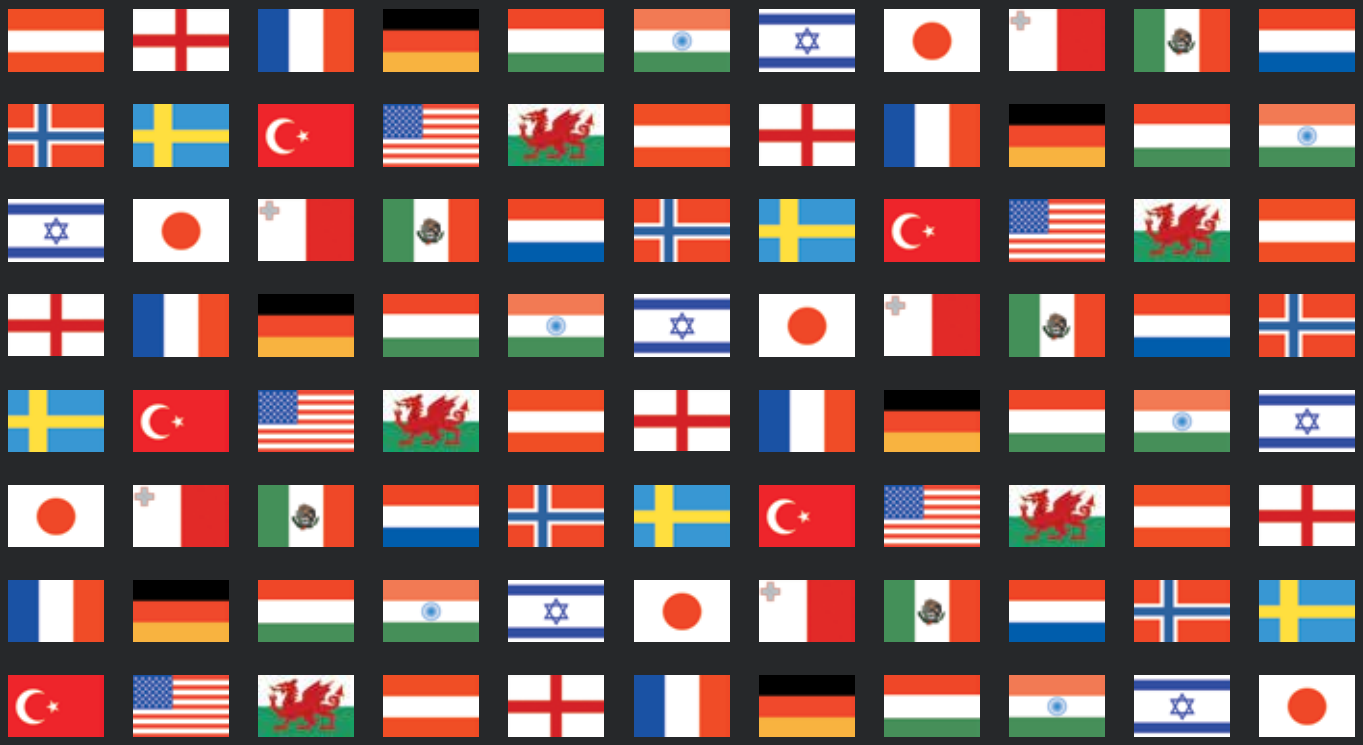
Cybersecurity

In 15 jurisdictions worldwide

Contributing editors
Benjamin A Powell and Jason C Chipman



2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2015

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@lbresearch.com

Adam Sargent
adam.sargent@lbresearch.com

Dan White
dan.white@lbresearch.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
First 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 increased interconnectivity and use of digital storage, cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime, and 'hacktivists' continue to grow. What used to be a technical issue for information technology personnel is increasingly the highest priority issue addressed by corporate counsel, senior executives, company boards and government agencies throughout the world. Cybersecurity intersects several legal disciplines, such as data privacy, surveillance, securities, criminal, intellectual property, information technology, digital protection and corporate governance. In many countries, cybersecurity is a geopolitical and military issue as well.

The growth and significance of cybersecurity is a product of the remarkable value of assets that are today increasingly 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 and espionage. Not only are digitally stored corporate secrets, such as customer information and lists, research, business planning, and internal corporate communications, frequently very valuable, but studies indicate they can be remarkably vulnerable as well. A 2012 survey by Infosecurity Europe found that 93 per cent of large corporations and 76 per cent of small businesses had a cybersecurity breach over the previous year, and a study conducted by the Japanese government found that more than 35 per cent of respondent firms had reported some form of technology loss. Indeed, the German government estimates that its companies lose between US$28 billion and US$71 billion (and 30,000 to 70,000 jobs) per year from economic espionage.

The potential damage from vulnerable computer networks varies among economic sectors. In the past few years alone, global criminal networks have targeted personal and financial information of customers in the retail and financial services industries; foreign nations have sought to steal 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 robust formal information security policies and incident response plans. Critical infrastructure sectors have become a particularly common target for cyber intrusions: a 2010 survey of 200 executives from the power, oil, gas, and water sectors in 14 countries found that 85 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 and, in 2013, proposed a new Directive on Network and Information Security. This measure would strengthen preparedness, cross-border cooperation and information exchange among EU member states, as well as require notification of certain cyber incidents having a significant impact on the security of core services in sectors such as energy, transport, health, information technology and financial services. The European Commission has also proposed 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. Similar changes to protect against cyber intrusions are taking place in other jurisdictions as well.

In the United States, more than 50 federal and state statutes address cybersecurity issues, but no overarching statutory framework exists. Key federal cybersecurity laws include the Computer Fraud and Abuse Act, which imposes fines and criminal penalties on interference with computers connected to the internet; the Electronic Communications Privacy Act, which prohibits electronic eavesdropping; and the Economic Espionage Act, which imposes criminal penalties against the theft of trade secrets. The US Congress has also 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.

Meanwhile, US agencies are expanding enforcement actions to address cybersecurity issues. For example, the Securities and Exchange Commission has issued new guidance requiring companies to disclose material information on the nature of any cyberthreats and challenged numerous companies on the adequacy of their disclosures. The Federal Trade Commission has also initiated enforcement actions against companies for failing to protect consumer personal data as an 'unfair or deceptive' trade practice and reached settlements with over 50 companies on data security practices. The US Congress has also launched its own investigations into various companies' cybersecurity practices. Moreover, companies that suffer a cyber breach frequently face litigation alleging tort or contract claims.

Many reforms are also taking place within industry and are customer-driven. 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
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
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
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

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