Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2018

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in January 2018
For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2015
Fourth edition
ISBN 978-1-912377-38-1

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

CONTENTS

Preface

Cybersecurity 2018

Fourth edition

Getting the Deal Through is delighted to publish the fourth edition of *Cybersecurity*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Australia, Italy, Philippines, Spain, Turkey and Ukraine.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
January 2018

Global overview

Benjamin A Powell, Jason C Chipman and Maury Riggan
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 syndicates and 'hacktivists' have continued to grow on a global basis. Recent high-profile data intrusions in the United States have brought particular attention to cyber extortion and cyberattacks perpetrated by nation states, prompting data and information security to become a major geopolitical topic for relations between the United States, Russia, China and several other nations. In Europe, passage of the European Union General Data Protection Regulation (GDPR) in April 2016 imposed new data security obligations on EU data controllers and processors, with GDPR enforcement set to begin in May 2018. Further, in China, the Cybersecurity Law, which became effective in June 2017, imposed new data security requirements on computer network operators and 'critical information infrastructure' providers. All this suggests that cybersecurity 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.

Cybersecurity has grown in importance as a distinct discipline and compliance issue, as all organisations have increasingly shifted valuable assets to digitised formats. Organisations around the world regularly suffer data security incidents, ranging from nuisance intrusions and petty theft to massive criminal conspiracies. The Ponemon Institute in the United States estimated in 2017 that the average cost of a data breach globally is US$3.62 million. Such losses are prompting more calls for reform and more emphasis on developing regulatory standards for minimum 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 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 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 report significant cyber breaches. Similarly, the European Parliament adopted the GDPR in April 2016, which requires data processors to implement a variety of security provisions and appoint data protection officers (the GDPR will be in force in May 2018).

In the United States, dozens of federal and state statutes address cybersecurity issues, and 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), but no overarching statutory framework governs cybersecurity in the US. Businesses in the US are encouraged by the government to cooperate with one another and with government authorities to share cybersecurity threat information, but such sharing is voluntary. 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 has 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 focused substantially on international action to enhance cybersecurity and data protection. 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. 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.

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. In addition, companies may require audits and other rights and remedies to address cybersecurity challenges.

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.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
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
Joint Ventures
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
Private M&A
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
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

ISBN 978-1-912377-38-1