Global overview

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

With interconnectivity and use of digital storage expanding, cyber-threats posed by nation states, commercial competitors, company insiders, transnational organised crime syndicates and 'hacktivists' have continued to grow on a global basis. High-profile data intrusions in the United States and Europe have brought particular attention to cyber -extortion -and cyberattacks perpetrated by nation states, and to business email compromises aimed at financial fraud by criminal groups. As a result, the general trend around the world is that cybersecurity will continue to grow as a dominant compliance topic, both because organisations have increasingly shifted valuable assets to digitised formats and because countries increasingly perceive cybersecurity threats to closely align with national security concerns.

Two particular developments merit special attention. First, many countries are strengthening requirements around user consent and control over the collection of personal data as organisations around the world regularly suffer data security incidents, ranging from nuisance intrusions and petty theft to criminal conspiracies. The Ponemon Institute in the United States estimated in 2018 that the average cost of a data breach globally is US$3.86 million. Such losses are prompting more calls for reform and more emphasis on developing regulatory standards for minimum safeguards. For example, in Europe, European Union General Data Protection Regulation (GDPR) became effective in 2019 and imposed new data security obligations on EU data controllers and processors.

In the United States, law makers and regulatory agencies are expanding enforcement actions to address cybersecurity issues, and to create more proscriptive data security standards. These efforts are largely decentralized. U.S. state attorneys general and consumer regulators have substantial authority to police data security compliance with regard to consumer businesses (along with the Federal Trade Commission). And agencies like the US Securities and Exchange Commission regularly issue guidance requiring companies to disclose material information on the nature of cyberthreats or to otherwise take steps aimed at enhancing cybersecurity compliance among U.S. businesses. But there are no national cybersecurity standards in the United States. The U.S. Congress held hearings in 2019 studying the concept of national privacy legislation, which would include minimum standards for safeguarding personal data, but such efforts appear unlikely to get traction in the near term. In the meantime, several U.S. states are creating their own data handling safeguards similar to GDPR requirements.

Second, countries are expanding foreign investment rules and import/export restrictions to protect important technologies and to help alleviate perceived cybersecurity vulnerabilities. Following China's Cybersecurity Law, which became effective in June 2017 and imposed data security requirements on computer network operators and 'critical information Infrastructure' providers, China issued the Measures for the Administration of Scientific Data on March 17, 2018 (with immediate effect), which restricts the export of scientific data while at the same time calling for wider access to such data within the country. In June 2019, Vietnam approved a new cybersecurity law in January 2019 requiring global technology companies with users in Vietnam to set up local offices and store data locally.

The United States has likewise expanded regulatory efforts designed to protect the country from a wide variety of perceived national threats associated with data security. US federal agencies promulgated in 2019 proposed new regulations designed to restrict imports associated with U.S. Information and communications technology services, and expanded government powers to review transactions where foreign persons acquire large amounts of sensitive U.S. person information (in part because of perceived cybersecurity threats). In August 2018, the White House announced a new national cyber strategy, which outlines efforts to increase the resiliency of U.S. information systems and deter threat actors from launching malicious attacks against the United States, including authorizing offensive cyber operations against foreign adversaries. In May 2017, President Trump issued an Executive Order, entitled Cybersecurity of Federal Networks and Critical Infrastructure, that focuses on US government agencies assessing cyber-preparedness to respond to various threats to electrical supply, defence infrastructure and other critical government functions. In 2016, President Obama issued an Executive Order authorising the imposition of economic sanctions against individuals or entities found to be engaged in malicious cyberactivity and agreed to a new cybersecurity framework with China intended to limit state-sponsored theft of corporate secrets.

The EU is likewise pursuing efforts broadly aimed at cyber resiliency. The European Council's Network and Information Security Directive imposes security obligations on 'operators of essential services' in certain important economic sectors, such as health, water supply, financial markets, banking and energy. Businesses in these sectors will be required to manage cyber risks and report significant cyber breaches. Similarly, the European Parliament adopted the GDPR in April 2016, which, as of May 2018, requires data processors to implement a variety of security provisions and appoint data protection officers. The European Commission issued a Joint Communication in September 2017, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', which focuses particular attention on the need to enhance cybersecurity protections as the internet of things continues to grow steadily in the developed world. In June 2018, the EU reached a political agreement on the EU Cybersecurity Act, which would a establish framework for certification schemes to apply to a range of online services and connected consumer devices and establish an EU Cybersecurity Agency.

Many reforms are also taking place within industries and are customer---driven. Payment card companies in the US are now requiring chips to tokenise payment card data. In a relatively new development for many companies, commercial customers around the world are increasingly adding cybersecurity requirements to contracts and demanding controls on how information technology suppliers hold data in cloud centres or otherwise demand special obligations related to protecting data. Cybersecurity provisions are frequently a key part of negotiations involving outsourcing of data and the sharing of data between companies, and cybersecurity diligence is of growing importance for M&A transactions. In addition, companies may require audits and other rights and remedies to address cybersecurity challenges.

All this suggests that cybersecurity related issues will remain a high-priority compliance issue for corporate counsel, senior executives and company boards. In this environment, maintaining an effective and global corporate cybersecurity programme is becoming the standard expectation for all businesses. Around the globe, the cybersecurity legal landscape continues to shift rapidly as governments consider new laws, regulations and enforcement policies. In the years ahead, companies will be faced with an increasingly complex array of cybersecurity compliance challenges and risks. At the same time, governments are working to determine the appropriate regulatory policy to govern the rapidly changing information technology environment, and the best framework for working with the private sector to improve the security of digital assets.