ALLEN & OVERY

# Cybersecurity – How we can support you

2022

allenovery.com

# Managing cybersecurity risk is a priority to all

Businesses today face an ever-growing threat from cyberattacks and subsequent data breaches. Their impact is almost always significant and can result in financial losses, loss of key data, business interruptions, reputation damage and regulatory sanctions and enforcement.

Taking proactive action to address the risk of (cyber)security incidents is a key priority for any business as there is a myriad of ways you can be affected. In the current interconnected economy your company as well as your supply chain and customers can experience a cyberattack or data breach. A robust (cyber) security approach is required to properly mitigate risk and be prepared.

**Facts**

Over **USD20bn** of estimated damage and ransoms paid in 2021

"Data breach costs rose to **USD4.24 million**." Cost of a Data Breach Report 2021, IBM

Over **620m** cyberattacks globally in 2021, double of 2020 and more than triple of 2019 (source: SonicWall).

**1,243** reported security incidents in 2021

"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

# How we can add value

Help you to identify and manage existing and emerging threats to your business

### A holistic approach

Managing the risk of a cyber incident starts with making sure your organisation has adopted the appropriate protective measures and agreed on approach to effectively respond to cyber incidents.

You need an adviser that can support you from cybersecurity preparation to response and impact mitigation. We offer an integrated team of legal experts and experienced cybersecurity consultants that can help you to build your operational cyber resilience and incident readiness as well as be your trusted adviser when faced with a security incident.

### Proven crisis management expertise

We understand you want clear guidance, pragmatic support and – if an incident happened – one central partner on your side to navigate through the crisis with you.

Our track record is exemplary in this regard and includes supporting our clients in a slew of security incidents globally as well as in other crisis situations (for example: regulatory investigations and fraud and white-collar crime cases).

We are recognised for our strategic and commercial support and for daring to take a stand and provide clear recommendations.

### 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 both through our strong network of cyber experts globally and access to experts in all legal areas that are key to prevent and effectively respond to an incident such as:

– data privacy

– investigations and litigation

– corporate (governance, directors liability, disclosure),

– employment,

– (cyber) insurance, (financial)

– regulatory

– IT.

### Seamless and integrated incident support

A successful response to a security incident requires a legal adviser that responds rapidly, and seamlessly coordinate with and/or involve external experts (IT security experts, forensic consultants, private investigators, etc.) when you need them.

We act as a central contact, supporting our clients in times of crisis. All support can be sourced internally or we can link in third parties through the network we built working on security incidents and investigations for many years. With just one call to us, you will receive all the support you need – quickly and reliably.

# How we can assist you

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

## Step 1

Build digital operational resilience

Ensure you discover and address any vulnerabilities, know what measures to implement to mitigate any cyber risks and related reputational risks and engage the right (external) experts to support you.

**How we can support you**:

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

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

– Strategize and advise you on how to structure and put in place the right policies

– Carry out a (periodic) and privileged Cyber Risk Health Check (see page X) on your company  supply chain or in case of M&A

– Review and negotiate contracts with Cyber-insurers and 3rd party providers (e.g. forensic, call centre, PR, IT)

## Step 2

Develop your cyber readiness

Partner with you and allow you to effectively respond to a cyber incident by developing 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**:

– Draft First Response Plan and Template incident log and incident question list in line with the notification duties and the regulators preferred way of working

– Incident breach preparation and response (incl. a cyber war game simulation)

– Cyber (risk) awareness training

– Board and senior leadership preparation incl. a review of your cyber risk management information and reporting

## Step 3

Build digital operational resilience

Be your trusted advisor on cyber incidents and use the strength of our network and extensive cyber and crisis management expertise to offer a holistic approach that provides you with dedicated access to all relevant disciplines 'in one go'.

**You can rely on us in high-pro ile incidents to provide**:

– Rapid 24/7 hands on crisis management expertise (under legal privilege)

– A thorough assessment of contractual and third party responsibilities and liabilities and the impact on employees, clients and customers

– Strategic advice on the steps to be taken to de-stress and contain the cyber incident and secure business continuity

– Effective remediation of the cyber incident including obtaining injunctive relief when data is posted on the dark web and liaising with law enforcement

– A sparring partner/hotline for engaging your incident response team, internal and external communication ad hoc questions

– One legal partner that can handle all notification duties, interaction with the supervisory authorities and liaise and coordinate (and where necessary bring in) with third parties (IT, PR, forensic, insurance, etc.)

## Step 4

Develop your cyber readiness

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

**Using our extensive Cyber experience we can**:

– Stop the flow of funds in cases where money was transferred during the cyber incident

– Take legal action against the cyber attacker (if known) and/or third parties who can be held liable

– Defend against private enforcement (class actions by consumers etc. ) and third party claims

– Respond to investigations/ 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 from cyber-attacks and 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 consulting and legal specialists will help you understand your cyber risk profile**.

Our Cyber Health Check can help you identify and manage the emerging threats that cyber risks pose 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; and

– Cyber risk culture.

Based on this, our report will provide you with an assessment and practical recommendations for enhancements across 6 elements:

1. Cyber Culture and Awareness: assessment of the current Cyber Risk Culture within your organisation and how culture is embedded in the current Cyber risk framework
2. Cyber Risk Governance: review and recommendations on cyber documentation, board oversight of the topic, and the overall cyber governance structure
3. Cyber Risk Management: review of Cyber Risk identification, risk assessments, reporting and MI, and the Cyber Risk control environment
4. Cyber Resiliency: review of incident breach preparation and response documentation, and assessment of existing operational resilience measures (e.g. incident and threat detection and monitoring)
5. Third-Party Risk Management (TPRM): review of third-party cyber risk assessments and the TPRM governance structure, and assessment of cyber risk due diligence conducted; and
6. Data Compliance: review of Personal Data Governance, and an assessment of the risk and control framework (e.g. 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 contaminating 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 liasing 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.
8. **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.
9. **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  inancial 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

### 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

### 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

### France

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

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

### Germany

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

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


## Luxembourg

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

## Italy

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

## Netherlands

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

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

## UK

**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

## Europe – Allen & Overy 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 – Hong Kong
Tel +852 2974 7207
Mob +852 9029 4911
fai.hung.cheung@allenovery.com

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

## Singapore

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

# APAC

## Hong Kong

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

## APAC – Allen & Overy Consulting

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

# U.S.

## New York

**Julian Moore**
Partner – U.S. – New York
Tel +1 212 610 6309
Mob +1 347 758 0379
julian.moore@allenovery.com

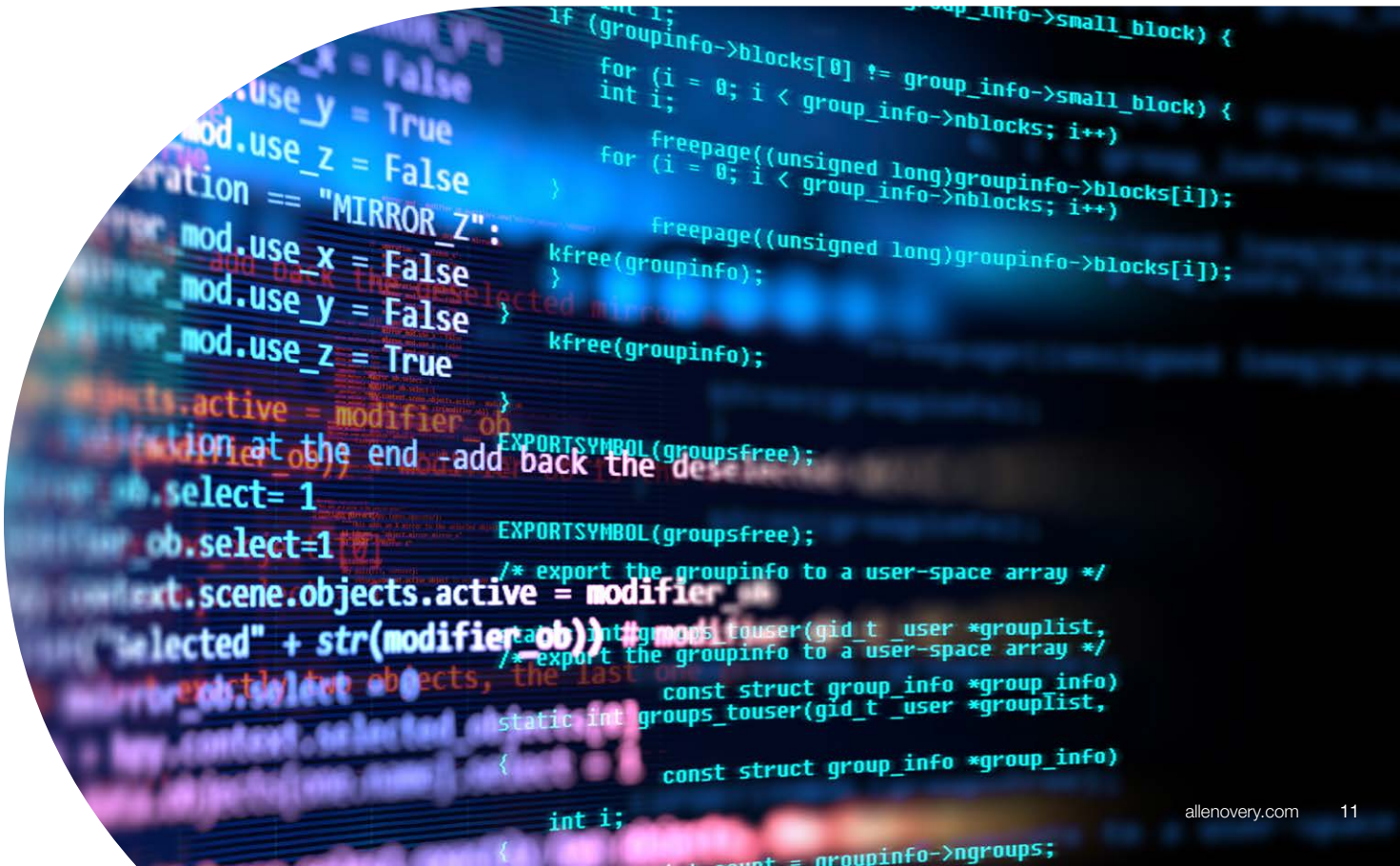
**Adam Chernichaw**
Partner– U.S. – New York
Tel +1 212 610 6466
adam.chernichaw@allenovery.com

## Washington, D.C

**Claire Rajan**
Partner – U.S. – Washington, D.C.
Tel +1 202 683 3869
Mob +1 202 308 9234
claire.rajan@allenovery.com

## U.S. – Allen & Overy 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-103209