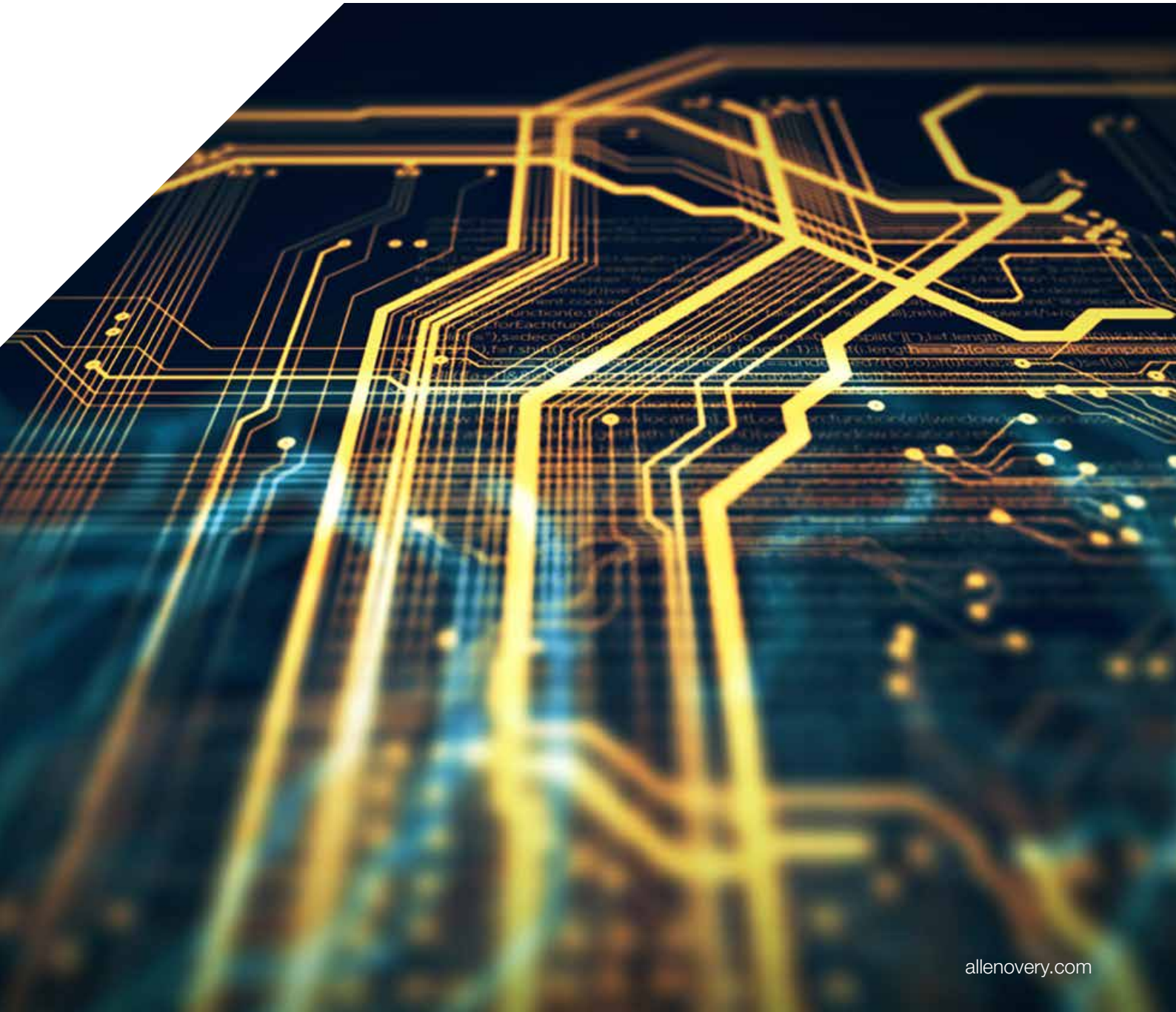
ALLEN & OVERY

Cybersecurity

2021

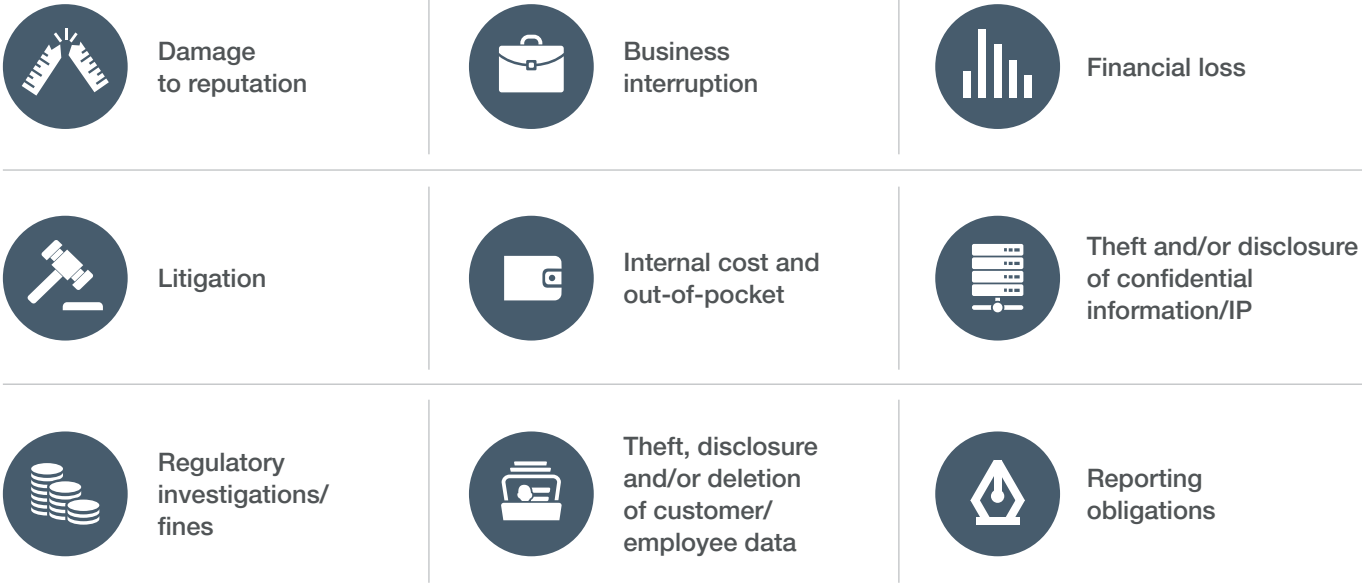


allenovery.com

Our cybersecurity practice

Computers, the internet, mobile devices and electronic transactions all play an important and ever-increasing role within the corporate environment, particularly for businesses with a strong online presence or with high volumes of customer data or other electronically stored information.

But the continued growth of "cyber" technologies and the growing phenomenon of cyber-attacks pose significant business risks. Cyber attackers are often quick to spot the potential vulnerabilities of new technologies and to exploit them (and to frustrate detection of those activities). Businesses need to have in mind the range of possible consequences of a cyber-attack.



All of these consequences can result in cost or financial loss. In a worst case scenario a cyber-attack could be catastrophic, putting a company out of business. The value of data has increased as the volume of data that is available and capable of being collected, processed and retained by organisations has exploded. The more data companies have access to, the better they get to know the market and their customers and the more value they can extract from it. In common with other valuable "assets", data is therefore subject to heightened risk of misuse, alteration, theft or loss.

Cybersecurity is about prevention of (and/or preparation for) cyber-attacks, but also about incident response once the risk has realised. It requires an integrated approach across traditional security disciplines proactively to understand, detect and respond to advanced and evolving threats. There is an important legal component and our integrated team of diverse practitioners reflects this requirement.

Overview of threats and trends

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	→	1. Malware	→	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	→	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	→	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	→	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	→	10. Physical manipulation/ damage/ theft/loss	→	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

This table is sourced from the European Networking and Information Security Agency publication, ENISA Threat Landscape Report 2018, published in 2019.

Trends

↓ Declining

→ Stable

↑ Increasing

Ranking

↑ Going up

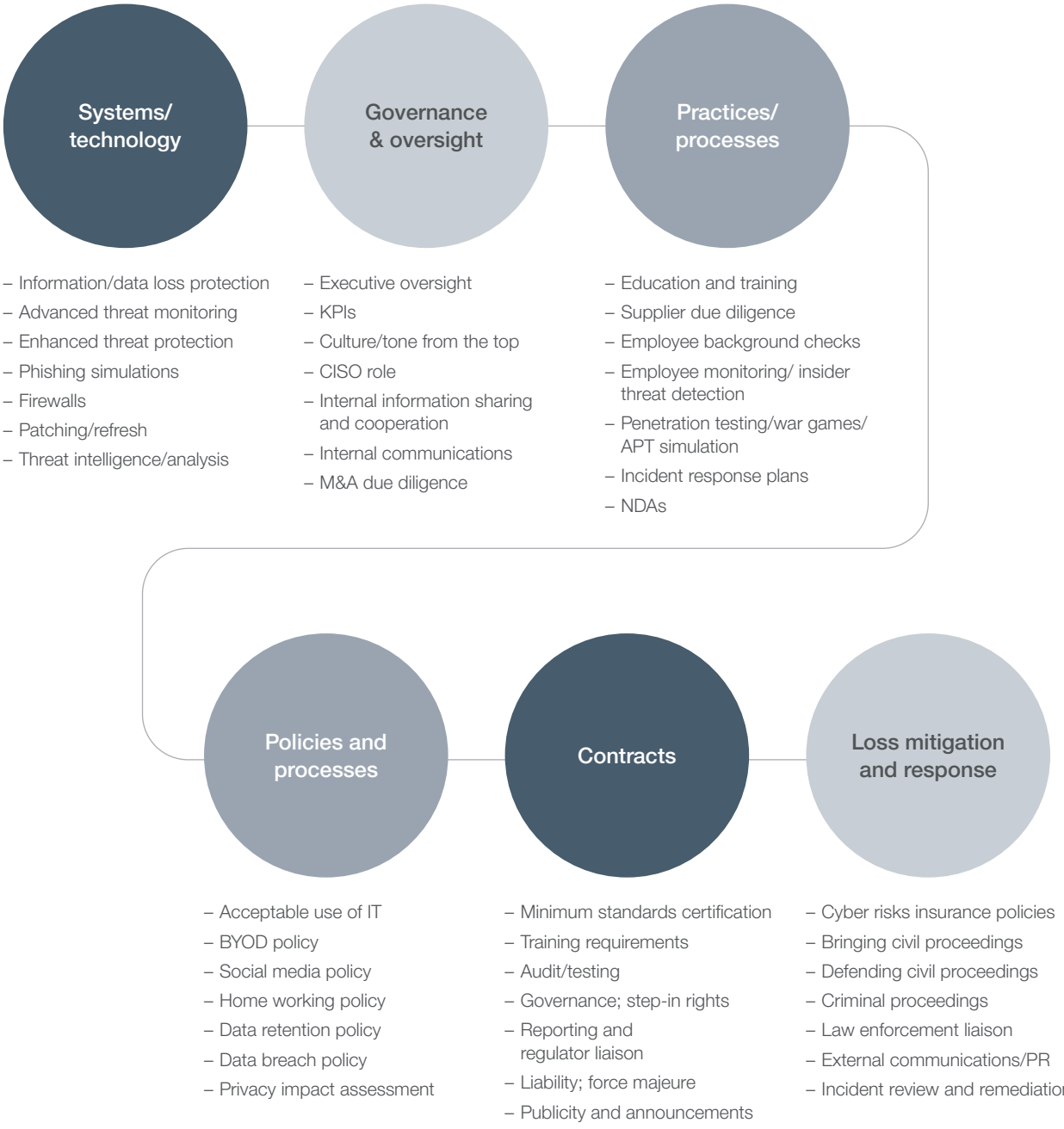
↓ Going down

→ Same

Legal risk management – a plentiful toolkit, but no magic bullets

From a business perspective, the ideal outcome would be to eliminate cybersecurity risk entirely. However, two things are clear. First, there is no panacea for the diverse and ever evolving range of threats that exists.

Second, there is no such thing as zero risk. Businesses must therefore design and implement plans that are focused on risk management and minimisation.



Our experience

A U.S.-based global bank

on developing a pro-active strategy for responding to cyber-attacks, including participation in wargames and preparation of court papers for the purpose of pursuing remedies through the courts.

A global financial services group

on an electronic denial of service attack set up by a former customer combined with threats and other offences.

A major UK retailer

on responding to a data breach perpetrated by an employee, including liaison with the ICO and other law enforcement authorities.

A leading provider of financial messaging services

on the legal aspects of the security of its global network, including provision of penetration testing by third party vendors.

A fund manager

on an assessment of its approach to cyber-risk management, including a training programme targeting all levels of the organisation.

An international bank

on the legal risks associated with taking private action against attacks on its online banking platform co-ordinated by botnets.

Toyota Motor Europe

on the review of data retention and encryption issues relating to the IT security policy code of Toyota Motor Europe.

A global bank

on assessing its risk of different modes of cyber-attacks from different actors/jurisdictions.

An online services provider

in relation to third party disclosure applications, requesting customer information for asset-tracing purposes. We successfully defended a number of these Norwich Pharmacal applications on behalf of our client.

A media organisation

on freedom of information request and related regulatory and communications issues and reputation management aspects following a widely publicised attack on its networks.

A global provider of service solutions

to the power generation industry, on data privacy issues in connection with the rollout of data loss prevent software. This advice covers 18 jurisdictions.

A major international hedge fund

in relation to the hacking and theft of highly valuable confidential information and trading strategies by a rogue employee. This was a critical case for the client and involved civil and criminal proceedings in multiple jurisdictions to ensure that the breach was controlled and the employee extradited for criminal trial.

An international bank

on cyber-attacks co-ordinated by botnets (in particular, fraudsters infecting customers' computers with trojans which hid on their computers until the customer navigated to the online banking website, and subsequently client information was captured and uploaded by malware to a "dropzone").

Several Luxembourg financial sector actors

(including banks and electronic payment services providers) on the approach to be taken in responding to a data breach affecting customer data from both a banking regulatory and data protection law perspective.

AVG Technologies

a computer security software provider, on the USD60m acquisition of Privax, a leading global provider of desktop and mobile privacy services for consumers and parent company of innovative VPN provider HideMyAss.

A life sciences company

on the implementation of various cyber-defence tools, including software tools, managed services and other solutions.

An emerging markets telecommunications firm

in investigating potential cybersecurity breach and theft of confidential information.

Key team members

Peter Eijsvoogel
Of Counsel – Amsterdam
Tel +31 20 674 1295
peter.eijsvoogel@allenovery.com

Filip Van Elsen
Partner – Antwerp
Tel +32 3 287 73 27
filip.vanelsen@allenovery.com

Peter Van Dyck
Partner – Brussels
Tel +32 2 780 2512
peter.vandyck@allenovery.com

Lawson Caisley
Partner – London
Tel +44 20 3088 2787
lawson.caisley@allenovery.com

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Philip Mansfield
Partner – London
Tel +44 20 3088 4414
philip.mansfield@allenovery.com

Nigel Parker
Partner – London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Mark Ridgway
Partner – London
Tel +44 20 3088 3720
mark.ridgway@allenovery.com

Chioma Benjamin
Counsel – London
Tel +44 20 3088 3557
chioma.benjamin@allenovery.com

Catherine Di Lorenzo
Counsel – Luxembourg
Tel +352 44 44 5 5129
catherine.dilorenzo@allenovery.com

Livio Bossotto
Counsel – Milan
Tel +39 02 2904 9678
livio.bossotto@allenovery.com

Jan Erik Windthorst
Partner – Frankfurt
Tel +49 69 2648 5583
jan-erik.windthorst@allenovery.

Alexandre Rudoni
Partner – Paris
Tel +33 1 40 06 50 34
alexandre.rudoni@allenovery.com

Ian Ong
Senior Associate – Sydney
Tel +612 9373 7832
ian.ong@allenovery.com

Laurie-Anne Ancenys
Counsel – Paris
Tel +33 1 40 06 53 42
laurie-anne.ancenys@allenovery.com

Krystyna Szczepanowska-Kozlowska
Partner – Warsaw
Tel +48 22 820 6176
krystyna.szczepanowska-kozlowska
@allenovery.com

Victor Ho
Managing Partner of A&O LLP in Beijing and Shanghai
Registered Foreign Lawyer (California) for A&O Hong Kong
Tel +86 10 6535 4381
victor.ho@allenovery.com

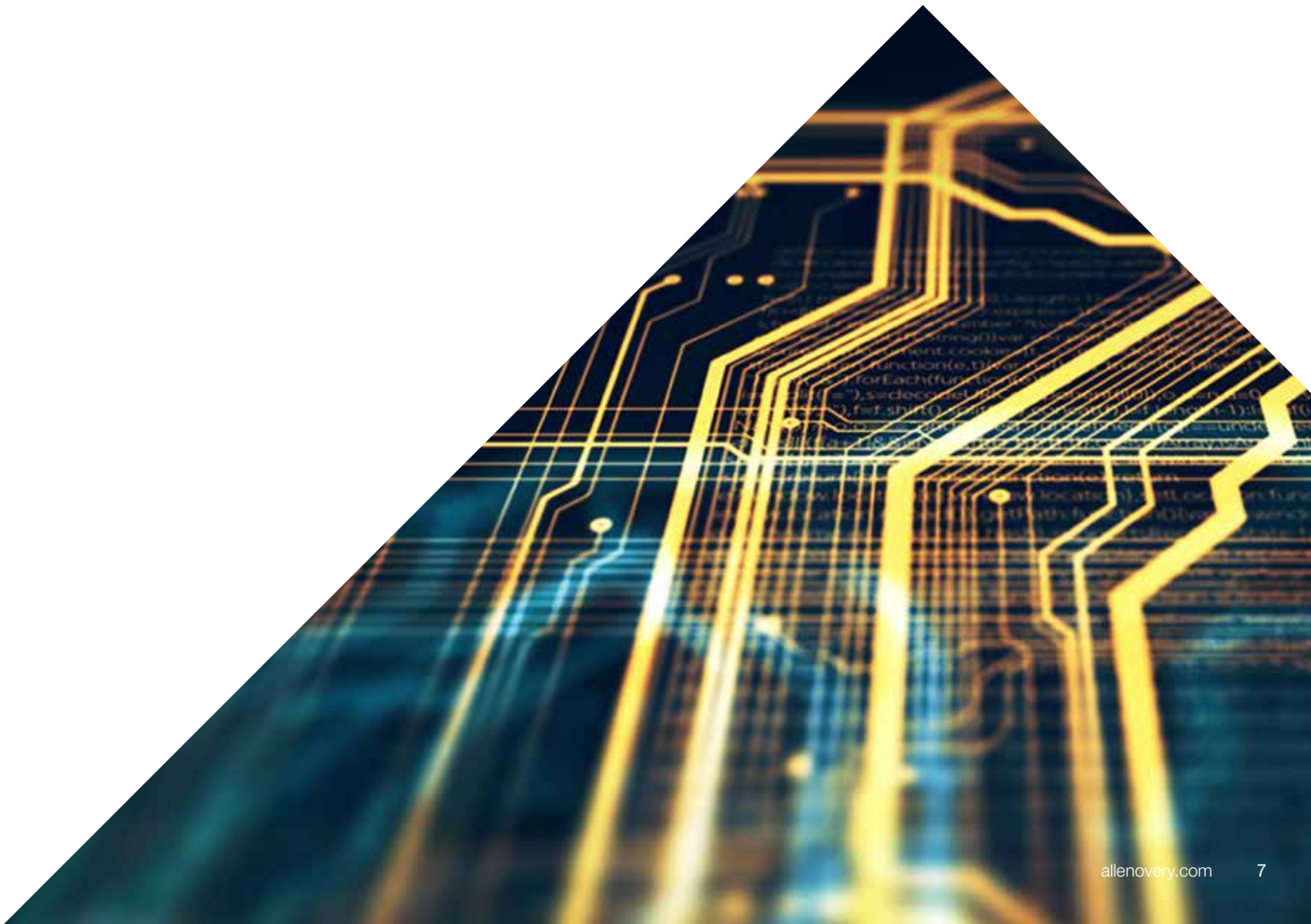
Will McAuliffe
Partner – Hong Kong
Tel +852 2974 7119
will.mcauliffe@allenovery.com

Lee Noyek
External Consultant – Tel Aviv
Tel +972 524 210 505
lee.noyek@allenovery.com

Laura Hall
Partner – New York
Tel +1 212 756 1171
laura.hall@allenovery.com

Paul Keller
Partner – New York
Tel +1 212 610 6493
paul.keller@allenovery.com

William White
Partner – Washington, D.C.
Tel +1 202 683 3876
william.white@allenovery.com



GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in over 40 offices worldwide.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term **partner** is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

UK
CS1911_CDD-57582_ADD-93627