

Morgan Lewis

GLOBAL PUBLIC COMPANY ACADEMY

**CYBERSECURITY
AND RELATED
DEVELOPMENTS**

Mark Krotoski

Emily Drazan Chapman



Overview

- I. Cyber Threat Environment**
- II. Significant Costs and Consequences**
- III. Recent Case Study**
- IV. Heightened Regulatory Enforcement**
- V. Morgan Lewis Guidance and Services**
- VI. Q&A**

Preliminary Note

- Comments during this presentation are based upon:
 - Publicly available information;
 - General observations and experience; and
 - Not on any specific client case information.

CYBER THREAT ENVIRONMENT



Reported Internet Crime



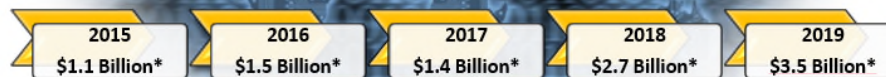
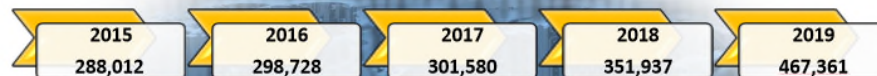
Reported Internet Crime



IC3 Complaint Statistics

Last Five Years

1,707,618 TOTAL COMPLAINTS

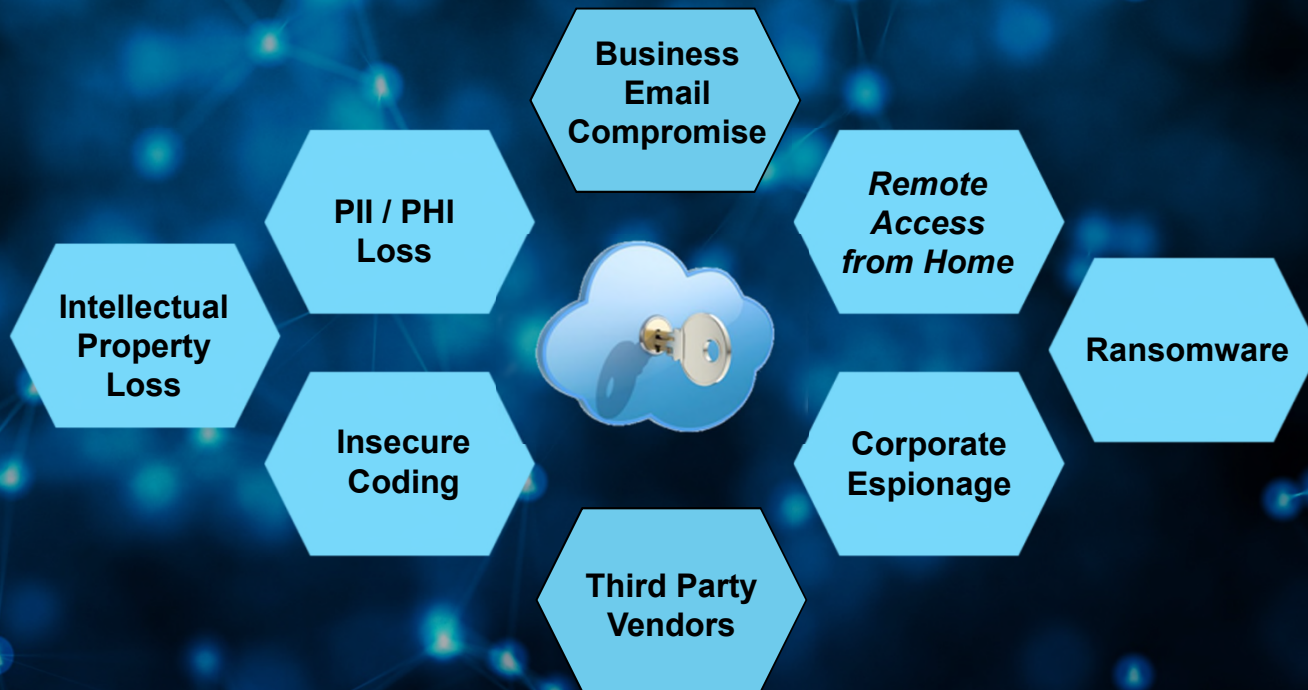


\$10.2 Billion TOTAL LOSSES*

(Rounded to the nearest million)



Cyber Landscape and Risks



Key Actors
Organized Cyber Crime
State Sponsored
Hackers for Hire
Hacktivists
Third Party Vendor Attacks
Insider Threat
Inadvertence

Spear Phishing Attacks

- Target particular users to entice them into opening an attachment or clicking on a link which launches malware on the system
 - Nearly “80% of all espionage-motivated attacks used either a link or attachment in a phishing email to gain access to their victim’s environment”
 - Cyber criminals are “more frequently incorporating website certificates—third-party verification that a site is secure—when they send potential victims emails that imitate trustworthy companies or email contacts”
- “Do not trust a website just because it has a lock icon or “https” in the browser address bar.”

Business Email Compromise



Upon compromising victim email accounts, cyber criminals analyze the content of compromised email accounts for evidence of financial transactions. Often, the actors configure mailbox rules of a compromised account to delete key messages. They may also enable automatic forwarding to an outside email account.

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

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 July 2019:

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

- 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: 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 fraudsters
- Stop funds
 - Alert the company's financial institution promptly concerning suspected fraud to stop the transfer of funds

Ransomware Demand



Ransomware Demands

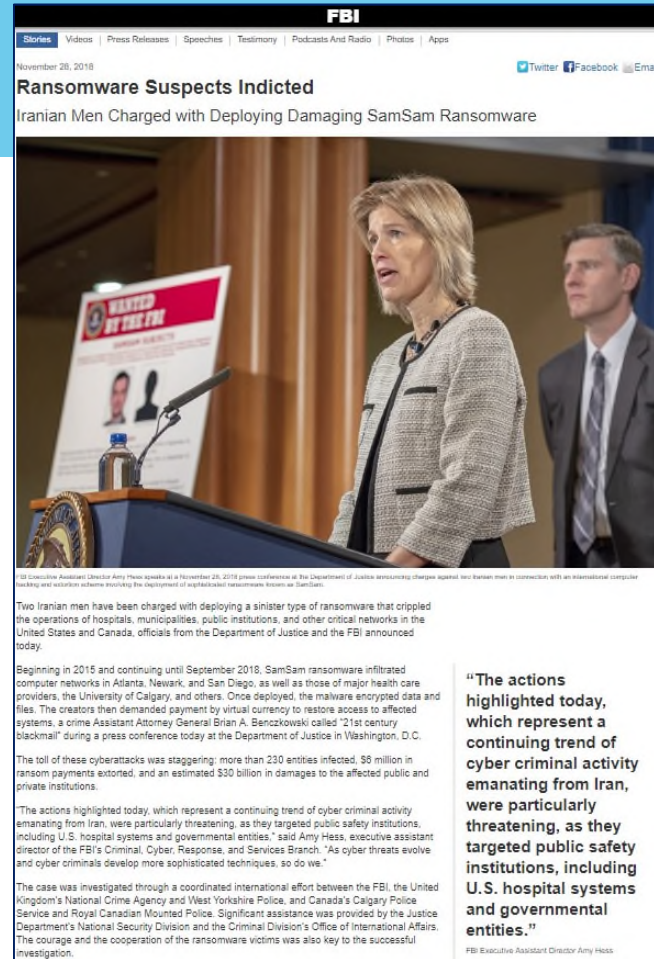
- “The FBI has observed cyber criminals using the following techniques to infect victims with ransomware:
 - Email phishing campaigns
 - Remote Desktop Protocol vulnerabilities
 - Software vulnerabilities
- “In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.”
- “The most important defense for any organization against ransomware is a **robust system of backups**. Having a recent backup to restore from could prevent a ransomware attack from crippling your organization.”

Ransomware Demands

- “Beginning in 2015 and continuing until September 2018, SamSam ransomware infiltrated computer networks in Atlanta, Newark, and San Diego, as well as those of major health care providers, the University of Calgary, and others. Once deployed, the malware encrypted data and files. The creators then demanded payment by virtual currency to restore access to affected systems.”
- “The toll of these cyberattacks was staggering: **more than 230 entities infected, \$6 million in ransom payments extorted, and an estimated \$30 billion in damages** to the affected public and private institutions.”
- “Victims were infected with the ransomware through vulnerabilities found in common software and network access points.” Executive assistant director of the FBI’s Criminal, Cyber, Response, and Services Branch, Amy Hess, stated, “We all need to do our part to make sure that our systems are as strong and secure and protected as possible.”

Morgan Lewis

<https://www.fbi.gov/news/stories/iranian-ransomware-suspects-indicted-112818>



The image is a screenshot of an FBI news article. At the top, the FBI logo is visible, along with navigation links for Stories, Videos, Press Releases, Speeches, Testimony, Podcasts And Radio, Photos, and Apps. The date is November 28, 2018. The article title is "Ransomware Suspects Indicted" and the sub-headline is "Iranian Men Charged with Deploying Damaging SamSam Ransomware". Below the text is a photograph of FBI Executive Assistant Director Amy Hess speaking at a podium during a press conference. A man in a suit stands behind her. A sign in the background reads "WANTED BY THE FBI".

108 Executive Assistant Director Amy Hess speaks at a November 28, 2018 press conference at the Department of Justice announcing charges against two Iranian men in connection with an international computer hacking and extortion scheme involving the deployment of sophisticated ransomware known as SamSam.

Two Iranian men have been charged with deploying a sinister type of ransomware that crippled the operations of hospitals, municipalities, public institutions, and other critical networks in the United States and Canada, officials from the Department of Justice and the FBI announced today.

Beginning in 2015 and continuing until September 2018, SamSam ransomware infiltrated computer networks in Atlanta, Newark, and San Diego, as well as those of major health care providers, the University of Calgary, and others. Once deployed, the malware encrypted data and files. The creators then demanded payment by virtual currency to restore access to affected systems, a crime Assistant Attorney General Brian A. Benzczkowski called “21st century blackmail” during a press conference today at the Department of Justice in Washington, D.C.

The toll of these cyberattacks was staggering; more than 230 entities infected, \$6 million in ransom payments extorted, and an estimated \$30 billion in damages to the affected public and private institutions.

The actions highlighted today, which represent a continuing trend of cyber criminal activity emanating from Iran, were particularly threatening, as they targeted public safety institutions, including U.S. hospital systems and governmental entities,” said Amy Hess, executive assistant director of the FBI’s Criminal, Cyber, Response, and Services Branch. “As cyber threats evolve and cyber criminals develop more sophisticated techniques, so do we.”

The case was investigated through a coordinated international effort between the FBI, the United Kingdom’s National Crime Agency and West Yorkshire Police, and Canada’s Calgary Police Service and Royal Canadian Mounted Police. Significant assistance was provided by the Justice Department’s National Security Division and the Criminal Division’s Office of International Affairs. The courage and the cooperation of the ransomware victims was also key to the successful investigation.

FBI Executive Assistant Director Amy Hess

“The actions highlighted today, which represent a continuing trend of cyber criminal activity emanating from Iran, were particularly threatening, as they targeted public safety institutions, including U.S. hospital systems and governmental entities.”



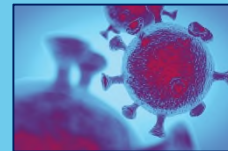
IF MY SYSTEM IS INFECTED, SHOULD I PAY THE RANSOM? SHOULD I CONTACT THE FBI?

The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to law enforcement. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

New Cybersecurity Threats



LILY HAY NEWMAN

SECURITY 03.19.2020 02:12 PM

Coronavirus Sets the Stage for Hacking Mayhem

As more people work from home and anxiety mounts, expect cyberattacks of all sorts to take advantage.



ComputerWeekly.com IT Management Industry Sectors Technology Topics Search Computer Weekly

Coronavirus now possibly largest-ever cyber security threat

The cumulative volume of coronavirus-related email lures and other threats is the largest collection of attack types exploiting a single theme for years, possibly ever

By Alex Scroton, Security Editor Published: 18 Mar 2020 15:47

The total volume of phishing emails and other security threats relating to the Covid-19 coronavirus now represents the largest coalescing of [cyber attack](#) types around a single theme that has been seen in a long time, and possibly ever, according to Sherrod DeGrippe, senior director of threat research and detection at Proofpoint.

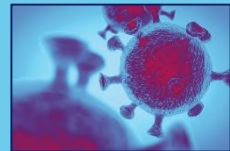
How to get the most out of the Internet of Things **CIO Trends #7**

Tailoring your IT operating model to the digital age **Free Download** ComputerWeekly.com

Morgan Lewis

<https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/>
<https://www.computerweekly.com/news/252480238/Coronavirus-now-possibly-largest-ever-cyber-security-threat>

New Cybersecurity Threats



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



April 01, 2020

Alert Number
I-040120-PSA

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

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

CYBER ACTORS TAKE ADVANTAGE OF COVID-19 PANDEMIC TO EXPLOIT INCREASED USE OF VIRTUAL ENVIRONMENTS

The FBI anticipates cyber actors will exploit increased use of virtual environments by government agencies, the private sector, private organizations, and individuals as a result of the COVID-19 pandemic. Computer systems and virtual environments provide essential communication services for telework and education, in addition to conducting regular business. Cyber actors exploit vulnerabilities in these systems to steal sensitive information, target individuals and businesses performing financial transactions, and engage in extortion.

As of March 30 2020, the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 1,200 complaints related to COVID-19 scams. In recent weeks, cyber actors have engaged in phishing campaigns against first responders, launched DDoS attacks against government agencies, deployed ransomware at medical facilities, and created fake COVID-19 websites that quietly download malware to victim devices. Based on recent trends, the FBI assesses these same groups will target businesses and individuals working from home via telework software vulnerabilities, education technology platforms, and new Business Email Compromise schemes.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



March 20, 2020

Alert Number
I-032020-PSA

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

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

FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC

Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them. Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. The FBI advises you to be on the lookout for the following:

Fake CDC Emails. Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.

Phishing Emails. Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. While talk of economic stimulus checks has been in the news cycle, government agencies are *not* sending unsolicited emails seeking your private information in order to send you money. Phishing emails may also claim to be related to:

- Charitable contributions
- General financial relief
- Airline carrier refunds
- Fake cures and vaccines
- Fake testing kits

Be Aware of COVID-19 Scams



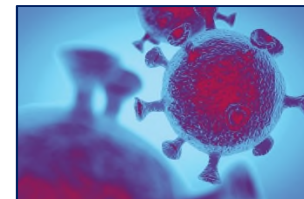
Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, April 22, 2020

Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams

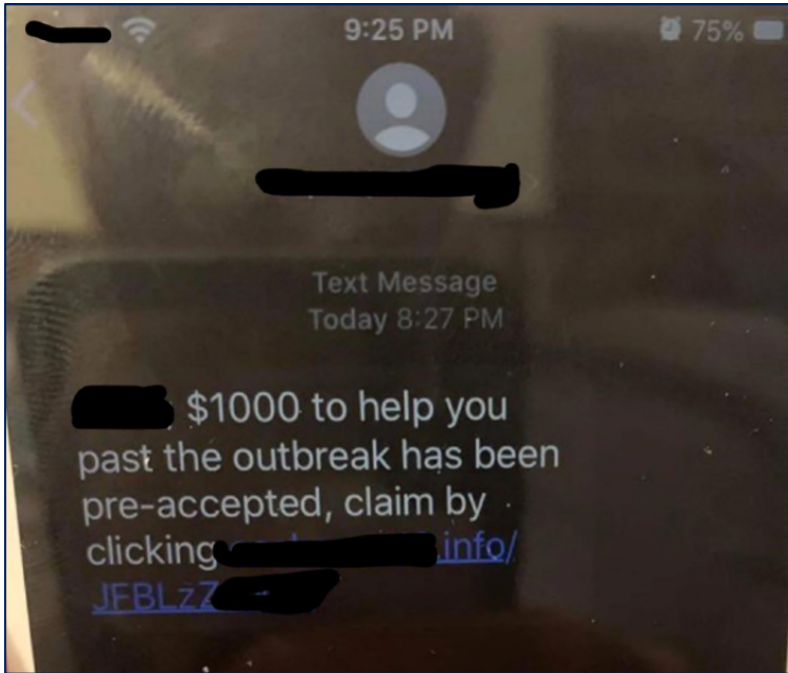
Hundreds of Domains Disrupted Through Public and Private Sector Cooperative Efforts

Federal authorities announced today that an ongoing cooperative effort between law enforcement and a number of private-sector companies, including multiple internet domain providers and registrars, has disrupted hundreds of internet domains used to exploit the COVID-19 pandemic to commit fraud and other crimes.



As of April 21, 2020, the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 3,600 complaints related to COVID-19 scams, many of which operated from websites that advertised fake vaccines and cures, operated fraudulent charity drives, delivered malware, or hosted various other types of scams. To attract traffic, these websites often utilized domain names that contained words such as "covid19," or "coronavirus." In some cases, the fraudulent sites purported to be run by, or affiliated with, public health organizations or agencies.

Be Aware of COVID-19 Scams



From: U.S Treasury [redacted]
Sent: [redacted] March 11, 2020 [redacted]
To: Recipients [redacted]
Subject: COVID-19 Funds Release Update.

New information is being released by The U.S. Treasury About The global funds release Programe, initiated by the world health organization (W.H.O) and empowered by The World bank Organisation.

Your are among the First Email ID batch list to receive payment \$450,000.00 on this exercise,the purpose for these funds is to give relief to the global citizens of the world, due to corona virus pandemic which is the reason the world bank decided to carry out this exercise of empowerment to humanity globally.

You are Assigned to a Senior supervisor Agent who will handle your filing and also monitor the processing of your funds release.He also will be responsible to give our office report about your empowerment funds usage.

We plan to create a world where every one becomes financially independent,stable and individual accountability. You are to reconfirm your details below for immediate payment filing.

Full Name :
Address:
City / Country:
Profession:
Phone Number:
Gender:
Birth Date:
Identification

Sincerely
U.S Treasury Headquarters.
Treasury Building 1500 Pennsylvania Avenue,
NW Washington, D.C.,
United States Of America.

Be Aware of COVID-19 Scams



- Independently **verify the identity** of any company, charity, or individual that contacts you regarding COVID-19.
- **Check the websites and email addresses** offering information, products, or services related to COVID-19.
 - For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov."
- Be **wary of unsolicited emails** offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the public this way.
- Do not click on links or open email attachments from **unknown or unverified sources**. Doing so could download a virus onto your computer or device.
- Make sure the **anti-malware** and **anti-virus software** on your computer is operating and **up to date**. Keep your operating system up to date as well.
- Ignore offers for a **COVID-19 vaccine, cure, or treatment**. Remember, if a vaccine becomes available, you will not hear about it for the first time through an email, online ad, or unsolicited sales pitch.
- Check **online reviews** of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.
- **Research any charities or crowdfunding sites** soliciting donations in connection with COVID-19 before giving any donation.
- **Be wary** of any business, charity, or individual requesting payments or donations in **cash, by wire transfer, gift card, or through the mail**. Do not send money through any of these channels.

Key Security Issues

- **Secure Connections**

- No public wi-fi or open internet connections
- VPN / Encrypted connections
- Password-protected connections
- Multi-Factor Authentication (MFA)

- **Secure End Points (Data At Rest)**

- Encryption
- Endpoint Protection Platforms
- Endpoint Detection and Response

- **BYOD**

- Layers of control on access to data
- Mobile device management

- **Strong Passwords**

- Computers, devices
- Network access

- **Secure Documents**

- Secure, locked storage
- Return for cross-shredding

- **Protecting Trade Secrets and Confidential Information**

- Reasonable measures
- Layers of security

- **Training**

- Alert and aware to new risks
- Promote culture of cybersecurity

- **Company Policies**

- Telework Security Policy
- Company Confidential Information Policy
- BYOD (Bring Your Own Device to Work) Policy

- **Test Incident Response Plan**

- Are you prepared for an incident?
- Emergency contact information
- Business continuity issues



SIGNIFICANT COSTS AND CONSEQUENCES

COMPLEX, COSTLY, BURDENSOME



2019 Cost of Data Breach Report

Key findings:

The average total cost of a data breach in the U.S. for the companies studied has grown from \$3.54 million in 2006 to \$8.19 million in 2019, a 130 percent increase over 14 years.

\$3.54^M

US total cost in 2006

\$8.19^M

US total cost in 2019

The Middle East had the highest average number of breached records, 38,800, compared to the global average of 25,575.

38,800

Middle East average number of breached records.

25,575

Global average of breached records.

The average total cost of a data breach in the healthcare industry was \$6.45 million, or 65 percent higher than the average total cost of a data breach.

\$6.45^M

Average total cost of a data breach in the healthcare industry.

65%

65 percent higher than the average total cost of a data breach.

Smaller organizations had higher costs relative to their size than larger organizations. The total cost for organizations with more than 25,000 employees averaged \$204 per employee.

\$204

per employee

\$3,533

per employee

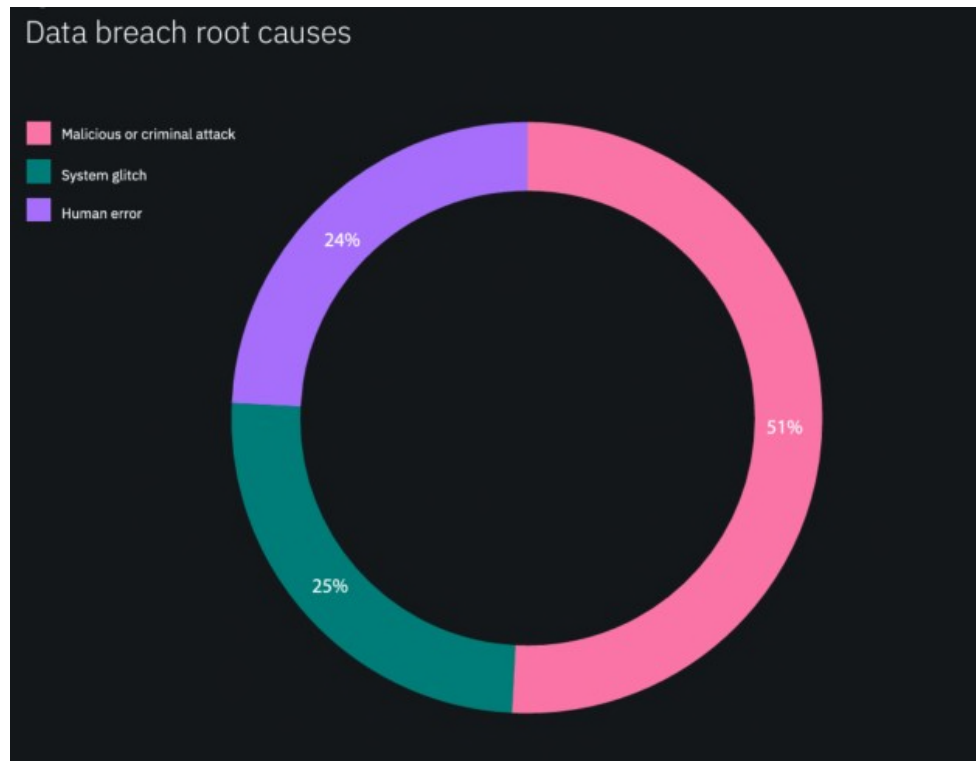
Organizations with between 500 and 1,000 employees had an average cost of \$3,533 per employee.

Breach costs at organizations with more than 25,000 employees averages \$204 per employee.

Breach costs at organizations with between 500 and 1,000 employees have an average cost of \$3,533 per employee.

Root Cause of Data Breach

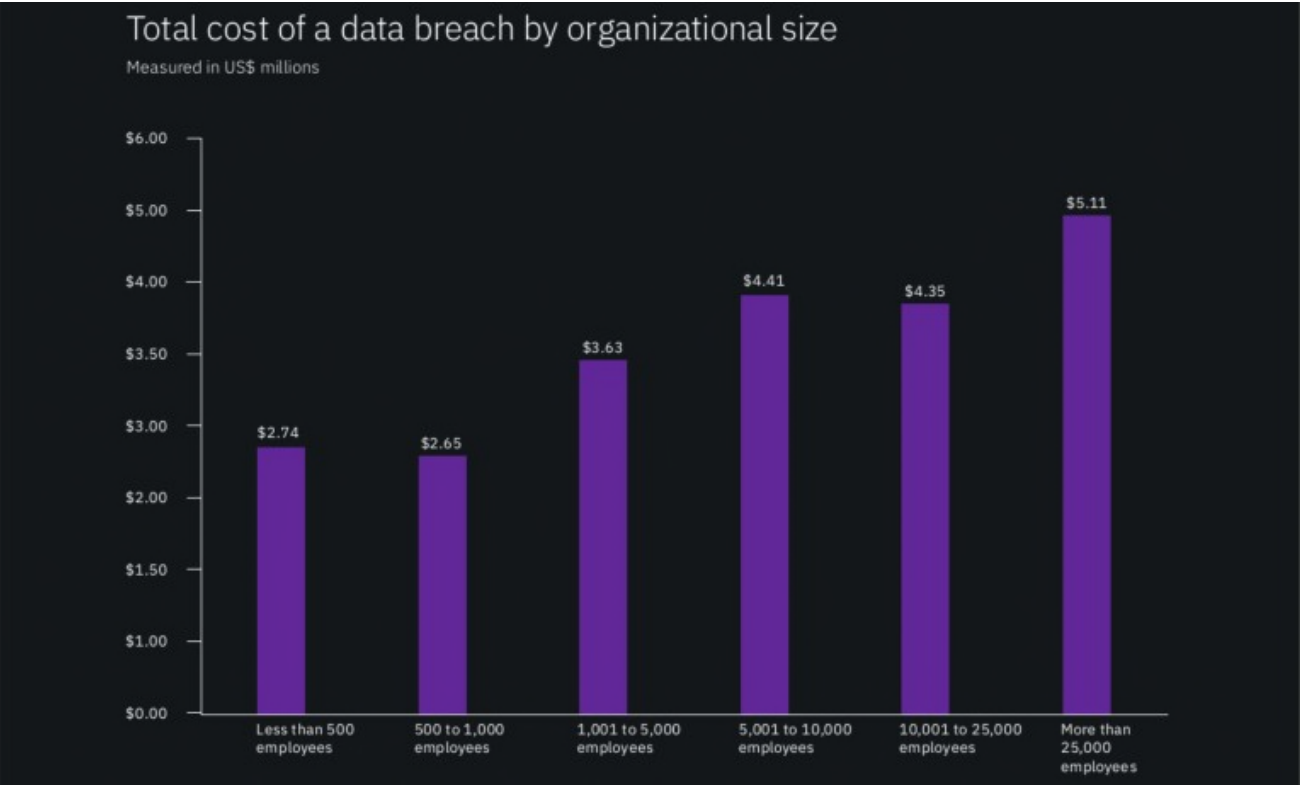
- Malicious attacks were the costliest, with a per record cost that was 25% higher than breaches caused by human error or system glitches.
- Malicious attacks have increased as a share of breaches, up 21% between 2014 and 2019 studies.



Cost Per Capita Based on Cause of Data Breach



Average Total Cost by Size



The Four Cost Components

The four cost components

Our study looked at the core process-related activities that drive a range of expenditures associated with an organization's data breach detection, response, containment and remediation. The four cost centers are:



Detection and escalation

Activities that enable a company to detect the breach and report it to appropriate personnel.



Post data breach response

Processes set up to help customers communicate with the company (e.g., call centers), as well as costs associated with redress and reparation.



Notification

Activities that enable the company to notify individuals who had data compromised in the breach and regulators.



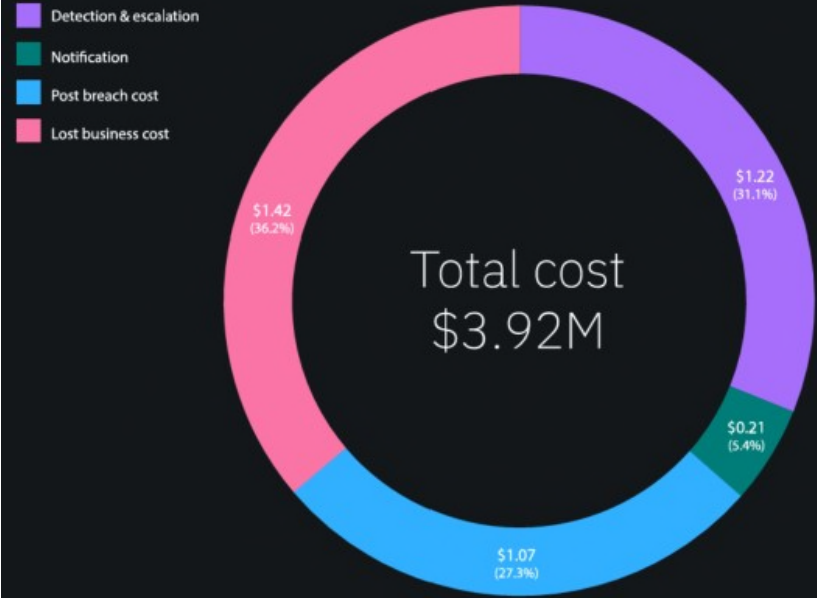
Lost business

Activities associated with cost of lost business including revenue loss, business disruption, system downtime, and new customer acquisition.

Figure 17:

Data breach total cost broken down into four cost categories

Measured in US\$ millions



Detection and Escalation Costs

Invest in governance, risk management and compliance programs.

Detection and escalation costs include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. An internal framework for satisfying governance requirements, evaluating risk across the enterprise and tracking compliance with governance requirements can help improve an organization's ability to detect and escalate a data breach.

Notification Costs

Have an incident response team and put incident response plans to the test.

To help mitigate the costs of a potential data breach, form of an incident response team and test the incident response plan. Organizations can help strengthen their ability to respond quickly to contain the fallout from a breach by establishing a detailed cyber incident playbook and routinely testing that plan through tabletop exercises or by running through a breach scenario in a simulated environment such as a cyber range.

Post Data Breach Response Costs

Key findings:

Formation of the IR team lowered the total cost of a data breach by an average of \$360,000 from the mean cost of \$3.92 million.

\$360,000

IR team lowers the total cost of a data breach by an average of \$360,000

Extensive testing of the IR plan reduced the total cost of a data breach by an average of \$320,000 from the mean cost of \$3.92 million.

\$320,000

IR plan reduces the total cost of a data breach by an average of \$320,000

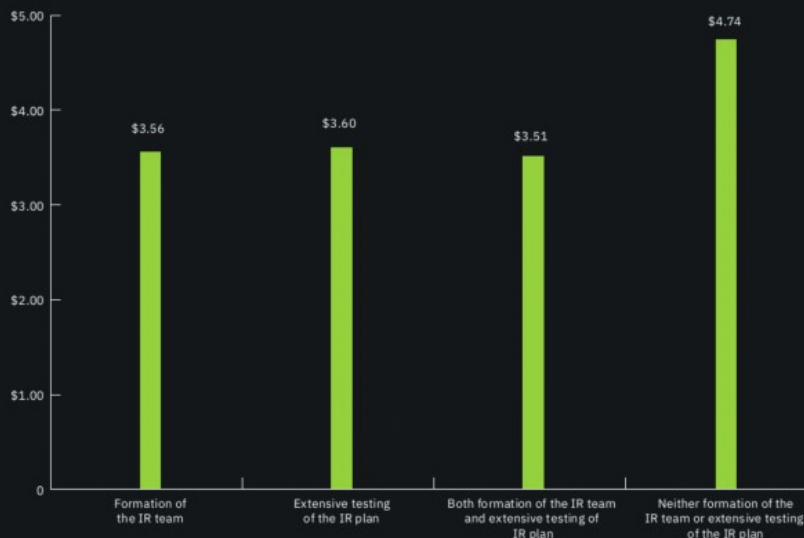
Organizations that both formed an IR team and extensively tested the IR plan saw the greatest savings – \$1.23 million less than organizations that neither formed an IR team or tested the IR plan.

\$1.23M

Savings from IR teams and testing the IR plan – \$1.23 million less than organizations that neither formed an IR team or tested the IR plan.

Combined effect of incident response team and testing the incident response plan

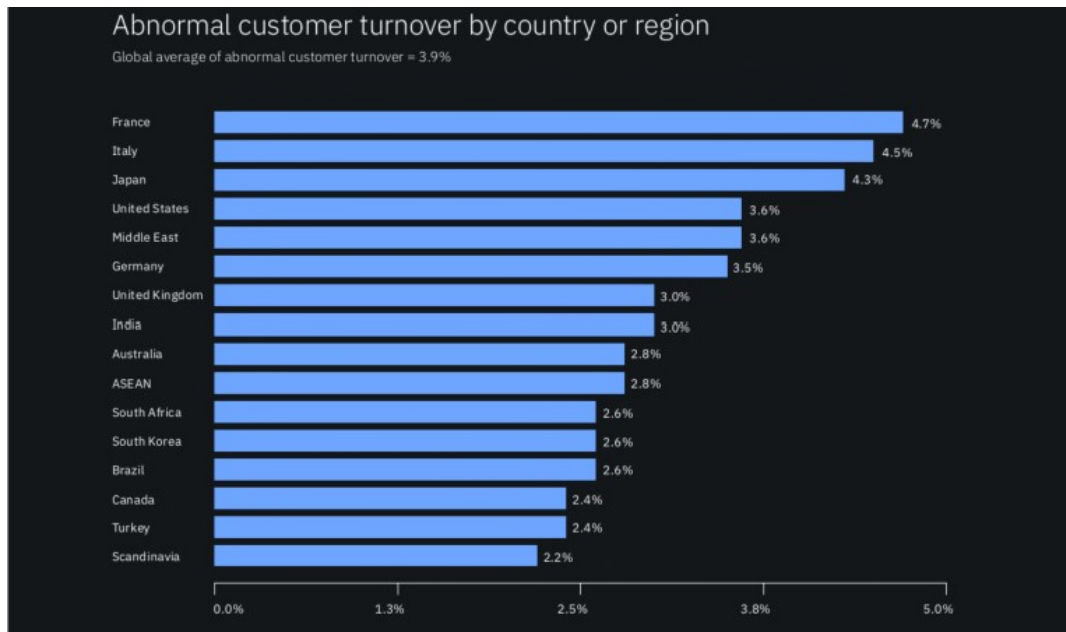
Total breach cost measured in US\$ millions



Lost Business Costs

Certain countries were more vulnerable to customer turnover.

Figure 23, reports the average abnormal customer turnover rates for all country or regional samples represented in this research. Results showed marked differences among countries. France, Italy and Japan experienced the highest abnormal customer turnover rates, whereas, Scandinavia, Turkey and Canada had the lowest.



“Under-Covered” for Cyber-Related Losses


- Equifax data breach (2017)
 - Cost approximately \$439 million to address (initial estimate)
 - Only \$125 million was covered by insurance (71% underinsurance rate).
 - Data breach cost Equifax around \$800 million to resolve most claims.

TECHNOLOGY NEWS MARCH 2, 2018 / 8:05 AM / 2 YEARS AGO

Equifax breach could be most costly in corporate history

John McCrank, Jim Fieldie 3 MIN READ

NEW YORK/TORONTO (Reuters) - Equifax Inc (EFX.N) said it expects costs related to its massive 2017 data breach to surge by \$275 million this year, suggesting the incident at the credit reporting bureau could turn out to be the most costly hack in corporate history.



FILE PHOTO: Credit reporting company Equifax Inc. corporate offices are pictured in Atlanta, Georgia, U.S., September 2, 2017. REUTERS/Tami Chappell/PLC Photo

The projection, which was disclosed on a Friday morning earnings conference call, is on top of \$164 million in pretax costs posted in the second half of 2017. That brings expected breach-related costs through the end of this year to \$439 million, some \$125 million of which Equifax said will be covered by insurance.

Preliminary Questions in Responding to an Incident

- Did a “data breach” occur?
- Determining scope of data breach or incident.
- When was cyber compromise/incident discovered?
 - How was cyber compromise/incident discovered?
- How did cyber compromise/incident occur?
- When did the cyber compromise/incident occur?
 - Early assessments can be revised
- Who caused cyber compromise/incident?
 - Attribution analysis
- What security risks?
- Which regulators?
- Notification issues
- Public relations
- Cyber Insurance coverage

RECENT CASE STUDY - EQUIFAX



Equifax Inc. – Incidents and Response Timeline

- **May 2017**

- Hackers began to access personal identifying information.

- **July 2017**

- Equifax discovered “suspicious network traffic” associated with its consumer dispute website. Its information security department applied the Apache patch.
- Equifax’s information security department observed further suspicious activity and took the web application offline.
- Equifax’s Chief Information Officer notified CEO Richard Smith of the suspicious activity.

- **August 2017**

- Three senior Equifax executives sold stock worth almost \$1.8 million.

- **Fall 2017**

- Equifax announced the security breach to the public on Twitter.
- Two Equifax executives resigned.
- Equifax issued a press release confirming that the vulnerability was Apache Struts CVE-2017-5638.
- Equifax CEO Richard Smith retired and Board of Directors appointed Paulino do Regos Barros Jr. as Interim CEO.
- Interim CEO Paulino do Regos Barros Jr. published a public apology on behalf of Equifax, and announced a new free service allowing people to lock and unlock their credit.

Equifax Inc. – Public Disclosures

A screenshot of the Equifax Inc. website's news page. The top navigation bar is dark red with white text for 'EQUIFAX', 'PERSONAL', 'BUSINESS', 'GOVERNMENT', and 'ABOUT US'. There are also icons for 'Support', a flag, and a search icon. Below the navigation, a breadcrumb trail reads 'About Us > Investor Relations > News and Events > News > 2017'. The main headline is 'Equifax Announces Cybersecurity Incident Involving Consumer Information'. Below the headline is a secondary navigation bar with links for 'Financial Information', 'News and Events', 'Stock Information', 'Stockholder Services', and 'Contact Us'. The date 'Sep 07, 2017' is displayed. The main text of the article begins with 'No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases' and 'Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers'. A sub-headline reads 'ATLANTA, Sept. 7, 2017 /PRNewswire/ -- Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers.'

EQUIFAX PERSONAL BUSINESS GOVERNMENT ABOUT US

Support

About Us > Investor Relations > News and Events > News > 2017

Equifax Announces Cybersecurity Incident Involving Consumer Information

Financial Information News and Events Stock Information Stockholder Services Contact Us

Sep 07, 2017

No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases
Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers

ATLANTA, Sept. 7, 2017 /PRNewswire/ -- Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers.

Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately **143 million U.S. consumers**. Criminals exploited a U.S. website application vulnerability to gain access to certain files.

Equifax discovered the unauthorized access on May 20 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

Public Apology

On Behalf of Equifax, I'm Sorry

A new free service will let consumers lock or unlock access to their credit data any time they like.

- On behalf of [Equifax](#), I want to express my sincere and total apology to every consumer affected by our recent data breach. People across the country and around the world, including our friends and family members, put their trust in our company. We didn't live up to expectations.
- **We were hacked.** That's the simple fact. But we compounded the problem with insufficient support for consumers. Our website did not function as it should have, and our call center couldn't manage the volume of calls we received. Answers to key consumer questions were too often delayed, incomplete or both. **We know it's our job to earn back your trust.**
- Interim CEO Paulino do Regos Barros Jr. (Sept. 27, 2017)

Equifax Inc. Litigation

- Securities Class Action – United States District Court, Northern District of Georgia
- Insider Trading Claims - SEC and DOJ Action
 - March 14, 2018, the SEC charged Jun Ying (former chief information officer) with insider trading in connection with a September 2017 data breach announcement by Equifax disclosing that the company had been hacked
 - Parallel proceeding by U.S. Attorney’s Office for the Northern District of Georgia
 - June 28, 2018, the SEC charged Sudhakar Reddy Bonthu (former software engineer) with insider trading in connection with the September 2017 data breach announcement by Equifax
 - Parallel proceeding by U.S. Attorney’s Office for the Northern District of Georgia
- DOJ Indictment – Announced February 10, 2020 charges against four Chinese military-backed hackers for the 2017 cyberattack against Equifax

Equifax Inc.:

Securities Class Action – Northern District of Georgia

- Federal Trade Commission, Plaintiff, v. Equifax, Inc., Defendant. – July 23, 2019
 - **\$575-700 million**
 - The settlement includes up to \$425 million to provide affected consumers with credit monitoring services.

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION	
FEDERAL TRADE COMMISSION, Plaintiff, v. EQUIFAX INC., Defendant.	Case No. <u>1:19-cv-03297-TWT</u> STIPULATED ORDER FOR PERMANENT INJUNCTION AND MONETARY JUDGMENT

Equifax Cases

Case	Case Name	Settlement Amount
FTC and CFPB and State Enforcement Actions	In re: Equifax Inc. Customer Data Security Breach Litigation (NDGA 1:17-md-2800-TWT)	\$575-700M
Securities Class Action	In re. Equifax Inc. Securities Litigation (NDGA 1:17-cv-03463)	\$149M
Derivative Lawsuit	In re. Equifax Inc. derivative Litigation (NDGA 1:178-cv-00317)	\$32.5M
Indiana	State of Indiana v. Equifax Information Services LLC (Marion County Circuit and Superior Court 49D11-1905-PL-018398)	\$19.5M settlement
New York State Department of Financial Services	In the Matter of Equifax Inc.	\$19.2M
Chicago	City of Chicago v. Equifax Inc. (NDIL 1:17-cv-07798)	\$1.5M settlement

Equifax Inc.:

SEC Action – Insider Trading Claims

- **Securities and Exchange Commission v. Jun Ying** – March 14, 2018
 - Jun Ying, a former chief information officer of a U.S. business unit of Equifax, who was next in line to be the company's global CIO, allegedly used confidential information entrusted to him by the company to conclude that Equifax had suffered a serious breach.
 - Before Equifax's public disclosure of the data breach, Ying exercised all of his vested Equifax stock options and then sold the shares, reaping proceeds of nearly \$1 million. According to the complaint, by selling before public disclosure of the data breach, Ying avoided more than \$117,000 in losses.
- **Securities and Exchange Commission v. Sudhakar Reddy Bonthu** – June 28, 2018
 - SEC charged that Equifax software engineering manager Sudhakar Reddy Bonthu traded on confidential information he received while creating a website for consumers impacted by a data breach.
 - The SEC alleges that Bonthu violated company policy when he traded on the non-public information by purchasing Equifax put options. Less than a week later, after Equifax publicly announced the data breach and its stock declined nearly 14 percent, Bonthu sold the put options and netted more than \$75,000, a return of more than 3,500 percent on his initial investment.
 - Bonthu, 44, was terminated from Equifax in March after refusing to cooperate with an internal investigation into whether he had violated the company's insider trading policy.

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION		
SECURITIES AND EXCHANGE COMMISSION,	Plaintiff,	Case No.
v.		
JUN YING,	Defendant.	JURY TRIAL DEMANDED
UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION		
SECURITIES AND EXCHANGE COMMISSION,	Plaintiff,	Case No.
v.		
SUDHAKAR REDDY BONTHU,	Defendant.	JURY TRIAL DEMANDED

Equifax Inc.:

DOJ Prosecutions – Insider Trading Claims

Department of Justice

U.S. Attorney's Office

Northern District of Georgia

FOR IMMEDIATE RELEASE

Tuesday, October 16, 2018

Former Equifax manager sentenced for insider trading

ATLANTA - Sudhakar Reddy Bonthu, a former manager at Equifax, was sentenced today after pleading guilty to insider trading. Bonthu bought and sold Equifax stock options before Equifax's data breach was publicly announced, while working as a member of the team assembled to respond to the company's massive data breach in 2017.

"Bonthu intentionally took advantage of information entrusted to him in order to make a quick profit," said U.S. Attorney Byung J. "BJay" Pak. "The integrity of the stock markets and the confidence of investors are impaired by those who use nonpublic information for personal gain."

"If we don't hold company insiders to the same rules that govern regular investors, the public's confidence in the stock market erodes," said Chris Hacker, Special Agent in Charge of FBI Atlanta. "The FBI will do everything in its power to hold accountable those who choose to take advantage of their inside knowledge."

Department of Justice

U.S. Attorney's Office

Northern District of Georgia

FOR IMMEDIATE RELEASE

Thursday, June 27, 2019

Former Equifax employee sentenced for insider trading

ATLANTA - Jun Ying, the former Chief Information Officer of Equifax U.S. Information Solutions, has been sentenced to federal prison for insider trading.

"Ying thought of his own financial gain before the millions of people exposed in this data breach even knew they were victims," said U.S. Attorney Byung J. "BJay" Pak. "He abused the trust placed in him and the senior position he held to profit from inside information."

"If company insiders don't follow the rules that govern all investors, they will face the consequences for their actions. Otherwise the public's trust in the stock market will erode," said Chris Hacker, Special Agent in Charge of FBI Atlanta. "The FBI will do everything in its power to stop anyone who takes unfair advantage of their insider knowledge."

Equifax Inc.: Department of Justice



- On February 10, 2020, “the U.S. Department of Justice announced charges against four Chinese military-backed hackers in connection with carrying out the 2017 cyberattack against Equifax.”
- “The intrusion led to the largest known theft of personally identifiable information ever carried out by state-sponsored actors.”
- “This data has economic value, and these thefts can feed China’s development of artificial intelligence tools as well as the creation of intelligence-targeting packages,” U.S. Attorney General William Barr said. “In addition to the thefts of sensitive personal data, our cases reveal a pattern of state-sponsored computer intrusions and thefts by China targeting trade secrets and confidential business information.”



Equifax Inc.: Department of Justice



- **Ongoing investigation**
- **Nine Count Indictment:** “Wu Zhiyong (吴志勇), Wang Qian (王乾), Xu Ke (许可) and Liu Lei (刘磊) were members of the PLA’s 54th Research Institute, a component of the Chinese military. They allegedly conspired with each other to hack into Equifax’s computer networks, maintain unauthorized access to those computers, and steal sensitive, personally identifiable information of approximately 145 million American victims.”
- **Ongoing Cooperation:** “Equifax cooperated fully and provided valuable assistance in the investigation.”

WANTED BY THE FBI

CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE

Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud

Wang Qian Xu Ke Liu Lei Wu Zhiyong

CAUTION

On January 28, 2020, a Grand Jury in the Northern District of Georgia returned an indictment charging Wang Qian, Xu Ke, Liu Lei, and Wu Zhiyong, with Computer Fraud, Economic Espionage, Wire Fraud, Conspiracy to Commit Computer Fraud, Conspiracy to Commit Economic Espionage, and Conspiracy to Commit Wire Fraud. The defendants were members of the 54th Research Institute, which was a component of the People's Liberation Army ("PLA"), the armed forces of the People's Republic of China.

As alleged in the indictment, beginning at least by on or about May 13, 2017, and continuing through on or about July 30, 2017, members of the 54th Research Institute conspired with each other to hack into the protected computers of Equifax, to maintain unauthorized access to those computers, and to steal sensitive personally identifiable information, proprietary database schemas, and data compilations. The PLA hackers obtained names, birth dates, and social security numbers for approximately 145 million American citizens, in addition to driver's license numbers for at least 10 million Americans stored in Equifax's databases. The hackers also collected credit card numbers and other personally identifiable information belonging to approximately 200,000 American consumers. In a single breach, the PLA obtained sensitive identifying information for nearly half of all American citizens and personally identifiable information belonging to nearly a million citizens of the United Kingdom and Canada.

If you have any information concerning these individuals, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Atlanta www.fbi.gov

HEIGHTENED REGULATORY ENFORCEMENT











Regulatory Landscape



Cybersecurity Landscape

Growing Patchwork of Laws

	<p>Data Breach Notification Statutes</p> <ul style="list-style-type: none"> • First: California Data Breach Notification Statute (2002) • Now: 54 US Jurisdictions (DC, Puerto Rico, Guam and Virgin Islands) 		<p>Federal Trade Commission</p> <ul style="list-style-type: none"> • Section 5: “unfair or deceptive acts or practices in or affecting commerce”
	<p>California Consumer Privacy Act of 2018</p>		<p>Securities and Exchange Commission (SEC) Statement and Guidance on Public Company Cybersecurity Disclosures</p>
	<p>Special Focus Statutes: South Carolina Insurance Data Security Act (H. 4655)</p>		<p>Health Insurance Portability and Accountability Act (HIPAA) of 1996</p>
	<p>New York Department of Financial Services (NYDFS) Cybersecurity Rule (March 2017)</p>		<p>European Union (EU) General Data Protection Regulation (GDPR) (May 2018)</p>

California Consumer Privacy Act Timeline



June 28, 2018
California enacts
CCPA
AB 375

Oct. 10, 2019
CCPA Proposed
Regulations by
the CA Attorney
General

Dec. 6, 2019
Public Comment
Period Ends
on CCPA
Proposed
Regulations

Sept. 23, 2018
Amendments
SB No. 1121

Oct. 11, 2019
Amendments
AB 25, 874,
1146, 1355, and
1564

Jan. 1, 2020
CCPA Takes
Effect

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

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



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.





- **Limited Consumer Private Right of Action**

- (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"

- **Opportunity to Cure**

- Statutory 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"

New York SHIELD Act



- New **reasonable security requirement** for companies to “develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of” private information of New York residents.
- Effective March 23, 2020.
- Reasonable safeguards include
 - Risk assessments, employee training, selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors, and disposal of private information within a reasonable time.

Government Agency Enforcement Actions



Equifax (June 27, 2018)

- **Written Risk Assessment** : Board review and approval
- **Audit**: Improve the oversight of the audit function.
- **Board and Management Oversight**: Improve the oversight of the Information Security Program:
 - Approve written Information Security Program and Information Security Policy annually
 - Review management annual report on the adequacy of the Security Program
 - Enhance the level of detail within the Technology Committee and board minutes, documenting relevant internal management reports
 - Review and approve IT and information security policies and ensure they are up-to-date
 - Security Incident Handling Procedure Guide includes up-to-date incident-related procedures and clarifies the roles and relationships of the groups involved in the incident response.

CONSENT ORDER

The purpose of this Consent Order (ORDER) is to require certain corrective actions in response to criticisms noted in the Multi-State Regulatory Agencies' Examination that are outlined below. The following terms are used in this ORDER:

Company:	Equifax Inc.
Board:	The Board of Directors of Equifax Inc.
Multi-State Regulatory Agencies:	Includes the Alabama State Banking Department, California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York State Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking.

The Company, by and through its duly elected and acting Board, has consented to the issuance of this ORDER without admitting or denying any charges of unsafe or unsound information security practices.

NOW, THEREFORE, The Multi-State Regulatory Agencies, acting under statutory authority and with consent of the Company, hereby order that the undersigned representatives take, on behalf of the Company, the following steps in furtherance of alleviating the regulatory concerns of the Multi-State Regulatory Agencies.

INFORMATION SECURITY

- 1) Within 90 days from the effective date of this ORDER, the Board shall review and approve the written risk assessment that identifies:
 - (a) foreseeable threats and vulnerabilities to the confidentiality of personally identifiable information (PII);
 - (b) the likelihood of threats;
 - (c) the potential damage to the Company's business operations; and
 - (d) the safeguards and mitigating controls that address each threat and vulnerability.

Equifax (June 27, 2018)

- **Vendor Management:** Improve oversight and documentation of critical vendors and ensure that sufficient controls are developed to safeguard information.
- **Patch Management:** Improve standards and controls for supporting the patch management function.
- **Information Technology Operations:** Enhance oversight of IT operations concerning disaster recovery and business continuity function.

Alabama State Banking Department, the California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking.

CONSENT ORDER

The purpose of this Consent Order (ORDER) is to require certain corrective actions in response to criticisms noted in the Multi-State Regulatory Agencies' Examination that are outlined below. The following terms are used in this ORDER:

Company:	Equifax Inc.
Board:	The Board of Directors of Equifax Inc.
Multi-State Regulatory Agencies:	Includes the Alabama State Banking Department, California Department of Business Oversight, Georgia Department of Banking and Finance, Maine Bureau of Consumer Credit Protection, Massachusetts Division of Banks, New York State Department of Financial Services, North Carolina Office of Commissioner of Banks, and Texas Department of Banking.

The Company, by and through its duly elected and acting Board, has consented to the issuance of this ORDER without admitting or denying any charges of unsafe or unsound information security practices.

NOW, THEREFORE, The Multi-State Regulatory Agencies, acting under statutory authority and with consent of the Company, hereby order that the undersigned representatives take, on behalf of the Company, the following steps in furtherance of alleviating the regulatory concerns of the Multi-State Regulatory Agencies.

INFORMATION SECURITY

- 1) Within 90 days from the effective date of this ORDER, the Board shall review and approve the written risk assessment that identifies:
 - (a) foreseeable threats and vulnerabilities to the confidentiality of personally identifiable information (PII);
 - (b) the likelihood of threats;
 - (c) the potential damage to the Company's business operations; and
 - (d) the safeguards and mitigating controls that address each threat and vulnerability.

SEC Guidance on Cybersecurity Disclosures



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

Press Release

SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures

FOR IMMEDIATE RELEASE

2018-22

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

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

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

SEC Investigative Report (Oct. 16, 2018)



- **SEC Investigative Report**

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

Press Release

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

FOR IMMEDIATE RELEASE

2018-236

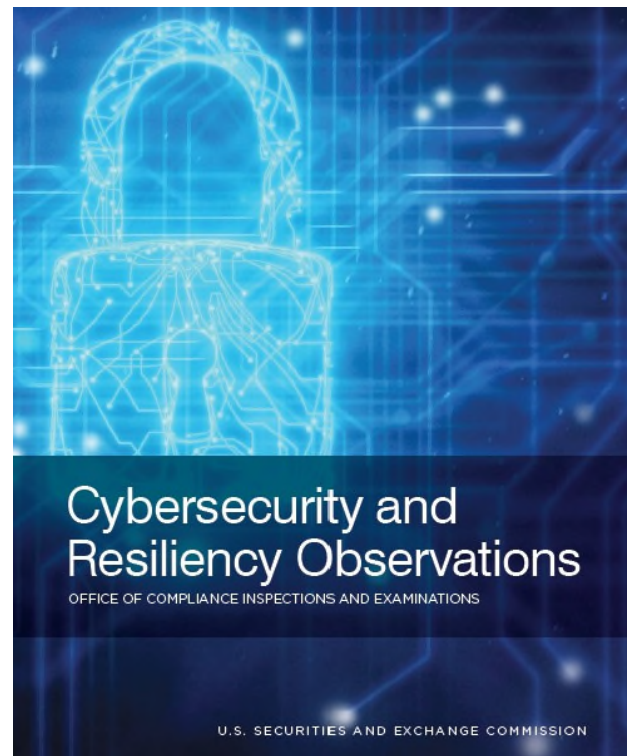
Washington D.C., Oct. 16, 2018 — The Securities and Exchange Commission today issued an investigative report cautioning that public companies should consider cyber threats when implementing internal accounting controls. The report is based on the SEC Enforcement Division’s investigations of nine public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

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

Cybersecurity and Resiliency Observations – Office of Compliance Inspections and Examinations



- 2020 Risk Report
- Through thousands of examinations of broker-dealers, investment advisers, clearing agencies, national securities exchanges and other SEC registrants, OCIE has observed various industry practices and approaches to managing and combating cybersecurity risk and the maintenance and enhancement of operational resiliency:
 - Governance and Risk Management
 - Access Rights and Controls
 - Data Loss Prevention
 - Mobile Security
 - Incident Response and Resiliency
 - Vendor Management
 - Training and Awareness





GOVERNANCE AND RISK MANAGEMENT

Effective cybersecurity programs start with the right tone at the top, with senior leaders who are committed to improving their organization's cyber posture through working with others to understand, prioritize, communicate, and mitigate cybersecurity risks. While the effectiveness of any given cybersecurity program is fact-specific, we have observed that a key element of effective programs is the incorporation of a governance and risk management program that generally includes, among other things: (i) a risk assessment to identify, analyze, and prioritize cybersecurity risks to the organization; (ii) written cybersecurity policies and procedures to address those risks; and (iii) the effective implementation and enforcement of those policies and procedures.

Governance and Risk Management (cont.)



OCIE has observed organizations utilizing the following risk management and governance measures:

- **Senior Level Engagement.** Devoting appropriate board and senior leadership attention to setting the strategy of and overseeing the organization's cybersecurity and resiliency programs.
- **Risk Assessment.** Developing and conducting a risk assessment process to identify, manage, and mitigate cyber risks relevant to the organization's business. This includes considering the organization's business model, as part of defining a risk assessment methodology, and working to identify and prioritize potential vulnerabilities, including remote or traveling employees, insider threats, international operations and geopolitical risks, among others.
- **Policies and Procedures.** Adopting and implementing comprehensive written policies and procedures addressing the areas discussed below and identified risks.
- **Testing and Monitoring.** Establishing comprehensive testing and monitoring to validate the effectiveness of cybersecurity policies and procedures on a regular and frequent basis. Testing and monitoring can be informed based on cyber threat intelligence.
- **Continuously Evaluating and Adapting to Changes.** Responding promptly to testing and monitoring results by updating policies and procedures to address any gaps or weaknesses and involving board and senior leadership appropriately.
- **Communication.** Establishing internal and external communication policies and procedures to provide timely information to decision makers, customers, employees, other market participants, and regulators as appropriate.



Practices and controls related to vendor management generally include policies and procedures related to:

- conducting due diligence for vendor selection;
- monitoring and overseeing vendors, and contract terms;
- assessing how vendor relationships are considered as part of the organization's ongoing risk assessment process as well as how the organization determines the appropriate level of due diligence to conduct on a vendor; and
- assessing how vendors protect any accessible client information.

OCIE has observed the following practices in the area of vendor management by organizations:

- **Vendor Management Program.** Establishing a vendor management program to ensure vendors meet security requirements and that appropriate safeguards are implemented. Leveraging questionnaires based on reviews of industry standards (*e.g.*, SOC 2, SSAE 18) as well as independent audits. Establishing procedures for terminating or replacing vendors, including cloud-based service providers.
- **Understanding Vendor Relationships.** Understanding all contract terms including rights, responsibilities, expectations, and other specific terms to ensure that all parties have the same understanding of how risk and security is addressed. Understanding and managing the risks related to vendor outsourcing, including vendor use of cloud-based services.
- **Vendor Monitoring and Testing.** Monitoring the vendor relationship to ensure that the vendor continues to meet security requirements and to be aware of changes to the vendor's services or personnel.

Training and Awareness

- Training and awareness are key components of cybersecurity programs. Training provides employees with information concerning cyber risks and responsibilities and heightens awareness of cyber threats.
- OCIE has observed the following practices used by organizations in the area of cybersecurity training and awareness:

- **Policies and Procedures as a Training Guide.** Training staff to implement the organization's cybersecurity policies and procedures and engaging the workforce to build a culture of cybersecurity readiness and operational resiliency.
- **Including Examples and Exercises in Trainings.** Providing specific cybersecurity and resiliency training, including phishing exercises to help employees identify phishing emails. Including preventive measures in training, such as identifying and responding to indicators of breaches, and obtaining customer confirmation if behavior appears suspicious.
- **Training Effectiveness.** Monitoring to ensure employees attend training and assessing the effectiveness of training. Continuously re-evaluating and updating training programs based on cyber-threat intelligence.

Office of Compliance Inspections and Examinations

2019 Examination Priorities: Cybersecurity

CYBERSECURITY

Cybersecurity protection is critical to the operation of the financial markets. The impact of a successful cyber-attack may have consequences that extend beyond the firm compromised to other market participants and retail investors, who may not be well informed of these risks and consequences. OCIE is working with firms to identify and manage cybersecurity risks and to encourage market participants to actively and effectively engage in this effort.

OCIE will continue to prioritize cybersecurity in each of its five examination programs. Examinations will focus on, among other things, proper configuration of network storage devices, information security governance generally, and policies and procedures related to retail trading information security. Specific to investment advisers, OCIE will emphasize cybersecurity practices at investment advisers with multiple branch offices, including those that have recently merged with other investment advisers, and continue to focus on, among other areas, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.



- A specialized unit dedicated to targeting cyber-related misconduct in the US markets.
- The SEC Cyber Unit has focused on alleged misconduct involving:
 - Issuer disclosure
 - Market oversight
 - Intrusions into retail brokerage accounts
 - The submission of false regulatory filings
 - Hacking to obtain material non-public information.

SEC Cyber Unit – Hacking / Insider Trading



- SEC v. Ly, Jonathan (December 5, 2016)
 - IT specialist at Expedia, Inc. allegedly hacked into the email accounts of senior executives of his employer to obtain nonpublic information on which he traded in advance of seven Expedia earnings announcements and two Expedia agreement-related announcements, profiting nearly \$350,000.
- SEC v. Hong, Iat, et al. (December 27, 2016)
 - Overseas traders hacked into two prominent New York-based law firms to obtain nonpublic information on which they traded, racking up almost \$3 million in illegal profits.

Please note that while in the case of SEC v. Hong, Iat, et al. the attack came from outside the organization, in the case of SEC v. Ly, the danger stemmed from an internal threat.

SEC Cyber Unit – Regulated Entities



- The Options Clearing House (September 4, 2019)
 - The Commission filed a settled cease-and-desist and administrative proceeding against Options Clearing Corporation for violating Exchange Act Rules 17Ad-22(b)(2) and (e)(1), (3), (4), (6) and (7), Reg. SCI, and Section 19(b)(1) of the Exchange Act and Rule 19b-4(c) thereunder as a result of its failures to establish and enforce policies and procedures involving financial risk management, operational requirements and information-systems security and changing of policies on core risk management issues without obtaining the required SEC approval.
 - The OCC was ordered to pay a combined \$20 million penalty.



- SEC v. Facebook, Inc. (July 24, 2019)
 - The Commission brought charges against Facebook Inc. for making misleading disclosures regarding the risk of misuse of Facebook user data.
 - “For more than two years, Facebook’s public disclosures presented the risk of misuse of user data as merely hypothetical when Facebook knew that a third-party developer had actually misused Facebook user data.”
 - Facebook ordered to pay \$100 million penalty.

MORGAN LEWIS GUIDANCE AND SERVICES



The Best Offense is a Good Defense

- **Governance**

- Board cyber risk management
- Cybersecurity risk oversight and personnel
- Cyber-risk management policies and practices
- Preparedness for cyber incident or attack

- **Written Information Security Program, Policies and Procedures**

- Best practice
- Mandatory for some states. *See, e.g.,* Massachusetts data security regulations (201 C.M.R. 17.00 et seq.)

- **Record of Reasonable Security Procedures and Practices**

- Based on risk assessments to identify, detect, analyze, manage, prioritize and mitigate cybersecurity risks
- Prepared to respond to regulatory investigation
- Reasonable security standard in about half the states
- Defense to CCPA private litigation

The Best Offense is a Good Defense

- **Internal Controls and Policies**

- “[M]aintain[] comprehensive policies and procedures related to cybersecurity risks and incidents”
 - Tailored to your cyber security needs
 - Identify, Protect, Detect, Respond and Recover
- Review controls to prevent and detect cybercrime (Section 21(a) Report)
- Emerging Reasonable Cybersecurity Standard

- **Training**

- Prepared for cyber risks
- Prevention
- Responding to cyber risks
 - Phishing and Business Email Compromise

- **Insider Trading**

- Insider Trading Policies and Procedures Related to Cyber Risks and Incidents
- “[P]olicies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents.”

- **Legal Review**

- Insider Trading Programs
- Internal Control Programs

The Best Offense is a Good Defense

• Managing Cyber Incident

- Multiple regulators
- Incident Response Plans and Testing
- Attorney-Client Privilege Cyber Investigations

• Address Disclosure Issues

- Timing
- Periodic Reports
 - Form 10-K
 - Management's Discussion and Analysis (MD&A) section
- Materiality Standard
- Cybersecurity Risk Factors
- Notifications to others including individuals and public agencies

• Responding to Regulators

- Victim of cyber crime
- Reacted reasonably under the circumstances

Morgan Lewis

DATA BREACH CHECKLIST

**PHASE I:
ALERT AND ORGANIZATION**

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

**PHASE II:
INITIAL SCOPING BEFORE CONTAINING AN ONGOING BREACH**

1. Identify, document, and preserve scope of compromise to the extent possible within 24–48 hours
2. Consider notifications or steps to take before stopping the breach that may prevent harm in

**PHASE III:
CONTAIN THE BREACH**

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

**PHASE IV:
INVESTIGATION**

1. Root cause analysis
2. Classify type of breach
 - a. Hacking
 - b. Internal
 - c. Loss/Theft of Tangible Data (computer, device, storage media)
 - d. Inadvertent Disclosure
 - e. Loss with No Known Disclosure
 - f. Other
3. Full identification of data compromised
 - a. Type of information compromised
 - i. Sensitive personal information
 1. Social Security numbers
 2. Credit card information
 3. Financial account data
 4. Medical information
 5. Usernames and passwords
 6. Driver's license numbers
 7. Other sensitive personal information (disclosure of which could cause harm)
 - ii. Other personal information
 1. Contact information (name, address, email address, phone number, etc.)

Prepared for All Cyber Incident Phases

- Assist before, during, and after a data breach.
- Data breach-prevention guidance:
 - Implementing policies and training regarding data breaches, including governance and risk assessments, data loss prevention, and vendor management.
- Guidance on managing data breach
 - Conducting confidential, privileged cyber incident investigations.
- Assist on enforcement investigations and actions by federal and state regulators
- Assist on class litigation or other litigation that often results from a data breach.
 - Successfully defended more than two dozen data privacy class actions – either winning motions to dismiss or defeating class certifications in lawsuits brought after data breaches or based upon alleged violations of a company’s privacy policy.

Q&A



Mark L. Krotoski



Partner

Morgan Lewis

mark.krotoski@morganlewis.com

+1.650.843.7212

Morgan Lewis

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices
 - Co-Head of Privacy and Cybersecurity Practice Group
 - More than 20 years' experience handling cybersecurity cases and issues
 - Assists clients on litigation, 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.
 - Variety of complex and novel cyber investigations and 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, in addition to other DOJ leadership positions, and as a cybercrime prosecutor in Silicon Valley.

Emily Drazan Chapman



Associate
Morgan Lewis

emily.chapman@morganlewis.com

+1.202.739.5699

Emily Drazan Chapman counsels companies with respect to the federal securities laws, corporate governance matters, and responding to activist shareholder campaigns. Prior to joining Morgan Lewis, Emily was an attorney-adviser with the US Securities and Exchange Commission (SEC) in the Division of Corporation Finance where she reviewed transactional filings under the Securities Act of 1933 and periodic reports and proxy statements under the Securities Exchange Act of 1934.

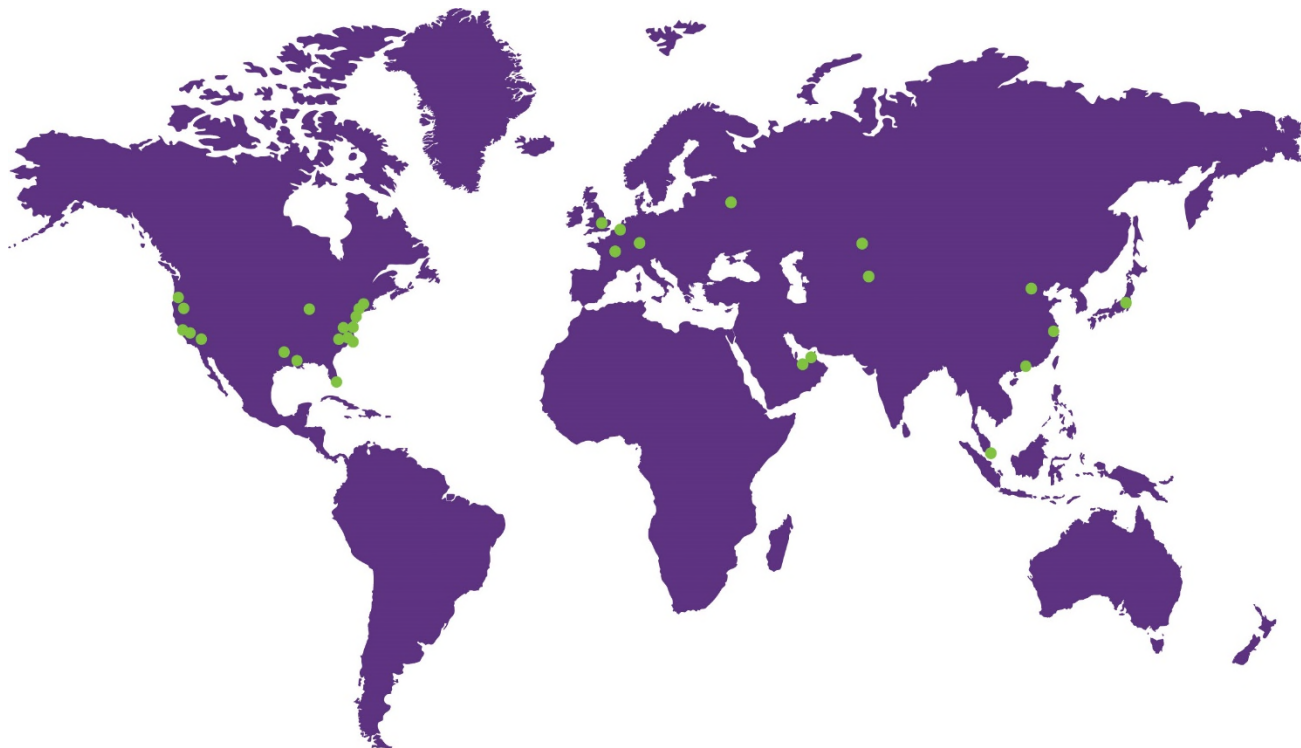
Emily also served in the SEC's Division of Corporation Finance's Office of Small Business Policy, where she provided interpretative guidance on exemptions to SEC registration and reviewed applications for bad actor waivers.

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

© 2020 Morgan, Lewis & Bockius LLP

© 2020 Morgan Lewis Stamford LLC

© 2020 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.

