ALLEN & OVERY

Cybersecurity and risk management

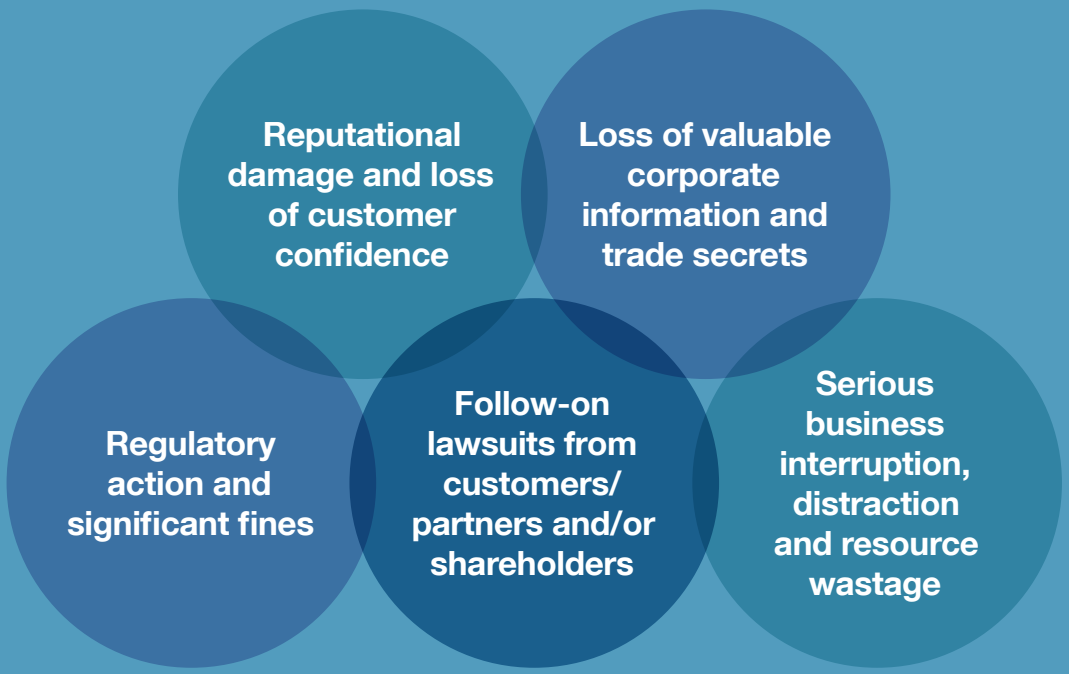
Our view

2016

The challenge *and risks*

The topic of cybersecurity is seldom out of the press these days, occupying the minds of business leaders and politicians alike. From a business perspective, the ideal outcome would be to eliminate cybersecurity risks 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 cybersecurity plans that are focussed on risk management and minimisation.

When considering the resources needed to devote to this exercise, businesses also need to have in mind the range of possible consequences of a cyber-attack. At a high level these include:



All of these ultimately result in costs and/or financial loss. Indeed, in a worst-case scenario, a cyber-attack could be catastrophic, putting a company out of business, although the severity of the consequences will also depend on the specific circumstances of each business (see further below).

Forming *a cybersecurity plan*

Bearing in mind the severity of the potential consequences, any cybersecurity plan should serve the dual purposes of, first, reducing the chances of any successful cyber-attack taking place, and, secondly, limiting the consequences of any cybersecurity breach.

We take the view that no single plan or standard is suitable for all companies, or even for all companies in an industry or sector. There is also no 'one-size fits all' solution or 'off the shelf' software package that can do the job. Instead, cybersecurity planning should follow a risk-based approach that is tailored to the operational components of each business.

FACTORS THAT MUST BE TAKEN INTO ACCOUNT AT THE PLANNING STAGE INCLUDE (AT LEAST) THE FOLLOWING:

1

The types of data held by the business

Some data types will be more sensitive than others, whether because of its inherent value or because of the damage that a leak could cause (eg customer, personal, financial, technical, medical or employee data, etc). Likewise, regulators will be concerned that companies should be more protective of some data types than others

2

The IT systems deployed and the repositories in which data is kept

An assessment of the risks and vulnerabilities within all IT systems, processes, networks and data stores is an essential starting point. The future IT development/ deployment roadmap should also be taken into account during cybersecurity planning

3

The people within the business, their methods of working and their locations

Employees will always be a major contributor to cybersecurity risk, whether due to inadvertent errors or deliberate action. The same is true for people interacting with the business as customers, suppliers or other third parties. Depending on how people work and their needs, cybersecurity risks may be easier or more difficult to guard against. Working practices will need to be considered, probably revised and certainly policed

4

The regulatory environment and the expectations of the regulator(s)

Some regulators are highly engaged with issues relating to cybersecurity and are taking the lead in setting expectations and, indeed, standards. Where this is the case, the views of the regulator must be noted particularly closely

5

Emerging industry practices/ standards

Whilst few industry standards yet exist, adherence to any emerging standards or practices should be taken into account. Engagement with industry bodies and governmental agencies in order to benchmark against the wider industry is key. Opportunities for benchmarking your approach and readiness against others should not be missed

6

Analysis of the most likely threats facing the business

Complete awareness of all threats will be impossible, but attempting to identify them is nonetheless essential. Certain features of the business/sector/ industry may also give rise to specific risks (eg targeting of the financial sector)

7

Analysis of interdependencies

Interconnectivity with outsourced vendors/suppliers, partners and customers forms a key part of the cybersecurity landscape. All of these stakeholders need to be involved to some extent in forming a coherent cybersecurity plan and, if possible, a common level of preparedness

A review of the above should lead to a comprehensive risk matrix that includes details of the likely impact of any given breach/failure (taking account of any interdependencies), as well as the potential steps available (and resources needed) to address or mitigate each of them.

This then forms the basis for a defence and response strategy setting out which risks and response elements are to be prioritised. The resources dedicated to each risk can then be tailored according to their severity and priority to ensure maximum realisation of the strategic goals and provide the greatest impact for the investment made.

Of course, budgetary reality will always play a part and no cybersecurity regime should be too ambitious for a company's means, or too elaborate to be followed on a daily basis. Companies will inevitably have to make choices, but they must be ones that are capable of justification when subject to later scrutiny – no actions should be taken (or not taken) simply by default.

It is also important to remember that the simplest measures should usually be the top priority. If an organisation's cybersecurity measures are ever subject to post-hoc scrutiny, whether by a regulator, a partner company, a court or the media, the failure to take basic steps will be the least easy thing to defend – it is little use engaging expensive and sophisticated solutions if more straightforward and well-known vulnerabilities exist.

Responding *to crises*

All that being said, a good cybersecurity plan must also recognise that it cannot guarantee success and that cyber-incidents will still occur. Preparation for the full range of possibilities is also prudent. Time is always of the essence when disaster strikes, both with regard to identification and control of the attack, and also in taking steps to mitigate its effects (eg communications, disaster recovery, etc).

To be successful, we believe any cyber-response plan must involve a wide range of stakeholders, both at inception and when put into action. A governance regime should be agreed in advance, with a "playbook" in place as to how incidents of different types should be dealt with, both internally and externally. Appropriate resources and advisers, including (forensic) technologists, public relations managers and legal and regulatory experts, can be identified and may need to be contracted ahead of time.

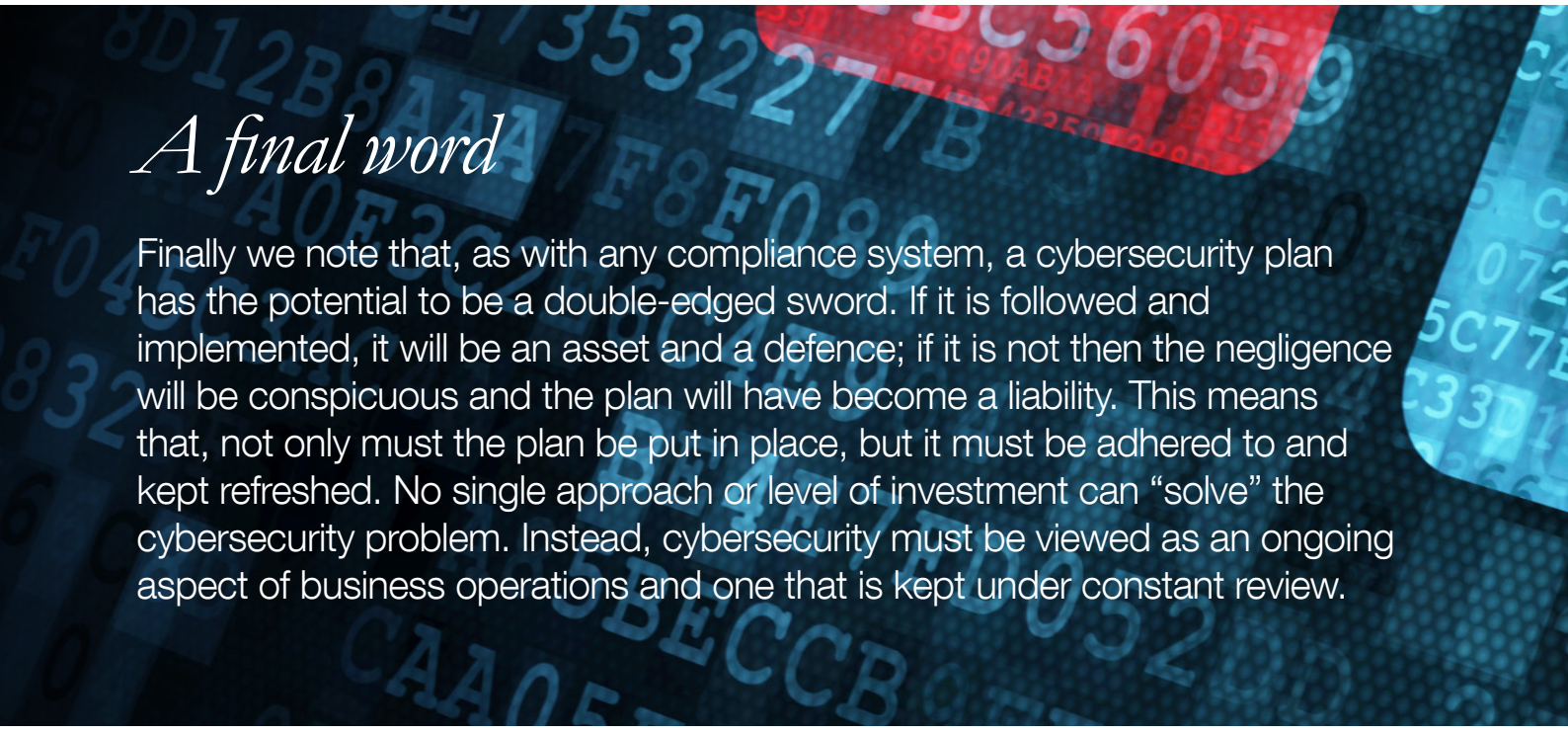
Policies *and education*

Given the potential for entire business processes to be affected, all staff must be educated to view threats to cybersecurity as a shared problem. Procedures should be documented and reinforced through training and drills. IT security fundamentals must not be forgotten (strong key and password management, awareness of phishing, etc). This should also be reinforced with frequent audits and communication from the Chief Information Security Officer, or even the CEO, to elevate the importance of the issue. This aspect of institutionalising approaches to cybersecurity is equally as important as other aspects of IT and data security (for example, a print-out of customer names and addresses left on a train by a careless manager has just as much potential to cause a problem as customer data stolen by a hacker).

The board and executive should also take ownership of setting the tone from the top, educating themselves as to the risks and ensuring that they receive meaningful reporting to allow preparedness and performance to be measured. Information should, in general, be shared with, and gleaned from, authorities, experts and peers, to allow an understanding of the evolving threat and best practices. However, involving authorities may also expose violations by the company or its executives, turning the company from a victim into a suspect. Consider whether legal privilege could help protect the business; if so, involving lawyers early on will maximise the scope of such protection.

Data protection, *trade secrets and cloud technologies*

For many companies, a thorough (re)consideration of cybersecurity risks will come at the same time as planning for other technological and legal developments. These include the potential transition of IT systems to the cloud, planning for compliance with the EU's new General Data Protection Regulation, and refreshing trade secrets strategies in view of the EU Trade Secrets Directive. Some will also be affected by the security and reporting regime to be introduced by the Network and Information Systems Directive or sector- specific rules and regulations. This only reinforces the need for all relevant stakeholders to be involved in planning for cybersecurity – a single plan which coherently deals with all of these issues will almost certainly be more successful than several separate plans formed in isolation.



A final word

Finally we note that, as with any compliance system, a cybersecurity plan has the potential to be a double-edged sword. If it is followed and implemented, it will be an asset and a defence; if it is not then the negligence will be conspicuous and the plan will have become a liability. This means that, not only must the plan be put in place, but it must be adhered to and kept refreshed. No single approach or level of investment can "solve" the cybersecurity problem. Instead, cybersecurity must be viewed as an ongoing aspect of business operations and one that is kept under constant review.

Key *contacts*

Peter Eijsvoogel
Partner – 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

Victor Ho
Partner – Beijing
Tel +86 10 6535 4381
victor.ho@allenovery.com

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

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

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

Ahmed Baladi
Partner – Paris
Tel +33 1 40 06 53 42
ahmed.baladi@allenovery.com

Benjamin Bai
Partner – Shanghai
Tel +86 21 2036 7001
benjamin.bai@allenovery.com

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

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

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

Connell O'Neill
Senior Associate – Sydney
Tel +612 9373 7790
connell.oneill@allenovery.com

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,000 people, including some 527 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (cooperation office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.