
Morgan Lewis
CYBER INSURANCE:
IS YOUR COMPANY COVERED?
Cyber Insurance Webinar Series
Mark L. Krotoski and Jeffrey S. Raskin
September 17, 2019
© 2019 Morgan, Lewis & Bockius LLP

Overview

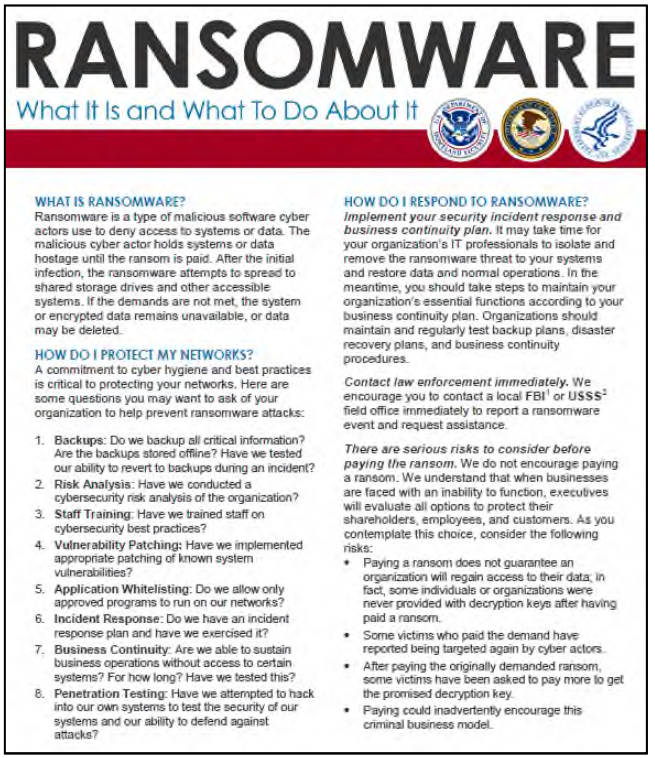
- Covered Options for a Ransomware Attack
- Common Regulatory and Enforcement Issues Following a Data Breach
- Insurance Coverage Issues Under the California Consumer Privacy Act (CCPA)
- Current Issues Under the "Act of War" Exclusion
- Business Email Compromise Issues

CYBER INSURANCE WEBINAR SERIES

WHAT ARE THE COVERED OPTIONS FOR A RANSOMWARE ATTACK?

Ongoing Impact

- "Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network."
- "On average, **more than 4,000 ransomware attacks have occurred daily** since January 1, 2016."
- "This is a **300-percent increase** over the approximately 1,000 attacks per day seen in 2015."



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

Demand


Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy
Check Payment
Decrypt

Baltimore

Baltimore transfers $6 million to pay for ransomware attack; city considers insurance against hacks

By LUKE BROADWATER
BALTIMORE SUN | AUG 28, 2019 | 12:32 PM

Analysis of ransomware used in Baltimore attack indicates hackers needed 'unfettered access' to city computers

By IAN DUNCAN and CHRISTINE ZHANG
MAY 17, 2019 | 4:55 PM

LIGHT FOR ALL
THE SUN
www.baltimoresun.com

https://www.baltimoresun.com/politics/bs-md-ci-ransomware-attack-20190517-story.html
https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html

Baltimore

Ransomware FAQ

Click here for a YouTube playlist of videos addressing Baltimore At Work.

Question: *Why don't we just pay the ransom?*

Answer: I know a lot of residents have been saying we should have just paid the ransom or asking why don't we pay the ransom. Well first, we were advised by both the FBI and Secret Service not to pay the ransom. Second, that's just not the way we operate. We won't reward criminal behavior.

If we paid the ransom:

- There is no guarantee they can or will unlock our system
- There is no way of tracking the payment or even being able to confirm who we are paying the money to, because of the way they requested the payment
- There is no way of knowing if they are leaving other malware on our system to hold us for ransom again in the future

Ultimately, we would still have to take all the steps we have taken to ensure a safe and secure environment. I am confident we have taken the best course of action.

Ransomware Protection and Issues

PRESS RELEASE | City of Borger, Texas

Contact:
Marisa Montoya, Communications Manager
City of Borger
(806) 395-1121
mmontoya@borgertx.gov

FOR IMMEDIATE RELEASE: August 19th, 2019

City of Borger Victim of Ransomware Attack Affecting Local Governments in Texas

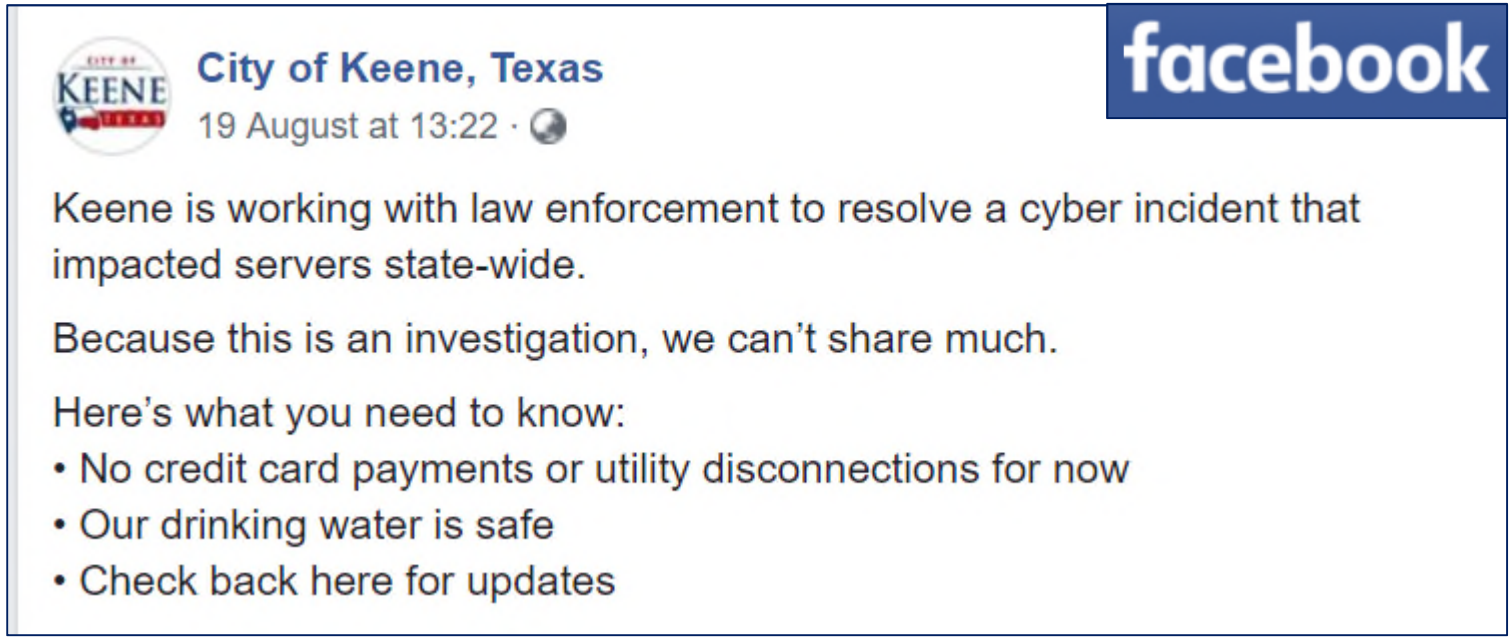
On the morning of August 16, 2019 the City of Borger was one of more than 20 entities in Texas that reported a ransomware attack. Later that morning the State Operations Center (SOC) was activated. At this time, various State and Federal agencies are supporting and responding to the incident; including Texas Department of Information Resources, Texas Division of Emergency Management, Department of Homeland Security, Federal Bureau of Investigation-Cyber Crimes Unit, Federal Emergency Management Agency and others. Responders have reduced the count of confirmed impacted entities to twenty-two. The majority of the affected entities were smaller local governments.The State of Texas computer systems and networks have not been impacted.

The evidence gathered indicates the attacks came from one single threat actor. This attack has impacted normal City business and financial operations and services, however, the City has implemented its continuity of operation plans and the City continues to provide basic and emergency services (Police, Fire, 9-1-1, Animal Control,Water, Wastewater and Solid Waste Collection). The City continues to actively work with responders to bring our computer systems back online and regain full operations. Responders have not yet established a time-frame for when full, normal operations will be restored.

Currently, Vital Statistics (birth and death certificates) remains offline, and the City is unable to take utility or other payments. Until such time as normal operations resume, no late fees will be assessed, and no services will be shut off. City staff along with Federal and State resources continue to make progress on service restoration to limit the duration of the impact. City phones remain active and we will continue to provide services that we are able.

https://www.borgertx.gov/DocumentCenter/View/687/PRESS-RELEASE--City-of-Borger-Victim-of-Ransomware-Attack-Affecting-Local-Governments-in-Texas

Ransomware Protection and Issues



City of Keene, Texas
19 August at 13:22 ·

Keene is working with law enforcement to resolve a cyber incident that impacted servers state-wide.

Because this is an investigation, we can't share much.

Here's what you need to know:
- No credit card payments or utility disconnections for now
- Our drinking water is safe
- Check back here for updates

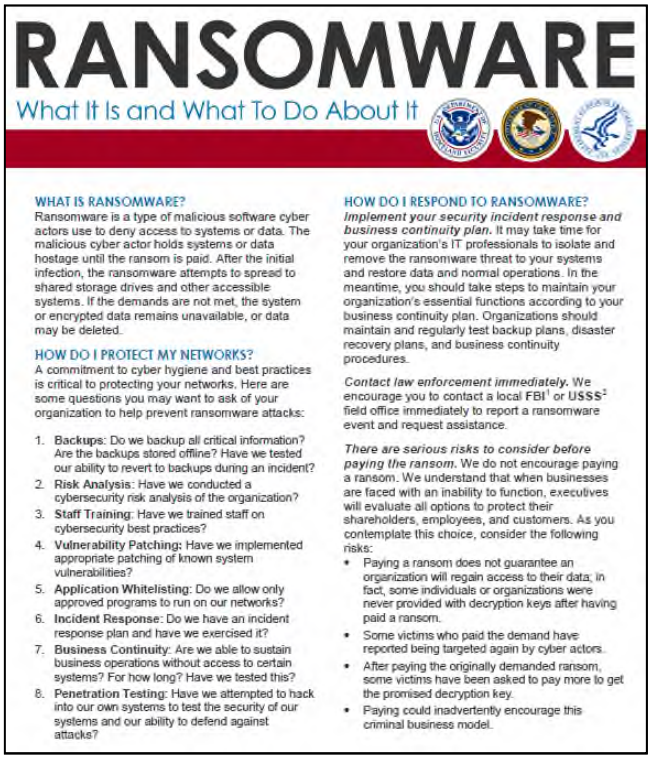
https://www.facebook.com/keenetx/posts/2191835520939218?__tn__=-R

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

Ransomware Protection and Issues

Protection and Prevention

- Offline and Secure Backups
- Avoiding Links or Phishing Schemes with Attachments Containing Malware
- Strong Passwords
- Update Operating Systems, Software, and Patches, and Use Antivirus Software
- 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

Insurance Coverage for Ransomware/Extortion

- Policies responsive to cyber-related incidents often provide first-party coverage against the costs associated with responding to a ransomware incident.
- This typically translates to the cost of money, digital currency, property, or other consideration surrendered as payment to prevent, limit, or respond to a cyber-extortion threat.
- The type of costs either paid or reimbursed, with insurer consent, also include those charged by breach response providers and third-party investigators and advisors assisting the insured in responding and resolving a cyber-extortion threat.

Insurance Coverage for Ransomware/Extortion

- Typical definition of "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.

CYBER INSURANCE WEBINAR SERIES

COMMON REGULATORY AND ENFORCEMENT ISSUES FOLLOWING A DATA BREACH

Yahoo! Inc.: Enforcement Action

- **Fine**: **$35 million**; SEC Order (April 24, 2019)
- **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.
- **Misleading Disclosures**: Risk factor disclosures in annual and quarterly reports (2014 through 2016) "were materially misleading" by claiming "the risk of potential future data breaches . . . without disclosing that a massive data breach had in fact already occurred."
- **Stock Purchase Agreement**: "Affirmative representations denying the existence of any significant data breaches in a July 23, 2016 stock purchase agreement with Verizon."
- Ongoing cooperation

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

Yahoo!, Inc. Litigation

- SEC Action – April 2018
- Securities Class Action – Santa Clara County
- Derivative Lawsuit – Northern District of California
- Individual Class Action – Northern District of California
- DOJ Prosecution Against Hackers

Yahoo! Inc. Litigation

- SEC Action – April 2018
  - **$35 million**; SEC Order (April 2019)
- Securities Class Action – Santa Clara County
  - **$80 million settlement**; (Sept. 2018)
- Derivative Lawsuit – Northern District of California
  - **$29 million settlement** (Jan. 2019)
- Individual Class Action – Northern District of California
  - **$117 million settlement** (July 2019)
- DOJ Prosecution Against Hackers

Coverage in the Wake of Regulatory Enforcement

First Party Coverage

- Data Breach
  - Any actual or reasonably suspected theft, loss, or unauthorized access to, or disclosure of data or hardware containing data that has, or may, compromise the integrity of personally identifiable information, protected health information or confidential business information.
  - Covered Response Costs
    - Reasonable and necessary cost charged by breach response providers to:
      - Respond to data breach reporting requirements
      - Perform computer forensics to determine the existence, cause and scope of the breach
      - Notify individuals of a data breach or suspected data breach.

Coverage in the Wake of Regulatory Enforcement

- Operate a call center to manage data breach inquiries.
- Provide credit or identity fraud monitoring services and restoration services for those whose personally identifiable information was or may have been breached
- Provide medical identity restoration for those whose protected medical information was or may have been breached
- Minimize reputational harm to the insured company by hiring a public relations or crisis management firm

Third-Party Coverage

- Privacy Regulatory Action
  - A written request for information, civil investigative demand, or civil proceeding brought by a governmental or regulatory authority

Coverage in the Wake of Regulatory Enforcement

- Coverage: Insurer will pay claims expenses and regulatory damages the insured is legally obligated to pay as a result of a privacy regulatory action first made against the insured during the policy period alleging a privacy or security wrongful act by the insured, a rogue employee, an outsource provider or a third-party vendor for whose wrongful act the insured is legally responsible
  - Privacy or security wrongful act:
    - Loss, theft, unauthorized acquisition of personally identifiable information, protected health information or confidential business information
    - Violation of law, statute or regulation governing the authenticity, availability, confidentiality, storage, integrity or use of personally identifiable information or protected health information
    - Violation of a data breach reporting requirement
    - Failure to prevent a cyber breach

CYBER INSURANCE WEBINAR SERIES

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

The California Consumer Privacy Act of 2018

- On June 28, 2018, California enacted the California Consumer Privacy Act (CCPA)
  - New unique and comprehensive consumer privacy law
  - New private right of action for security breaches and potential statutory damages

- Effective **January 1, 2020**
  - By September 13, 2019, possible amendments
  - Fall 2019, California Attorney General Regulations

- Broad Impact
  - IAPP estimates that the law will likely affect more than 500,000 US companies doing business in California

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 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

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 CA 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 user name 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, 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 be forgotten
- Right to opt out of the sale of personal information to third parties
- Right to equal service and price

Attorney General Enforcement

- $2,500 and injunctive relief for each violation that the business fails to cure within 30 days of notice of noncompliance
- $7,500 for each intentional violation of the CCPA

- New Consumer Privacy Fund
  - "to fully offset any costs incurred by the state courts and the Attorney General in connection with this title"

Civil Penalties

- **Limited Consumer Private Right of Action**
  - consumer
    (1) Nonencrypted or 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"

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"

Potential Insurance Coverage Challenges Arising from the CCPA

1. Liability can be imposed even in the absence of harm.
2. Many policies may not capture the CCPA's expansive definition of personal information.
3. Many policies do not cover fines or penalties authorized by the CCPA.
4. Many policies have insufficiently narrow "wrongful act" exclusions.
5. Many policies do not pay the costs of defending against actions seeking injunctive or declaratory relief.

Liability Policies Traditionally Cover the Insured for Acts and Omissions That Cause Damage or Harm

- The historical function of liability insurance coverage is to indemnify the insured for the money it pays as damages for bodily injury, property damage, advertising injury, defamation, etc.
- A fairly typical cyber coverage insuring agreement:

  "The Insurer will pay on behalf of an Insured claims expenses and damages . . . that the Insured is legally obligated to pay as a result of a claim . . . alleging a privacy and security wrongful act."

  "Privacy Regulatory Defense, Awards and Fines

  The Insurer will pay on behalf of an Insured claims expenses and regulatory damages . . . that the Insured is legally obligated to pay as a result of a privacy regulatory action . . . alleging a privacy or security wrongful act."

Liability Policies Traditionally Cover the Insured for Acts and Omissions That Cause Damage or Harm

- A narrow definition of "Privacy or Security Wrongful Act" with reference to personally identifiable information:

> "Loss, theft or unauthorized acquisition of personally identifiable information . . . ."

- The CCPA permits the filing of actions by the Consumers as a result of the misuse or improper handling of personal information. The Attorney General can bring an action based on a general failure to comply with the CCPA. Neither consumers nor the Attorney General are required to show that any person was actually harmed to bring an action.

Liability Policies Traditionally Cover the Insured for Acts and Omissions That Cause Damage or Harm

- Consumers and the Attorney General must only provide 30 days written notice and provide an opportunity to cure before bringing an action.
    - "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)). Statutory damages, actual damages and injunctive and declaratory relief are available.

Liability Policies Traditionally Cover the Insured for Acts and Omissions That Cause Damage or Harm

- "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.

Liability Policies Traditionally Cover the Insured for Acts and Omissions That Cause Damage or Harm

- 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).

Liability Policies Traditionally Cover the Insured for Acts and Omissions That Cause Damage or Harm

- Potential solutions:
  - Expand the definition of "Privacy or Security Wrongful Act" quoted above so that it reads: "Loss, theft, ***failure to protect, failure to secure*** or unauthorized acquisition of personally identifiable information . . . ."
  - Include a broad definition of the type of "regulatory enforcement action" to which the policy responds: "A written request for information, ***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***."

Policies May Not Capture the CCPA's Expansive Definition of Personal Information

- Devising a definition of "Personal Information" or "Personally Identifiable Information" that captures the breadth of the CCPA is a solvable challenge.
- A somewhat broad definition appearing in current cyber policies: "Information, whether printed or digital, encrypted or unencrypted, in the care, custody or control of the Insured, or outside provider, that alone or in conjunction with other information or data, can be used to uniquely identify an individual"

Policies May Not Capture the CCPA's Expansive Definition of Personal Information

- Add a separate part (b) of the definition: "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."
- A separate part (c) of the definition can expand the definition to include "personal information" or "personally identifiable information" within the meaning of the laws of other states or the federal government to the extent that they come into being during the term of the policy.

Many Policies Do Not Cover Penalties the Attorney General Is Authorized to Seek

- Insurance coverage for "fines" and "penalties" has historically been a difficult question. "Fines" and "penalties" are not considered to be "damages" typically covered under an insurance policy, but rather punishment for a violation of law.
- Underwriters traditionally would not cover fines and penalties, in part, because they are not considered to be a normal risk of doing business.
- Fines and penalties are not legally insurable on a state-by-state basis to the extent that they are imposed because of intentional misconduct, reckless misconduct, intentionally caused harm, or recklessly caused harm. Jurisdictions vary considerably.

Many Policies Do Not Cover Penalties the Attorney General Is Authorized to Seek

- Include within the liability portion of the policy coverage for "regulatory defense, awards, fines and penalties":
    - "The Insurer will pay on behalf of an Insured claims expenses, regulatory damages, privacy regulatory fines . . . that the insured is legally obligated to pay because of a privacy regulatory action . . . alleging a privacy or security wrongful act . . . ."
    - Define "privacy regulatory fines" 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."

Many Policies Do Not Cover Penalties the Attorney General Is Authorized to Seek

- Address the jurisdictional variance on the insurability of fines and penalties with a provision that the law of the jurisdiction ***most favorable to the insurability of fines and penalties*** will apply. Potentially applicable jurisdictions, besides California where the penalty was assessed, include the jurisdiction in which the insured is incorporated or maintains its principal place of business, or the jurisdiction where the insurer is incorporated or maintains its principal place of business.

"Intentional," "Deliberate," and "Fraudulent" Harm Exclusions Are Often Too Broad

- Insurance coverage is generally unavailable as a matter of law for intentionally, deliberately, or fraudulently caused injury or harm. Public policy views this as not providing a disincentive against deliberately causing injury.

- A problem ensues because lawsuits often allege that the defendant committed deliberate misconduct, knowingly or purposefully wrongful actions or fraud. Most cases, however, are resolved long before a judge or jury assesses whether this, in fact, occurred.

- Many policies contain blanket exclusions for losses arising out of "fraudulent" or "dishonest" acts, "knowingly wrongful" acts, or an "intentional" violation of law by the insured. This can lead to disputes.

"Intentional," "Deliberate," and "Fraudulent" Harm Exclusions Are Often Too Broad

- To avoid disputes, and to facilitate the payment or advancement of the costs of defense by the insurer while an action proceeds, the policy should say that this type of exclusion (however worded) will only apply if there is a final, nonappealable judgment adjudicating that the insured engaged in the kind of intentional, fraudulent, or deliberate misconduct not covered under the policy. The likelihood that the exclusion, with the appropriately worded limitation, will bar coverage is small.

"Intentional," "Deliberate," and "Fraudulent" Harm Exclusions Are Often Too Broad

- Further protections are potentially available:
    - "Most favorable" jurisdiction provision, as discussed above, can be inserted here.
    - A provision "imputing" the knowledge or conduct of a particular person to the insured entity can be limited to an Executive Officer: For purposes of determining the applicability of this exclusion, the knowledge or conduct of: (1) A natural person Insured shall not be imputed to any other Insured; but (2) an Executive Officer shall be imputed to the Insured Company.
    - Executive Officer can be defined as, for example, "any duly elected or appointed Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Privacy Officer, Chief Security Officer, Chief Technology Officer, Risk Manager, General Counsel, and in-house attorney in charge of litigation or the functional equivalent of any of the foregoing, of an Insured Company."

Claims Expenses Can and Should Be Payable for the Costs of Defending Actions Seeking Declaratory nd/or Injunctive Relief

- Insurance policies typically do not cover the costs of complying with declaratory relief and injunctions. These do not involve the paying of damages and often involve particularized business expenses not subject to meaningful advanced underwriting.

- The costs of defending against suits seeking declaratory or injunctive relief are, however, normal litigation expenses of the type insurers typically pay.

Claims Expenses Can and Should Be Payable for the Costs of Defending Actions Seeking Declaratory nd/or Injunctive Relief

- Typical definition of payable "claims expenses": "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."
- This 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 seeking injunctive and/or declaratory relief***."
- If the policy has an exclusion for declaratory and injunctive relief, it could "except" the payment of claims expenses incurred defending such actions.

CYBER INSURANCE WEBINAR SERIES

CURRENT ISSUES UNDER THE "ACT OF WAR" EXCLUSION

Cyber Threats and Risks

- 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

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

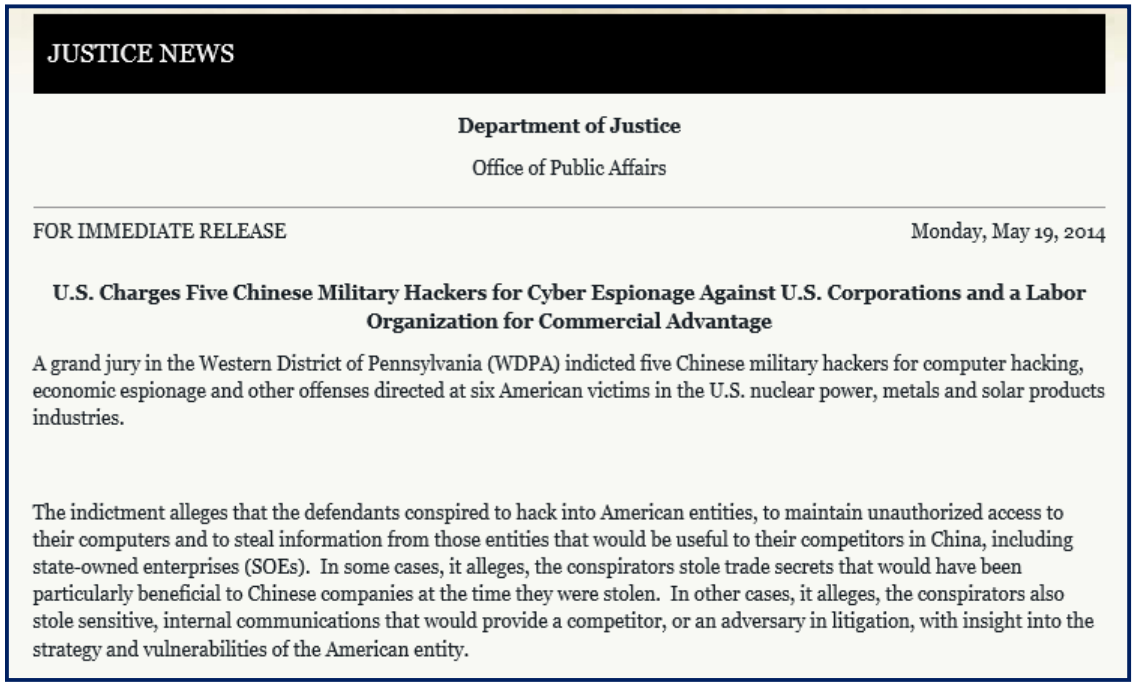
FBI National Press Office
(202) 324-3691

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.

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

Chinese Military Hackers



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Monday, May 19, 2014

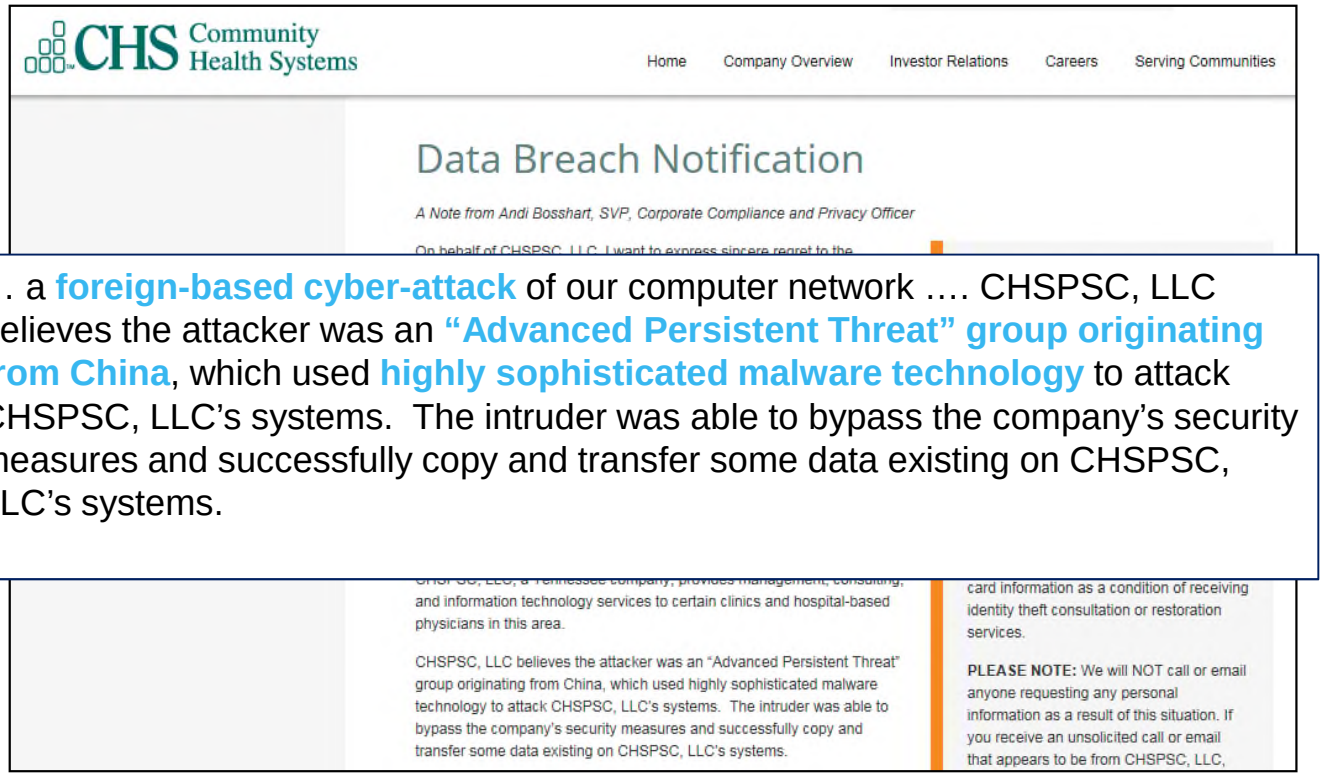
U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.

http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

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.

NotPetya

Statement from the Press Secretary

FOREIGN POLICY | Issued on: February 15, 2018

★ ★ ★

In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.

The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.

https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

Exclusion

This Policy **excludes loss or damage directly or indirectly caused by or resulting from any of the following** regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss . . .

2) a) **hostile or warlike action in time of peace or war**, including action in hindering, combating, or defending against an actual, impending, or expected attack by any:

(i) government or sovereign power (de jure or de facto);

(ii) military, naval, or air force; or

(iii) agent or authority of any party specified in i or ii above.

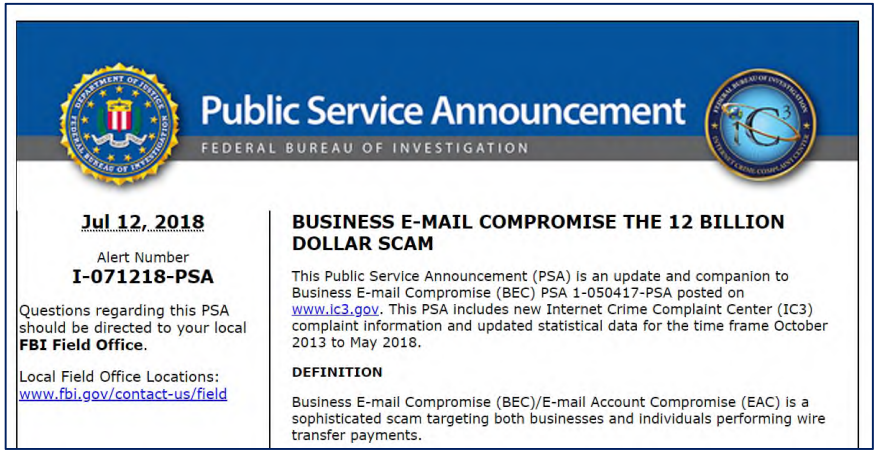
"Act of War" Exclusion Questions

- What is a "warlike action"?
- What is a "warlike action in time of peace"?
- To what extent is the use of physical force required for a "warlike action" to have occurred? Is using a computer to launch a cyber attack the employment of "physical force" against a network or other computers?
- Who determines whether a "hostile or warlike action" attributed to a "government or sovereign power" occurred? Who determines that it was effectuated by an "agent or authority" of a government or sovereign power? The United States government? The government of France? The government of Syria? The government of the People's Republic of China? Will these governments share the basis of their determination? Would it be classified? Secret? Confidential?

CYBER INSURANCE WEBINAR SERIES

BUSINESS EMAIL COMPROMISE ISSUES

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

Criminal Prosecutions

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Tuesday, September 10, 2019

281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes

74 Alleged Fraudsters Arrested in the United States

Federal authorities announced today a significant coordinated effort to disrupt Business Email Compromise (BEC) schemes that are designed to intercept and hijack wire transfers from businesses and individuals, including many senior citizens. Operation reWired, a coordinated law enforcement effort by the U.S. Department of Justice, U.S. Department of Homeland Security, U.S. Department of the Treasury, U.S. Postal Inspection Service, and the U.S. Department of State, was conducted over a four-month period, resulting in 281 arrests in the United States and overseas, including 167 in Nigeria, 18 in Turkey and 15 in Ghana. Arrests were also made in France, Italy, Japan, Kenya, Malaysia, and the United Kingdom (UK). The operation also resulted in the seizure of nearly $3.7 million.

BEC, also known as "cyber-enabled financial fraud," is a sophisticated scam often targeting employees with access to company finances and businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The same criminal organizations that perpetrate BEC also exploit individual victims, often real estate purchasers, the elderly, and others, by convincing them to make wire transfers to bank accounts controlled by the criminals. This is often accomplished by impersonating a key employee or business partner after obtaining access to that person's email account or sometimes done through romance and lottery scams. BEC scams may involve fraudulent requests for checks rather than wire transfers; they may target sensitive information such as personally identifiable information (PII) or employee tax records instead of, or in addition to, money; and they may not involve an actual "compromise" of an email account or computer network. Foreign citizens perpetrate many BEC scams. Those individuals are often members of transnational criminal organizations, which originated in Nigeria but have spread throughout the world.

https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds

Update on Business Email Compromise Claims

- Basic definition: "Business Email Compromise" (BEC) is an exploit in which an attacker obtains access to a business email account and imitates the owner's identity, in order to defraud the company and its employees, customers or partners. Often, an attacker will create an account with an email address almost identical to one on the corporate network, relying on the assumed trust between the victim and their email account. BEC is sometimes described as a 'man-in-the-email attack' . . . .

- At an appropriate time – usually when the employee being impersonated is out of the office – the attacker will send a bogus email to an employee in the finance department. A request is made for an immediate wire transfer, usually to any trusted vendor. The targeted employee thinks the money is being sent to the expected account, but the account numbers have been altered slightly, and the transfer is actually deposited in the account controlled by the criminal group." (Definition from Barracuda Networks)

Update on Business Email Compromise Claims

- *Childrens Place, Inc. v. Great American Insurance Company*, 2019 WL 1857118 (D.N.J. April 25, 2019):
  - TCP alleged that a sophisticated scheme over a six-week period caused it to send nearly $1,000,000 to an account that it believed erroneously to be owed by one of its vendors. The perpetrator did the following:
    - Falsified email domain names to appear virtually identical to those of individuals working at TCP's vendor
    - Accessed and infiltrated the vendor's web email service, and intercepted emails sent between the vendor and TCP
    - Intercepted TCP's Vendor Setup Form, which included payment instructions, and sent it to the vendor, making it appear to come from TCP. The vendor completed the form and returned it to the perpetrator, believing it actually came from TCP

Update on Business Email Compromise Claims

- Altered the payment instructions on the Vendor Setup Form to include directions to pay a bank account associated with the perpetrator.

- In short, the perpetrator "intercepted an email conversation between TCP" and [the vendor] "inserted itself into the conversation"; "requested a change of bank information"; and fraudulently "direct[ed] TCP to pay [the vendor] using [the] new bank account number."

- TCP's "Crime Protection Policy" defined "computer fraud":
  - "Loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money, securities or other property from your premises or banking premises to a person, entity, place or account outside your control."

Update on Business Email Compromise Claims

- The insurer asserted on a motion to dismiss that TCP could not plead that the perpetrator gained "direct access" to its "computer system" in order to cause a transfer of money to the perpetrator's account. The court disagreed. It noted that TCP alleged that the perpetrator gained access to TCP's email system, intercepted email messages between TCP and the vendor, and inserted itself into conversations between TCP and the vendor. The court held that, if proven, this would satisfy the "direct access" requirement for coverage under the Crime Protection Policy.

- The insurer also asserted that TCP did not plead satisfaction with the causation requirement in the computer fraud coverage. The court rejected this assertion, as well, because TCP alleged that its employees transferred funds erroneously to the perpetrator's account as a direct result of the perpetrator's access to TCP's computer system. The insurer's proposed conclusion "that the [perpetrator's] activities 'were not the cause of the actual funds transfers' is 'premature at the motion to dismiss stage.'"

Update on Business Email Compromise Claims

- *SS&C Technologies Holdings, Inc. v. AIG Specialty Insurance Co.*, U.S. Dist. Court, S.D.N.Y., 19-cv-7859 (filed Aug. 21, 2019).
    - New filing seeking coverage under a $10,000,000 professional liability policy resulting from a business email compromise.
    - SS&C administered the accounts of Tillage Commodities Fund LP, and also made transactions on its behalf. Perpetrators used "spoofed" and "lookalike" emails to cause SS&C to make fraudulent transfers of $5.9 million from Tillage accounts in Hong Kong over a three-week period.

Update on Business Email Compromise Claims

- Tillage sued SS&C. The case settled in May 2019.
- Although the insurer defended the lawsuit, it refused to cover the settlement based on six policy exclusions, including a fraudulent or dishonest acts exclusion, an exclusion for funds lost during interinsured transactions, an exclusion for contractually assumed obligations, and an exclusion for losses resulting from SS&C's alleged discretionary authority over client accounts.

- The two cases show that insurers will continue to contest coverage for business email compromise claims based on issues of causation and based on the application of exclusions to coverage.

Cyber Insurance Webinar Series

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

December 10, 2019

https://www.morganlewis.com/events/cyber-insurance-is-your-company-covered-december-2019

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

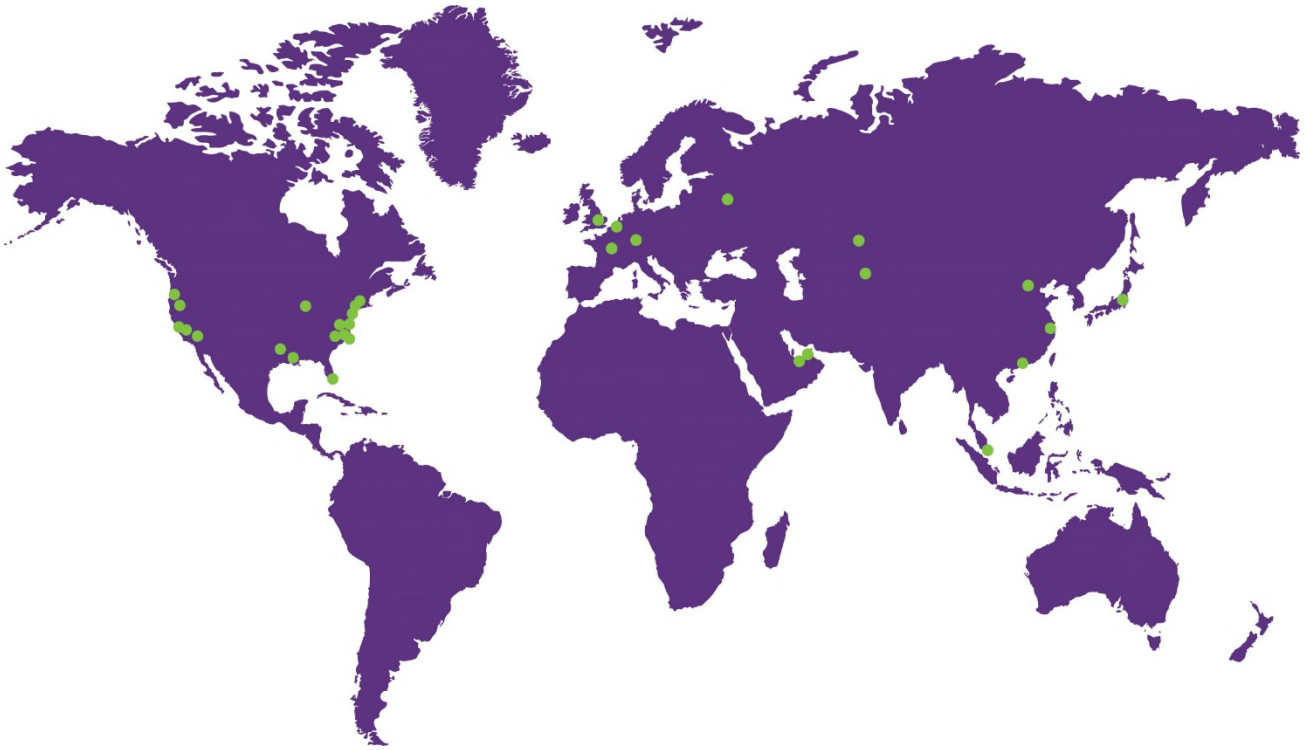
- Jeffrey is the head of Morgan Lewis's Insurance Recovery Practice in the San Francisco office. He advises clients in litigation, mediation, and arbitration around insurance coverage matters, and intellectual property, commercial, real estate, and environmental disputes. Head of Morgan Lewis's Insurance 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

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

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.