by consumers or the state attorney general under the California Consumer Privacy Act (CCPA). Today, we offer four *additional* suggested coverage enhancements for consideration in advance of the CCPA's January 20, 2020, effective date:

4. Our prior post discussed seeking the enhancement cyber-related liability policies so that they cover "penalties" the state attorney general may seek under the CCPA. An additional enhancement is needed, however, since "penalties" might not be legally indemnifiable under the law of a particular jurisdiction whose law could apply to an insured's policy. A standard "choice of law" provision is not optimal because it would fix the law of a single state as necessarily applying to the policy.

A better approach to the jurisdictional variance on the insurability penalties is a provision that the law of the jurisdiction *most favorable to the insurability of penalties will determine* whether the insured can enforce the insurer's agreement to indemnify it for the payment penalties. This provides the insured with many potential choices of law, instead of the law of a single state chosen at the policy's time of issuance.

Potentially applicable jurisdictions under this approach include: (i) California, where the penalty was assessed; (ii) the jurisdiction in which the insured is incorporated; (iii) the jurisdiction in which the insured maintains its principal place of business; (iv) the jurisdiction in which the insured's risk management functions are conducted; (v) the jurisdiction in which the insurer is incorporated; (vi) the jurisdiction in which the insurer maintains its principal place of business; and (vii) the jurisdiction in which the policy was brokered, etc.

5. Liability insurance policies do not indemnify insureds against deliberate wrongdoing, intentionally caused harm, or purposefully fraudulent conduct. The law generally prohibits indemnification for this type of conduct, as well. Lawsuits routinely allege that the defendant committed deliberate misconduct, knowingly or purposefully wrongful actions or purposeful fraud. Most cases, however, are resolved long before a judge or jury assesses whether any of this, in fact, occurred.

To minimize disputes with insurers, and to facilitate the payment of the costs of defense by the insurer

while a CCPA action proceeds, the policy should say that this type of exclusion (however worded) will apply *only* if a final, non-appealable judgment or other decision is entered adjudicating that the insured engaged in the kind of intentional, fraudulent, or deliberate misconduct not covered under the policy. Further protection, in the form of the "most favorable jurisdiction" provision discussed above, is also available.

The likelihood that a "deliberate misconduct" exclusion will bar coverage in the face of an appropriately worded limitation and a "most favorable jurisdiction" choice of law provision is small.

6. An insured can insulate itself further from a "deliberate misconduct" exclusion by isolating the act or knowledge of a "rogue" employee that willfully or knowingly violates the CCPA. A typical provision found in certain liability policies provides that *only* the knowledge or conduct of high-level company executives such as the chief executive officer, chief financial officer, chief information officer, chief privacy officer, chief security officer, chief technology officer, risk manager, general counsel, or similarly identified persons, will be imputed to the insured company. Cyber-related liability policies can include this provision, as well.

7. The CCPA permits courts to issue injunctive or declaratory relief. The cost of complying with this relief is not typically indemnifiable because it does not result in the payment of damages. It usually involves particularized business expenses not subject to meaningful advanced underwriting by the insurer.

The costs of defending against suits seeking declaratory or injunctive relief are, however, normal litigation expenses of the type insurers typically pay. The type of "claims expenses" payable by an insurer under a cyber-related liability policy can be expanded so that it reads:

"Reasonable and necessary fees for a claim defended by an attorney ... as well as other reasonable and necessary fees, costs, and expenses that result from the investigation, adjustment, negotiation, arbitration, defense or appeal of a claim or an action, **including an action seeking injunctive and/or declaratory relief.**"

This would require the insurer to pay the cost of defending a lawsuit seeking injunctive or declaratory relief even though it would not be obligated to pay any compliance costs that might result from the action.

The cyber-related coverage enhancements to address insurance challenges posed by the CCPA, as discussed in this post, are not unique to the CCPA. They appear in many "financial lines" insurance policies such as Directors & Officers, Errors & Omissions, and Fiduciary Liability policies. They do not tend to expand underwriting intent, but rather seek to confirm and codify underwriting intent. Insureds and their brokers should examine their cyber-related liability policies in advance of the January 1, 2020, effective date of the CCPA to determine whether amendments or endorsements to coverage grants and exclusions are needed to address the act's challenges.

Cyber Insurance Webinar Series

Please save the date for our next webinars in the
Cyber Insurance Webinar Series:

February 13, 2020

<https://www.morganlewis.com/events/cyber-insurance-is-your-company-covered-february-2020>

May 7, 2020

<https://www.morganlewis.com/events/cyber-insurance-is-your-company-covered-may-2020>

Mark L. Krotoski



Mark L. Krotoski

Silicon Valley

+1.650.843.7212

mark.krotoski@morganlewis.com

Morgan Lewis

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues.
- Co-Head of Privacy and Cybersecurity practice
- 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.

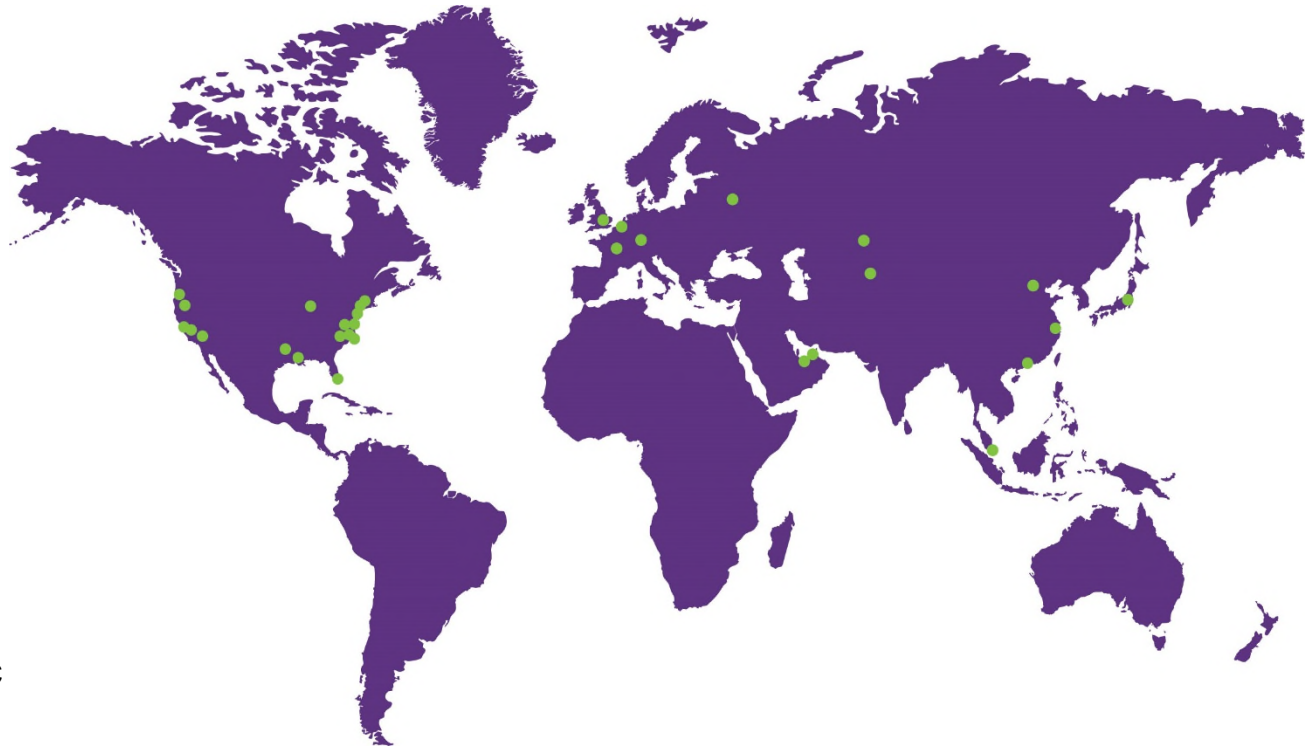
Morgan Lewis

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
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

© 2019 Morgan, Lewis & Bockius LLP
© 2019 Morgan Lewis Stamford LLC
© 2019 Morgan, Lewis & Bockius UK LLP

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.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

Morgan Lewis