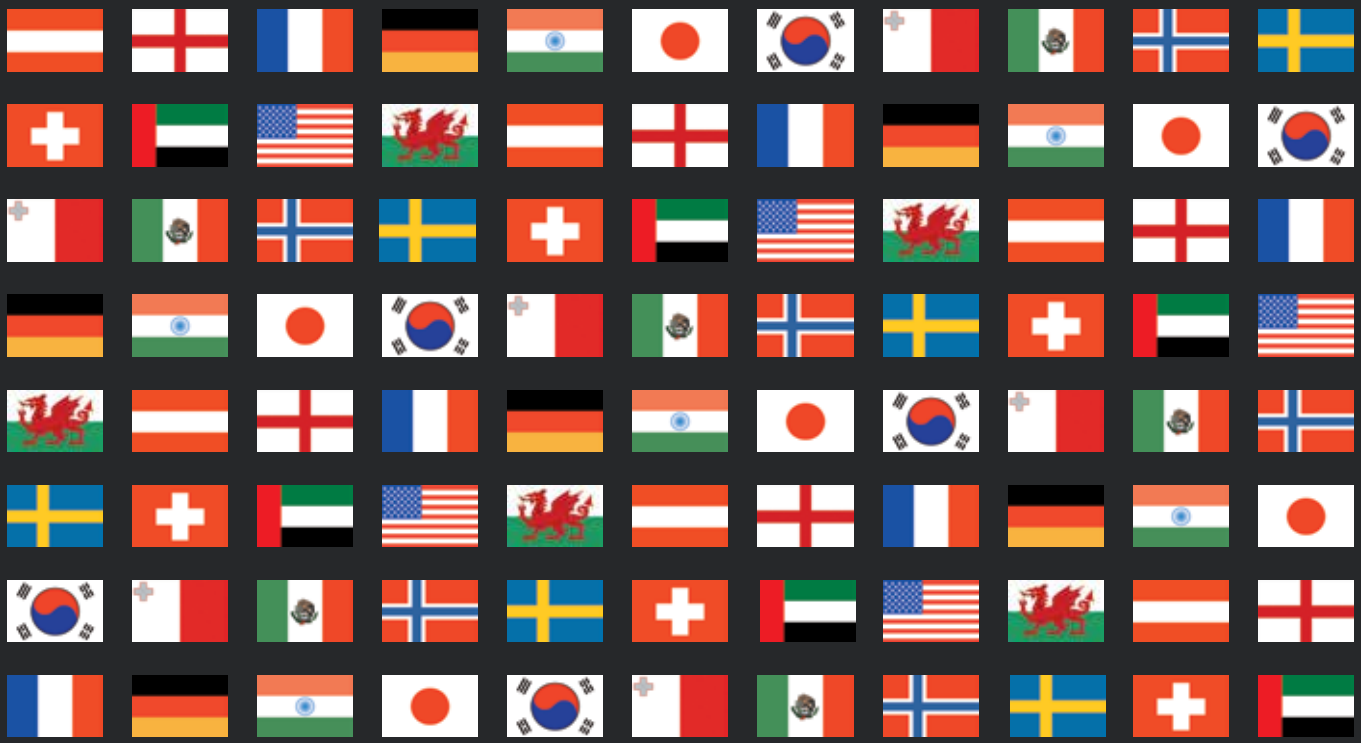
Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman



2016

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2016

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2015
Second edition
ISSN 2056-7685

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

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' are growing on a global basis. Recent high-profile data intrusions in the United States have brought particular attention to cyber espionage and cyber 'attacks' perpetuated by nation states, prompting data and information security to become a major geopolitical topic for relations between the United States and China, as well as several other nations. For commercial enterprises, 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 likewise growing in importance.

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. Such data thefts 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 cyber defence policy and promote industrial cooperation. On 7 December 2015 the European Union agreed on the final text for a Network and Information Security Directive, which would improve cybersecurity cooperation and capabilities among member states and require operators of 'essential services' in certain sectors to take appropriate security measures. On 15 December 2015, the European Union reached an agreement on the final text for a new General Data Protection Regulation, which is likely to be approved by the European Parliament in early 2016. The Regulation will replace a 1995 Data Protection Directive that has been the basis for national data protection laws of EU member states. On 15 December 2015, the European Union also approved the final text of a new directive to protect against the theft of trade secrets and other confidential business information, which would introduce common definitions, provide more effective redress for theft and prioritise enforcement of such types of theft. In October 2015, the European Court of Justice issued a landmark decision that called into question the validity of US-EU 'safe harbour' arrangements, which had provided legal protections for companies that transferred personal data between the two jurisdictions. How this decision may impact the flow of data important for cybersecurity measures is not yet clear.

In the United States, dozens of federal and state statutes address cybersecurity issues, but no overarching statutory framework exists. The US Congress has considered several legislative proposals focused on enhancing critical infrastructure protection, bolstering information sharing, strengthening the protection of personal data and increasing criminal penalties for economic espionage and theft. A 2013 US Executive Order directed the development of a voluntary cybersecurity framework to incorporate industry best practices and called for an expansion of information sharing and collaboration between government and the private sector. 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, the United States has increased 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
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
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
Enforcement of Foreign Judgments
Environment & Climate Regulation
Executive Compensation & Employee Benefits
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
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 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