

Morgan Lewis

GLOBAL PUBLIC COMPANY ACADEMY

CYBERSECURITY AND RELATED DEVELOPMENTS

**Mark Krotoski
Emily Drazan Chapman**



Presenters



Mark Krotoski



Emily Drazan Chapman

Morgan Lewis

Overview

- **Cyber Threat Environment**
- **Significant Costs and Consequences**
- **Recent Case Study: SolarWinds Supply Chain Attack**
- **Attorney Client Privilege Work Product Special Issues**
- **Heightened Regulatory/Enforcement Environment**
- **Recent Case Study: Marriott International**
- **Morgan Lewis Guidance and Services**
- **Q&A**

Preliminary Note

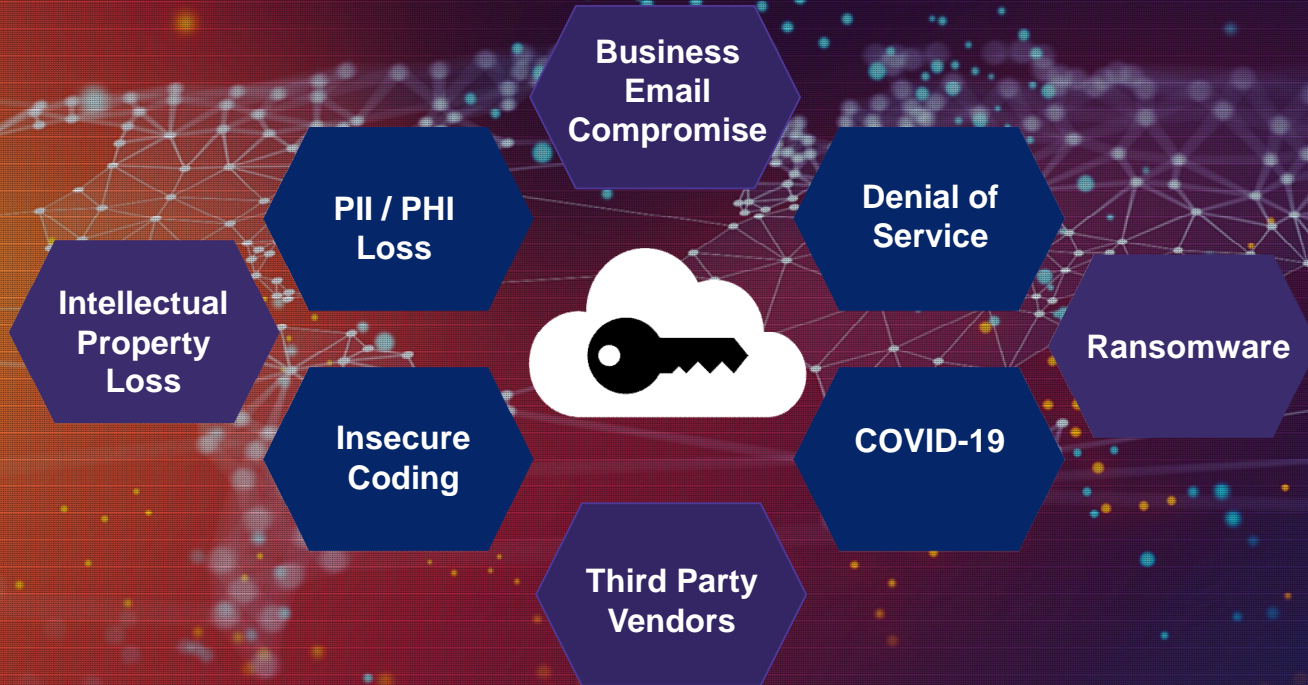
- Comments during this presentation are based upon:
 - Publicly available information;
 - General observations and experience; and
 - ***Not*** on any specific client case information.

Cyber Threat Environment

Morgan Lewis

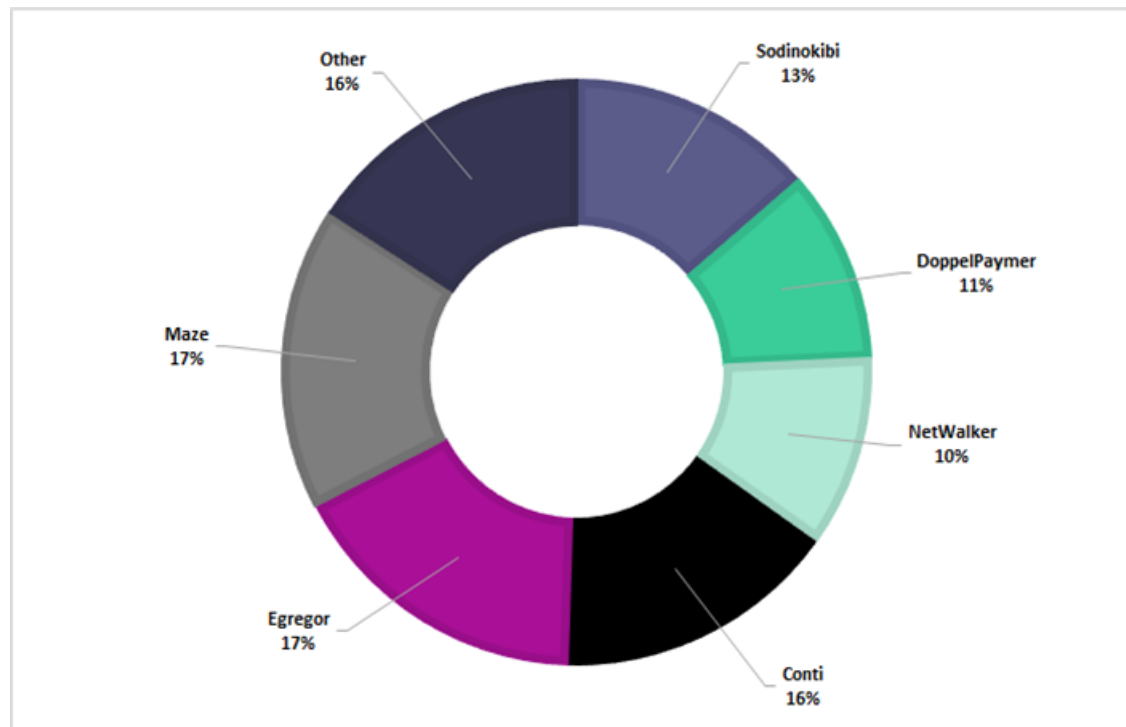


Cyber Landscape and Risks



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

Ransomware Variants



Ransomware Demands - DoppelPaymer

DoppelPaymer

██████████ Inc. Your network has been penetrated.

This link and your decryption key will expire in 14 days after your systems were infected. Sharing this link or email will lead to the irreversible removal of the decryption keys.

NO TIME remains for special price.


All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted.

No any working decryption software is available from other sources.

Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.

Also, we have gathered all your private sensitive data. So if you decide not to pay, we would share it. It may harm your business reputation.

- Your reference ID: **135**
(we recommend to put the reference ID as the subject when contacting us)
- BTC wallet for payment:

Online chat 

Ransomware Demands – Egregor



Egregor

Greetings

We have hacked your network, downloaded and encrypted your data.

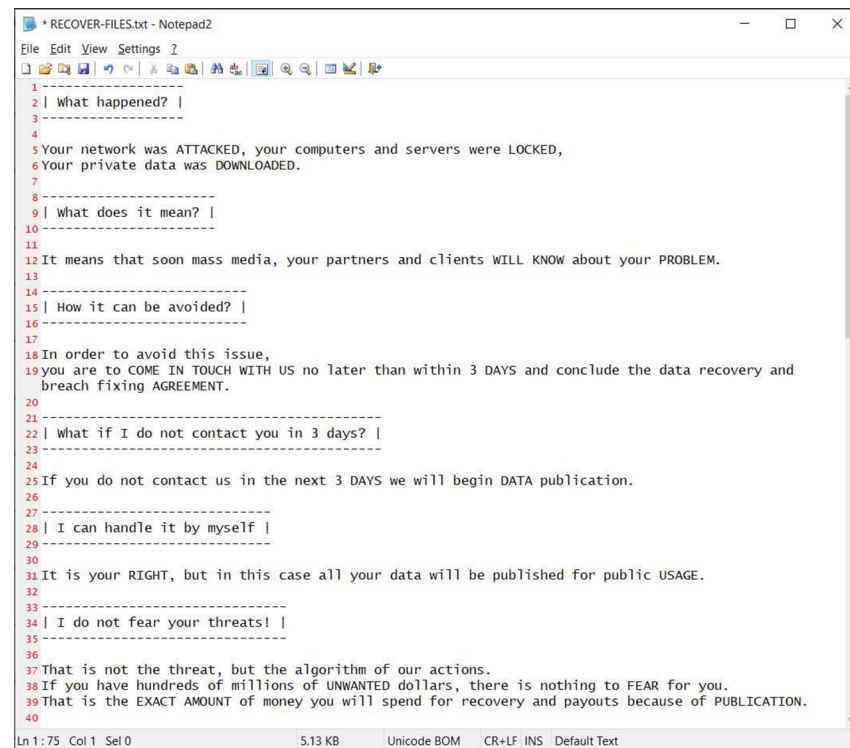
You can recover your data and prevent data leakage to public.

Please upload your note **RECOVER-FILES.txt** using the form below and start recovering your data.

After you upload note, you will be provided with further instructions.

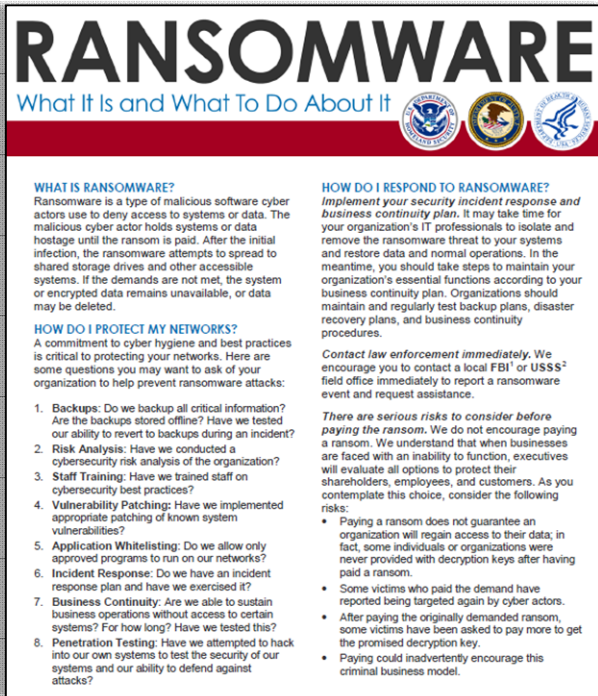
Ransomware Demands – Egregor

- The FBI first observed Egregor ransomware in September 2020.
- Threat to publish exfiltrated data.
- “This is not a threat, but the algorithm of our actions.”
- Egregor actors often utilize the print function on victim machines to print ransom notes.



```
* RECOVER-FILES.txt - Notepad2
File Edit View Settings ?
-----
1
2 | What happened? |
3 -----
4
5 Your network was ATTACKED, your computers and servers were LOCKED,
6 Your private data was DOWNLOADED.
7
8 -----
9 | What does it mean? |
10 -----
11
12 It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.
13
14 -----
15 | How it can be avoided? |
16 -----
17
18 In order to avoid this issue,
19 you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and
20 breach fixing AGREEMENT.
21 -----
22 | What if I do not contact you in 3 days? |
23 -----
24
25 If you do not contact us in the next 3 DAYS we will begin DATA publication.
26
27 -----
28 | I can handle it by myself |
29 -----
30
31 It is your RIGHT, but in this case all your data will be published for public USAGE.
32
33 -----
34 | I do not fear your threats! |
35 -----
36
37 That is not the threat, but the algorithm of our actions.
38 If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
39 That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.
40
Ln 1: 75 Col 1 Sel 0 5.13 KB Unicode BOM CR+LF INS Default Text
```

Payment?



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 FBI¹ or USSS² 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.

“We do not encourage paying a ransom.

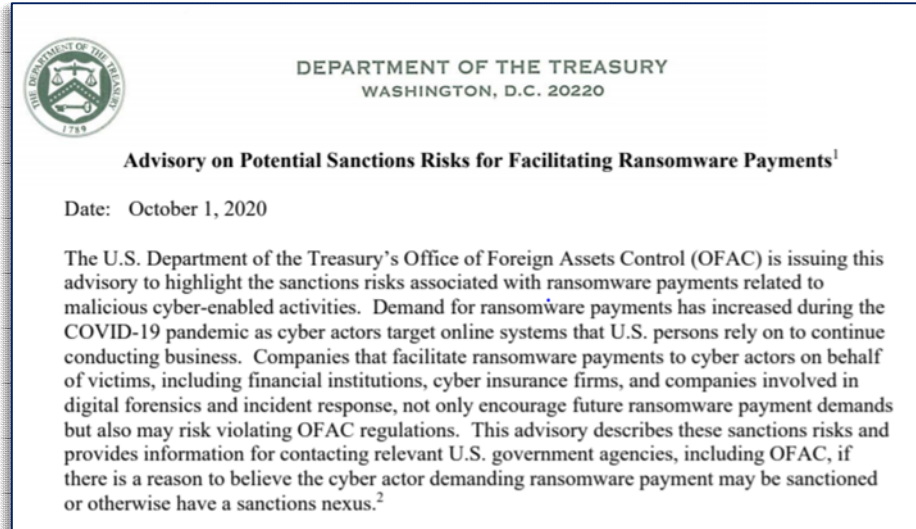
As you contemplate this choice, consider the following risks:

- 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.”



U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Advisory



- U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities (“persons”) on OFAC’s **Specially Designated Nationals and Blocked Persons List (SDN List)**, other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).”
- “OFAC may impose civil penalties for sanctions violations based on **strict liability**, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.”



Business Email Compromise



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

April 06, 2020

Alert Number
I-040620-PSA

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

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

Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than \$2 Billion

Cyber criminals are targeting organizations that use popular cloud-based email services to conduct Business Email Compromise (BEC) scams. The scams are initiated through specifically developed phishing kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds. Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling more than \$2.1 billion in actual losses from BEC scams using two popular cloud-based email services. While most cloud-based email services have security features that can help prevent BEC, many of these features must be manually configured and enabled. Users can better protect themselves from BEC by taking advantage of the full spectrum of protections that are available.



DEFINITIONS

Cloud-based email services are hosted subscription services that enable users to conduct business via tools such as email, shared calendars, online file storage, and instant messaging.

Business Email Compromise is a sophisticated scam targeting businesses that perform electronic payments such as wire or automated clearing house transfers. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques resulting in an unauthorized transfer of funds.

- Past decade trend from on-site email systems to cloud-based email services.
 - Common attack phishing emails designed to steal email account credentials and identify financial transactions in email accounts.
- Between Jan. 2014 and Oct. 2019, the Internet Crime Complaint Center (IC3) received complaints totaling over **\$2.1 billion** in actual losses from BEC scams targeting the largest platforms.
- Increased BEC losses every year since 2013.
- US and Global Impact: Reported in all 50 states and in 177 countries.

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:

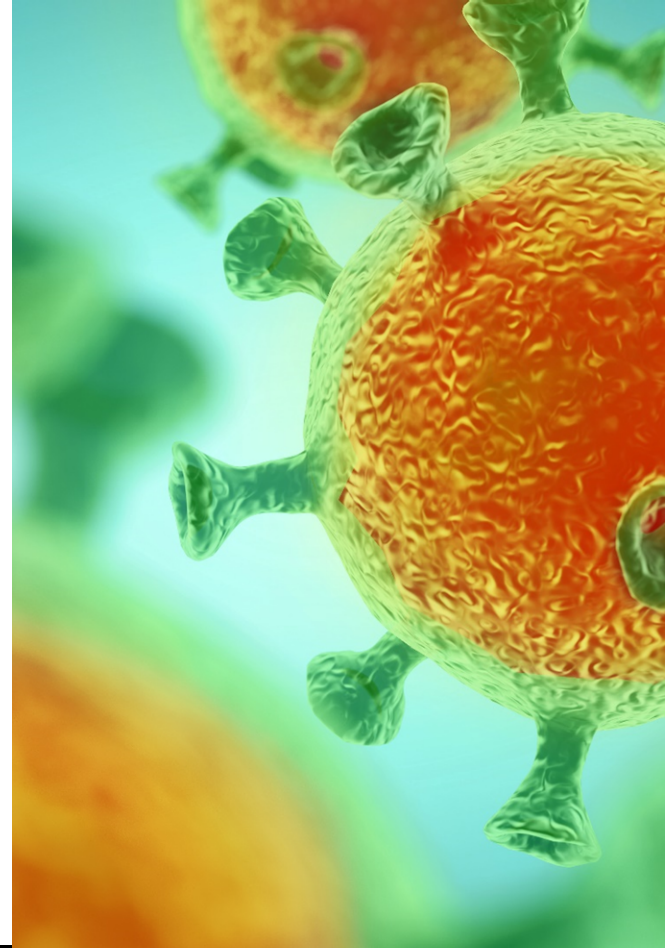
Fake CDC Emails. Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your 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

COVID-19 Impact on Cyber Environment

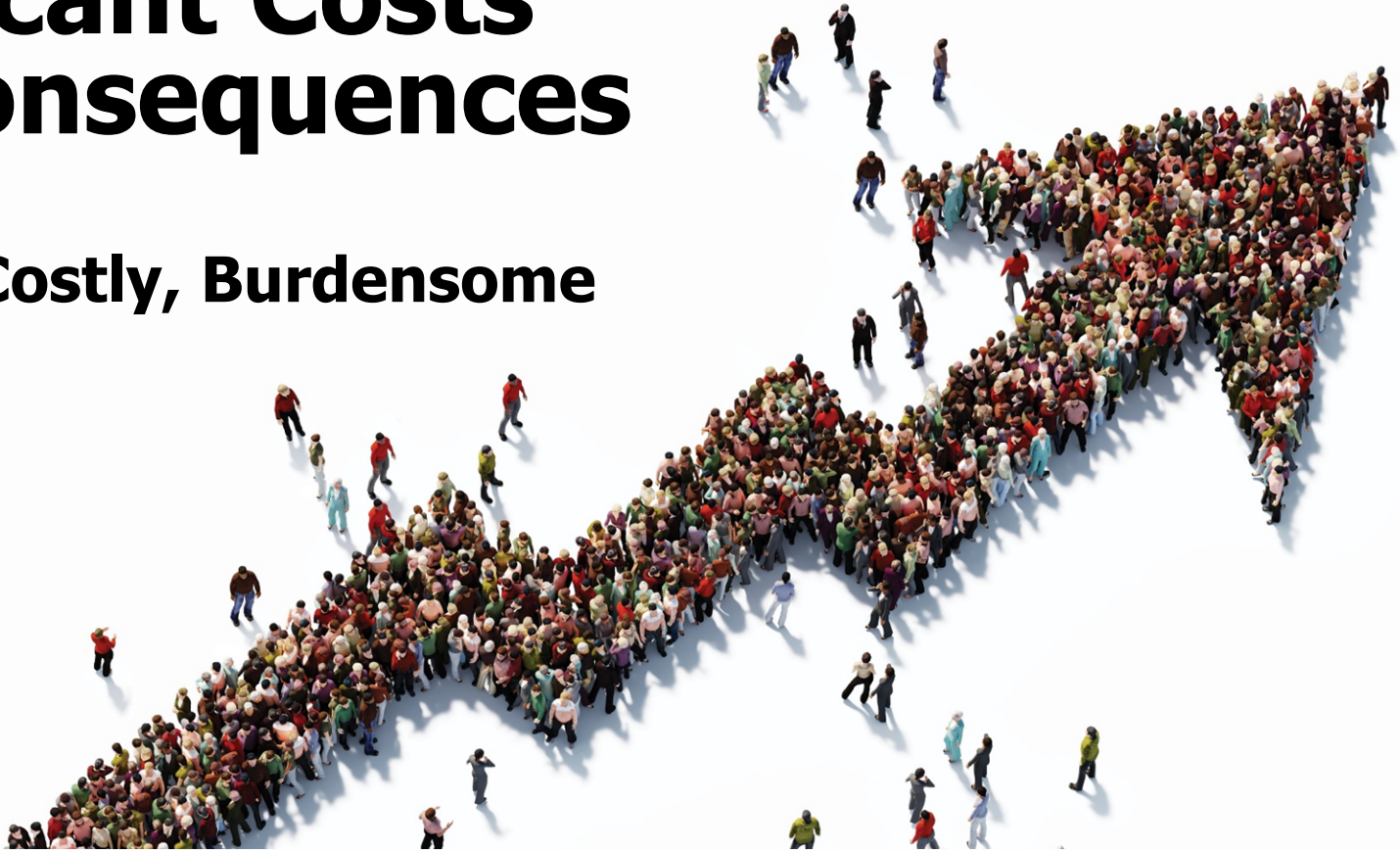
- Ransomware attacks rose 148% in March, 2020.
- Attacks targeting home workers rose five-fold six weeks into lockdown.
- Coronavirus was blamed for the 238% rise in attacks on banks.
- Cloud based attacks rose 630% between January and April 2020.
- Half a million Zoom user accounts were compromised and sold on a dark web forum in April 2020.
- The worldwide information security market is forecast to reach \$170.4 billion in 2022.



Significant Costs and Consequences

Complex, Costly, Burdensome

Morgan Lewis



2020 Cost of Data Breach Report

KEY FINDINGS:

\$7.13 million

The average cost of a data breach in the healthcare industry, an increase of 10% compared to the 2019 study

80%

Share of breaches that included records containing customer PII, at an average cost of \$150 per record

\$5.52 million

Average total cost of a breach at enterprises of more than 25,000 employees, compared to \$2.64 million for organizations under 500 employees

\$291,870

Increase to the average total cost of a data breach associated with complex security systems

51%

Share of organizations with cyber insurance that used claims to cover the cost of consulting and legal services

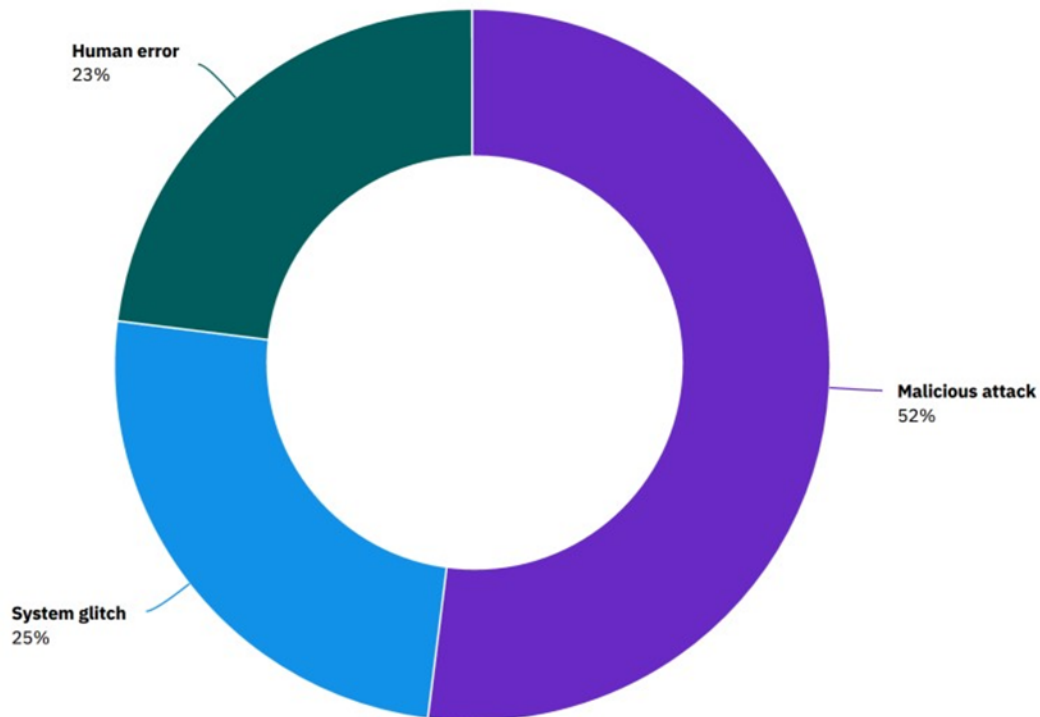
46%

Share of respondents who said the CISO is most responsible for the data breach

Root Cause of Data Breach

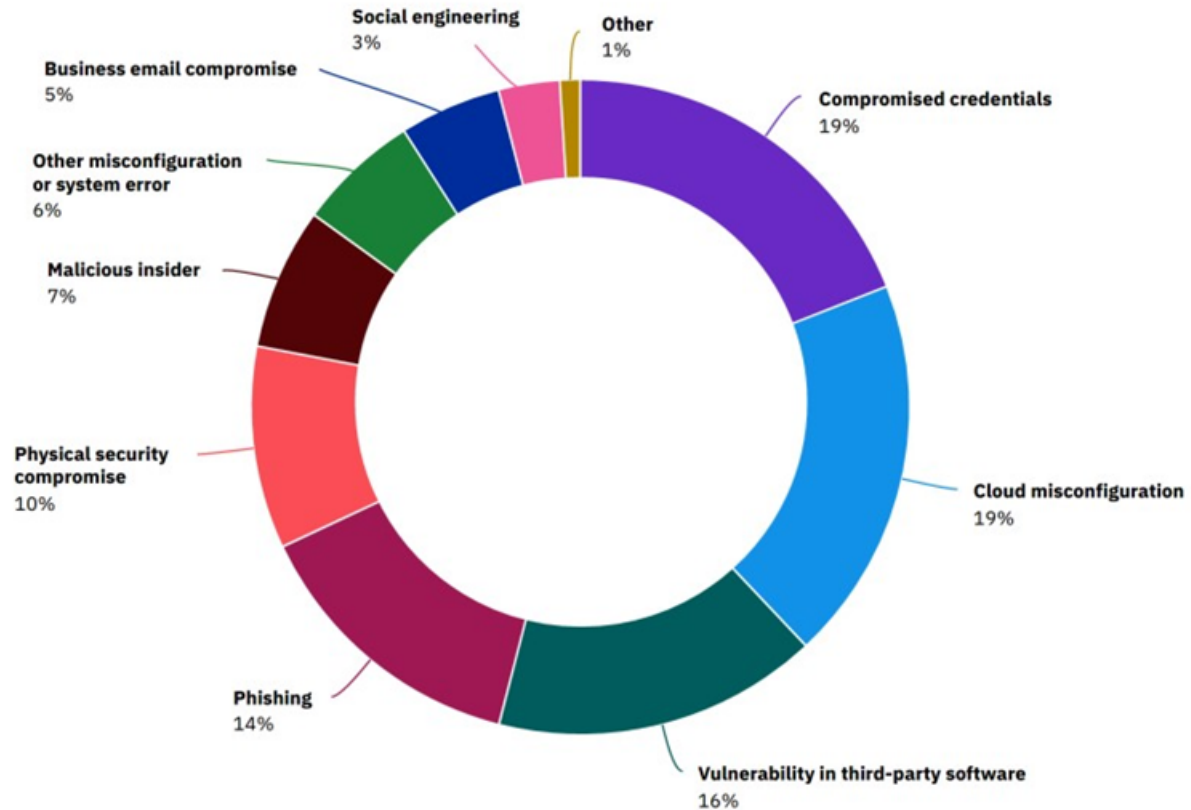
- 52% of breaches were caused by malicious attacks at an average cost of \$4.27 million.
- Malicious attacks have remained the costliest root cause over the past 5 years and has increased nearly 12% since the 2016 study.

Data breach root cause breakdown in three categories

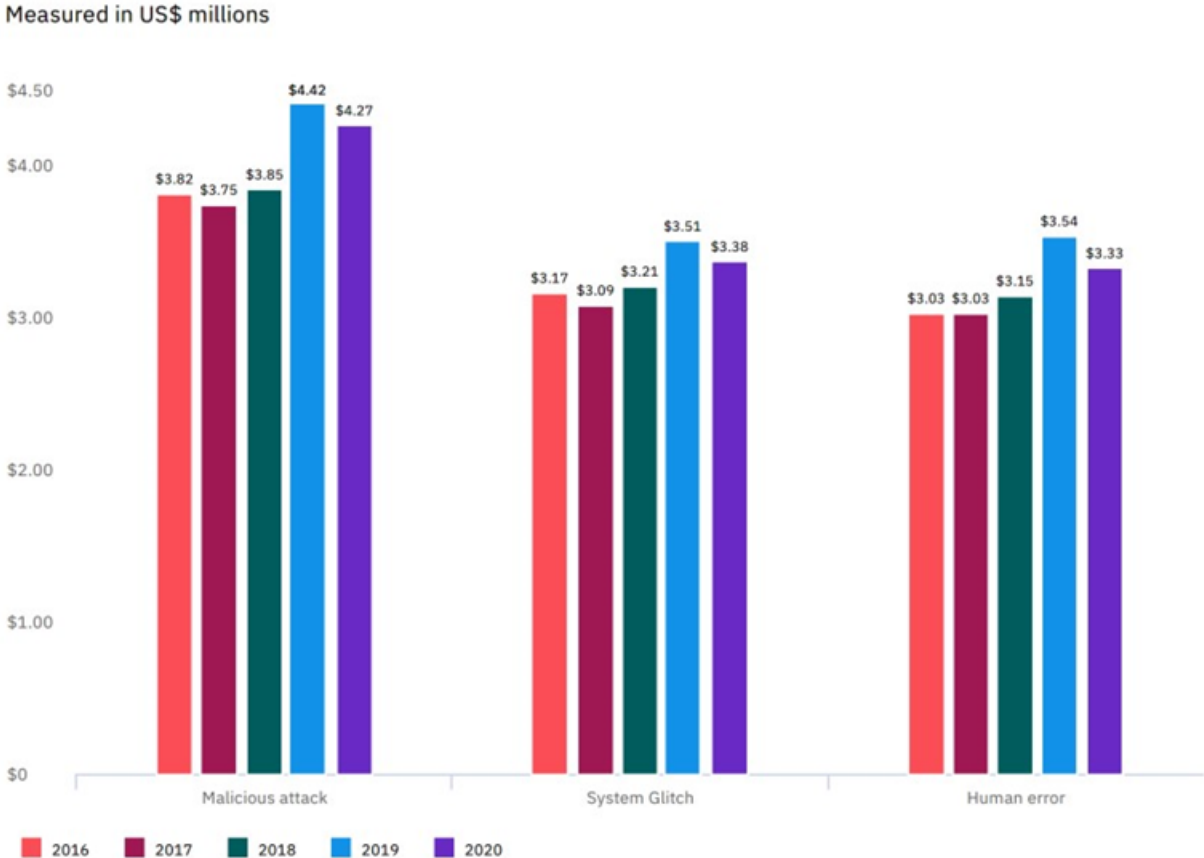


Breakdown of Malicious Attacks

- A majority of malicious breaches were caused by compromised credentials, cloud misconfiguration or a third-party software vulnerability.



Trend in Average Cost by Root Cause of the Data Breach

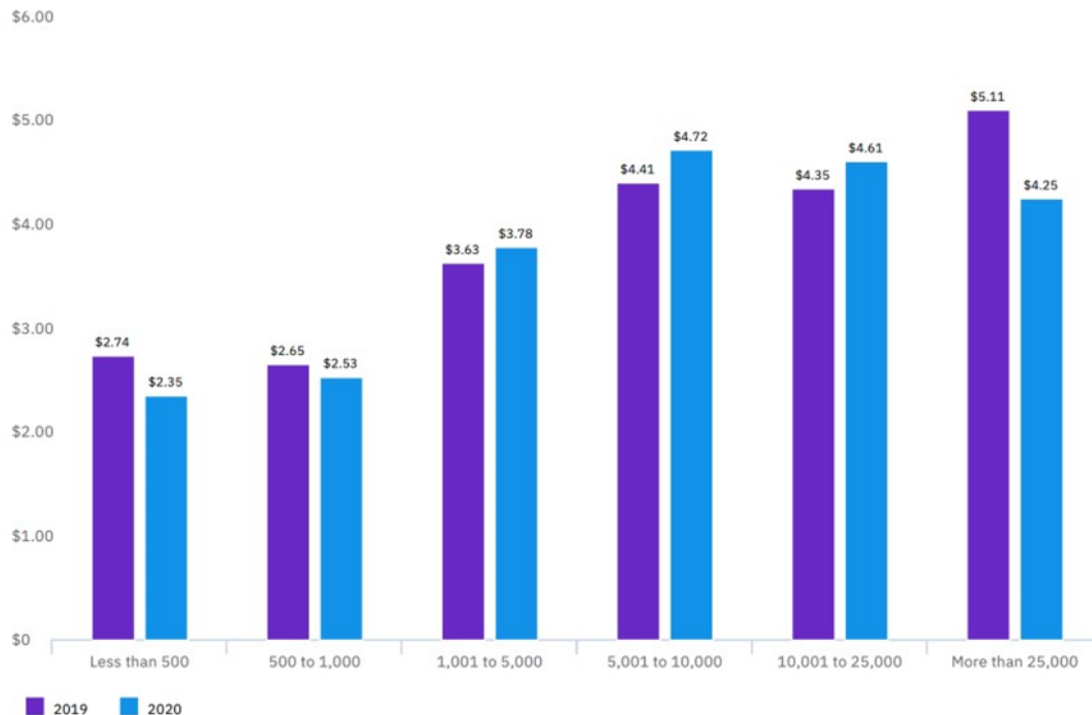


Average Total Cost by Size

The average cost of a data breach increased for mid-sized organizations.

Figure 14 shows the average total cost of a data breach decreased between the 2019 and 2020 studies for the smallest organizations (1,000 or fewer employees) and for the largest organizations (more than 25,000 employees). Organizations with more than 25,000 employees experienced a drop in average total costs from \$5.11 million in 2019 to \$4.25 million in 2020, which is a 16.8% decrease. For mid-sized organizations, however, total breach costs increased on average. In the 5,001 to 10,000 employee range, breach costs increased from an average of \$4.41 million in 2019 to \$4.72 million in 2020, a 7% increase. Proportionately, smaller organizations had higher average costs per employee.

Measured in US\$ millions



The Four Cost Components

Data breach average total cost divided into four categories

Measured in US\$ millions

The four cost centers are described below.



Detection and escalation

Activities that enable a company to reasonably detect the breach.

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards



Notification

Activities that enable the company to notify data subjects, data protection regulators and other third parties.

- Emails, letters, outbound calls or general notice to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts



Lost business

Activities that attempt to minimize the loss of customers, business disruption and revenue losses.

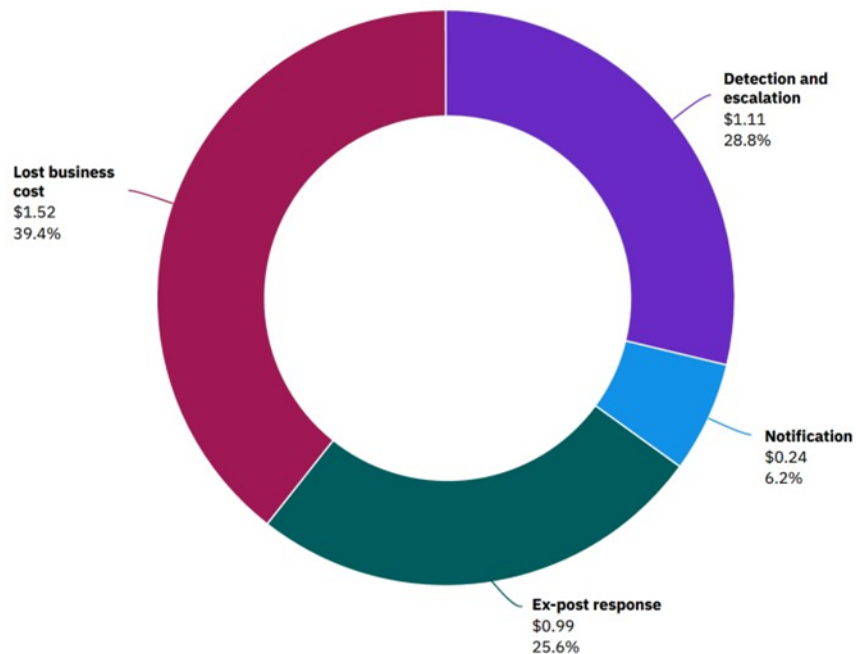
- Business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill



Ex-post response

Activities to help victims of a breach communicate with the company and redress activities to victims and regulators.

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fines



Post Data Breach Response Costs

KEY FINDINGS:

21%

Share of organizations in 2020 with fully deployed security automation, up from 15% in 2018

30%

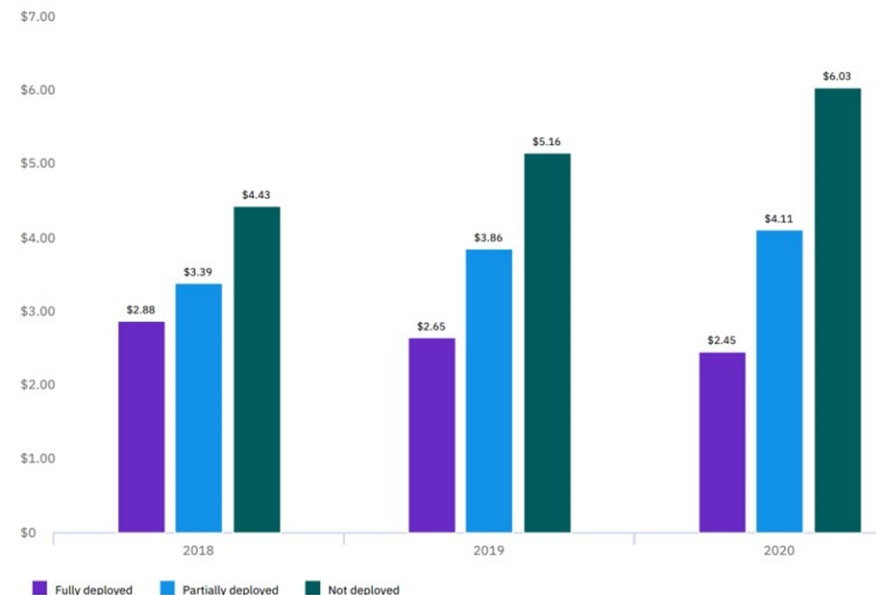
Share of organizations in Germany with fully deployed security automation, highest of any nation

\$3.58 million

Difference in the average total cost of a data breach for organizations without security automation deployed vs. organizations with automation fully deployed

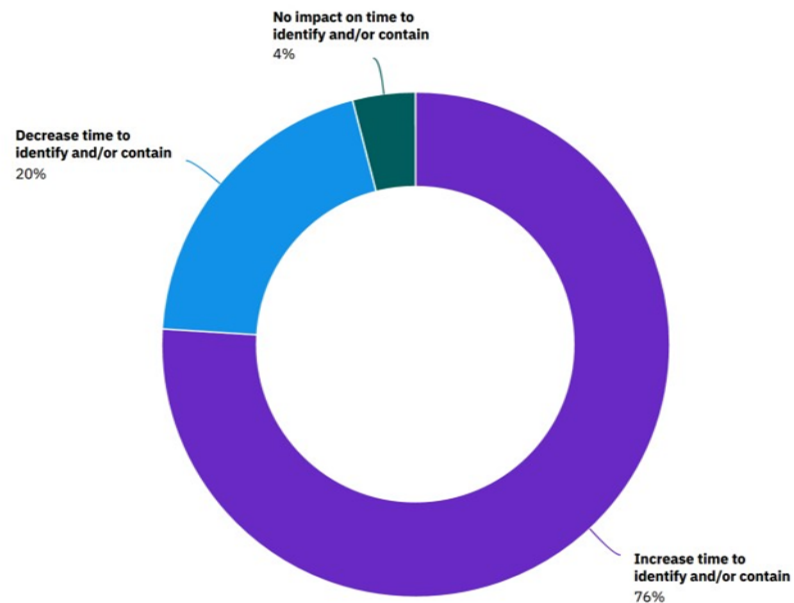
Average total cost of a data breach by security automation deployment level

Measured in US\$ millions

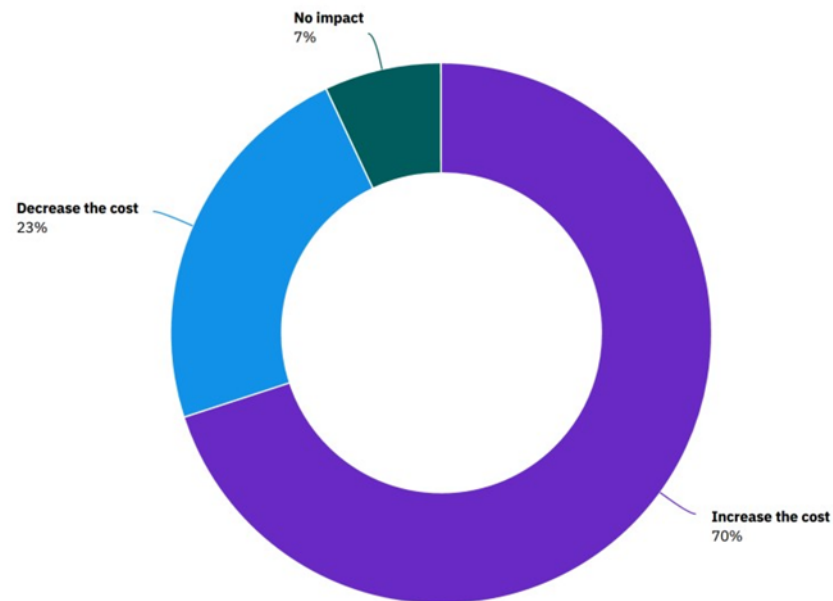


COVID-19 Impact on Costs

How would remote work impact your ability to respond to a data breach?



How would remote work impact the cost of a data breach?

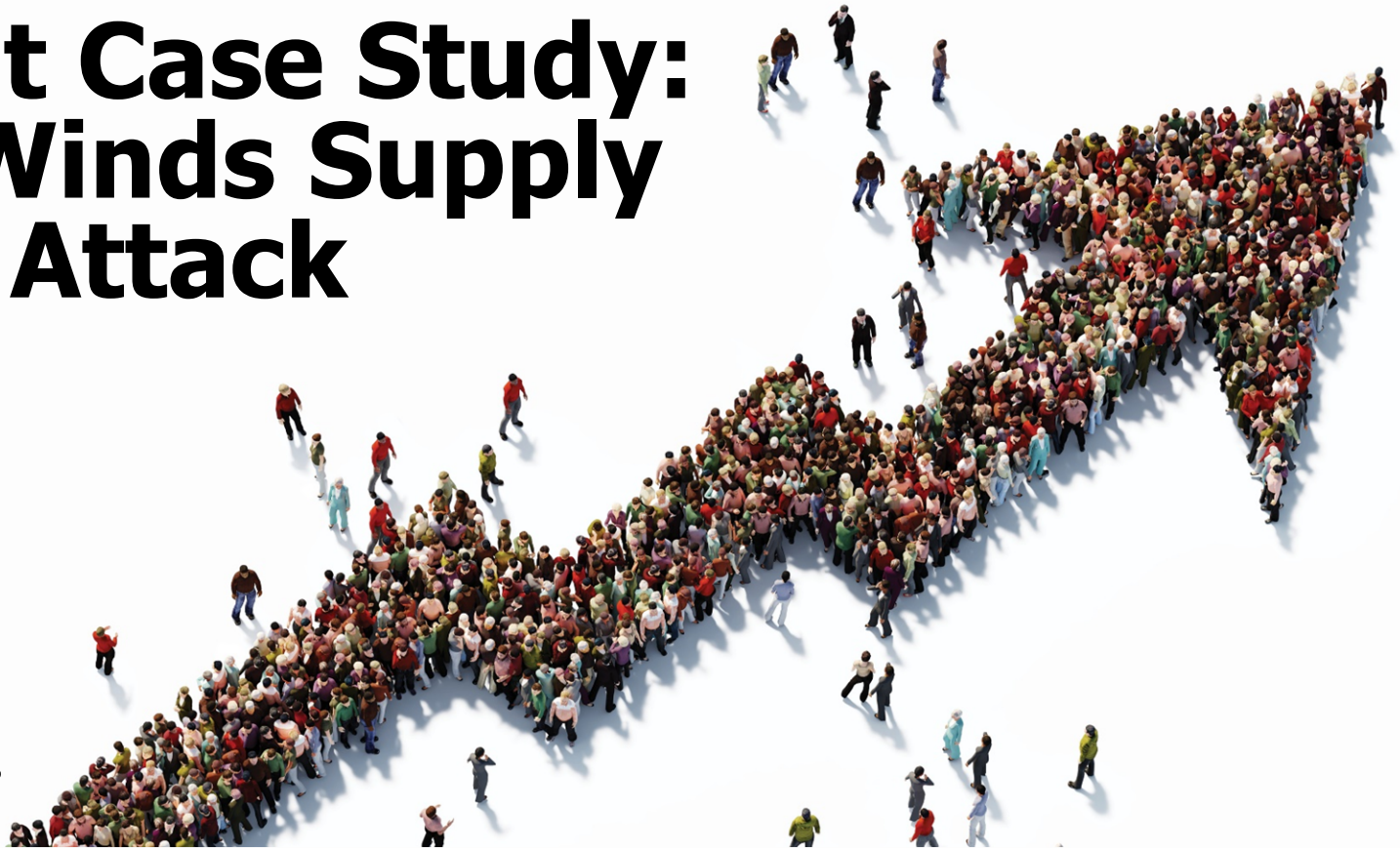


Preliminary Questions

- 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: SolarWinds Supply Chain Attack

Morgan Lewis



Disclosure

- SolarWinds has been advised that this incident was likely the result of a highly sophisticated, targeted and manual **supply chain attack by an outside nation state**, but SolarWinds has not independently verified the identity of the attacker.
- SolarWinds has retained **third-party cybersecurity experts** to assist in an investigation of these matters, including whether a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans.
- SolarWinds is **cooperating** with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM 8-K

CURRENT REPORT

PURSUANT TO SECTION 13 OR 15(d) OF
THE SECURITIES EXCHANGE ACT OF 1934

December 14, 2020
Date of Report (Date of earliest event reported)

SOLARWINDS CORPORATION
(Exact name of registrant as specified in its charter)

FBI Advisory

- If an entity determines that they have downloaded the trojanized SolarWinds plug-in, they should conduct additional research to determine whether or not their systems have been further compromised.



Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 December 2020

PIN Number
20201222-001

Please contact the FBI with any questions related to this Private Industry Notification.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This product was coordinated with members of the Federal Unified Coordination Group (UCG).

This PIN has been released **TLP: WHITE**. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

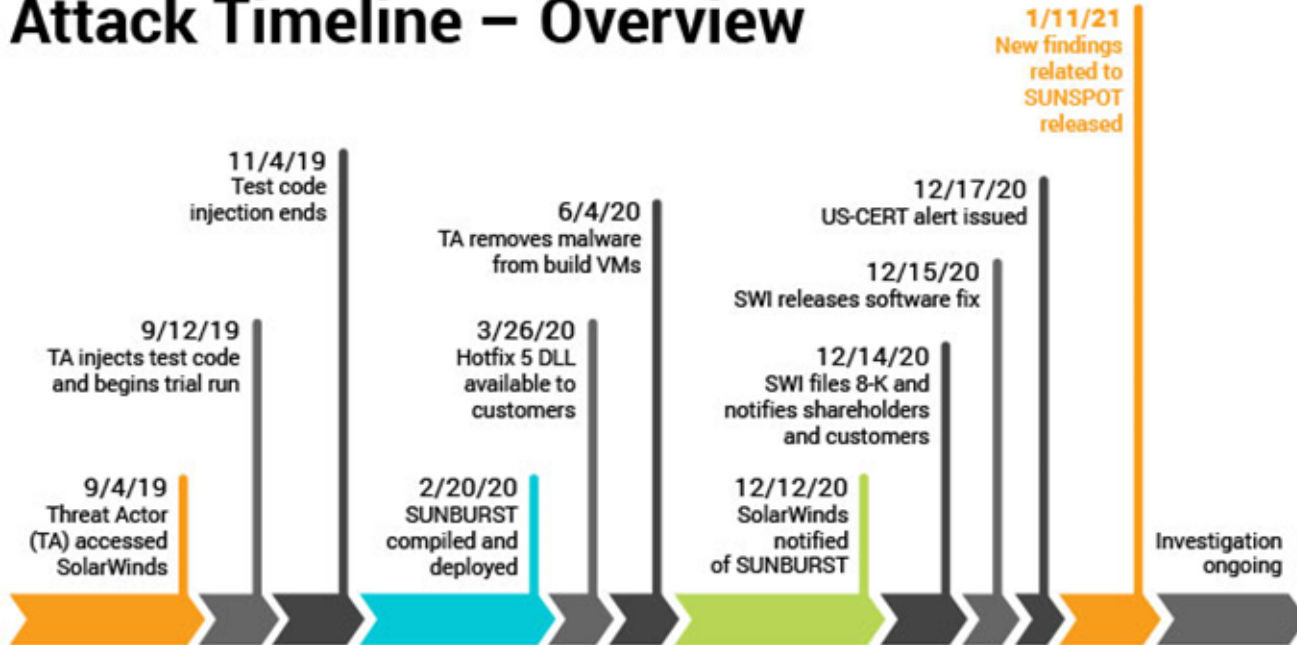
Advanced Persistent Threat Actors Leverage SolarWinds Vulnerabilities

Summary

Based on the wide ranging scope of the investigation into SolarWinds

SolarWinds – Incidents and Response Timeline

Attack Timeline – Overview

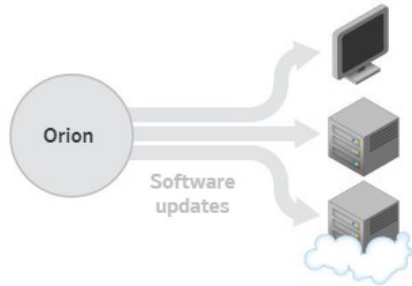


All events, dates, and times approximate and subject to change; pending completed investigation.

SolarWinds – Inside the Hack

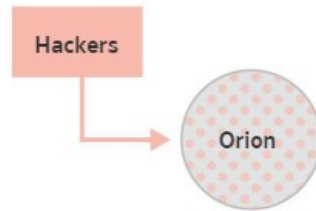
1

SolarWinds makes network management software, called Orion, that's widely used by government agencies and Fortune 500 companies. Like most software makers, they push regular updates to their customers.



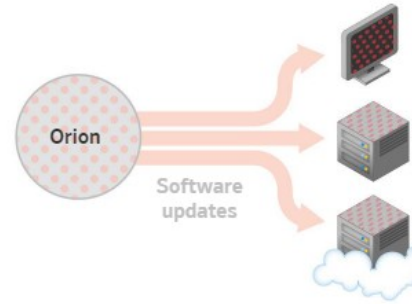
2

Hackers compromised SolarWinds and inserted their own malicious software in updates the company distributed between March and June of this year.



3

About 18,000 customers downloaded these updates, which acted like Trojan Horses, awaiting instructions from the hackers



4

For some percentage of these customers, the instructions came, and the SolarWinds computer downloaded more code, giving hackers a way to sneak around the network and steal data. They were able to access emails, download software and perform reconnaissance on the network.



Focus on Supply Chain

- This attack used cyber tools never before seen in a previous attack, with a strategy that zeroed in on a **weak link in the software supply chain** that all U.S. businesses and government institutions rely on.
 - Never been used on U.S. targets in a concerted way.
- The SolarWinds attack eluded U.S. security measures
 - Not discovered by intelligence officials but due to an automated security alert sent in recent weeks to an employee at FireEye, which itself had been quietly compromised.
- The hackers accessed the Department of Homeland Security, State Department, Treasury and Commerce departments, among others.
- As many as 18,000 companies downloaded the malicious update.

SolarWinds – Public Disclosures

- New CEO joins Solar Winds in Jan. 2021.
 - Accepted position “before the Company was notified of the cyberattack.”
- On Jan. 7, 2021, CEO released a statement highlighting response.
 - Committed to securing internal environment through deploying additional threat protection software, resetting credentials for all users, and consolidating remote and cloud access avenues for accessing the SolarWinds network.
 - Plan to enhance the product by performing ongoing forensic analysis and moving to a new build environment with stricter access controls.
 - Plan to ensure the security and integrity of the software delivered to customers through a series of future steps.

Annual Report

- Based on investigation, “malicious code, or Sunburst, was injected into builds of our Orion Software Platform that we released between March 2020 and June 2020.”
- Since the “Orion Software Platform is installed ‘on-premises’ within customers’ IT environments,” ... “we are **unable to determine** with specificity the **number of customers** that installed an affected version or that were compromised as a result of Sunburst.” Believed “to be fewer than 18,000.”
- Possible “broader **nation-state** level cyber operation designed to target public and private sector organizations.”
- “[T]here are underway **numerous investigations** and inquiries by domestic and foreign law enforcement and other governmental authorities related to the Cyber Incident, including from the Department of Justice, the Securities and Exchange Commission, and various state Attorneys General.”

UNITED STATES SECURITIES AND EXCHANGE COMMISSION Washington D.C. 20549	
FORM 10-K	
<small>(Mark One)</small>	
<input checked="" type="checkbox"/>	ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the fiscal year ended December 31, 2020 or
<input type="checkbox"/>	TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the transition period from Commission File Number: 001-38711 to
SolarWinds Corporation <small>(Exact name of registrant as specified in its charter)</small>	
<small>Delaware</small> <small>(State or other jurisdiction of incorporation or organization)</small>	<small>81-0753267</small> <small>(I.R.S. Employer Identification No.)</small>
<small>7171 Southwest Parkway, Building 400</small> <small>Austin, Texas</small> <small>(address of principal executive offices)</small>	<small>78735</small> <small>(Zip Code)</small>

SolarWinds: Class Action – US District Court

- Jan. 4, 2021, a putative securities class action complaint filed against SolarWinds and the Company's CFO and CEO.
- The SolarWinds investigation is still ongoing and the extent of the consequences is still unknown.

IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS	
TIMOTHY BREMER, Individually and on behalf of all others similarly situated, Plaintiff, v. SOLARWINDS CORPORATION, KEVIN B. THOMPSON, and J. BARTON KALSU, Defendants.	Case No: 1:21-cv-2 CLASS ACTION COMPLAINT FOR VIOLATION OF THE FEDERAL SECURITIES LAWS JURY TRIAL DEMANDED

SEC Inquiry

- The SEC probe comes after the largest investors in SolarWinds sold \$315 million in shares of the company days before the hack was revealed.
 - Former SEC official, Jacob S. Frenkel, stated that the SEC would likely try to determine whether the investors withheld information about the possibility of a hack before unloading their stakes in SolarWinds.



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



Equifax Prosecution

- October 16, 2018, Sudhakar Reddy Bonthu
 - Former manager at Equifax
 - Sentenced to eight months of home confinement, fined \$50,000, ordered to forfeit \$75,979.
- June 27, 2019, Jun Ying
 - Former chief information officer of a U.S. business unit of Equifax
 - Sentenced to four months in prison and one year of supervised release, ordered to pay restitution \$117,117.61, and fined \$55,000.

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."

U.S. v. Jun Ying (N.D. Geo. 1:18-cr-00074)
U.S. v. Bonthu (N.D. Geo. 1:18-cr-00237)

Other Regulators NYDFS Guidance

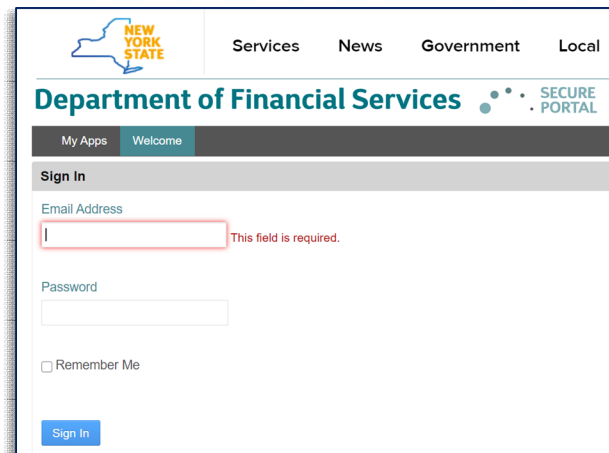
Instructions on filling a supply chain compromise notice with DFS

File a notice immediately if your institution used an affected SolarWinds Orion product or if your institution has been notified that any affiliate that has access to your network or your nonpublic information used an affected product.

Go to the DFS cyber portal linked here: <https://myportal.dfs.ny.gov/web/cybersecurity/>

Submit the following information, at a minimum:

1. Indicate the affected SolarWinds Orion product(s) used and include the specific version(s).
2. Indicate any other SolarWinds products that are also used.
3. Have you disconnected from your network or powered down the affected SolarWinds products?
4. Have you patched the affected SolarWinds products?
5. Have you been notified by an affiliate or a third party who has access to your network or your nonpublic information that the affiliate or third party used an affected SolarWinds product?
6. If the answer to question 5 is yes, identify the affiliate or third party and the name and version of the affected product used.
7. In the contact field, provide the name and contact information of an individual at your institution who is qualified to discuss this matter with DFS.



The screenshot shows the top navigation bar with the New York State logo and links for Services, News, Government, and Local. Below this is the Department of Financial Services logo and the 'SECURE PORTAL' badge. The main content area is titled 'Sign In' and contains an 'Email Address' field with a red border and the message 'This field is required.', a 'Password' field, a 'Remember Me' checkbox, and a 'Sign In' button.

Current Status of SolarWinds

- Cybersecurity and Infrastructure Security Agency (CISA):
 - Other companies were compromised.
 - CISA's acting director stated "this campaign should not be thought of as the SolarWinds campaign."
- Companies checking for vulnerabilities or exposure.
- Based on the wide ranging scope of the investigation into SolarWinds Orion compromises by Advanced Persistent Threat (APT) actors and fast paced release of private network analysis, the FBI is providing cyber security professionals and system administrators collated and verified information to assist in determining whether APT actors have exploited the SolarWinds vulnerabilities present on their systems.

Attorney Client Privilege Work Product Special Issues



Morgan Lewis

Current Cases on Protecting Forensic Reports During Investigations with Attorney-Client Privilege

- ***Wengui v. Clark Hill, PLC***, No. 1:19-cv-03195 (D.D.C. Jan 12, 2021) (“Mem. Op.”).
 - Judge granted the plaintiff’s motion to compel production of a data breach forensic report and other materials prepared by a third-party forensic consultant.
- ***In re Capital One Consumer Data Sec. Breach Litig.***, No. 1:19-md-02915 (AJT/JFA) (E.D. Va. May 26, 2020).
 - Where, as here, the relevant document may be used for both litigation and business purposes, the court must determine “the driving force behind the preparation of” the requested document.
 - Courts have applied what has become known as the RLI test, based on the pronouncements in *RLI Insurance Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007).
 - The court focuses on (1) whether the document at issue was created “when [the] litigation is a real likelihood, [and not] . . . when that litigation is merely a possibility[.]” RLI, 477 F. Supp. 2d at 748 (citing *National Union Fire Ins. v. Murray Sheet Metal*, 967 F.2d 980, 984 (4th Cir. 1992); and (2) whether the document would have been created in essentially the same form in the absence of litigation, *id.* at 747 (citing cases).

Current Cases on Protecting Forensic Reports During Investigations with Attorney-Client Privilege

- ***In Re Premera Blue Cross Customer Data Sec. Breach Litig.***, 296 F. Supp. 3d 1230 (D. Or. 2017).
 - Provider was already conducting a "review [of] Premera's data management system" when it discovered the data breach at issue, after which it continued its work in investigating the breach; and the court found that Provider's data breach investigation was not protected as work product because "[t]he only thing that appear[ed] to have changed involving [the Provider] was the identity of its direct supervisor, from Premera to outside counsel."
- ***In Re Dominion Dental Services United States***, 429 F. Supp. 3d 190 (E.D. Va. 2019).
 - Finding defendant's "conclusory statement" in affidavit that report was prepared in anticipation of litigation "rebutted by extensive evidence in the record."

Heightened Regulatory Enforcement

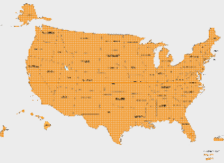





Morgan Lewis

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>California Consumer Privacy Act of 2018 California Privacy Rights Act (Jan. 1, 2023)</p>
	<p>Virginia Consumer Data Protection Act (Jan. 1, 2023)</p>
	<p>New York Department of Financial Services (NYDFS) Cybersecurity Rule (March 2017)</p>

	<p>Federal Trade Commission</p> <ul style="list-style-type: none"> • Section 5: “unfair or deceptive acts or practices in or affecting commerce”
	<p>Securities and Exchange Commission (SEC) Statement and Guidance on Public Company Cybersecurity Disclosures</p>
	<p>Health Insurance Portability and Accountability Act (HIPAA) of 1996</p>
	<p>European Union (EU) General Data Protection Regulation (GDPR) (May 2018)</p>

California Privacy Rights Act – Effective Jan. 1, 2023



- Companies must now provide notice to consumers at or before collection of their personal information of
 - (1) the categories of personal information collected about the individual;
 - (2) the purposes for the collection or use of that information;
 - (3) whether the business sells or shares the personal information;
 - (4) the categories of “sensitive” personal information;
 - (5) the purposes for the collection or use of that sensitive information; and
 - (6) whether the business sells or shares that sensitive information.
- Businesses must take “commercially reasonable efforts” to correct inaccurate information in response to verified requests.
- CPRA Enforcement begins July 1, 2023.

California Privacy Rights Act – Effective Jan. 1, 2023



- Allows Californians to opt out of the sale or sharing of their personal information.
- Creates a new agency, the CalPPA
 - Maintains the administrative authority and jurisdiction to implement audit, and enforces the CCPA.
 - Enforcement authority currently rests with the California Attorney General's Office.
- Expands the private right of action to apply to data breaches resulting in the compromise of a consumer's email address in combination with a password or security question and answer that would permit access to the consumer's account.
- Limits the defense that businesses may have to private actions
 - "[T]he implementation and maintenance of reasonable security procedures and practices ... following a breach does not constitute a cure with respect to that breach."

Virginia Consumer Data Protection Act Effective Jan. 1, 2023



- Enacted March 2, 2021
 - Virginia House of Delegates adopted HB 2307 (Jan. 29, 2021)
 - Virginia Senate approved an identical companion bill, SB 1392 (Feb. 5, 2021)
- Virginia second state with a comprehensive privacy law after California.
- CDPA key similarities to the California Consumer Privacy Act, the California Privacy Rights Act, and the European Union’s General Data Protection Regulation
- Follows a similar framework with proposed data privacy bills pending in other statehouses.
- Effective January 1, 2023.

Virginia Consumer Data Protection Act



- The CDPA applies to all persons that conduct business in Virginia or “produce products or services that are targeted to residents of the Commonwealth” and, during a calendar year, either (i) control or process personal data of at least 100,000 consumers or (ii) derive over 50% of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.
- The term “consumer” means a natural person who resides in Virginia, and does not include any person acting in a commercial or employment context, which is a departure from California’s laws.
- It also is notable that “publicly available information” is defined much more broadly than under the CCPA, such that “personal data” that is protected is narrower under the proposed Virginia law than under California’s law.

Virginia Consumer Data Protection Act



- Consumers afforded rights of (i) access, (ii) correction, (iii) deletion, and (iv) portability of their personal data.
- Right to opt-out of the processing of personal data for purposes of targeted advertising, the sale of their personal data to third parties, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
- Data controllers must limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the purposes for which the data is processed. When processing sensitive data, controllers would be required to seek “consent” from consumers.

Virginia Consumer Data Protection Act Enforcement



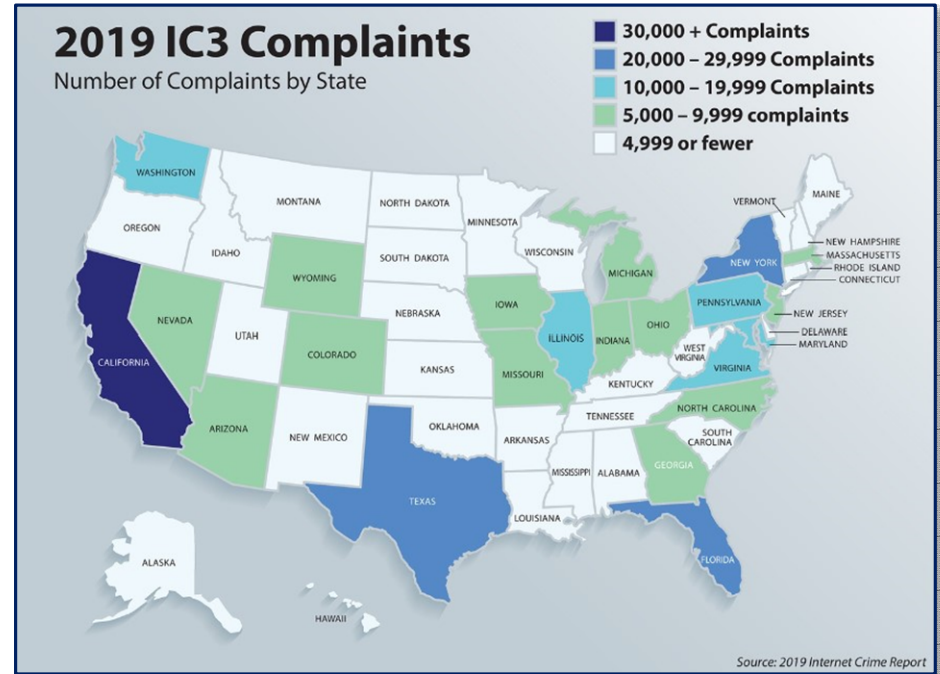
- The attorney general of Virginia has the power to request the disclosure of data protection assessments without court order.
 - The CDPA provides specific provisions that prevent the waiver of attorney-client privilege and work product protection.
- Under the CDPA, the attorney general is granted the exclusive right to enforce the law, subject to a 30-day cure period.
- The attorney general may seek up to \$7,500 per violation, injunctive relief, and recovery of reasonable expenses incurred in investigating and preparing the case, including attorney fees.
- Private rights of action are expressly barred.

State Data Breach Notification Laws

- **54 US Jurisdictions**

- At least 21 states, the District of Columbia and Puerto Rico considered measures in 2020 that would amend existing security breach laws.
- Bills were enacted in six states in 2020— Illinois, Maine, New York, South Carolina, Vermont, Washington and the District of Columbia.

- Notification may be required to customers, government, and credit agencies.
- Enforcement and Actions
 - Separate **AG enforcement action** may be brought
 - Some States **private right of action**



Government Agency Enforcement Actions



Office of Compliance Inspections and Examinations

2021 Examination Priorities: Cybersecurity



- The Division will review whether firms have taken appropriate measures to: (1) safeguard customer accounts and prevent account intrusions, including verifying an investor's identity to prevent unauthorized account access; (2) oversee vendors and service providers; (3) address malicious email activities, such as phishing or account intrusions; (4) respond to incidents, including those related to ransomware attacks; and (5) manage operational risk as a result of dispersed employees in a work-from-home environment.
- The Division is acutely focused on working with firms to identify and address information security risks, including cyber-attack related risks, and encourages market participants to actively and effectively engage regulators and law enforcement in this effort.

DID YOU KNOW?

The increase in remote operations in response to the pandemic has increased concerns about, among other things, endpoint security, data loss, remote access, use of third-party communication systems, and vendor management.



SEC Cyber Unit

- A specialized unit established in 2017 dedicated to targeting cyber-related misconduct in the US markets.
- The Cyber Unit focuses on violations involving
 - Cybersecurity controls at regulated entities;
 - Issuer disclosures of cybersecurity incidents and risks;
 - Trading on the basis of hacked nonpublic information;
 - Digital assets, initial coin offerings and cryptocurrencies; and
 - Cyber-related manipulations, such as brokerage account takeovers and market manipulations using electronic and social media platforms.

Recent Case Study: Marriott

Morgan Lewis



Marriott International, Inc. – Incidents and Response Timeline

- **September 2016**

- Marriott acquires Starwood hospitality group.

- **September 2018**

- An internal security tool prompted and flagged a suspicious attempt to access the guest reservation database for Marriott's Starwood brands.
- Marriott was notified by Accenture.
- Marriott discovered that the Starwood network had been compromised sometime in 2014 by a Remote Access Trojan ('RAT'), malware that allows an attacker to covertly access, surveil, and even gain control over a computer.

- **November 2018**

- Marriott decrypts data that the attackers had encrypted and attempted to remove from the Starwood systems and discovers that it included information from up to 500 million guest records, including credit card and passport numbers.
- Marriott releases a statement on November 30, 2018 about the breach.

- **March 2020**

- Marriott announces that it suffered a second major breach in 16 months, with up to 5.2 million guests at risk.
- The intrusion dates back to January 2020, when someone used the credentials of two franchise property employees to access an "unexpected amount of guest information."
- Marriott disabled the credentials, started an investigation, and contacted guests affected in March.

- **October 2020**

- The UK Information Commissioner's Office fined Marriott International ~\$23.7 million for the 2018 breach.

Marriott – Public Disclosures

- Disclosed both incidents in its news center and by contacting affected guests.
- Continues to update information about the 2018 Starwood Data Security Incident in its annual reports.
 - In the 2020 10K, Marriott stated that the Starwood reservations database is no longer used for business operations.
 - Continues to address expenses and insurance recoveries, litigation claims and government investigations related to the 2018 breach.



President's Statement – 2018

Marriott Announces Starwood Guest Reservation Database Security Incident

NOVEMBER 30, 2018 – BETHESDA, MD

- "We deeply regret this incident happened," Marriott's leadership said in the statement announcing the breach. "We fell short of what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward."
- "Today, Marriott is reaffirming our commitment to our guests around the world. We are working hard to ensure our guests have answers to questions about their personal information, with a dedicated website and call center. We will also continue to support the efforts of law enforcement and to work with leading security experts to improve. Finally, we are devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network."

Marriott – Litigation – 2018

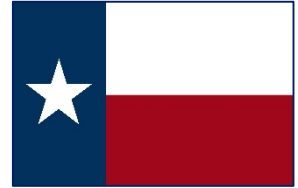
- **Class Actions**

- As of December 21, Marriott faced **nearly 60 federal putative class actions** filed after it announced the breach that targeted Starwood, these eventually consolidated in the District of Maryland’s Southern Division.
 - *Bell, et al v. Marriott International, Inc.*
 - *Helen Kim v. Marriott International, Inc. et al*
 - *Sprowl et al v. Marriott International, Inc.*
 - *Fox et al v. Marriott International, Inc. et al*
 - *IN RE: Marriott International, Inc., Customer Data Security Breach Litigation*

Accenture's Liability in the 2018 Breach

- ***In Re: Marriott International, Inc., Customer Data Security Breach Litigation***
 - A Maryland federal judge found that the cyberattack could be considered traceable to the alleged negligence of Marriott's consultants at Accenture, who first alerted Marriott to the attack.
 - Cybercriminals were able to breach the Starwood database and siphon out sensitive data, including information about more than 9 million credit and debit cards, for at least four years without being detected despite Accenture's IT services and security protocols it provided to Starwood and Marriott, both before and after the merger.
 - Claims include charges that Accenture breached its duty of care to consumers by allegedly being negligent under Maryland, Connecticut and Florida law.

Marriott – Texas Attorney General Statement



November 30, 2018

AG Paxton Begins Investigation Into Marriott Data Breach Affecting 500 Million Customers Worldwide

SHARE THIS:       2

AUSTIN – Attorney General Ken Paxton today announced that his office served an investigative subpoena – also known as a Civil Investigative Demand – on Marriott International, the world’s largest hotel chain. Marriott, which operates nearly 7,000 properties, revealed that its Starwood reservation system was hacked, potentially compromising the personal information of up to 500 million guests.

“The Marriott data breach has the potential of leaving hundreds of thousands of Texans vulnerable to the nightmare of identity theft,” Attorney General Paxton said. “My office is taking immediate action to seek documents and other information from Marriott to examine the nature and extent of this data breach, including how and why this massive hack occurred.”

Marriott – New York and Illinois Attorney Generals



Privacy & Data Security Law

Marriott Data Breach Target of New York, Illinois State Probes

By Daniel R. Stoller

Nov. 30, 2018, 7:00 AM

- Passports, emails of 327 million Starwood guests potentially exposed
- State data breach investigations can lead to higher fines than federal probes


Marriott International Inc.'s global data breach that impacted about 500 million guests will go under the spotlight of two states' top law enforcement agencies.

New York State Attorney General Barbara Underwood (D) announced in a Nov. 30 tweet that the state has opened an investigation the Marriott data breach. "New Yorkers deserve to know that their personal information will be protected," she wrote.

Illinois is also investigating Marriott for the data security incident, Maura Possley, communications director for the state attorney general's office, told Bloomberg Law in an email.

Marriott discovered the security breach Nov. 19 that hit reservation information on or before Sept. 10, 2018. Out of the company's 500 million guests, about 327 million Starwood guests may have had their passport numbers, email, and other personal data taken. Credit and payment card data also may have been stolen.

Marriott – Tennessee Attorney General Statement



News Release

Office of the Attorney General

FOR IMMEDIATE RELEASE
November 30, 2018
#18-31

CONTACT: Samantha Fisher
(615) 741-5860
Samantha.Fisher@ag.tn.gov

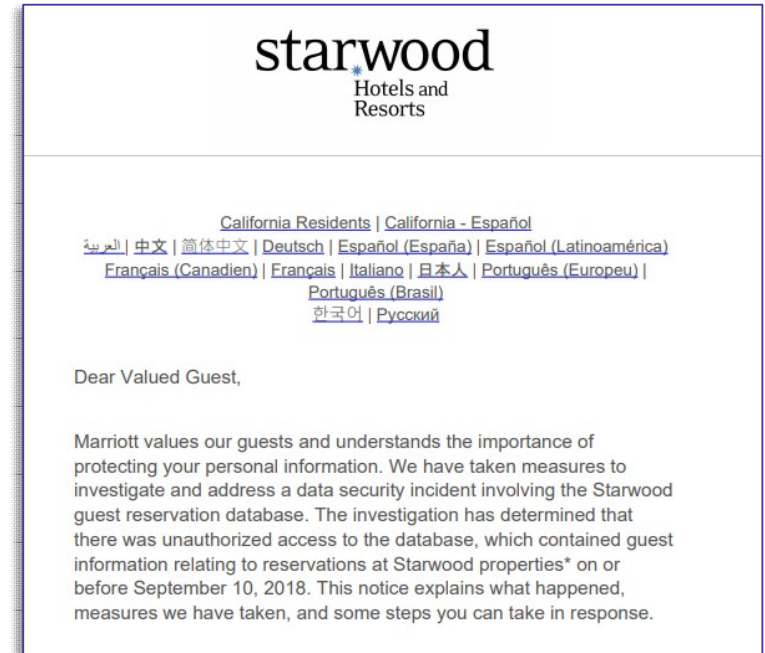
Statement from the Office of the Attorney General regarding the Marriott data breach:

We actively enforce state law that protects Tennesseans from data breaches. We are very concerned about the major breach announced by Marriott this morning: the hundreds of millions affected, the nature of the information potentially accessed, and the time that passed since the first breach. We are gathering additional information and looking at what went wrong.

Marriott – California Attorney General Notification



- The California State Attorney General sample breach notification required under California law.
 - Marriott began sending emails on a rolling basis on November 30, 2018 to affected guests whose email addresses are in the Starwood guest reservation database.



Senate Testimony (March 7, 2019)



**Before the
Senate Committee on Homeland Security & Governmental Affairs
Permanent Subcommittee on Investigations
March 7, 2019**

Chairman Portman, Ranking Member Carper, and Members of the Subcommittee, thank you for the opportunity to testify today.

The subject the Subcommittee is tackling – private sector cyber-attacks – is an increasingly urgent one that has hit Marriott International directly with the data security incident that we announced on November 30, 2018. We deeply regret this incident. We are committed to supporting our affected guests and enhancing security measures to protect against future attacks.

Marriott – Litigation – 2020

- ***Arifur Rahman v. Marriott International, Inc. et al***
 - Marriott won dismissal of the proposed federal class action in California stemming from hackers improperly accessing 5.2 million guests' personal information using Russia-based login credentials, after an internal probe found that no "sensitive" data was exposed.
- ***Springmeyer v. Marriott International, Inc.***
 - A Marriott guest's proposed class action related to the data breach did not proceed because the complaint failed to properly allege facts about the hotel giant's cybersecurity or steps it could have taken to prevent the breach.

Marriott – UK Information Commissioner’s Office

[About the ICO](#) / [News and events](#) / [News and blogs](#) /

[ICO fines Marriott International Inc £18.4million for failing to keep customers’ personal data secure](#)

ICO fines Marriott International Inc £18.4million for failing to keep customers’ personal data secure

Date **30 October 2020**

Type **News**

The ICO has [fined Marriott International Inc £18.4million for failing to keep millions of customers’ personal data secure](#).

Marriott estimates that 339 million guest records worldwide were affected following a cyber-attack in 2014 on Starwood Hotels and Resorts Worldwide Inc. The attack, from an unknown source, remained undetected until September 2018, by which time the company had been acquired by Marriott.

The personal data involved differed between individuals but may have included names, email addresses, phone numbers, unencrypted passport numbers, arrival/departure information, guests’ VIP status and loyalty programme membership number.

Morgan Lewis Guidance and Services



Morgan Lewis

The Best Offense is a Good Defense

- **Governance**

- Board cyber risk management
- Board oversight of corporate cybersecurity assessments, policies, and procedures
- Board reports
- Engagement with management
- Preparedness for cyber incident or attack
- Who is responsible for managing cyber program?

- **Internal Controls, Policies, Procedures and Standards**

- “[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

The Best Offense is a Good Defense

- **Risk Assessment and Management Program**

- Risk assessment process
- Identify and address cyber risks
- Safeguard key assets and information
- Testing and monitoring
- Patch management
- Network segmentation
- Assess controls policies, procedures and standards
- Address red flags

- **Access Management**

- Appropriate restrictions
- Password policies
- MFA
- Consider termination policies
- Monitoring access issues
- Insider threat issues

The Best Offense is a Good Defense

- **Training**

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

- **Third Party Vendors**

- Contractual obligations
- Notification requirements
- Security measures
- Encryption
- Independent audits

- **Address Disclosure Issues**

- Timeliness
- Periodic Reports
 - Form 10-K
 - Management's Discussion and Analysis (MD&A) section
- Materiality Standard
- Cybersecurity Risk Factors

- **Managing Cyber Incident**

- Multiple regulators
- Incident Response Plans
- Business Continuity Plans
- Test Plans for preparedness
- Attorney-Client Privilege

The Best Offense is a Good Defense

- **Address Unique Jurisdiction Standards and Requirements**

- Mandatory WISP
- Disposal standards
- NYDFS Annual Certification Requirement

- **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**

- Compliance standards and issues
- Insider Trading Programs
- Internal Control Programs

Prepared for All Cyber Incident Phases

- 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.
- Regulatory enforcement investigations and actions by federal and state regulators.
- Class action 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

- 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

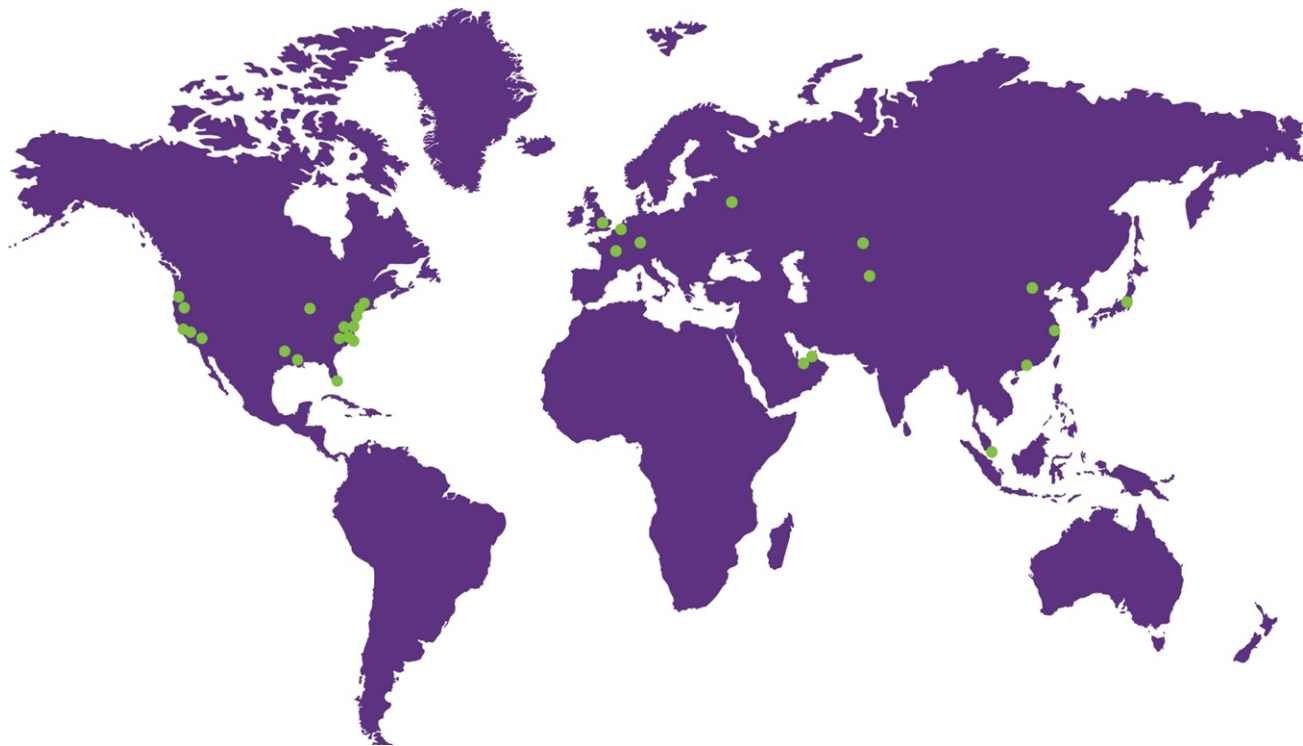
- Emily Drazan Chapman counsels companies with respect to the federal securities laws, corporate governance matters, and responding to activist shareholder campaigns. Prior to joining Morgan Lewis, Emily was an attorney-adviser with the US Securities and Exchange Commission (SEC) in the Division of Corporation 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

© 2021 Morgan, Lewis & Bockius LLP
© 2021 Morgan Lewis Stamford LLC
© 2021 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 & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. 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.