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

Israel

Eli Greenbaum
Yigal Arnon & Co

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Israel does not currently have any laws dedicated specifically to cybersecurity matters. At the same time, a number of statutes, regulations and government resolutions address cybersecurity issues.

Israel instituted a formal national cybersecurity policy in 2002. In that year, Government Resolution 84/B established the National Information Security Agency, which was tasked with regulating and advising critical infrastructure on cybersecurity matters. The Security in Public Bodies Law implemented this Resolution by requiring public bodies to appoint security officers, and such officers were responsible for executing the National Information Security Agency directives. The Law defined public bodies broadly to include specified utilities, telecommunication companies, financial and public transportation bodies and government agencies. In 2011, Government Resolution 3611 reorganised national cybersecurity policy by establishing the National Cyber Bureau (NCB). The NCB was to provide policy guidance in cybersecurity, advance Israel as a world-class centre in the development of information technology and encourage cybersecurity cooperation between academia, industry and the government. In 2015, Government Resolution 2444 established the National Cyber Defense Authority (NCDA) as the civilian operational arm of the NCB. The NCDA is intended to be responsible for national cybersecurity policy in the civilian sector, but legislation setting forth the authority and responsibilities of the NCDA has yet to be brought to the Knesset.

A number of statutes and regulations impose specific cybersecurity requirements on private and public bodies. The Protection of Privacy Law 1981 (the Privacy Law) is a generally applicable data privacy and data security statute. The Privacy Law also established the Registrar of Databases (the Registrar), which was later folded into the Privacy Protection Authority (PPA). The Registrar serves as Israel's data protection authority and represents Israel in international privacy matters. Over the years, the Registrar has issued regulations and guidelines that mandate additional data security measures, such as the Privacy Regulations (Transfer of Information to Databases outside of the State's Boundaries) 2001 (the Data Transfer Regulations), which regulate international data transfers, and the Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data Between Public Bodies) (the Data Possession Regulations), which impose certain data security requirements. In 2017, the Privacy Regulations (Information Security) 2017 (the Information Security Regulations) received parliamentary approval. The Information Security Regulations, which will enter into effect in May 2018, impose specific granular requirements with respect to personal data collected and maintained in databases, including basic data breach notification requirements.

Israel's financial regulators have issued a number of directives that address cybersecurity in the financial sector. These include Bank of Israel Directive 361 – Proper Conduct of Banking Business, which sets out a general framework for cyber risk management in the banking sector, and Directive 357 – Information Security Management, which details information security controls for banking corporations and is intended to be compliant with the Risk Management Principles for Electronic Banking issued by the Basel Committee in 2003. The Ministry of Finance has also issued Circular 2016-9-14, which addresses cybersecurity in insurance companies and pension funds. The recently enacted Credit Information Law 2016 authorises the Bank of Israel to promulgate information security requirements for credit bureaus.

The Computers Law 1995 addresses computer crimes, including the unauthorised access to, or disruption of, devices. The Computers Law was amended in 2012 for consistency with the Budapest Convention on Cybercrime, although Israel has yet to become a signatory to the convention.

Israel is not a member of the Wassenaar Arrangement on export controls, but its domestic export control regime under the Defence Export Control Law 2007 and associated regulations generally tracks the Wassennaar control lists. As such, exports of cybersecurity technology from Israel are generally controlled to the extent that these items are controlled under the Wassennaar Arrangement. Applications for the export of dual-use technology to military end users are generally made to the Defence Export Control Agency in the Ministry of Defence, while applications for civilian end users are generally made to the Ministry of the Economy.

Surveillance law is governed by the Wiretap Law 1979, which generally requires investigative authorities to obtain a court order before engaging in electronic surveillance. However, electronic surveillance for purposes of national security requires only the approval of the Minister of Defence or Prime Minister.

Encryption controls are imposed by the Order for the Supervision of Products and Services (Encryption) 1974, which was updated in 1998 (the Encryption Order). The Encryption Order imposes broad licensing requirements for the use, development or distribution of encryption technology in Israel. Encryption licences are usually granted as a matter of course, but such licences can impose additional export controls or restrictions on the transfer of source code abroad.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Israel boasts a strong domestic industry in the production and export of cybersecurity software products. In early 2016, the Israeli Defence Export Controls Agency (DECA) proposed new regulations concerning the export of such cybersecurity products that would have strongly impacted the sector. These proposed regulations went substantially further than the export control regime of the Wassenaar Arrangement. The domestic cybersecurity software industry pushed back strongly against these proposed regulations. As a result of this industry pressure, DECA eventually withdrew the proposed regulations. Nonetheless, Israeli domestic law continues to incorporate the control lists of the Wassenaar Arrangement, and it is currently unclear how strictly government regulators will interpret those controls. This uncertainty has weighed heavily on the domestic software cybersecurity industry.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Government Resolution 2443 sets forth general principles for cybersecurity regulation in Israel. Resolution 2443 generally provides that local Israeli regulation should be based on international standards to the extent possible. More specifically, Resolution 2443 points to ISO 27001 as the applicable standard for organisational cybersecurity and ISO 15408 as the applicable standard for certifying cybersecurity products.

Under Resolution 2443, government offices are required to satisfy ISO 27001 and government procurement procedures are also required to ensure that all purchased equipment and services also satisfy that standard.

In 2012, the Ministry of Health published Circular 18/2012, which requires all healthcare institutions to obtain certification under ISO 27799. The Circular also requires all service providers to such institutions that hold either medical information or information regarding the infrastructure of the institution to comply with the standards of ISO 27799.

In addition, a number of Israeli regulatory authorities have recommended (but not required) that entities look to ISO 27001 in prescribing information security requirements. For example, in 2011, PPA published Directive 2-2011, which sets forth certain requirements concerning the outsourcing of data processing activities. The Directive requires all entities that outsource data processing activities to consider possible cybersecurity risks and require the service provider to sign a data security agreement. PPA suggests that the parties look to ISO 27001 in detailing applicable data security requirements in this agreement. The Ministry of Finance Circular 2016-9-14, addressing the management of cybersecurity risks in insurance companies and pension funds, expressly requires the CEO of such financial institutions to consider the adoption of ISO 27001 standards.

Section 20 of the Information Security Regulations provides that the Registrar has discretion to accept compliance with specified international standards as satisfaction of the regulatory data security requirements.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The Privacy Law requires data owners to appoint a 'data manager', which is defined as either the 'active manager' of the legal entity possessing the data or an individual authorised by such person for purposes of managing the data. The Privacy Law and section 19 of the Information Security Regulations provide that the data manager (together with the owner and holder of the data) is responsible for appropriate data security.

Certain sector-specific regulations impose more detailed obligations on personnel and directors. Bank of Israel Directives 357 and 361, for example, require directors of banking corporations to regularly consider information governance matters, receive regular reports on cyberthreats, and organise annual meetings concerning cybersecurity risks. The board of directors must also approve the institution's cybersecurity policies. In certain circumstances, the directors and officers of a banking corporation can bear liability for the failure to satisfy the requirements of the Directives.

The Ministry of Finance Circular 2016-9-14, which addresses cybersecurity risks in insurance companies and pension funds, details the obligations of such institutions' directors and officers to consider and address cybersecurity issues. The Circular, for example, requires directors to appoint an information security officer and a cybersecurity committee, and to consider cybersecurity issues annually. Chief executive officers that disregard the requirements of the Circular can be subject to personal liability under the Supervision of Financial Services Law 1981.

5 How does your jurisdiction define cybersecurity and cybercrime?

The terms cybersecurity and cyberspace are used in Government Resolution 3611 to delineate the authority and responsibilities of the NCB. The Resolution defines cybersecurity as 'policies, defence mechanisms, operations, guidelines, risk management and technological means for the protection of cyberspace', where cyberspace is defined as 'both the physical and intangible arenas, composed of computer systems, computing and communication networks, digital information, content transmitted by computers and communications and control data, and the users of all of the foregoing'. The government has expressed its intention to enact legislation that more clearly demarcates the respective spheres of authority of the NCB (responsible for data security) and PPA (responsible for data privacy), but such legislation has yet to be brought before the Knesset.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The Privacy Law imposes general obligations on data controllers concerning information security. These include general mandates to ensure the integrity of the data and protect it from unauthorised use or copying. The recently approved Information Security Regulations mandate specific and detailed requirements concerning physical, administrative and technical security measures to be used in the protection of data. These include, for example, segregation of computer system elements that enable access to database information from other systems elements, mandatory use of firewalls, antivirus or malware programs where appropriate, and mandatory encryption of database information transmitted over public networks. The Information Security Regulations also require data owners to perform an annual data minimisation assessment.

Other regulatory bodies have imposed additional minimum protective measures for specific sectors. For example, Bank of Israel Directive 361 (applicable to banking corporations) requires applicable entities to perform vulnerability assessments and penetration testing to assess their exposure to cyberthreats. Banking corporations must institute a range of proactive cyber defences including, for example, technologies for detection and analysis of network anomalies and unusual transactions, and deceptive techniques (such as honeypots) to set back any cyberattack. Banks must minimise the attack surface by minimising user access permissions.

Ministry of Finance Circular 2016-9-14 (applicable to insurance companies and pension funds) imposes specific and detailed cybersecurity requirements, including, for example, requiring all regulated institutions to impose user access, user identification and password policies, and to audit user access permissions regularly. Internal networks must be appropriately separated from the internet, and all data transmitted externally must be encrypted.

Circular 18/2012 identifies a number of cyberthreats particular to healthcare institutions, such as denial of service attacks that would impede the provision of healthcare services and the theft or unauthorised modification of medical data. As such, the Circular details specific defences that must be employed by healthcare institutions, such as monitoring and minimising user access permissions and encrypting information in transit.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Israel does not currently have any laws or regulations that specifically address cyberthreats to intellectual property. The Computers Law, however, does impose aggravated penalties for the use of digital means to commit criminal acts. Such aggravated penalties could in certain circumstances apply, for example, to the unauthorised access of a network to misappropriate trade secrets or other intellectual property.

The Unfair Trade Practices Law 1999, in defining what constitutes a trade secret, provides that the owner of the proprietary information 'takes reasonable measures to protect the confidentiality' of such information. In 2012, the Tel Aviv District Court in 2117/07 *Gamida MedEquip Ltd v Fisher Scientific Company LLC* held that the use of reasonable data security measures are sufficient to show that information should constitute a trade secret, even if such measures in practice proved to be inadequate in protecting the information. The decision raises the possibility that information that is not protected by reasonable data security measures may not be protected as a trade secret under Israeli law.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The Security in Public Bodies Law authorises the issuance of binding directives concerning cybersecurity matters to certain listed entities operating critical infrastructure. The regulatory authority authorised to issue such directives is either the Israeli Security Agency or the NCB, depending on the specific entity. Listed entities include the Israel Electric Corporation, the national railway company, airports and certain telecommunications providers.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Israel does not have any laws or regulations that specifically restrict the sharing of cyberthreat information. The gathering of cyberthreat information without the consent of network users could potentially violate both the Wiretap Law and the Privacy Law. To the extent that such cyberthreat information contains personal information, the unauthorised sharing of such personal information could also potentially violate the Privacy Law.

Bank of Israel Directive 361 requires banking corporations to share cyberthreat information that can assist other banks in handling cyberthreats. The collection and sharing of such information, however, is subject to the requirements of applicable law.

Section 8(4) of the Wiretap Law provides that licensed telecommunications providers (generally, telecommunications and cable companies and internet service providers) may conduct surveillance for the purpose of 'providing services or determining the proper operation of a line'. The statutory language could be interpreted as permitting surveillance to the extent necessary to protect telecommunications networks, but does not address the sharing of such data.

In 2017, the Israeli Antitrust Authority released a draft opinion paper, which generally opined that the sharing of information concerning cyberthreats should not constitute a 'restrictive trade practice' so long as the shared information does not touch on the commercial activities of the parties or contain information that would be sensitive from the perspective of competition law.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The Computers Law generally imposes criminal liability for the unauthorised use or access of devices or networks, and also prohibits the development, distribution or use of malware. The Wiretap Law provides that unauthorised electronic surveillance, or the unauthorised use of electronic surveillance devices, can constitute a criminal offence. Violations of the Privacy Law, including the unauthorised sharing of personal data or the failure to appoint a security officer when required, can also constitute criminal offences.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The Information Security Regulations set forth generally applicable data security requirements with respect to the outsourcing of data processing activities. Entities intending to engage cloud service providers must consider possible security risks in structuring the engagement. The Regulations further require the imposition of a contract with a service provider that specifies the scope of the service provider's access and processing activities, how the service provider will ensure that applicable data security requirements are satisfied and provide for notification to the data owner in the event of a security incident. The service provider must provide the data owner with an annual report detailing the service provider's compliance with its legal and contractual obligations.

In addition, the Data Transfer Regulations provide that data can only be transferred to jurisdictions outside of Israel if, among other conditions, local law mandates the use of appropriate measures for the security of such data.

Aside from these generally applicable requirements, certain sectors are subject to more specific requirements concerning the use of cloud service providers. Banking corporations, for example, are required to obtain the consent of the Supervisor of the Banks pursuant to Circular 357 prior to outsourcing certain services, including the storage of customer data on systems that are not under the corporation's sole control. Healthcare institutions subject to Circular 18/2012 are prohibited from using external service providers except to the extent necessary to provide services, and are only permitted to engage service providers that comply with ISO 27799. Insurance companies and pension funds subject to Ministry of Finance Circular 2016-9-14 must consider cybersecurity risks prior to engaging a cloud service provider, limit data access to specified IP address and ensure that sensitive data transferred abroad be encrypted both in transit and storage.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Foreign organisations doing business in Israel are obligated to comply with the same laws and regulations that apply to Israeli organisations.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As detailed above, certain regulations provide that data controllers should consider compliance with the ISO 27001 standards.

14 How does the government incentivise organisations to improve their cybersecurity?

Israel does not currently provide grants or tax credits for the improvement of an organisation's cybersecurity. At the same time, Israel makes available a range of grant opportunities for research and entrepreneurship in the cybersecurity arena.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

As mentioned above, Government Resolution 2443 generally provides that Israel's national cybersecurity strategy should be based on international standards. Government offices are required to be in compliance with ISO 27001 and government procurement standards are required to ensure that all purchased equipment and services also satisfies that standard.

The Israeli Privacy Protection Council has also published a set of non-binding guidelines to assist data holder in implementing the data security requirements of the Privacy Law. The Privacy Protection Council is a statutory body that advises the Ministry of Justice and the Registrar on matters of data privacy and data security.

16 Are there generally recommended best practices and procedures for responding to breaches?

Israeli law and regulations do not currently provide for generally applicable recommendations in responding to breaches. The Information Security Regulations, however, require that the Registrar be 'immediately' notified of certain specified 'serious security incidents'. The Registrar may require that the data subjects be notified of the incident.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The NCB has set up CERT-IL, which is a civilian centre for addressing and coordinating responses to cyber events. CERT-IL collects cyberthreat information from a variety of sources, including private entities that have volunteered to share information. Prior to collecting cyberthreat information from a private source, CERT-IL's policy is to confirm that such entity is aware of CERT-IL's own policies for the categorisation and sharing of such information. Moreover, to the extent the private entity may share personal data with CERT-IL, the entity is required to disclose such practices to its employees and customers.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In 2012, the NCB commenced a multi-stakeholder process aimed towards developing comprehensive cybersecurity regulations for the Israeli economy. The consultation process involves representatives from academia, the government and industry. The NCB is currently continuing the process and expects to present recommendations and legislative recommendations in the near future.

The NCB has also partnered with academic institutions to establish cybersecurity research centres at Ben Gurion and Tel Aviv Universities. The centre at Tel Aviv University in particular includes engineers and scientists as well as researchers from the fields of law, management and social studies, and aims to impact cybersecurity policy decisions.

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Insurance against damage from cybersecurity breaches is available in Israel. It is common for medium or large companies to obtain such cybersecurity insurance, often in response to customer demands.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Registrar (now part of the PPA) has, historically, enforced compliance with the data security requirements of the Privacy Law. With the recent establishment of the NCDA, however, Israel has two agencies that regulate potentially overlapping aspects of data security. In principle, government resolutions have outlined a framework where NCDA focuses on cybersecurity matters and PPA focuses on data privacy matters, including compliance with and enforcement of the Privacy Law. However, legislation implementing this framework, and clearly demarcating the regulatory authority of each agency, has yet to be brought to the Knesset.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Privacy Law requires that a database be registered with the Registrar (now part of the PPA) before the data can be used. The Registrar has, in certain circumstances, delayed the registration of a database until the data holder has shown that it employs adequate cybersecurity measures. In addition, under the Privacy Law, the Registrar may, in its enforcement capacity, question individuals and demand documents, and may enter and search non-residential premises and seize personal property. Court orders are required to enter and search a private residence. Criminal indictments for violation of the Privacy Law are currently brought by the criminal enforcement authorities.

The Supervisor of the Banks at the Bank of Israel has broad investigatory authority to determine whether any banking corporation is in compliance with the Directives concerning cybersecurity.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

To date, no criminal or civil decisions concerning inadequate data security have been issued by Israeli courts. In contrast, administrative agencies have been active in the enforcement of data security requirements. The PPA Internet site currently indicates that in 2017 the PPA brought approximately 15 enforcement actions concerning inadequate data security.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The Registrar may impose administrative fines for violations of the Privacy Law, including the provisions of the law concerning data security. The Registrar is also authorised to suspend or terminate the registration of a database for violations of the law, which has the practical effect of legally precluding the use of such data. Failure to appoint a security offer where required by the Privacy Law is a criminal offence punishable by one year's imprisonment.

The Supervisor of the Banks at the Bank of Israel may impose a fine of 1 million shekels on any banking corporation that does not comply with the Directives concerning cybersecurity.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Currently, Israel does not provide for any generally applicable breach notification requirements. In past enforcement actions, however, the Registrar has required companies to disclose data breaches. Failure to satisfy this requirement could in certain circumstances result in the termination of the registration of the applicable database, which would legally preclude use of the applicable data.

The Supervisor of the Banks at the Bank of Israel may impose a fine of 1 million shekels on any banking corporation that does not comply with the breach notification requirements of the Directives.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Under the Privacy Law, the failure to provide adequate data security as required by the statute or regulations is actionable as a civil tort. To date, no civil actions asserting inadequate data security have been brought to the courts, so little jurisprudence exists examining how courts would evaluate the harm resulting from the use of inadequate data security. Courts have yet to authorise a class actions suit asserting a failure to use adequate data security, though courts have authorised class action suits for other violations of the Privacy Law.

The Computers Law provides that unauthorised cyberactivity, such as the distribution of malware or the unauthorised access to or disruption of computing devices, is also actionable as a civil tort.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

See question 6.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

The Information Security Regulations require data owners to retain records of incidents that 'raise a suspicion' that the integrity of the data has been compromised or that there has been unauthorised access to the data. Such records must be retained for 24 months.

Bank of Israel Directive 361 requires banking corporations to record cyber events and document in real-time decisions and actions taken in response to such events. The Directive does not specify a minimum period of time that such records must be retained.

YIGAL ARNON & CO.
LAW FIRM

Eli Greenbaum **elig@arnon.co.il**

22 Rivlin St
Jerusalem
Israel

Tel: +972 2 623 9200
Fax: +972 2 623 9236
www.arnon.co.il

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

The Information Security Regulations require that the Registrar be 'immediately' notified of certain specified 'serious security incidents'. The Registrar has the discretion to require that the data subjects be notified of the incident. In addition, certain sectors may be subject to additional reporting requirements. Banking corporations, for example, are required under Directive 361 to report cyber events and cyberthreats to the Supervisor of the Banks.

29 What is the timeline for reporting to the authorities?

As detailed above, the Information Security Regulations require the 'immediate' notification of certain specified 'serious security incidents'.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Pursuant to the Information Security Regulation, the Registrar may require that data subjects be notified of a 'serious data breach'.

In addition, Companies publicly traded on the Tel Aviv Stock Exchange (TASE) are required to report certain breach events to the TASE. Significant data breaches or cybersecurity threats would need to be included in the company's public filings.

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