Navigating Emerging Cybersecurity Threats and Developments in Data Security and Privacy Laws

By Anna Mercado Clark and Jeffrey D. Coren
Phillips Lytle LLP

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP
Partner

Jeffrey D. Coren
Senior Associate

Data security and privacy will continue to be critical in the coming year. Over the past year, federal agencies issued new cybersecurity regulations and updated guidance. Data security and privacy laws were passed and/or updated. Cyberattacks exploited various security vulnerabilities, and remote work continued to make organizations of all sizes susceptible. These trends will require organizations to remain vigilant about their cybersecurity posture and regularly review their data practices and policies with the help of trusted advisors.

Evolving Cybersecurity Threats

Cyberattacks are becoming increasingly complex. Ransomware attacks may involve double or triple extortion, where attackers not only encrypt vital data, but also threaten to expose stolen data, or cripple an organization by shutting down essential machines or networks unless a ransom is paid. Zero-day attacks—where attackers exploit known security flaws before companies can fix the vulnerability—are also on the rise. For instance, zero-day attacks on ubiquitous Microsoft Exchange Servers in March 2021 impacted more than 100,000 mail servers, and well-known ransomware groups are exploiting the recently discovered vulnerability in Log4j, which is software commonly used by apps and websites. Left unmitigated, these vulnerabilities can allow attackers to infiltrate private systems, infect networks with malicious software, or steal data and log-in information.

Cyberattacks continue to target health care, retail, information technology and financial services sectors, but energy, manufacturing and production sectors are also becoming increasingly common targets. Attacks may target a company directly or indirectly, such as through a vendor or commonly used software. As companies of all sizes and in all industries are likely to continue remote and flexible work arrangements, cyberattacks are likely to cause significant business disruption and financial losses, which can be costly. IBM Security reported that the average cost of a data breach increased by nearly 10% in 2021, with a total average cost of $4.24 million and an average per record cost of $161. Having the right policies and procedures, training, technology and controls can mitigate these risks and allow companies to respond rapidly when an attack is successful.

New Data Security and Privacy Laws and Regulations

The California Privacy Protection Agency—the first dedicated, state-wide privacy enforcement agency in the nation—has begun the rulemaking process for implementation of the California Consumer Privacy Act (as amended by the California Privacy Rights Act), which takes effect in 2023. Virginia and Colorado enacted comprehensive data privacy laws, which will also take effect in 2023. Further, Connecticut, Texas, Utah and Nevada updated their data breach notification laws, and New York City enacted a biometric privacy law.

Federal agency enforcement activity continues to rise across various industries. For instance, in November 2021, the Office of the Comptroller of the Currency, the Federal Reserve Board and the Federal Deposit Insurance Corporation approved a joint rule, effective April 1, 2022 with a compliance deadline of May 1, 2022, that will require federally regulated banking organizations to notify their primary regulator of certain computer security incidents within 36 hours, among other things. Around the same time, these agencies also issued a joint statement previewing forthcoming guidance regarding crypto-asset-related activities. On September 15, 2021, the Federal Trade Commission clarified that certain health applications and connected devices are subject to data breach notification requirements, while on September 21, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control warned about potential sanctions that may result from ransomware payments. Federal agencies also issued data security regulations for rail carriers and critical pipelines.

Foreign laws also continue to impact U.S.-based companies, such as Europe's General Data Protection Regulation (GDPR), for which new guidance and standard contractual clauses were issued; the UK GDPR, resulting from Brexit; and other countries enacting or updating their own laws that seek to apply extraterritorially (e.g., China's Data Security Law and Personal Information Protection Law). Accordingly, compliance solely with domestic laws or the GDPR may no longer be sufficient, and compliance strategies should be revisited regularly.

Looking Ahead to 2022

Data protection risks continue to evolve. At the same time, organizations are frequently subject to new data security and privacy laws and increased regulatory requirements. Businesses should have a capable and experienced team of experts to navigate these ever-changing legal requirements and respond quickly in the event of a cyberattack.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, 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.

Jeffrey D. Coren is a senior associate at Phillips Lytle LLP and a member of the firm's Data Security & Privacy Practice Team. He can be reached at jcoren@phillipslytle.com or (716) 847-7024.