AN AFC COVID-19 RESOURCE

Fraud and Emerging Tech:

Cybercrime on the Rise during COVID-19

November 2020

AFC

Despite numerous other challenges faced by companies during one of the most disruptive times in recent decades, cybersecurity remains top of mind for businesses as they respond to the COVID-19 pandemic. This post, part of an emerging technology series from the Anti-Fraud Collaboration, examines the implications of cybercrime during the crisis.

THE CURRENT ENVIRONMENT: HEIGHTENED RISK OF CYBERCRIME

While many companies have been compelled to shift their priorities in response to COVID-19, the pandemic also presents a challenging environment from a cybersecurity threat perspective. As evidenced by PwC's 2020 Global Economic Crime and Fraud Survey, cybercrime is the second most frequently experienced type of fraud, making up 34 percent of overall fraud events. Several factors have elevated the risks of cybercrime during COVID-19, including remote work, virtual crime, and persistent threats, to name a few.

Remote work has exposed new vulnerabilities that need to be addressed to protect companies from the increase in cybersecurity threats. Workforce challenges combined with technological advancements have brought a surge in data breaches, ransomware, and intrusions, along with an increase in business email compromises (BEC) and phishing attempts. Microsoft tracks email phishing campaigns that cover millions of targeted messages each day, of which nearly 60,000 include COVID-19-related attachments or malicious URLs.

In addition to typical phishing and ransomware attacks, the following are examples of social engineering scams that have emerged in light of the pandemic:

+ **Email masquerading as government announcements –** Phishing and BEC emails with logos and other imagery associated with the Centers for Disease Control and Prevention and the World Health Organization include links to items of interest, such as "updated coronavirus cases near you."

+ **False advice and cures –** Not surprisingly, emails purporting to hail from regional medical providers were among the first coronavirus-related phishing attacks that included invites to download attachments containing "secret cures" for the virus.

+ **False charity –** Phishing campaigns solicit donations to stop the spread of the virus and urge victims to donate using Bitcoin or other forms of payment.

+ **Hidden malware –** Malicious emails direct recipients to educational and health-related websites that can be riddled with malware. For example, coronavirus maps have enticed users to click on maps loaded from legitimate sources that run malware in the background.

+ **Operational and industry disruption –** BEC campaigns target industries that have been disrupted, including manufacturing, finance, pharmaceuticals, healthcare, and transportation companies.

+ **Fraud that goes beyond business email compromise –** Fraudsters may also target different groups and products within a company as customers change behaviors and preferences amid the crisis and economic downturn.

Another emerging risk enabled by technological advancements during COVID-19 is untested web and mobile applications that can expose different areas of a company's operations. For example, many companies transitioned to remote work overnight without preparation and were forced to adopt videoconferencing tools, such as Zoom, to facilitate remote work at scale. However, a large volume of users reported incidents of "Zoombombing," where an unauthorized user hijacks a video call and posts hateful, racist, or other inappropriate content. Although Zoombombing did not pose an immediate risk of fraud to users, Zoom faced both legal and reputational ramifications as a result of the security breaches. As more sophisticated cases of cyberattacks are being committed daily, companies ought to be proactive in detecting fraudulent activity perpetrated through the use of emerging technology.

ASSESSING THE RISKS AND IMPACT OF CYBERATTACKS

As cyberattacks and frauds proliferate during times of crisis, companies need to regularly assess their cyber risks and prepare for potential threats. Some of the key risk areas companies should consider include the following:

+ Targeted phishing, malware, and social engineering

+ Strains on infrastructure and security controls

+ Disruptions and operational changes related to third parties

Cyber risk is unique to every company as a company's cyber risk profile is based in part on the potential threats. For example, the type of information that the company collects, stores, or processes will vary by industry sector. During COVID-19, healthcare and technology companies have experienced an increased risk in cyberattacks due to personal data that is collected (*e.g.*, personally identifiable information, protected health information). A company's cyber risks can be further explored based on the following threat categories:

+ **Regulatory and compliance** – Attacks that reveal noncompliance with industry and legal requirements that may result in lawsuits or fines.

+ **Business and financial** – Attacks that can interrupt key business processes or result in loss of data, assets, or funds.

+ **Technical and operational** – Attacks that destroy or block access to critical technical assets.

+ **Strategic** – Attacks aimed at theft of materials with long-term value, such as intellectual property.

In terms of risks related to a company's business processes and financials, the impact of cyberattacks can range from the financial cost of a breach, data loss, potential financial misstatement, disclosure obligations, legal and regulatory actions, to reputational damage. According to IBM's 2020 Cost of a Data Breach Report, the global average total cost of a data breach in 2020 was $3.86 million, with the US leading with the highest country average cost of $8.64 million. Cyberattacks pose a higher risk for certain industries over others; IBM found that the average industry data breach costs have fluctuated between $3.5 million and $4 million in the past six years.

While the risks of cyberattacks remain high, so do the costs. The investment and resources devoted to readily assessing and mitigating cyber risks can be significantly less than the legal and financial consequences of a major cyber breach or ransomware attack.

Chart A presents an overview of the average total cost of a data breach by industry in 2020.

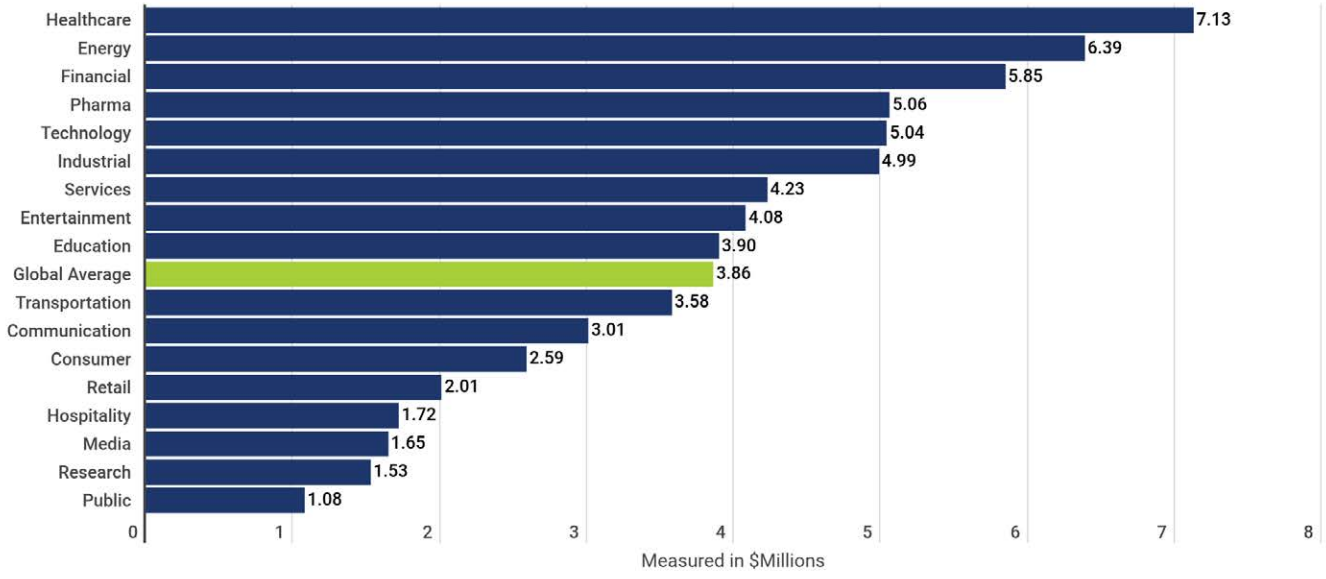
MITIGATING THE RISKS OF CYBERCRIME AND FRAUD

In addition to analyzing the impact of cyberattacks, IBM also found that 76 percent of survey respondents said that remote work would increase the time to identify and contain a data breach as a result of the COVID-19 pandemic. Considering the increased risks in cyberattacks and decreased response time, companies should focus on the fundamentals to mitigate their cyber risks.

Develop a risk-based prioritized security strategy to strengthen basic security coverage: Cybersecurity teams should work with the company's fraud risk management teams to coordinate detection and response activities.

Implement and scale security controls for a mobile workforce: It is critical to establish security controls to prevent threat actors from compromising unsecured or vulnerable employee networks to gain access to sensitive data (*e.g.,* financials, bank account information, payroll, Social Security number).

Chart A: Average Total Cost of a Data Breach by Industry (in US Dollar)



Communicate with and train employees to take an active role in security: Employees are a company's first line of defense and play a critical role in protecting against cyber threats. Companies are only as strong as their weakest link, so employees should be encouraged to be skeptical of emails from unknown or suspicious sources.

Prioritize business and security needs over technology: Companies are increasingly relying on mobile and web applications, chatbots, data reporting, and other tools to enable employees to collaborate in a remote environment. Be proactive in prioritizing security and business drivers when vetting and deploying new technology.

Have an incident response plan ready: Incident response is knowing your threats and being prepared to address those threats. A strong incident response plan starts with a robust cyber risk assessment that includes third-party considerations.

Emerging technologies are becoming more prevalent and can be used for malicious intent—from the phone in one's hand to drones flying overhead—so the cyber risks are endless. Yet threat actors are more likely to choose the traditional, arguably simpler, approach of using phishing schemes to perpetrate fraud. Thus, by being aware of the potential threats unique to them, companies will be more equipped to protect against, detect, and respond to a cyberattack.

Where can I learn more about cybersecurity?

+ AFC: *Anti-Fraud in Action: Insights from the SEC Coronavirus Steering Committee*
+ AFC: *Anti-Fraud in Action: The Fraud Risk Landscape of COVID-19*
+ BDO: *BDO Cyber Threat Insights Fall 2020 Report*
+ CAQ: *The Role of Auditors in Company-Prepared Cybersecurity Information: Present and Future*
+ CAQ: *Understanding Cybersecurity and the External Audit in the COVID-19 Environment*
+ Crowe: *3 Common Misconceptions about Cybersecurity Risk*
+ Deloitte: *Cyber Perspectives & Insights*
+ EY: *COVID-19: Five Steps to Defend Against Opportunistic Cyber Attackers*
+ FEI: *Corporate Shield: What You Need to Know to Protect Your Organization in the Upended Risk Climate*
+ FEI: *Protection vs. Preparation: The Critical Difference between Cybersecurity and Cyber Resilience*
+ Grant Thornton: *Cyber, Privacy and Security Actions in COVID-19*
+ The IIA: *OnRisk 2021: A Guide to Understanding, Aligning and Optimizing Risk*
+ The IIA: *Rethinking Preparedness: Pandemics and Cybersecurity*
+ KPMG: *Cyber Security in the New Reality*
+ NACD: *Emerging Technology: Friend or Foe?*
+ NACD: *NACD Director's Handbook on Cyber-Risk Oversight*
+ PwC: *How to Protect Your Companies from Rising Cyber Attacks and Fraud amid the COVID-19 Outbreak*
+ RSM: *Cyberthreats Continue to Evolve and Companies Must Be Prepared*

Where can I find more COVID-19 resources?

+ CAQ: *COVID-19 Resource Collection*
+ FEI: *COVID-19 Dashboard*
+ The IIA: *COVID-19 Resources Exchange*
+ NACD: *COVID-19 Resource Center*

ANTIFRAUDCOLLABORATION.ORG

WE WELCOME YOUR FEEDBACK

Please send comments or questions to antifraudcollaboration@thecaq.org