

ALLEN & OVERY

Cybersecurity
in life sciences:
*what is your
duty of care?*

2016

A rapidly-changing cybersecurity risk landscape for life sciences companies

Cybersecurity continues to be headline-grabbing news, particularly following recent reports of high-profile cyber attacks on a number of major well-known corporations. Conscious of their fiduciary duties, boardrooms of global companies are paying increased attention to cybersecurity, which now ranks as a global risk preoccupying the minds of captains of industry, heads of state, academics, and law enforcement, who all gathered in January 2016 at the World Economic Forum (WEF) in Davos to debate the best policy and legislative strategy for cybersecurity. To coincide with Davos 2016, the WEF issued a report that warns that failing to improve cybersecurity could cost the global economy USD3 trillion.

*“Now the board of directors, the CEOs of the companies are paying attention. There is a new sense of urgency.”
Carlos Moreira, CEO of Swiss cyber-security firm WISeKey speaking at the WEF in Davos.*

BBC News, Davos, 22 January 2016

“Cybersecurity for the healthcare and pharmaceutical sectors of the S&P 500 index worsened at a faster rate than for the other sectors.”

Financial Times, May 2014

Governments and security experts have already singled out the life sciences sector as being significantly vulnerable to cybercrime. In cybersecurity terms, innovation is fast becoming a double-edged sword for life sciences clients. A UK Government report pointed to the high levels of revenue generated by the life sciences sector, combined with high investment in R&D and manufacturing, and the high level of reliance on IT systems and providers, as reasons why this sector’s cybersecurity risk profile is dominated by industrial espionage, intellectual property (IP) theft, and service denial. Of 26 business sectors analysed in the report, it identified life sciences as the main target of IP theft, costing the UK GBP9.2 billion, of which it attributed GBP1.8bn to theft of pharmaceutical, biotechnology, and healthcare IP.

In January 2016 another major life sciences company fell victim to alleged theft of valuable trade secrets relating to promising scientific research for a new cancer treatment when two company scientists and three others were charged by prosecutors with stealing research and manufacturing secrets potentially worth hundreds of millions of dollars for sale in China, where pharmaceuticals is a sector targeted by the Chinese Government for strategic growth. With estimates that put the out-of-pocket cost of developing a prescription drug that gains market approval at USD1.4bn, life sciences companies should rightly be concerned about safeguarding their valuable digital assets.

As government concern increases, so does the level of government outreach work with life sciences companies, for example by inviting major companies to participate in cross-industry working groups and encouraging collective industry action, in order to raise awareness of the importance of cybersecurity across the sector and to support companies to communicate effective cybersecurity messages. In the UK, this culminated in the publication of a Ten-Step Guide on board responsibility for managing cybersecurity risk, which the Government claims is used by around two thirds of the FTSE350. Then in March 2016, the UK Cabinet Office confirmed that the UK’s new National Cybersecurity Centre (NCSC) will open in October and work closely with the private sector in managing cybersecurity risk. Commenting on the NCSC, the Director General of Cybersecurity at GCHQ, Robert Hanningan, has highlighted the role of the new agency in helping to combat the online threats that exist to what he calls “the industrial-scale theft of IP from UK companies and universities”.

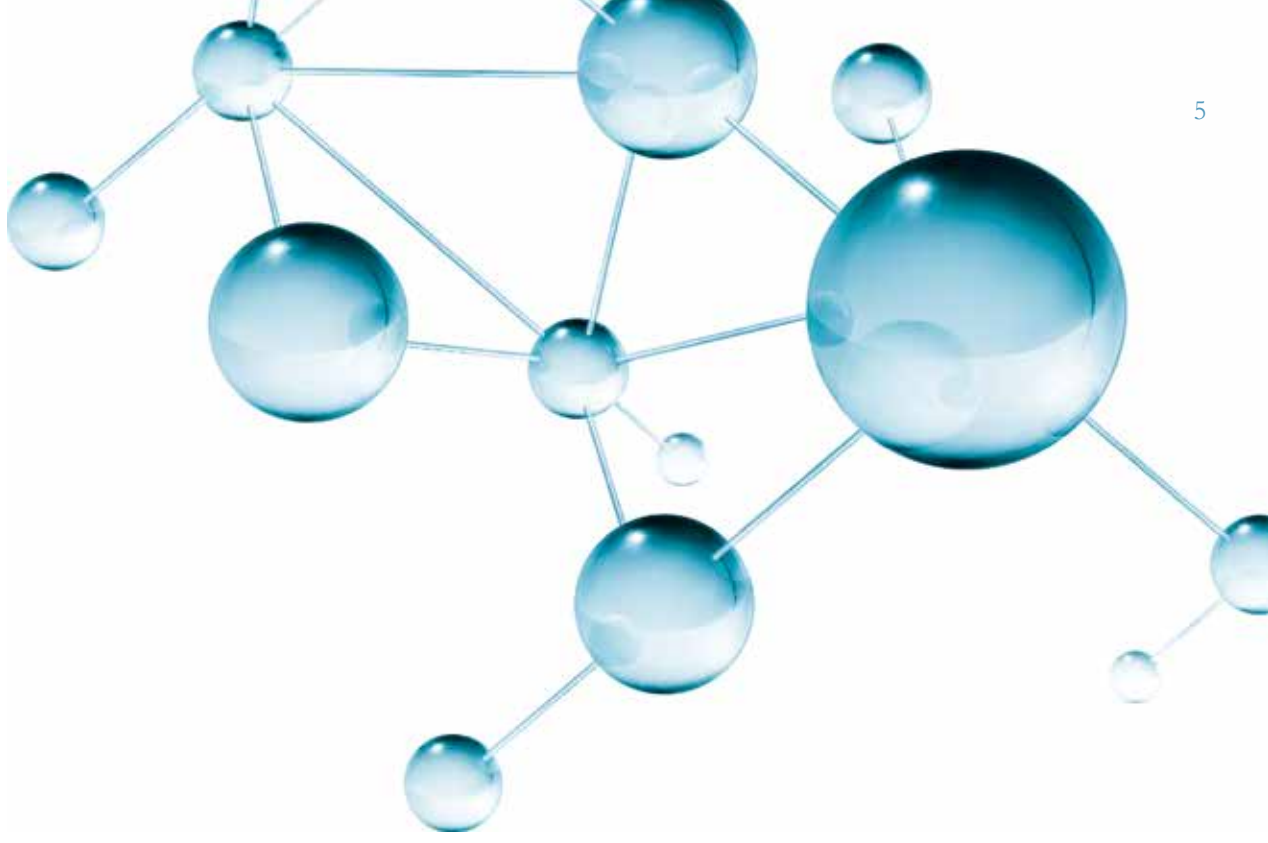
The particular risks to life sciences companies and the myriad of legal and regulatory requirements to which they are subject can vary significantly in a cybersecurity context depending on exactly where and how they do business. Larger life sciences companies can have several business lines with different geographical footprints, each with their own particular cybersecurity risk profiles necessitating a risk-based but still integrated approach to risk management at an enterprise level to avoid duplication or gaps.

In common with most industries, cybersecurity in the life sciences sector is only as good as the weakest link in terms of a company’s staff, processes, and technology. Against this backdrop, life sciences companies are understandably concerned about what standard of care they should adopt and how to structure and deploy resources to comply with the rapidly evolving cybersecurity legal landscape with new and emerging laws on the horizon. This report highlights the key cybersecurity issues for life sciences companies, developments in the law, and what they should do to keep on top of the risk.

What you need to know

“Boards that choose to ignore or minimize the importance of cybersecurity oversight responsibility do so at their own peril.”

SEC Commissioner, Luis Aguilar, June 2014, NYSE



An overview of the cybersecurity legal framework

There is no comprehensive, integrated legal framework addressing cybersecurity risk. Rather it is an overlapping patchwork of national and international law and regulation coupled with government and industry regulation, guidance, and technical standards. The main international cybersecurity legal instrument is the Council of Europe Cybercrime Convention of 2001 (also known as the Budapest Convention on Cybercrime), which has been ratified by most EU Member States as well as a number of other countries. The Convention's stated purpose is to pursue a common criminal policy aimed at the protection of society against cybercrime, by adopting legislation and fostering international cooperation – cybercrime legislation, like the internet and cybercrime, knows no geographical jurisdictional limits, so the Convention is a means of ensuring common cooperation and enforcement between states.

One of the main EU legal instruments currently in force is Directive 2013/40/EU on attacks against information systems, which came into force in August 2013 and builds on a number of aspects of the European Convention by creating four substantive criminal offences of illegal access to information systems, system interference, data interference, and interception. The deadline for transposition of the Directive into national law passed in September 2015, though most Member States had already enacted national legislation meeting the requirements of the Directive before the deadline. More recently, the Directive on security of network and information systems (the “Cybersecurity” Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. The Cybersecurity Directive will be discussed further on in this report.

Across the Atlantic, the United States Congress passed the Cybersecurity Act of 2015, which was signed into law on 18 December 2015, and purports to establish a voluntary cybersecurity information-sharing process to encourage public and private sector entities to share cyber threat information, without legal barriers and the threat of unfounded litigation, while protecting private information. Section 405 in particular is dedicated to improving cybersecurity in the healthcare industry and requires the Department of Health and Human Services to establish a task force of industry stakeholders and cybersecurity experts with the goal of making recommendations to reduce cybersecurity risks.

A number of countries in Asia have also passed, or are in the process of debating, national cybersecurity laws. Singapore, for example, announced a new cybersecurity bill in January 2016, which is intended to give Singapore's cybersecurity government agency wider powers to protect critical infrastructure, including in the health sector. China also proposed similar new draft legislation that could have cybersecurity implications for all companies operating websites accessible in China.

Where cybersecurity and life sciences converge

CORPORATE GOVERNANCE

Just as life sciences companies can be subject to sector-specific regulation, those companies whose securities are traded on relevant exchanges can also find themselves subject to additional corporate governance requirements.

Boards of public life sciences companies are required to maintain sound risk management and internal control systems and, in certain instances, to confirm in their annual report that they have carried out a robust assessment of the principal risks facing the company, including those that would threaten its business model or future performance.

In 2014, the UK Government published specific guidance on managing cybersecurity risk for non-executive directors of UK public companies. Life sciences companies should therefore bear in mind that there is potential legal exposure to investors depending on how a cybercrime affected the company and the timing and accuracy of any information or material disclosed to the market. For example, when news broke in early 2016 of the alleged theft of trade secrets from its internal research databases, GSK immediately sought to reassure investors that it did not expect the breach to have a material impact on its business or R&D activity.

In March 2016, the UK Institute of Directors published a study (a link to which is available below), *Cyber Security: Underpinning the Digital Economy*, indicating businesses are not taking cybersecurity seriously enough and emphasising the need to make it a boardroom priority and not a risk left exclusively to the IT department to manage. The author of the study, Richard Benham, described cybercrime as “one of the biggest business challenges of our generation and companies need to get real about the financial and reputational damage it can inflict.”

Public or private, we see life sciences companies becoming increasingly concerned to know what standard of care they should adopt to mitigate cybersecurity risks. The reality is that there is no one-size-fits-all approach in this regard and the question of what standard is applicable to a life sciences company will be a function of a number of considerations, in particular where the ultimate parent company is headquartered because that jurisdiction will determine the duties of the main board in identifying and mitigating cybersecurity risk, available government guidance and resources, and the laws governing the operations of the company at home and abroad.

Under Swiss and English laws governing directors duties, for example, there is an objective test applicable to the level of care required that would, in our view, weigh in favour of seeking professional advice from knowledgeable counsel and information security consultants in order to discharge performance of an obligation in relation to risks that should be in the board’s contemplation. Non compliance can potentially lead to both civil and criminal liability for corporates and individuals depending on the nature and severity of the breach. Continuous board oversight of the risk is critical to ensure policies and procedures are adequate to meet applicable legal requirements and that proportionate technical and organisational measures are in place and working to counter unauthorised access to, or loss of, networks and data.

In addition, we think it is reasonable to take the position generally that a board of directors of a life sciences company that has satisfied itself as to the company’s position in relation to cybersecurity risk will not have failed to discharge its fiduciary duty. And furthermore, provided systems are in place to ensure ongoing oversight and review by the board of the risk and implemented mitigating controls, errors of business judgment should not expose individual board directors to personal liability.

“It takes 20 years to build a reputation but just 5 minutes to ruin it with a data breach...and then up to 2 years to rebuild it.”

Manufacturing Chemist Pharma, September 2015

DATA PROTECTION

According to a survey of data breaches in the pharmaceutical sector, 60% of IT decision makers in the sector said that their company had lost important data and almost a quarter reported that their company had suffered a hack. Protecting data has therefore never been more important for life sciences companies.

General information security requirements applicable to life sciences companies are currently covered by relevant data protection legislation which typically sets minimum standards regarding technical and organisational measures to be taken by life sciences companies when processing and safeguarding personal data.

Life sciences companies will already be familiar with the unique challenges of compliance with EU data protection law in the context of outsourcing initiatives (particularly the increasing trend in contracting cloud-based solutions to support regulatory compliance and safety data exchange systems), sales and marketing activities, clinical research and development, pharmacovigilance, international data transfers, healthcare professional disclosure requirements, internal investigations, product liability litigation, and a host of other routine business activities. With the advent of the General Data Protection Regulation (GDPR), these challenges are set to continue, and potentially increase and become more complex, particularly with regard to the requirements to undertake privacy impact assessments (PIAs), consult with data protection authorities, and notify competent authorities of certain data security breaches.

It is therefore important that legal and compliance departments of life sciences companies understand which regulatory agencies will potentially need to be consulted on PIAs and receive and get involved in data breach notifications in order to ensure they are adequately prepared for a cybersecurity incident. The new mandatory notification requirement and obligation to implement appropriate technical and organisational measures in the GDPR overlap with requirements in the new Cybersecurity Directive, which will also be of significant interest and importance to life sciences companies and is discussed further below.

The threat of enforcement for data security breaches is increasing in likelihood with evidence emerging of rising data protection regulatory enforcement in the UK healthcare sector, for example. In 2015 the UK Information Commissioner's Office (ICO) issued a monetary penalty notice to Pharmacy2U, an online pharmacy that sold customer details (without their informed consent) to third parties. The penalty is the first of its type to be issued for a breach of the first data protection principle, regarding fair and lawful processing of personal data. At the

end of 2015, the ICO also fined the Bloomsbury Patient Network in London after it inadvertently revealed the identities of HIV patients through an email error. Also, in 2014 the British Pregnancy Advice Service (BPAS, a UK charity) was fined after a serious breach of the Data Protection Act revealed thousands of people's details to a malicious hacker. The hacker threatened to publish the names of the individuals whose details he had accessed, though that was prevented after the information was recovered by the police following an injunction obtained by the BPAS.

Although the ICO cases, and similar cases in other jurisdictions, do not directly implicate life sciences companies, in the ordinary course of business these companies can and do enter into collaborations and partnerships with these and many other healthcare organisations, patient organisations, and charities that handle sensitive health data that may require them to consider data security risks more proactively to avoid legal and reputational harm if personal data is not processed in a compliant way or is subject to a security breach, particularly as life sciences companies step up their efforts in the digital health space. What these and other similar cases also show is that cybersecurity in the life sciences and broader healthcare sectors is not always about sophisticated, expensive systems designed to counter criminal threats but can entail the most basic procedural failures leading to inadvertent disclosure of personally-identifiable information. For example, two enforcement actions¹ taken against HIPAA-covered entities by the U.S. Department of Health provide useful insights into how easily the security of sensitive information can be compromised by employees and the practical steps companies can take to ensure corrective and preventative action.

Life sciences companies could find themselves defending contractual and other claims from partner organisations and third parties for the consequences of data security breaches, as well as regulatory scrutiny and fines – the case of *Vidall-Hall v Google* in the English courts highlights the increasing risk of companies being sued and of the potentially global reach of litigation over cybersecurity breaches. In the U.S., the litigation threat obviously goes further with the potential for class actions and shareholder derivative suits (as has already happened in the cybersecurity space, with class actions relating to data breaches in the life sciences sector being brought under a range of state and federal data breach and security laws, for example HITECH and HIPAA).

You can keep up to date with general developments in the GDPR via the link below to our client alert.²

¹ <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/linicare/index.html>

<http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html>

² <http://www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf>

THE CYBERSECURITY DIRECTIVE

In December 2015, The European Council and Parliament reached agreement on the text of the new Cybersecurity Directive. The Cybersecurity Directive is the EU's latest response to the increasing frequency and scale of cybercrime attacks to public bodies and private companies across the European Union. Such attacks can pose a serious threat to health, safety, and the economy. The aim of the Directive is therefore to ensure a common level of cybersecurity risk management practice across the EU and will create a new regulatory regime for a number of key sectors of the economy, including health, not currently subject to similar requirements, which will create an obligation to report significant cybersecurity incidents to the competent authorities and to implement technical and organisational risk management measures.

The Directive entered into force in August 2016, with Member States having 21 months to implement it into national law and an additional six months to identify so-called "operators of essential services" in individual Member States in accordance with specified criteria, namely:

- Whether the service is critical for society and the economy;
- Whether the service depends on network and information systems; and
- Whether an incident could have significant disruptive effects on its provision or public safety

The Directive is of importance to life sciences companies because health is listed in the Directive as an "essential service" sector and identified market operators in the health sector will be subject to mandatory security breach and incident notification requirements and have to put in place appropriate technical and security measures. The Directive overlaps with provisions in the GDPR on security, and in particular requirements to notify regulators of security breaches affecting data identifying individuals, which form part of the new GDPR.

Beyond hospitals and other public health service providers it is not yet clear if life sciences companies will qualify as operator of an essential service under the Cybersecurity Directive. This will fall to be determined by each individual Member State in accordance with the criteria outlined above. It is not inconceivable that life sciences companies could potentially fall within the definition as they are considered core components of both the GDP of national economies and the critical infrastructure. In the UK for example, the Government Cyber Security Strategy included the pharmaceutical sector in a joint

public/private sector strategy hub following meetings by the prime minister with the heads of some of the largest UK companies from key sectors of the economy, which resulted in the creation of the hub as an innovative approach to managing cybersecurity risk on a collective basis. This suggests that certain life sciences companies are considered sufficiently important to the National Health Service from a public health and safety perspective and to the broader economy such that a material cybersecurity incident could potentially result in significant disruptive effects, for example the interruption in supply of critical medicines for which there is only one or a small number of manufacturers or the theft of IP relating to technology for diseases that represent a particular threat or burden to public health.

Qualification as an operator of essential services also seems likely when you consider the activities of medical affairs departments against the definitions of "healthcare provider" in Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, and public service regulatory obligations of life sciences companies under the EU Community code relating to medicinal products for human use (Directive 2001/83). Under national implementing laws, pharmaceutical manufacturers and wholesalers have a general legal duty to ensure that patients' needs in all 28 Member States are met; in particular manufacturers must ensure they have robust supply arrangements in place that ensure medicines are distributed to pharmacies and dispensing doctors in an efficient and timely way. Manufacturers of products with supply commitments to public health procurement agencies, or classed as essential by the WHO, or for rare diseases or diseases which represent a particular burden on, or threat to, public health in a country or region, will be concerned to ensure the integrity of their supply chain is not compromised by cybersecurity.

Even if individual companies do not ultimately qualify as an operator of essential services, the Cybersecurity Directive is still of relevance and importance to life sciences companies because, in the absence of specific sector guidance and requirements, it is likely to be looked upon as a de facto minimum cybersecurity standard by most corporates operating in the EU.

CYBERSECURITY AND DIGITAL HEALTH – PRODUCT LIABILITY AND PERSONAL INJURY CONCERNS

The digital revolution in the life sciences sector continues to gather pace with e-Health and m-Health remaining very high up on the EU's policy agenda to give patients more information, and more involvement in their healthcare, leading to improved access to health advice and treatment and more efficient national healthcare systems. However the highly regulated nature of the industry coupled with the risks posed by cybersecurity to businesses, products, patients, and consumers mean there are traps for the unwary.

There is growing concern in the life sciences sector, for example, over the implications of cybersecurity for the medical device sector, and the increased risk to manufacturers of product liability and to patients of safety and effectiveness for devices targeted by cyber attacks, particularly for those companies active in the M2M market, or the "Internet of Things", for example connected wearable technology, or in developing m-Health apps. The current EU Medical Devices Directive does not make explicit reference to cybersecurity design requirements; however, certain European-harmonised ISO standards for medical devices arguably set indirect standards concerning security measures for software used in medical devices. Current proposals for a new Medical Device Regulation in Europe do discuss the merits of more specific software design requirements, but still do not address cybersecurity directly. Some consider this to be a legislative gap that may eventually be addressed only as medical devices in the m-Health space continue to be the target of cyber attacks.

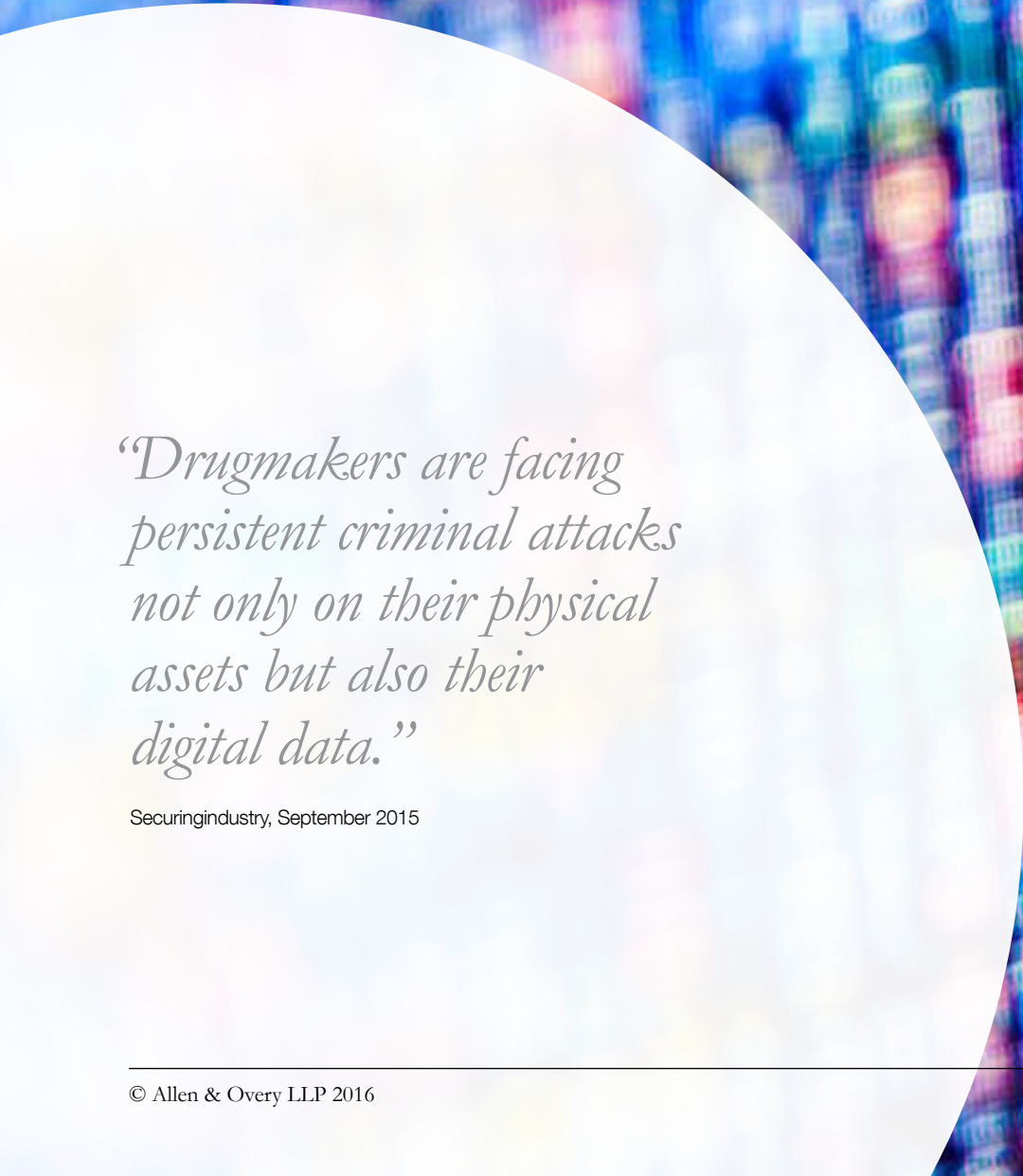
The notion of cybersecurity leading to potential physical harm is not as far-fetched as it may first appear, particularly in the context of medical devices where networked medical device cybersecurity as a means of ensuring patient safety is of considerable importance to medical device manufacturers – Medtronic, one of the leading manufacturers of health devices in Britain, commented: "We are committed to addressing the industry-wide issue of wireless hacking." Medical device companies are therefore acutely aware of the cybersecurity risks for the literally hundreds of thousands of medical devices such as patient monitors, pumps, ventilators, and imaging equipment to name but a few – many of which are life-supporting devices – that operate on the networks of healthcare organisations that could be hacked, not to mention all the medical devices that are operated via wireless technologies, for example insulin pumps and pacemakers.

Patient safety is also high on the agenda of regulatory agencies, with a recent example in the U.S. of regulators advising hospitals to stop using a particular manufacturer's pump device after a live demonstration of a cyberattack on the device revealed that the dosage

the pump delivers could be compromised by hackers. In a real-world example of the risk to patient safety and to life sciences companies of litigation, a Los Angeles hospital reported in early 2016 that it had paid a bitcoin ransom to recover patient medical records after hackers had apparently attacked its systems via a phishing email containing a virus which encrypted their files.

The U.S. Food & Drug Administration, the main regulatory agency for medical products and devices, is actively addressing this issue and in January 2016 issued draft guidance for consultation to inform industry and FDA staff of the agency's recommendations for managing post-market cybersecurity vulnerabilities for marketed medical devices. In addition to the specific recommendations contained in the guidance, the FDA encourages manufacturers to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device, in other words "cybersecurity by design". As the medical device sector continues to innovate in the development and manufacture of connected devices, the FDA's guidance potentially takes cybersecurity risk management to a new level by recommending the adoption of a corporate disclosure policy as a security practice. Such a policy effectively lets would-be hackers inform manufacturers of cybersecurity vulnerabilities in a device without fear of legal consequences.

Cybersecurity is also having an impact on EU pharmaceutical regulation. January 2016 saw the publication of an Opinion of the European Economic and Social Committee on "Towards digital health – electronic information for safe use of medicinal products". The Opinion is an endorsement of the Commission's efforts to make e-Health a priority as part of the broader EU Digital Agenda and makes specific reference to the need to take account of the data protection implications of m-Health initiatives, particularly the use of smartphone apps. The Opinion also reinforces the obligations of the life sciences industry to ensure the availability of accurate and up-to-date information on its products, and therefore mandates that any technological solution to facilitate the efficient electronic distribution of patient information leaflets and technical information approved by licensing authorities in the form of Summaries of Product Characteristics be developed in close collaboration with industry to ensure, amongst other things, adequate supervision by licensing authorities.



“Drugmakers are facing persistent criminal attacks not only on their physical assets but also their digital data.”

Securingindustry, September 2015

CYBERSECURITY AND PHYSICAL LIFE SCIENCES ASSETS

In a life sciences context cybersecurity is also linked to physical security, particularly in terms of the strategies companies deploy to protect their tangible assets. A lot of valuable know-how is generated and held on computer databases and networks at research and development and manufacturing sites that often use standalone IT systems. It is therefore important that life sciences companies assess the risks of cybersecurity in parallel with site security, particularly those companies whose facilities may be considered critical national infrastructure because they research, develop, or manufacture products that are considered sensitive from a national security perspective, for example, chemical or biological material or products that protect against bioterrorist attacks.

Terrorist attacks against company facilities are not uncommon. BP suffered such an attack at its gas facility in Algeria in 2013, which led to multiple claims against the company in the High Court concerning the deaths of several oil executives at its Algerian plant, with claimants alleging that BP failed to put in place adequate security

measures to prevent the deaths. More recently in 2015 a van driver, who was under investigation by the authorities over concerns of radicalisation, carried out an attack on a gas factory near Lyon in France not long after the Charlie Hebdo attacks. The terrorist attacks in Paris in November 2015 and the March 2016 attacks in Brussels also prompted businesses to review their corporate security arrangements. Many life sciences companies, in common with the oil, gas, and extractives industries, have significant physical assets and infrastructure in countries where the level of terrorist attack is perceived to be high. It is therefore not difficult to see how a cyber attack targeting the operations of a major pharmaceutical research or manufacturing plant – particularly one that handles dangerous or hazardous materials – could lead to a major security breach potentially leading to health and safety and environmental concerns that ultimately result in legal and other exposure for life sciences companies, with some companies already seeking advice on legal liability arising from a terrorist attack to critical infrastructure.

CYBERSECURITY AND TRADE SECRETS

As already noted, IP theft is considered a major cybersecurity threat to life sciences companies, a view reinforced by the prevalence of trade secrets theft incidents in the life sciences sector.

The latest draft of the “Trade Secrets” Directive, published in December 2015 and designed to harmonise the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, will be of interest to life sciences companies concerned about cybersecurity risks and the measures in place in their organisations to protect against unauthorised access to and use of company information. The Directive notes that innovative businesses, which would clearly embrace life sciences companies, are increasingly exposed to dishonest practices targeted at misappropriating trade secrets, such as theft, unauthorised copying, economic espionage, breach of confidentiality requirements, whether from within or from outside of the Union. Recent developments, such as globalisation, increased outsourcing, longer supply chains, increased use of information and communication technology contribute to increasing the risk of those practices.

Similar to the Cybersecurity Directive, the Trade Secrets Directive focuses on attacks on business secrets and information and consequently reinforces the need for better cybersecurity policies and procedures, particularly as life sciences companies operate in a sector

that is highly active in M&A and collaboration transactions, which drive innovation and therefore generate new, valuable intellectual property, know how, and insider information requiring protection.

The need to protect business secrets and know how is also reflected in new regulatory requirements for life sciences companies, such as new Directive 2011/62/EU on the prevention of the entry into the supply chain of falsified medicinal products. This Directive expressly recognises that repository systems containing information on product safety features might contain commercially sensitive information that must be appropriately protected. This ties in with the afore-mentioned EESC Opinion on the electronic distribution of patient information and the importance of ensuring the security of product data.

Trade secrets concerns have also increased in the U.S. life sciences sector, with prominent companies in the sector showing public support in a letter to the Senate for the Defend Trade Secrets Act of 2015, a bill that creates a federal cause of action for trade secret misappropriation. The concerns about misappropriation set out in the draft European Directive are echoed by the Senate Committee responsible for the bill, with Chairman Senator Charles Grassley commenting “between global competition and increasingly mobile data, misappropriation that before might have taken a truck, today only takes a USB key slipped in somebody’s pocket.”

What you need to do

As directors of life sciences companies get to grips with their duty of care in relation to cybersecurity risk, there are eight key preventative steps we believe should be high on the agendas of boards and senior management teams in order to maintain a proactive and proportionate cybersecurity stance to counter unauthorised access to, or loss of, networks and data:



STAY INFORMED

Cybersecurity is a broad, complex subject that you may know little or nothing about. It is therefore important to take steps to inform yourself about the subject and the risk profile for your business on an ongoing basis. You can do this by seeking professional advice from knowledgeable legal counsel and information security consultants.



ESTABLISH A FRAMEWORK OF ACCOUNTABILITY

Do you know who retains day-to-day management responsibility for cybersecurity in your company? Directors cannot relinquish overall responsibility and oversight for cybersecurity risk so it is important the risk is owned by a senior-level employee with sufficient technical expertise that has clear accountability to the board and is supported by a cross-functional operational team. The board is then well-positioned to exercise continuous oversight and stay informed of material issues by receiving updates and technical briefings and asking questions to satisfy itself that the risk is being adequately managed with sufficient resources.



UNDERTAKE A CYBERSECURITY RISK ASSESSMENT

There is no one-size-fits-all approach to cybersecurity risk management and your degree of exposure, and the measures that you should put in place to mitigate that exposure, will depend on a range of considerations as outlined above, such as your lines of business, geographical footprint, the value of identified intellectual property, proprietary information and know how, working practices (who can access what and from where), the business impact of a breach, the IT infrastructure and reliance on systems providers, and interactions with staff and third parties, to name but a few. To reduce the compliance burden, it may also be prudent to consider integrating cybersecurity activities with other business processes such as physical security and data privacy risk assessments and audits.

You can read more about how you might formulate a cybersecurity risk management strategy in our separate paper complementing this report entitled “Cybersecurity and risk management – Our view”, which is available in the link below.



PUT IN PLACE WRITTEN STANDARDS

You should ensure your company has clear, accessible, up-to-date written policies and procedures, to demonstrate that you are striving to meet the prevailing legal requirements, and that they are used in regular communications and training with staff to ensure they understand their obligations to use IT resources responsibly and protect information, and know what to do if they suspect an actual or potential breach.

<http://www.allenoverly.com/publications/en-gb/Pages/Cybersecurity-and-risk-management---Our-view.aspx>



HAVE A CYBERSECURITY INCIDENT RESPONSE PLAN

Should an incident occur it is important to have a clear, proportionate strategy to deal with the fallout in a timely fashion. There will be a myriad of internal and external issues and stakeholders to consider depending on the nature and extent of the incident, including mobilising cross-functional response, crisis management, and business continuity teams, considering the legal and contractual implications, and potential disclosure requirements to cybersecurity and industry regulators, law enforcement, listing authorities, customers, and suppliers.



THIRD PARTY OVERSIGHT

All life sciences companies have critical third party relationships in place providing goods and services to all parts of the business. It is important you consider cybersecurity risk in the context of those third party relationships, ensuring risk-based due diligence is conducted on the third party's policies, procedures, and standards, checking appropriate security and technical measures are in place to enable the secure flow of information and communications, and suitable contractual obligations and protections are included in written agreements with the third party, for example obliging them to notify you promptly of cybersecurity breaches, requiring coordination with competent authorities, and liability and insurance provision that do not leave you legally or financially 'high-and-dry' in the event of a major incident.



INSURANCE

Given the increased risks to life sciences companies posed by cybercrime, particularly in terms of the potential liabilities that can flow from breach, you should review your insurance arrangements to determine whether your existing categories of cover provide adequate protection against cybersecurity risk, for example, public and product liability or directors and officers liability insurance, or whether standalone cover is recommended. The TalkTalk cybersecurity breach reported last year serves as a good example of the potential benefit of insurance protection – the CEO reported that “The estimated one-off costs are between GBP30m and GBP35m – that’s covering the response to the incident, the incremental calls into our call centres, obviously the additional IT and technology costs, and then the fact that over the last three weeks until yesterday our online sales sites have been down, so there will be lost revenue as a result.” TalkTalk reportedly had cybersecurity cover in place that may go some way to softening the financial blow of a cybersecurity incident.



STAFF PRACTICES

Whilst many cybersecurity incidents are the result of innocent mistakes or lack of awareness of policies and procedures, the reality is staff in life sciences companies, whether through carelessness or malicious intent, can create significant cybersecurity exposure. Although no company is immune from cybersecurity attack, you should review your employer recruitment and contractor engagement practices to be confident people working in your organisation are selected following careful pre-employment vetting and, where circumstances warrant and laws permit, enhanced risk-based screening against government watch lists – the new U.S. cybersanctions regime is likely to mean life sciences companies are well advised to conduct risk-based sanctions screening to mitigate the risk of cyberespionage involving designated Chinese and other parties. For roles that are considered to raise specific cybersecurity risks, for example, roles providing access to particularly valuable or confidential information or know-how such as research data for a promising new compound, ongoing monitoring may be warranted in accordance with applicable privacy and employment legislation.

You can read more about cybersecurity and employees in the link below to our blog on this topic.

<http://aoemploymenttalk.com/uncategorized/cybersecurity-and-employees/>

Core team contacts

A&O's Life Sciences team is well-positioned to advise on cybersecurity matters and would be pleased to discuss any of the matters covered in this report. If you would like further information or specific advice, please contact one of the team below.



Nicola Dagg

Partner – London

Tel +44 20 3088 3871
nicola.dagg@allenoverly.com



Filip Van Elsen

Partner – Antwerp

Tel +32 3 287 73 27
filip.vanselsen@allenoverly.com



Alexandre Rudoni

Partner – Paris

Tel +33 1 4006 5034
alexandre.rudoni@allenoverly.com



Mark Ridgway

Partner – London

Tel +44 20 3088 3720
mark.ridgway@allenoverly.com



Nigel Parker

Partner – London

Tel +44 203 088 3136
nigel.parker@allenoverly.com



Mark Mansell

Partner – London

Tel +44 20 3088 3663
mark.mansell@allenoverly.com



Steven Rix

Senior PSL – London

Tel +44 20 3088 4884
steven.rix@allenoverly.com

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,200 people, including some 530 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

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

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.

© Allen & Overy LLP 2016 | CS1601_CDD-44247_ADD-63066