ALLEN & OVERY

Cybersecurity – How we can support you

Managing cybersecurity risk is a priority to all

Businesses today face an ever-growing threat from cyberattacks and data breaches. Their impacts are always significant, with financial losses, business interruptions, reputational damage and regulatory sanctions the potential results.

Addressing the risk of cybersecurity incidents is a priority for every organisation. In the interconnected economy, your company, your supply chain and your customers can all experience a cyberattack or breach. You need a robust approach to cybersecurity that mitigates risk and prepares you to respond.

> "Cyber threats are constantly evolving and have been growing in number, posing a risk to the EU's financial stability."

Public Statement from the Joint Committee of the European Supervisory Authorities, January 2022

Facts

Ethical hackers were able to discover over **65,000** vulnerabilities in 2022 alone, up by **21%** over 2021. Source: HackerOne 2022 Security report

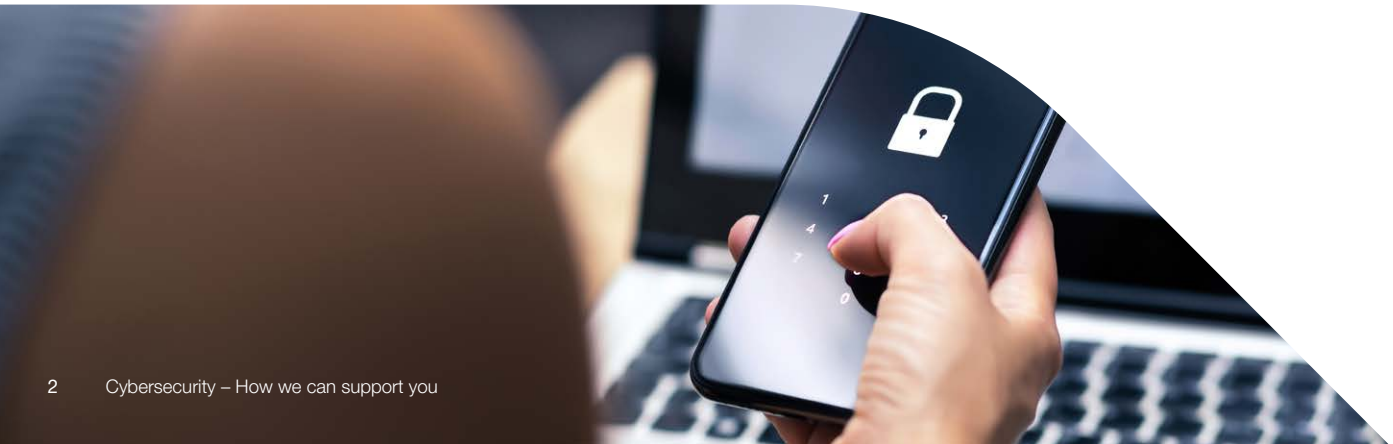
The cost of cybercrime is predicted to hit **USD8 trillion** in 2023 and will grow to **USD10tn** by 2025. Source: Cybercrime report 2022 by eSentire

Over **USD20 billion** of estimated damage and ransoms paid in 2021

"The average cost of a data breach is **USD4.24 million**." – IBM Report 2021

Over **620m** cyberattacks globally in 2021, three times the number in 2019 – SonicWall

1,243 businesses reported cyber(security) incidents in 2021



How we can add value

Helping to identify and manage existing and emerging cyber threats

A holistic approach

Managing cyber risk starts with making sure you have appropriate protective measures in place across your organisation. You should also have a cyber incident response policy and plan ready to activate.

We are the trusted adviser to support you with cybersecurity preparation and impact mitigation. Our integrated team of legal experts and experienced cybersecurity consultants can help you build your operational resilience and incident readiness.

Proven crisis management expertise

We understand you want clear guidance, pragmatic support and an experienced guide and central point of contact to help navigate any crisis.

Our track record is exemplary. We have successfully supported clients in resolving security incidents across the globe. We are present for our clients in other crisis situations, helping to manage regulatory investigations, fraud and white-collar crime. Our strategic and commercial support is recognised worldwide. Our ability to take immediate action and provide clear recommendations makes us the partner of choice.

Global reach and local depth

Security incidents are by nature cross-border, but their resolution is still driven locally. At A&O, we can cater for and offer national and multinational solutions and support. We have a strong network of cyber specialists and experts in directly relevant legal areas such as:

– data privacy

– investigations and litigation

– corporate governance, directors liability, disclosure

– employment

– (cyber) insurance

– financial

– regulatory

– IT

This allows us to help prevent and effectively respond to any cyber incident.

Seamless and integrated incident support

A successful response to a security incident requires rapid and seamless legal advice. Your advisor needs to be flexible and coordinate with external experts – such as IT security specialists, forensic consultants and private investigators – when needed.

We act as a critical facilitator for our clients in times of crisis. We provide core legal support and can link in third parties from the extensive network we have built while working to resolve security incidents and investigations over many years.

With just one call, you will receive all the support you need – quickly and reliably.

How we can assist you

Your strategic, trusted advisor across all areas of cyber risk management and mitigation.

Step 1

Build digital operational resilience

Discover and address any vulnerabilities, take measures to implement to mitigate cyber risks and related reputational threats, engage the right experts to support you.

To help you, we take a holistic approach:

– Design and implement governance structures to protect and limit your liability and that of your directors from direct and third party risk

– Map your notification duties globally in case of cyber incidents and data breaches

– Advise on the right strategies and put in place the right policies

– Carry out a periodic and privileged Cyber Risk Health Check on your company and its supply chain

– Review and negotiate contracts with cyber-insurers and third party forensic, call centre, PR and IT providers

Step 2

Develop your cyber readiness

Partner with you to develop an incident response plan that:

– Assigns clear responsibilities and actions to all stakeholders involved

– Defines escalation channels, including a first response team

– Puts in place the right monitoring tools, working closely with a forensic consultant

To help you, we have developed a cyber response toolkit which includes:

– A Draft First Response Plan - including template incident logs and incident question lists in line with notification duties and regulators' expectations

– Incident breach preparation and response – including a cyber war-game simulation

– Cyber risk awareness training

– Board and senior leadership preparation including a review of your cyber risk management and reporting structures

Step 3
Effective incident response

Using the strength of our network, extensive cyber and crisis management expertise, we act as your trusted adviser and central contact that provides you with dedicated access to all relevant disciplines at once.

In high-profile critical incidents we to provide:

– Rapid response hands-on crisis management expertise under legal privilege

– A thorough assessment of contractual and third party responsibilities and liabilities

– Analysis of the impact on employees, clients and customers

– Strategic advice on the steps to take to de-stress, contain cyber incidents and secure business continuity

– Effective remediation of cyber incidents including obtaining injunctive relief in case of data posting on the dark web, and liaising with law enforcement

– A communication hotline for your incident response team, answering internal, external and ad hoc questions

– One legal partner that can handle all notification duties, interaction with the supervisory authorities, and liaison and coordination of third party experts

Step 4
Incident impact mitigation

Mitigate the aftermath of a cyber-incident - avoiding liability pitfalls, limiting the risk and impact of any follow-on actions and evaluating the incident to identify lessons learnt to help you develop and grow your cyber readiness.

Using our extensive experience we can:

– Stop the flow of funds in cases where transfers happened during the cyber incident

– Take legal action against the cyber attacker or liable third parties

– Defend against private enforcement, such as class actions by consumers and third party claims

– Respond to investigations and enforcement actions by regulators

– Advise and assist with disciplinary actions against employees

– Recap and review the incident under privilege to identify areas for improvement in your operational resilience or response

Cyber Risk Health Check

Businesses today face an ever-growing threat of cyber-attacks. Having a comprehensive understanding of your cyber risk exposure is essential to operating successfully in today's environment. There can be a huge cost for companies who get this wrong.

Our combined team of consulting and legal specialists will help you understand your cyber risk profile.

Our Cyber Risk Health Check can help you identify and manage the emerging threats posed to your business. We measure your firm's maturity, advise on regulatory requirements and help you understand your full cyber risk profile.

This takes into account national and international standards, frameworks, regulatory guidance and best practice, including NCSC, ISO and NIST.

Our cyber risk review – based on interviews, assessments and surveys – spans key areas of:

- **Regulatory compliance**
- **Industry best practice**
- **Effectiveness of existing cyber framework**
- **Cyber risk alignment to enterprise risk management and overall strategy**
- **Cyber risk culture**

Based on our review, our report provides you with an assessment and practical recommendations for enhancements across six verticals:

1. **Cyber Culture and Awareness:** An assessment of the current cyber risk culture within your organisation and how embedded culture is in the current cyber risk framework
2. **Cyber Risk Governance:** Our review and recommendations of your cyber documentation, board oversight, and the overall cyber governance structure
3. **Cyber Risk Management:** A review of Cyber Risk identification, risk assessments, reporting and MI, and the Cyber Risk control environment
4. **Cyber Resiliency:** A review of incident breach preparation and response documentation, and assessment of existing operational resilience measures (eg incident and threat detection and monitoring)
5. **Third-Party Risk Management (TPRM):** A review of third-party cyber risk assessments and the TPRM governance structure, and assessment of cyber risk due diligence conducted
6. **Data Compliance:** A review of Personal Data Governance, and an assessment of the risk and control framework (eg GDPR).

Significant cases we supported our clients on over the past years

01. An **online gaming company** on the response to a distributed denial-of-service or 'DDoS' attack. Indicative of a recent trend in cyber crime, the incident started with a demonstration attack involving a significant ransom demand. Following the gathering of swift threat intelligence and immediate mitigation measures, we succeeded in containing the incident and avoiding further harm.
02. **A media company** on its response to a high-profile ransomware attack caused by the DoppelPaymer malware. This malware encrypts files and prevents victims from accessing these encrypted files. A significant ransom is demanded to regain access to the encrypted files or the 'stolen' files are gradually posted on the dark web.
03. **A terminal operator** on its response to a major ransomware attack that significantly impacted port operations by disrupting automatic terminal management systems in multiple European companies.
04. **A large service provider** in connection with a ransomware attack that affected all its IT systems. We assisted with restoring its systems, understanding how the attack happened, what remediation actions need to be taken, preparing for data potentially being leaked and liaising with the relevant authorities and police globally.
05. **A fund manager** in relation to a blackmail attempt by a malicious party who hacked into the company's systems and threatened to publish confidential customer data unless a ransom was paid.
06. **A financial services provider** on a cyber security incident at a Central-American financial institution, a multi-million dollar cyber-attack involving Europe and Asia and several cyber frauds, including an attempted cyber heist.
07. **A leading international hotel group** on numerous cybersecurity incidents in China, including reporting and mitigations steps.
08. **A major international hedge fund** in relation to the hacking and theft of highly valuable confidential information and trading strategies by a rogue employee who fled to Hong Kong.
09. **A listed fashion company** in connection with a cybercrime incident and related payments of several hundred thousand euro to an account in Hong Kong. We were able to stop a significant portion of the erroneous payments and help our client recover the stopped amounts via a court in Hong Kong.
10. **A large shipping company** in connection with a cybercrime incident and the related payment of ~USD 2 million.
11. **A major financial institution** in relation to an electronic denial-of-service attack set up by a former customer combined with threats and other offences. The customer applied software which blocked the email boxes and telephone lines of the customer services department and the legal department by sending thousands of emails and placing as many automatic telephone calls.
12. **A global wholesale bank** on designing and developing a war-game scenario including a large-scale cyber-attack event to stress test Board and executive preparedness for crisis management.
13. **A media organisation** on regulatory and communications issues and reputation management following a widely publisheded attack on its networks.
14. **A lifesciences company** on the implementation of various cyber-defence tools, including software tools, managed services and other solutions.

The team that would support you globally

Seamless integration across our global network through our combined team of legal specialists and consultants in 30 countries.

Europe

UK

Susanna Charlwood
Partner
Tel +44 20 3088 2645
Mob +44 7834 801 142
susanna.charlwood@allenovery.com

Nigel Parker
Partner
Tel +44 20 3088 3136
Mob +44 7717 341 948
nigel.parker@allenovery.com

Jane Finlayson-Brown
Partner
Tel +44 20 3088 3384
Mob +44 7767 674 407
jane.finlayson-brown@allenovery.com

Luxembourg

Catherine Di Lorenzo
Partner
Tel +352 44 44 5 5129
Mob +352 621 372 410
catherine.dilorenzo@allenovery.com

France

Hippolyte Marquetty
Partner
Tel +33 1 40 06 53 98
Mob +33 6 20 10 39 73
hippolyte.marquetty@allenovery.com

Laurie-Anne Ancenys
Counsel
Tel +33 1 40 06 53 42
Mob +33 7 62 27 40 21
laurie-anne.ancenys@allenovery.com

Belgium

Filip Van Elsen
Partner
Tel +32 3 287 73 27
Mob +32 495 59 14 63
filip.vanelsen@allenovery.com

Thomas Declerck
Senior Associate
Tel +32 2 780 2483
Mob +32 473 57 30 34
thomas.declerck@allenovery.com

Germany

Tim Mueller
Partner
Tel +49 69 2648 5996
Mob +49 151 1976 3347
tim.mueller@allenovery.com

David Schmid
Counsel
Tel +49 69 2648 5774
Mob +49 172 683 8714
david.schmid@allenovery.com

Catharina Glugla
Senior Associate
Tel +49 211 2806 7103
Mob +49 172 686 5914
catharina.glugla@allenovery.com

Italy

Livio Bossotto
Partner
Tel +39 02 2904 9678
Mob +39 333 874 5762
livio.bossotto@allenovery.com

Netherlands

Hendrik Jan Biemond
Partner
Tel +31 20 674 1465
Mob +31 653 380 164
hendrikjan.biemond@allenovery.com

Nicole Wolters Ruckert
Counsel
Tel +31 20 674 1401
Mob +31 646 033 725
nicole.woltersruckert@allenovery.com

Eastern Europe

Krystyna Szczepanowska-Kozlowska
Partner
Tel +48 22 820 6176
Mob +48 609 779 272
krystyna.szczepanowska@allenovery.com

Justyna Ostrowska
Counsel
Tel +48 22 820 6172
Mob +48 694 442 071
justyna.ostrowska@allenovery.com

Europe – A&O Consulting

Tom Lodder
Managing Director
Tel +44 20 3088 2061
tom.lodder@allenovery.com

Tom Balogh
Executive Director
Tel +44 20 3088 2595
tom.balogh@allenovery.com

Middle East

Israel

Lee Noyek
External Consultant
Tel +44 20 3088 4437
Mob +44 7825 384 798
lee.noyek@allenovery.com

UAE

Tom Butcher
Partner
Tel +971 2 418 0414
Mob +971 50 189 4485
tom.butcher@allenovery.com

Yacine Francis
Partner
Tel +971 4 426 7228
Mob +971 56 656 3244
yacine.francis@allenovery.com

China

Fai Hung Cheung
Partner
Tel +852 2974 7207
Mob +852 9029 4911
fai.hung.cheung@allenovery.com

Melody Wang
Partner
Tel +86 21 2067 6988
Mob +86 139 1098 1678
melody.wang@allenoveryly.com

APAC

Hong Kong

Matt Bower
Partner
Tel +852 2974 7131
Mob +852 9664 1223
matt.bower@allenovery.com

Singapore

Cédric Lindenmann
Senior Associate
Tel +65 6671 6035
Mob +65 9754 9035
cedric.lindenmann@allenovery.com

APAC – A&O Consulting

Lee Alam
Managing Director
Tel +612 9373 7722
lee.alam@allenovery.com

U.S.

New York

Julian Moore
Partner
Tel +1 212 610 6309
Mob +1 347 758 0379
julian.moore@allenovery.com

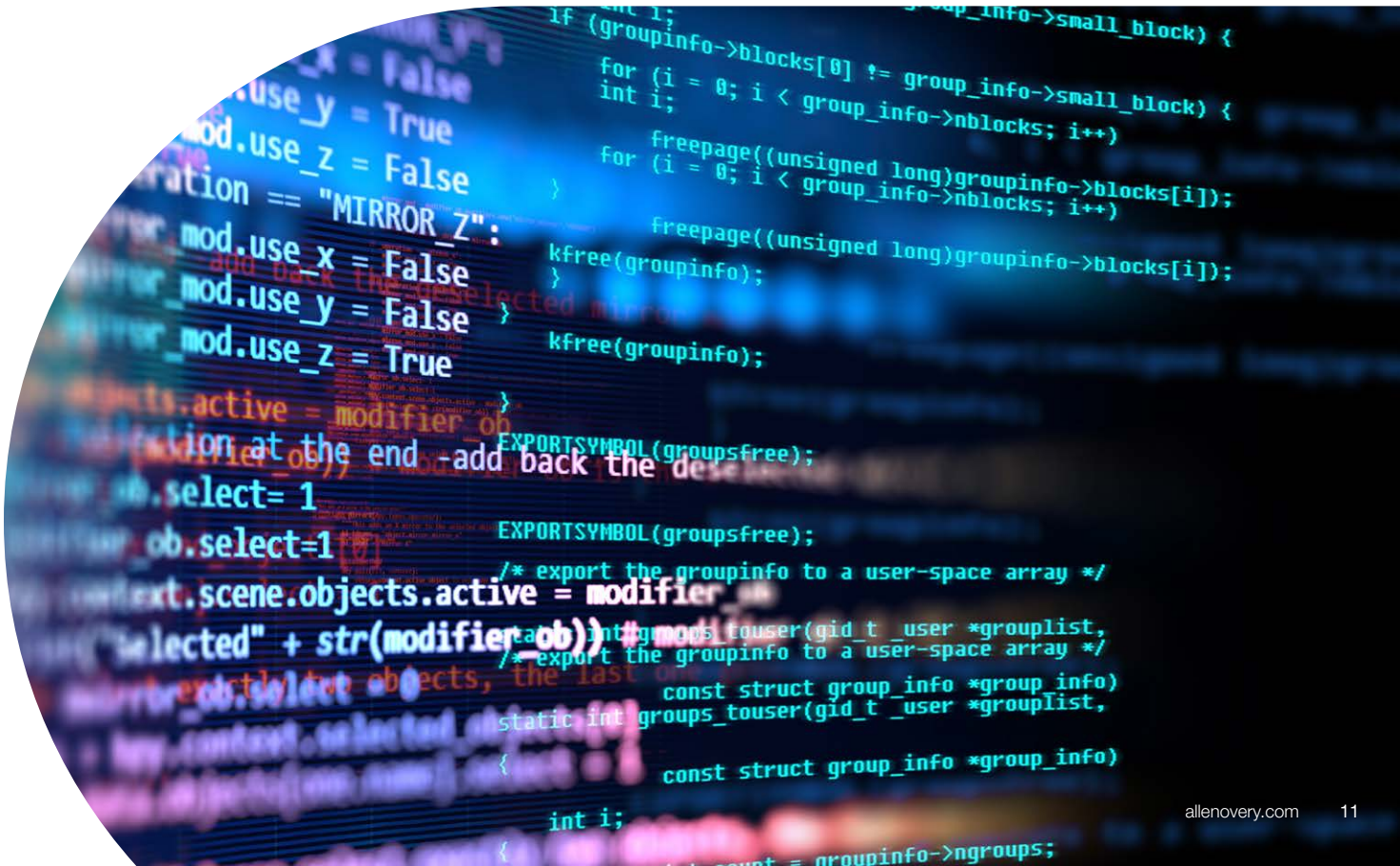
Adam Chernichaw
Partner
Tel +1 212 610 6466
adam.chernichaw@allenovery.com

Washington, D.C

Claire Rajan
Partner
Tel +1 202 683 3869
Mob +1 202 308 9234
claire.rajan@allenovery.com

U.S. – A&O Consulting

Catie Butt
Executive Director
Tel +1 646 344 6653
catie.butt@allenovery.com



Global presence

Allen & Overy is an international legal practice with approximately 5,600 people, including some 580 partners, working in more than 40 offices worldwide. A current list of Allen & Overy offices is available at www.allenovery.com/global_coverage.

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.

GB
CS2209_CDD-70328_ADD-105720