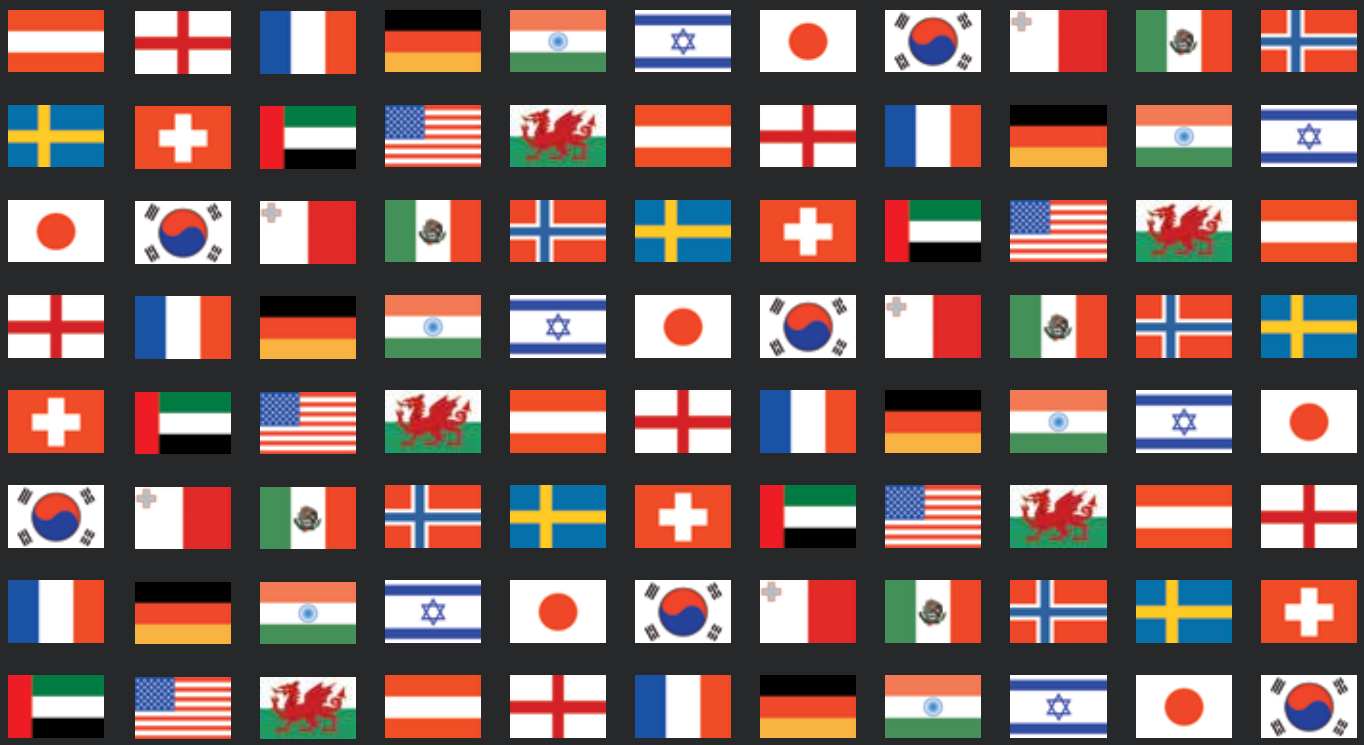
Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman



2017

GETTING THE DEAL THROUGH

Global overview

Benjamin A Powell, Jason C Chipman and Marik A String
Wilmer Cutler Pickering Hale and Dorr LLP

With interconnectivity and use of digital storage expanding, cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists' have continued to grow on a global basis. Recent high-profile data intrusions in the United States have brought particular attention to cyberespionage and cyber 'attacks' perpetuated by nation states, prompting data and information security to become a major geopolitical topic for relations among the United States, Russia, China and several other nations. In Europe, passage of the EU General Data Protection Regulation (GDPR) in April 2016 is imposing new data security obligations on EU data controllers and processors. All of these events suggest that for commercial enterprises throughout the world, cybersecurity is no longer a technical issue for information technology personnel; it is a high priority for corporate counsel, senior executives and company boards. In this environment, maintaining an effective corporate cybersecurity programme is becoming the standard expectation for all businesses.

The growth of cybersecurity as a distinct discipline is a result of the remarkable value of assets accessible within companies and across national borders in digitised formats. Organisations around the world regularly suffer data security incidents ranging from nuisance intrusions and petty theft to massive criminal conspiracies. The German government recently estimated that its companies lose between US$28 billion and US$71 billion (and 30,000 to 70,000 jobs) per year from economic espionage, and the Ponemon Institute in the United States estimated in 2016 that the average cost of a data breach in the United States is US$4 million. Such losses are prompting more calls for reform and more emphasis on developing regulatory standards for minimal safeguards.

Some economic sectors are more vulnerable than others. In the past few years, global criminal networks have targeted personal and financial information of customers in the retail and financial services industries, foreign nations have stolen valuable intellectual property, and anonymous hackers have sought to destroy or embarrass corporations and executives. Nevertheless, despite these real threats, a surprising number of companies lack formal information security policies and incident response plans. Critical infrastructure sectors have become a particularly common target for cyber intrusions: a 2014 survey by the Ponemon Institute of 599 executives from the power, oil, gas and water sectors in 14 countries found that 70 per cent of respondents had experienced network intrusions.

In response to these challenges, governments from around the world are implementing legal reforms and shifting enforcement priorities. In the European Union, the legal framework for cybersecurity among member states is evolving to deal with new threats. The European Commission has issued a Cybersecurity Strategy to bolster cyber resilience, develop a more coherent cyberdefence policy and promote industrial cooperation. On 27 May 2016, the European Council adopted the Trade Secrets Directive, which will be implemented by member states in 2018 and will create more uniform intellectual property protections across the EU. On 17 May 2016, the European Council adopted the Network and Information Security Directive, which 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 to report significant cyber breaches. Similarly, the European Parliament adopted in April 2016 the GDPR, which requires data processors to implement a variety of security provisions and to appoint data protection officers.

In the United States, dozens of federal and state statutes address cybersecurity issues, but no overarching statutory framework exists. The US Congress enacted legislation in late 2015 to encourage businesses to voluntarily share cyberthreat data with one another and with the government. In December 2016, the Commission on Enhancing National Cybersecurity, which was created by a presidential directive, issued more than 50 recommendations for improving cybersecurity in the United States. Notable recommendations included developing ways to incentivise companies to implement cybersecurity programmes, creating standards for security of the Internet of Things and creating a new ambassador position in the US government focused on cybersecurity. Although cybersecurity standards are largely a product of voluntary efforts in the United States, US regulatory agencies are expanding enforcement actions to address cybersecurity issues. For example, the US Securities and Exchange Commission has issued guidance requiring companies to disclose material information on the nature of any cyberthreats and challenged numerous companies on the adequacy of their disclosures. Similar efforts to protect against cyber intrusions are taking place in other jurisdictions as well.

Following several high-profile cyber-intrusion events in 2015 and 2016, the United States has continued to focus on international action to enhance cybersecurity and data protection. The US President 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 Trans-Pacific Partnership trade agreement, which was recently agreed between the United States and 11 other nations, also contains added protections for the theft of trade secrets and confidential information using computer systems.

Many reforms are also taking place within industry 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 demand 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. In addition, companies may require audits and other rights and remedies to address cybersecurity challenges.

Around the globe, the cybersecurity legal landscape continues to rapidly shift 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.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Cybersecurity
ISSN 2056-7685

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law