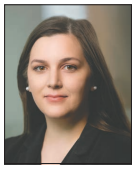
Rise in Cyberattacks Causes Significant Financial and Legal Risk for Business

By Anna Mercado Clark and Mary-Jane R. Morley
Phillips Lytle LLP

COVID-19 has impacted the global cybersecurity landscape in many ways. The rapid transition to remote working and learning will likely continue beyond the pandemic. Many organizations have discovered that they can efficiently conduct their business virtually and have significantly invested in software and technology to do so. This, however, increases cyber risks for all organizations, irrespective of size or industry. For instance, there has been a significant increase in both targeted ransomware attacks and business email compromise attacks causing significant business disruptions, financial losses and legal liability. Additionally, there may be long-lasting damage to an organization's reputation and relationship with consumers, employees and business partners. The question organizations are facing is not if a cyberattack will happen, but when.

Anna Mercado Clark
Partner



Mary-Jane R. Morley
Attorney

Ransomware

Since March 2020, when organizations quickly transitioned to remote work, organizations of all sizes, including FORTUNE 500 companies, primary and secondary schools, colleges and universities, and even small businesses, have been experiencing unprecedented levels of attacks. The FBI reports that over 2,474 ransomware incidents were reported in 2020 *resulting in losses of over $29.1 million.* Cybercriminals typically gain such unauthorized access to networks by compromising remote desktop passwords, engaging in email phishing campaigns, or taking advantage of software, hardware or network vulnerabilities. Ransomware encrypts data, making it inaccessible to the organization. These attacks have grown in sophistication and can sometimes also result in data exfiltration or deletion. Attackers then offer to unencrypt the data in exchange for payment or threaten to expose the data publicly if payment is not made. Payment of the ransom, however, is not a guarantee that the data can be restored or that it won't be publicly released. Payment to certain criminal organizations may also expose the organization to government sanctions. If personal data is exposed, there may be a patchwork of state and international laws with which the organization would have to comply.

Email Compromise Attacks and the Unfortunate Results

Another rapidly evolving type of cyberattack both locally and nationally, is the uptick in email account compromise. In 2020 alone, 19,369 email compromise attacks were reported to the FBI *resulting in losses of over $1.8 billion.* Email compromise attacks target both businesses and individuals, particularly those involved in electronic funds transactions. These types of attacks are frequently carried out when a cybercriminal compromises legitimate email accounts through social engineering, which has increased since the COVID-19 pandemic began. The pandemic has allowed cybercriminals to pose as trusted sources, such as government agencies or health care resources, making the scams more difficult to detect. Attackers may also use credentials and passwords that have been compromised from other data breaches. Cybercriminals prey on human error, carelessness and weak security controls to facilitate these attacks.

Cybercriminals may stay dormant, reviewing emails for months until they see an opportunity to strike. Commonly, as someone is preparing to wire funds relating to a business transaction, the cybercriminal hijacks the party's email communications and replaces legitimate wiring instructions with fraudulent ones. The buyer then unknowingly wires the funds to the cybercriminal instead of the intended recipient. The impact of the transfer is not always noticed until the seller asks where the funds are, and at that time, it can be too late.

Phillips Lytle LLP understands that the pandemic has caused organizations to significantly invest in the technology required to shift to virtual operations. However, as the number of cyberattacks continues to rise, it is essential that organizations remain proactive and diligent with respect to third-party vendor management, internal policies and continuous employee training, among other things. Organizations should also have a plan in place, in the event of a cyberattack, which includes having a capable team of experts that can be quickly activated to respond and mitigate potential risks and losses.

Anna Mercado Clark, CIPP/E, CIPP/US, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400, ext. 6466.

Mary-Jane R. Morley is an attorney at Phillips Lytle LLP and a member of the firm's Data Security & Privacy Practice Team. She can be reached at mmorley@phillipslytle.com or (716) 847-8348.