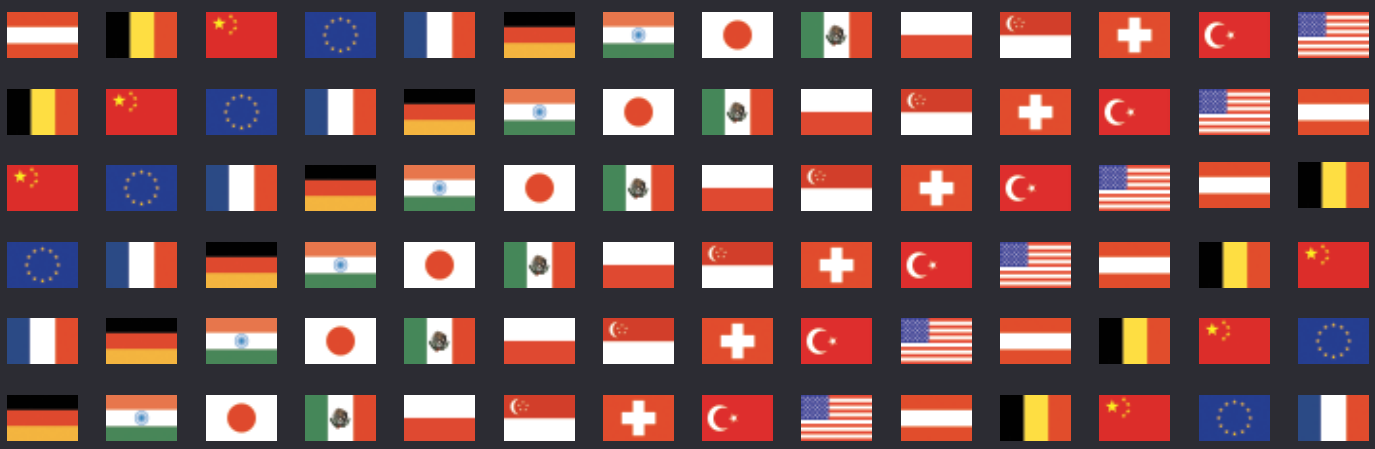
Cybersecurity 2021

Contributing editors
Benjamin A Powell and Jason C Chipman



LEXOLOGY®
Getting The Deal Through

GDR

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2015
Seventh edition
ISBN 978-1-83862-643-3

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

Cybersecurity
2021

Contributing editors
Benjamin A Powell and Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

Lexology Getting The Deal Through is delighted to publish the seventh edition of *Cybersecurity*, which is available in print and online at www.lexology.com/gtdt.

Lexology 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 Lexology 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 a new chapter on Belgium and the European Union.

Lexology 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.lexology.com/gtdt.

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.

Lexology 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.

LEXOLOGY
Getting The Deal Through

London
February 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in March 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

Global overview

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Around the globe, data about individuals, businesses and strategically significant technology is increasingly stored in digital formats. As a result, cyberthreats are growing and cybersecurity is an increasingly significant compliance and regulatory issue for private companies and governments. Some cyber threats are well known – hackers backed by nation states, commercial competitors, company insiders, transnational organised crime syndicates and 'hacktivists' have continued to grow on a global basis over the past year. Other threats represent new targets of opportunity associated with businesses moving operations online as a result of the covid-19 pandemic. High-profile data intrusions in the United States and Europe have brought particular attention to cyber extortion and to business email compromises aimed at financial fraud.

Two trends in this area will be particularly important in 2021. 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. For example, EU regulators have issued guidance in recent months on the handling of data related to covid-19, calling for a uniform approach to mobile apps and related technologies deployed to track infections. In China, personal information security requirements were promulgated in March 2020. These new rules are voluntary but Chinese regulators may expect companies operating in China to comply with the requirements, such as allowing individuals to have control over how their personal information is used and rules on protecting personal information obtained by companies. In the United States, federal regulators are issuing warnings about new and sophisticated fraud schemes aimed at capitalising on perceived vulnerabilities associated with businesses doing more work remotely during the pandemic.

Second, countries are expanding the use of tools associated with statecraft to protect critical data, such as new foreign investment controls, and import and export restrictions to protect important technologies and to address perceived cybersecurity vulnerabilities. For example, in 2019 China promulgated a new foreign investment law that empowers Chinese regulators to review certain foreign investment that may result in foreign access to critical data, among other things. Likewise, in 2020 the Trump administration promulgated new rules associated with evaluating foreign actors allowed access to the US telecommunications system, and the US expanded government powers to review transactions where foreign persons acquire large amounts of sensitive US person information (in part because of perceived cybersecurity threats). Separately, US federal agencies have increasingly signalled that companies associated with the Chinese government will be blocked from US commerce, presumably on the grounds of cybersecurity threats. These efforts are consistent with the 2018 White House national cyber strategy, which outlined efforts to increase the resiliency of US information systems and deter threat actors from launching malicious attacks against the United States, including authorising offensive cyber operations against foreign adversaries. And the Trump administration has continued to impose 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.

Like its US counterparts, the European Union has issued special warnings throughout 2020 about potential data security threats associated with covid-19, and has issued new rules empowering EU states to evaluate foreign transactions that may result in access to sensitive data. For example, EU Regulation 2019/452 entered into force on 10 April 2020, with rules establishing a general framework for the screening of foreign investment in the EU on the grounds of security or public order, including special focus on investments that may result in access to sensitive data about EU data subjects.

And EU data security requirements continue to be enforced in earnest. 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 are required to manage cyber risks and report significant cyber breaches. Similarly, the General Data Protection Regulation requires data processors to implement a variety of security provisions and to appoint data protection officers.

Many reforms are also taking place within industries and are customer driven. Payment card companies in the United States 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 the 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.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
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
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
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 M&A
Public Procurement
Public-Private Partnerships
Rail Transport
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
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-643-3