Adapting to Evolving Cybersecurity Risks and Updated Data Security and Privacy Laws

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

This past year continued the trend of an increased focus on data security and privacy with the enactment of new laws and increased regulatory activity. Cyberattacks made national headlines as remote work continued to make organizations more vulnerable. Accordingly, organizations should regularly review and update their security posture with the assistance of knowledgeable experts.

Increase in Cybersecurity Threats

Cyberattacks are becoming increasingly sophisticated and widespread. High-profile ransomware attacks in 2021 shut down one of the nation's largest fuel pipelines and halted operations at the world's largest meat processing company, prompting the FBI to declare in June 2021 that the ransomware threat was comparable to the threat of global terrorism after September 11, 2001. Further, as companies of all sizes continue to adjust to remote work, cyberattacks — including ransomware, business and personal email compromise, and attacks on third-party service providers — are on the rise, causing significant business disruption and financial losses. Having the right policies and procedures, training, technology (including hardware) and controls, can mitigate these risks and allow companies to respond rapidly when an attack is successful.

New Data Security and Privacy Laws

This past year saw a flurry of data security and privacy legislation at the federal, state and local levels. The California Consumer Privacy Act (CCPA) went into effect in 2020, and the states of Virginia and Colorado followed by enacting comprehensive data privacy laws in 2021. Although some provisions in these laws mirror some of the consumer data rights and data controller responsibilities set forth in the CCPA, there are enough distinctions that companies cannot rely solely on existing programs to ensure compliance with all of these state laws. The California Attorney General issued new regulations to clarify how it intends to enforce the CCPA. CCPA enforcement is in full swing, and other states such as Connecticut, Texas, Utah and Nevada updated their data breach laws. And at the local level, New York City enacted a biometric privacy law that requires certain commercial establishments to notify customers of biometric collection activity and makes it unlawful to sell, lease or profit from biometric information. Many other laws are pending, so additional obligations are likely.

State and Federal Regulatory Developments

State and federal regulators were also busy this year. The New York State Department of Financial Services (DFS) reached multimillion dollar cybersecurity settlements with numerous entities. At the federal level, the U.S. Securities and Exchange Commission entered into significant settlements with several entities related to their deficient disclosure of cybersecurity incidents. In addition, the U.S. Department of Homeland Security's Transportation Security Administration announced several Security Directives for critical pipelines, and the U.S. Department of Labor issued guidance concerning best practices related to cybersecurity for retirements plans, among other things. Regulatory agencies have wide latitude in enforcing data protection standards and requirements, so it is best to anticipate potential issues before they arise and attract the attention of government agencies.

International Data Transfers

There were also several updates related to international data transfers. For example, the European Commission published new standard contractual clauses ("SCCs") governing cross-border data transfers under the General Data Protection Regulation (GDPR), largely in response to the recent Schrems II decision, which invalidated the EU-U.S. Privacy Shield. The UK Information Commissioner's Office also recently launched a consultation on the International Data Transfer Agreement, which will replace the UK SCCs, among other things.

Anna Mercado Clark
Partner

Looking Ahead to 2022

The data security and privacy landscape will continue to change in 2022 with more countries, states and localities likely to update their data protection laws. At the same time, cybersecurity threats are likely to become more prevalent and sophisticated, especially as companies continue to adapt to the new demands of a pandemic-impacted workplace. To maintain compliance with evolving data privacy laws, and to safeguard against these developing cybersecurity risks, organizations should continuously evaluate and update their data protection program with the assistance of knowledgeable experts. Organizations should also have a capable and experienced team of experts available to respond quickly in the event of a cyberattack.

Jeffrey D. Coren
Senior Associate

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