Top Cyber Attacks of 2020 and How to Build Cyber Resiliency

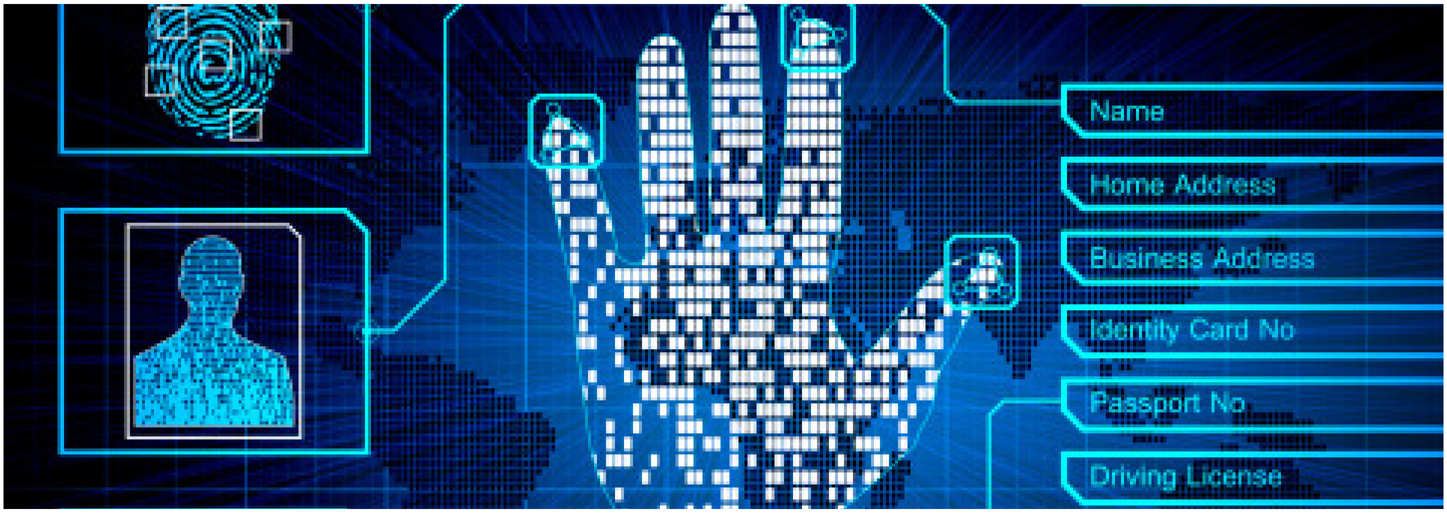
Cyber attacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US $6 trillion by 2021.[1]

As a result, cybersecurity is high stakes from Wall Street to C-Suite, with the threat to enterprises expected to increase in frequency and force. In fact, 53 percent of respondents to ISACA's State of Cybersecurity 2020 report expect a cyber attack within 12 months.

Globally, cybercrime damages are expected to reach **US $6 trillion** by 2021.[1]

To help CISOs, CSOs, CIOs and other business executives further strengthen their proactive cybersecurity resilience, this article details some of the most impactful incidents of 2020 to date, lessons learned and how **ISACA's CMMI Cybermaturity Platform,** which helps enterprises mitigate cybersecurity risk by identifying weaknesses and building resilience, could have helped reduce the impact of these threats. This industry-leading global solution provides a comprehensive cyber assessment, which walks users through threats their organization will face worldwide, and provides a step-by-step roadmap and reporting to improve cyber maturity, specifically increasing the sophistication of organizational security controls, making them more prepared for future incidents.

It helps mitigate enterprise cybersecurity threats with a risk-based approach to strategically measure, assess and report on cybersecurity resilience. Its continuously updated framework addresses risk considerations, threat trends and security controls and aligns with leading global frameworks including NIST CSF, NIST 800-171, FFIEC, CMMC and the Threat Kill Cycle.



Twitter

Some of the most recognized and highly-regarded global Twitter handles were compromised and used to fraudulently tweet about Bitcoin. The accounts requested Bitcoin from their followers, promising double in return. Even though the tweets were only live for a short time, they generated Bitcoin worth more than US $100,000. Those duped into sending Bitcoin received nothing in return.

Perpetrators used a phone spear phishing attack to obtain the credentials of Twitter employees who had access to internal support tools, and they targeted 130 Twitter accounts, successfully tweeting from 45, accessing the direct messages inbox of 36 and downloading the Twitter data of seven. Twitter issued a statement saying “We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools. We have locked accounts that were compromised and will restore access to the original account owner only when we are certain we can do so securely.”

Apple and Uber were among the company accounts targeted, as well as Bill Gates, Elon Musk, Jeff Bezos, Warren Buffet, Kanye West and Floyd Mayweather. Twitter plays a major role in political discussions and decisions, so it was also concerning that the accounts of former President Barack Obama, Presidential Candidate Joe Biden and former New York Mayor Michael Bloomberg were also affected. Several suspects have been charged in relation to this attack.

Marriott

In its second significant data breach within two years, Marriott revealed that personal details of approximately 5.2 million hotel guests were fraudulently accessed in 2020. The personally identifiable information taken included names, addresses, phone numbers, birth dates and airline loyalty information. Hackers often target hotel chains both to sell personal information of guests and to track the travel of government officials with security clearances and business leaders.

Marriott is one of the largest hotel brands with 7,300 hotel and resort properties in 134 countries. The company said the guest information was hacked in mid-January via login credentials of employees at a franchised property and it was alerted to the incident at the end of February. Marriott disabled those logins and is supporting authorities in the investigation. According to a statement from Marriott, they don't believe the data breach affected their Marriott Bonvoy account passwords or PINs, payment card information, address, emails, passport information, or driver's license numbers.

This came at a difficult time for the company as it, like many other travel and hospitality companies, temporarily furloughed a large number of employees to help it survive the global drop in travel due to the coronavirus pandemic.

In 2018 Marriott announced that information on approximately 500 million guests who made a reservation at a Starwood property had been subject to unauthorized access, making it one of the largest known data breaches in history. This data included passport and credit card numbers, and was found to have been attacked as early as 2014, prior to Marriott acquiring the Starwood brand properties.

MGM Resorts

In another travel-related incident, personal data on more than 10.6 million guests of MGM Resorts properties was shared on a hacking forum. Details included full names, home addresses, phone numbers, birth dates and email addresses for globally recognized personalities (reportedly including singer Justin Bieber and Twitter CEO Jack Dorsey), senior executives and employees of major companies, reporters, government leaders and FBI agents.

MGM Resorts, a global entertainment company with luxury resorts and casinos, said that the data that was published in the forum was obtained through an incident that occurred in 2019 and that it is confident that no financial, payment card or password data was involved in the matter. It promptly notified impacted hotel guests and retained two leading cybersecurity forensics firms to conduct an internal investigation into the server breach.

A class action lawsuit has been filed on behalf of MGM Resorts International guests whose personal data was compromised during the breach.

Zoom

With the rapid increase of people working from home due to COVID-19, Zoom went from a barely known boutique service to one of the most recognized and widely-used video and audio conferencing platforms nearly overnight. It experienced revenue growth of 355% year-over-year in Q2 2020. As to be expected with such dramatic explosive growth, Zoom experienced several security incidents, notably the approximately 500,000 user accounts that emerged for sale on a dark web forum. Reportedly, the accounts were obtained by using user IDs and passwords that were exposed in previous breaches, which is also known as credential stuffing.

Hackers could then gain access to important personal or corporate information that should have been kept secure. In addition, Zoom codes were easily guessable, so users could join meetings without an invitation and interrupt or share inappropriate materials, also known as Zoom bombing.

Zoom said it has hired intelligence firms to investigate incidents and that it is implementing additional technology solutions. It also enabled meeting passwords for those joining with a meeting ID.

Magellan Health

A social engineering phishing plan was used against Magellan Health to conduct a cyber attack that involved exporting data and launching ransomware. Overall, eight Magellan Health entities and approximately 365,000 patients were impacted by the attack, making it one of the largest health care data breaches reported in 2020.

Malicious actors first obtained employee credentials to access the targeted server. Patient and employee data was compromised, including information on treatment, health insurance, email addresses, phone numbers, physical addresses and Social Security numbers.

According to Magellan, immediately after discovering the incident they reported it to law enforcement, including the FBI, and retained a leading cybersecurity forensics firm to help conduct a thorough investigation.

Finastra

Finastra, which provides software solutions to worldwide financial institutions, including 90 of the top 100 banks globally, was the victim of a ransomware attack that disrupted operations and caused it to temporarily disconnect affected servers from the internet.

With a global footprint and a broad set of financial technology solutions, Finastra has US $1.9 billion in revenues, 9,000+ employees and approximately 8,600 customers.

According to Bad Packets, a firm that monitors and identifies cybersecurity threats, Finastra also may have been a target because of a history of issues related to outdated security practices and equipment, such as having four Citrix (NetScaler) servers vulnerable to CVE-2019-19781 running in early January 2020.

A Finastra statement noted “isolation, investigation and containment” was used to enable it to bring the servers back online as quickly as possible, with minimum disruption to service. They did not find evidence that customer or employee data was accessed or exfiltrated, and said that clients’ networks were not impacted. They also informed and cooperated with relevant authorities and reached out directly to customers that were impacted as a result of disrupted service.

Greek Banking System

After a Greek travel website was hacked, Greece’s four main banks followed security protocols and had to cancel and replace approximately 15,000 customer credit or debit cards.

In a joint statement, Alpha Bank, Piraeus Bank, Eurobank and the National Bank of Greece, said that although only a few customers were actually charged with transactions they didn’t make, they decided to take precautionary measures and will gradually replace all the cards that have made even one transaction on that website in the past. The travel website was used to book airline tickets, ferry tickets, hotels, cars and purchase travel insurance.

A key source of the inquiry is whether or not the tourist website followed the Payment Card Industry Data Security Standards (PCI DSS). Major credit card companies, such as Visa and MasterCard, are also involved in the investigation. If the website is fully compliant with PCI DSS, then investigators will examine other potential causes of the breach.

Lessons Learned and How the CMMI Cybermaturity Platform Builds Cybersecurity Resiliency

The following covers some of the most frequent and growing types of cyber threats.

> According to ISACA's **State of Cybersecurity 2020 report**, social engineering is the most popular method of attack, with **15 percent of compromised respondents** saying it was the method used as a vehicle of entry.

Advanced persistent threat was the second most common source at 10 percent. Ransomware and unpatched systems tied for the third most common method, at nine percent each.

The CMMI Cybermaturity Platform addresses all of these attack vectors, as well as threats categorized by people, process and technology. The assessment tool generates a unique risk profile for their enterprise. It then prioritizes gaps in capabilities, identifies the maturity required to achieve organizational goals and recommends options to address the gaps.

Social engineering

The Twitter and Magellan Health incidents are both prime examples of successful social engineering attacks. Even with a staff cybersecurity education program in place, all it takes is one person to let their guard down for attackers to achieve their goals. It is vital to not only have identification policies in place, but to ensure that they are adhered to and that their maturity is at an appropriate level that matches the threat risk to the organization.

In the Twitter example, the CMMI Cybermaturity Platform would have helped ensure that people are subject to a stringent identity verification process. In Magellan's case, the Platform would have identified and ensured Magellan had a multi-factor authentication system in place. For example, requiring users to enter a number or code sent by email, text or phone to log in.

Data security

Marriott, MGM Resorts, Zoom and the Greek banking system were all affected by failures of data security, both at rest and in transit. A lesson learned here is to ensure robust encryption policies exist and are rigorously followed. If strong encryption is used, then, to some extent, it reduces the harmful impact if the data is stolen or otherwise exfiltrated.

The CMMI Cybermaturity Platform assessment tool addresses the cyber attack threats across the world, including what encryption policies are in place and how well they're adhered to. It also provides steps and guidance on how companies can improve their encryption actions to increase their cyber readiness, tailored to their specific needs.

Ransomware

Although ransomware attacks, such as Magellan Health and Finastra's, traditionally have a goal of a large financial payout or harming an organization's reputation, recent attacks on hospitals have increased dramatically in the COVID-19 world. Patient records are often inaccessible, literally making this a life and death situation.

The increase of ransomware in health care has been the most significant trend in cybersecurity in the past year, according to a Corvus Security Report[2], which found a 350 percent in ransomware attacks on health care entities in Q4 2019 vs. Q4 2018. Given that 91 percent of ransomware attacks are the result of phishing exploits, health care organizations should improve email security, including using scanning and filtering tools.

Enterprises in all sectors need to practice strong data hygiene. The CMMI Cybermaturity Platform enables organizations to strengthen their risk profiles by providing a guide to implementing a mature program to rebuff ransomware attacks.

Patch management

Magellan Health and Finastra also experienced issues related to patch management. It is critical to ensure that patch management procedures are timely, applicable, leveraged and appropriately applied. They must be continuously reviewed to enable organizations to defend themselves from vulnerabilities and risks. An aggressive patch management program can help mitigate or avoid situations such as ransomware attacks.

ISACA’s CMMI Cybermaturity Platform

This leading Enterprise solution provides a quantifiable, risk-based approach to build cyber maturity based on globally recognized frameworks and standards. As board of directors and senior executives continue to increase awareness of the need to invest in cybersecurity, this leading cybersecurity solution becomes a vitally important, scalable solution to focus cyber investments on the threats that will have the greatest impact.

To learn how **ISACA’s CMMI Cybersecurity Platform** can improve your Enterprise cyber resilience or to schedule a demo, visit www.cmmiinstitute.com/cybermaturity.

[1] Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cyberattacks%20are%20the%20fastest%20growing,in%20size%2C%20sophistication%20and%20cost.&text=%E2%80%9CDDoS%20attacks%2C%20ransom-ware%2C%20and,Shark%20on%20ABC’s%20Shark%20Tank

[2] Corvus Security Report, https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf