How Cybersecure Is Your Organization? The 2020 Cyber Pandemic: Lessons and Tips From Four Major Cyberattacks

By **Antonia Savaria** and **Caroline A. Morgan** | May 7, 2021

Did the COVID-19 pandemic cause a cyber pandemic by exposing the vulnerabilities of organizations forced to work remotely? In this article we examine cybersecurity incidents that occurred in four high profile organizations in 2020 in order to: (1) highlight relevant cybersecurity, privacy, and data breach legislation and regulations; (2) demonstrate that all industries and organizations can be victims of cybercrimes; (3) discuss the diversity of cyberattacks; (4) compare the organizations' responses and mitigation efforts; and last but not least (5) provide practical tips to avoid loss. We begin by highlighting the major data privacy and cybersecurity regulations that could be triggered by cyberattacks.

Navigating the Maze: The Legislative and Regulatory Angle

What cybersecurity, privacy, and data breach notification laws and regulations could be implicated in a cyberattack? It depends.

Many federal cybersecurity laws apply to industry-specific businesses. The Health Insurance Portability and Accountability Act (HIPAA), for example, applies to healthcare organizations, while the Gramm-Leach-Bliley Act (GLBA) applies to financial organizations. These industry-specific businesses also need to follow the cybersecurity guidance of industry-specific federal regulators and other regulatory organizations, such as—in the case of financial organizations—the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA) and the National Futures Association (NFA). There are more recent federal cybersecurity laws, such as the Cybersecurity Enhancement Act of 2014 and the Cybersecurity Act of 2015 (that includes the Cybersecurity Information Sharing Act (CISA)), and federal laws that are not specifically focused on cybersecurity but have cybersecurity provisions.

Organizations need also be aware that cyberattacks may trigger violations of the increasing number of state privacy laws, such as the California Consumer Privacy Act (CCPA) that became effective in January 2020 and the more recently enacted California Privacy Rights Act (CPRA) that goes into effect in January 2023. Further, Virginia's privacy law—the Consumer Data Protection Act (CDPA)—was signed into law in March 2021 and also goes into effect in January 2023. Foreign data privacy laws—such as the European Union's General Data Protection Regulation (GDPR) that became effective in May 2018 and after which the CCPA is modeled—may also come into play.

Private and governmental entities must also comply with data breach notification laws. All 50 states (and four territories) have enacted such laws. In New York, the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) went into effect in March 2020 and, among other things, amended the prior data breach notification law by imposing additional data security program requirements.

In connection with state-specific and industry-specific cybersecurity regulations, in 2019 the New York State Department of Financial Services (DFS) created a Cybersecurity Division responsible for enforcing and issuing guidance on the DFS Cybersecurity Requirements promulgated in 2017 and applicable to DFS-regulated financial institutions.

Having highlighted some of the cybersecurity, privacy, and data breach notification laws and regulations that may apply, we take a closer look at the cyberattacks of four high-profile organizations from four different industries.

Marriott: Fool Me Once, Shame on You, Fool Me Twice …

Industry: Hospitality

Date of Occurrence: January-February 2020

Type of Cybersecurity Incident: Data breach using employee credentials

On the heels of Marriott's 2018 data breach, where an unauthorized party copied and encrypted information from a guest reservation database involving approximately 500 million guests' information from contact details to payment card numbers, the 2020 data breach it suffered affected approximately 5.2 million guests and included a variety of data from contact details like phone numbers to personal details like company and gender. Marriott disclosed few details—compared with Twitter, for example, as discussed below, which demonstrated more transparency in its cyberattack disclosure—stating the information may have been accessed through an application to help provide services to guests using the login credentials of two employees at a franchise location.

Remediation Efforts and Practical Tips: Since the discovery of the breach, Marriott implemented heightened monitoring and is providing affected guests a personal information monitoring service, in addition to a dedicated website and call center resources with additional information. As COVID-19 has caused companies to become even more reliant on technology, there has been a 15% increase in cyberattacks using new methods compared to pre-pandemic times. In the long run, appropriately budgeting for data breach protection, including customer data protection, can be more cost effective than remediation efforts or defending against a class action even if, like Marriott, a company can get it dismissed.

World Health Organization (WHO): Who Is Targeting WHO?

Industry: Healthcare/Non-for-profit Organization

Date of Occurrence: March-April 2021

Type of Cybersecurity Incident: Password attack/phishing or spear phishing

At a time when words such as "pause" and "lockdown" became everyday vernacular, the COVID-19 pandemic caused our physical world to suddenly change. Hackers invaded our digital world that we

began to rely on for remote work, including targeting a non-for-profit organization, the WHO, which was vital in responding to the pandemic.

In February 2020, WHO published a cybersecurity alert titled "*Beware of criminals pretending to be WHO*," warning of hackers and cyber scammers' phishing attempts, where fraudulent email and WhatsApp messages are sent to trick the recipients into clicking on malicious links or to open attachments, which can potentially lead to stealing money or sensitive information. In March, the FBI warned against an uptick in COVID-19-related hacks and hackers who impersonate official health care agencies, such as the Centers for Disease Control and Prevention (CDC). Indeed, the WHO suffered a two-fold increase in cyberattacks in March 2020 and a five-fold increase a month later.

The WHO confirmed that in March hackers attempted to steal passwords of multiple staffers. Then, in April, hackers continued to target the WHO, including staff's computers in South Korea and in a separate incident, employees at its headquarters in Geneva. 2,000 employees' passwords were reportedly compromised and leaked to other websites, while the WHO itself was not hacked.

Many of the attacks were phishing or spear phishing attacks, trying to lure employees into clicking on a malicious link contained in an email that can download malware on the employee's computer or cell phones. The WHO determined passwords of some employees were obtained from other sites, where, for example, an employee may have used their work email to register an account.

Remediation Efforts and Practical Tips: The WHO had already implemented two-factor authentication and it determined that none of the stolen passwords can be used to access sensitive information. Also, in response to these attacks, the WHO doubled its cybersecurity team, began working with five different security companies, shut down some of its systems that were identified as vulnerable to attack and bolstered the security of internal email. Significantly, enabling two-factor authentication is easily implementable and a crucial security measure that may effectively prevent 99.9% of cyberattacks on accounts. Additional considerations include engaging a third-party expert to perform an independent test like penetration testing or hiring a security company.

Zoom: Reusing Passwords Can Come Back To Haunt You

Industry: Communications Technology

Date of Occurrence: Early April 2020

Type of Cybersecurity Incident: Credential stuffing

While the coronavirus crushed numerous businesses, it made Zoom a household name. According to the New York Attorney General (NYAG) who investigated Zoom over privacy concerns, in the first few months of the pandemic the company saw a 2,000% increase in the number of daily meeting participants it hosted; however, the boon was not without consequences as more users led to greater privacy concerns.

In 2020, Zoom became a target of credential stuffing, a type of cyberattack where cybercriminals betting that people will reuse passwords take stolen credentials to gain access to a different account. The cyberattack reportedly led to the exposure of over 500,000 Zoom usernames and passwords. Though the attack was not as publicized as the teleconference hijacking dubbed Zoombombing, its effects were serious and remediations important.

Remediation Efforts and Practical Tips: To end the NYAG's probe, Zoom agreed to enhance data security practices and privacy controls, including determining whether a login request comes from a human or automation and automatic password resets for compromised credentials. Since credential stuffing is on the rise, as the FBI has warned, companies should consider the FBI's recommended precautionary measures to mitigate against cyberattacks. Companies should also note that enforcement of the SHIELD Act is a top priority for the NYAG as seen in the NYAG's recently published Year in Review. With a section dedicated to "Holding Companies Accountable for Cyberattacks," it touts penalties and millions secured for victims. To mitigate against credential stuffing and potentially avoid related investigations by the NYAG, the FBI or other regulators, companies can take proactive measures like checking account credentials against known breached credentials or implement two-factor authentication, among others.

Twitter: The Social Engineering Attack That Compromised the Social Media Giant

Industry: Internet/Social Media

Date of Occurrence: July 14, 2020

Type of Cybersecurity Incident: Social engineering/phone spear phishing

The Twitter attack started with a social engineering scheme to manipulate people to divulge confidential or personal information that is later used for fraudulent purposes. Through a phone spear phishing attack the attackers manipulated a small number of employees, obtained their credentials, and accessed Twitter's internal system. But they did not stop there.

In phase two of the attack, as detailed in the New York State Department of Financial Services (DFS) Twitter Report, the attackers targeted accounts with desirable usernames or handles (known as original gangster (OG) accounts) to sell access to them. In phase three, the attackers accessed and tweeted from accounts, including "verified" Twitter accounts (meaning, accounts of public interest) that are authenticated by Twitter as original, then escalated the scam to compromised cryptocurrency-related accounts (such as Binance, and DFS-regulated Coinbase, Gemini Trust Company and Square), and eventually to high profile public figures' accounts (such as Former President Obama, Michael Bloomberg, Elon Musk, Warren Buffet, Kanye West and Bill Gates and the corporate account of Apple and Uber). The fraudulent tweets from these accounts were bitcoin scams that reached millions and victimized many. Approximately $118,000 were stolen and transferred to the attackers.

Remediation Efforts and Practical Tips: Twitter—with the help of its Detection and Response Team (DART)—took immediate measures: It secured and revoked access to internal systems to prevent the

attackers from further accessing the systems or individual accounts; restricted functionality to accounts or locked accounts where a password had been recently changed; accelerated several pre-existing security workstreams and improvements to its tools; improved methods for detecting and preventing inappropriate access to internal systems; and, it implemented two-factor identification. The platform also adopted employee training and employee background checks and continued to organize ongoing company-wide phishing exercises. Many of Twitter's measures are steps that organizations can take as part of their cybersecurity program to prevent or mitigate the impact of cyberattacks.

Can Your Organization Spare $3.86 Million?

This is the question that every organization—globally—needs to answer. Why? Because this number represents the global average total cost of a data breach in 2020. Organizations in the United States need to be more concerned as the country has the highest data breach expense at $8.64 million. While lost business accounts for 40% of the cost of data breaches, other considerations such as suspension of operations, fines associated with compliance violations, enforcement and litigation expenses, plunge in stock prices, and reputational risk may all impact organizations after a data breach.

Takeaways

While cyberattacks have been on the rise for some time, COVID-19 precipitated their increase. Last year's cyberattacks demonstrate that no organization is immune and that the cost to bad actors is all too low, while the cost to organizations can reach millions. By learning from the remediation actions of those recovering from cyber incidents, proactively monitoring legislative and regulatory developments related to cybersecurity, privacy, and data breach notifications, and following the above practical tips (which are not mutually exclusive!), organizations can effectively minimize short-term costs, including operational risks like business interruption, and mitigate long-term consequences, including reputational harm caused by cyberattacks.

Antonia Savaria *is founder and CEO of Atlantia Advisers.* **Caroline A. Morgan** *is a partner at Culhane Meadows.*