STEPHENSON HARWOOD

Cybersecurity in the life sciences industry: Fail to prepare; prepare to fail

Introduction to the increasing cyber threat

The level of cybercrime continues to grow at an unprecedented rate in the UK and across the globe, with UK Government figures from 2021 showing that nearly 40% of businesses surveyed had suffered cyber security breaches or attacks in the last year. Over recent years the threat of attacks has been exacerbated by the increase in staff working from home, and from increased political tensions and activity from hostile states.

Key takeaways

- The current threat level is high.
- The life sciences sector is a key target.
- Supply chain often creates the most material vulnerabilities.

Key actions

- Audit and test technical security measures in place.
- Review, refresh and test response plans.
- Map, audit and test supply chains.
- Produce a "grab sheet" with key information on a couple of pages.
- Engage third party professionals – forensic IT and legal – so they are available in an emergency.
- Refresh training to key stakeholders.

During the pandemic, the UK's National Cyber Security Centre (NCSC) reported over 200 attacks specifically related to the pandemic, including attacks on vaccine research "almost certainly" from Russian intelligence services. For example, in 2020 Dr Reddy's Laboratories was forced to halt production at several facilities following a cyber-attack, which impacted data centres and plants in multiple jurisdictions. In December 2020 the European Medicines Agency (EMA) also confirmed that it had been subject to a cyber-attack enabling the unlawful access to certain documents relating to the Pfizer/BioNTech vaccine. It has also been reported that North Korean hackers had used a spear-phishing campaign to target AstraZeneca and also tried to steal vaccine information from Johnson & Johnson and Novovax.

Ransomware continues to be a focus of cybercriminals and is now the most prominent and immediate cyber threat to businesses, and one which should be at the top of the agenda for organisations in the life sciences industry. However, many organisations seem to be inadequately prepared.

There seems to be no obvious trend in the target of ransomware attacks, other than being levied against organisations which have the means to pay the demands and would face immediate (financial, reputational, and regulatory) pressures to resume business as usual. This makes the life sciences sector, and those operating in its supply chain, extremely susceptible to attacks.

In this latest insight we look at why life sciences organisations are particularly exposed, the regulatory landscape, and cover the technical and practical ways that they can prepare for, and plan their response to, an inevitable attack.

Life sciences as a key target

Life sciences organisations typically have complex collaboration structures and supply chains, with significant specialist services being outsourced. This results in a number of weak points in the integration of services and information exchange points and opens up vulnerabilities that cybercriminals can exploit. From an internal perspective, internal IT functions may be under resource pressure, and systems may be outdated, which adds to the exposure risk.

They are at a heightened risk of being subject to attacks from cybercriminals due to several key factors:

- it is imperative that they can maintain the confidentiality of their intellectual property – this puts pressure on organisations to comply with ransom requests in order to protect their IP assets, and puts them at increased risk of industrial espionage;
- they hold a significant amount of valuable and sensitive data, in particular personal health data – this can be sold by attackers on the black market or encrypted as part of a ransomware attack;
- there is an increased reliance on IT systems and outsourced processes, and new growth in the "software as a medical device" and related products – this introduces technical weak points; and
- many companies are under prepared – it is important to understand that cybercriminals are now "professionals", undertaking their own detailed research on which sectors are most vulnerable and who to attack.

Life sciences organisations are also at an increased risk of attacks from foreign states looking to disrupt critical drug and treatment supplies or steal technology and other IP assets to help their own domestic firms compete.

What is at risk?

Cyber security breaches or attacks carry a number of risks to life sciences organisations, including:

- data/information loss – sensitive data and confidential information, such as clinical trial and product data, could be exposed to third parties;
- business interruption – systems could be corrupted, or encrypted beyond use;
- extortion – ransomware attackers request payments for de-encrypting data and systems;
- additional expense – breach remediation can be costly and a drain on internal resources;
- exposure to regulatory fines – organisations could be fined for breach of their legal obligations;
- reputational damage – adverse publicity can be damaging to the organisation and any associated products, projects or partnerships;
- company valuations – at a time of enhanced M&A activity in the life sciences sector, a cyber-attack could adversely affect a company's valuation or share price; and
- legal claims - individual and group actions could be taken against the organisations.

Regulatory requirements

Whilst there is currently an obvious lack of detailed cyber regulation specific to the life sciences industry, there are a number of regulatory requirements that need to be considered in relation to cyber threats and reporting. In the future, however, pending the UK Government's consultation on expanding the scope of Network and Information Systems Regulations 2018, it is likely that more specific regulation will apply to the life sciences industry (and a similar expansion to cover the manufacturers of medical devices and pharmaceuticals is also well progressed at an EU level). The MHRA is also consulting on the future of regulation for "software as a medical device" ("SaMD"), and in particular is considering imposing specific cyber security requirements related to SaMD product lifecycle risks.

From a corporate governance perspective, publicly listed life sciences companies are required to maintain appropriate risk management and internal control systems and, in some instances, may need to confirm in their annual report that they have carried out a robust assessment of the main risks facing the company, which may now likely include cyber security risks.

Life sciences organisations must comply with their obligations under relevant data protection laws, including the obligations under the General Data Protection Regulation to have clearly documented policies and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This is a broad obligation and imposes duties to ensure both internal and external systems are robustly protected.

In the event of a cyber-attack, organisations (and potentially other connected data controllers affected by the breach) must report any personal data breach to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned, and in some instances they must also communicate the personal data breach to the data subjects themselves.

It is worth noting that an incident may be reportable even if data is not extracted or publicly released – unauthorised access to personal data constitutes a personal data breach under the GDPR and can trigger reporting obligations.

Penalties for non-compliance with data protection laws can be up to the greater of £17m/€20m or 4% of total annual worldwide turnover of the group.

The main cyber security threats

Ransomware, a form of malware, is now the biggest cyber threat to most businesses, including those in the life sciences industry. This malicious software is used to encrypt target data/information and disable access to systems, so that cybercriminals can extort a ransom in exchange for the decryption key.

Typically, ransomware attacks are delivered through phishing emails, that then enable attackers to gain access to the underlying network to deploy encryption software on the data assets. In combination with this, cybercriminals also often extract files and data/information that they can share with the target as proof of their control and access over the network. They also often threaten to release these files if the ransom is not paid.

This type of attack would paralyse most life sciences businesses, by disabling access to systems and data/information, preventing business as usual transactions, and threatening the security of underlying sensitive intellectual property. As a result, life sciences organisations often face the difficult discission of having to consider paying the ransom demands, often in cryptocurrencies that are almost impossible to recover at a later date.

When faced with the prospect of paying a ransom demand, careful consideration needs to be given to compliance with anti-money laundering regulations and international sanctions and counter-terrorism legislation. Most pharmaceutical regulators, including UK's Medicines & Healthcare Regulatory Agency (MHRA), are yet to confirm their stance on paying ransoms, but in many instances such payments are not illegal.

Other key threats include:

- Phishing: seeking to obtain information whilst appearing to be from a legitimate source or contact. These attacks can be used to target individuals (spearfishing) e.g., to appear to be a genuine email from a CFO requesting a revenue controller to make an urgent payment or to request sensitive payment details.
- Hacking: gaining access to systems via IT vulnerabilities to steal information, such as bank account details, or to obtain valuable intellectual property. There are also threats from hacking by individuals who hack systems as a "hobby", or to test and train their cyber skills.
- Data leakage: obtaining access to data and confidential information through vulnerabilities and unauthorised transmissions – these can occur through the sharing of unencrypted files, or

backdoors on websites. Data leaks by internal personnel, both by error and maliciously, also pose a threat.

Supply chain risks

When considering cyber vulnerabilities, it is imperative that the analysis covers all potential supply chain vulnerabilities. Whether that is collaboration partners, suppliers of internal systems, or other third-party service providers. These can often be easy and rewarding targets for cybercriminals, as gaining access to their environment may more easily allow access to multiple underlying end users. For example, in 2020 Blackbaud, a US cloud software provider, was subject to a cyber attack that impacted over 100 healthcare organisations, universities and charities and over 12 million patient records.

In order to assess these potential risks, it is important to gather relevant information, undertaking a detailed mapping exercise to understand what third parties are being engaged, the nature of the services they provide, what access they have to underlying data/information and financials, and what access and integrations there are into the organisation's systems (or systems of other suppliers). To kick off this mapping exercise, it can be helpful to work with finance and IT teams to run through each supplier engaged by the business.

This information can then be used to create a supply chain risk map, to categorise "high risk" suppliers and particular vulnerabilities.

The next step is to conduct a detailed review of the obligations and protections set out in each contract. For example, checking that the contracts impose adequate minimum-security requirements, rights to conduct penetration testing (where appropriate), and contain audit rights and security breach notification requirements. It is also important to consider the contractual allocation of risk and governance responsibilities, liability and exclusions, and gather information on reporting lines and key contacts.

In relation to new contracts (or renewals of existing contracts) now is a good time to ensure that procurement policies and standard templates - contracts, security requirements, governance schedules etc. - are appropriate and up to date.

In assessing and managing the supply chain risks, it is important to:

- document key contractual information, reporting obligations and contact details in an easily accessible format – in the event of a breach, it is vital to have this basic information readily to hand;
- ensure documented minimum-security requirements are kept under review to ensure they reflect industry best practice;
- maintain a dialogue with key suppliers to understand how they are taking action to mitigate evolving cyber risks;
- carry out security audits to ensure suppliers are complying with their security and data handling obligations,
- where relevant, carry out routine penetration testing on supplier systems and interfaces (or ensure suppliers carry out and report back on such testing); and
- include your key suppliers in your business continuity plans and get them to participate in continuity testing activities.

What should organisations in life sciences be doing to implement appropriate security measures?

Life sciences organisations should ensure that they have access to expert internal IT resources, and where relevant external specialists should be engaged to assist with implementing, monitoring, and updating technical security measures.

As a minimum, organisations should ensure that the following security fundamentals are implemented:

- carry out regular (or ideally real-time) back-ups of systems and data and implement continuity arrangements for failover support;
- monitor the network to check for suspicious activity or unauthorised access - typically using endpoint threat detection and response (ETDR) software;
- disable the use of removeable media such as USB memory sticks or ensure that systems force scans on them for malware;
- limit access controls to highly sensitive data, information, and systems to only those that need access to fulfil their specific role;
- regularly test networks and systems for vulnerabilities and test the interfaces and data exchanges with third parties;
- ensure staff are trained on cyber security, have read, and understood policies on the acceptable use of IT, and are aware of their own obligations to maintain the security and confidentiality of information and data assets and to report any potential breaches; and
- monitor key threats and updates, such as from the National Cyber Security Centre who publish threat reports (and provide other excellent resources and services).

Lifesciences organisation should also be cognisant of the fact that a lot of valuable know-how is often generated and stored on servers and networks at separate R&D and manufacturing sites that may use standalone IT systems. These should be included within the scope of any cyber security measures.

Cyber incident response planning

It is almost impossible to respond to, and mitigate the effect of, a cyber security breach or attack if you do not have adequate response processes and tools in place. However, the temptation is often to produce lengthy, detailed, policy documents and response plans. These can be useful reference points when checking security requirements or supplier assurance steps during a procurement process, but they aren't necessarily helpful on a Friday afternoon when an incident comes to light (and in practice, can be so cumbersome they are totally disregarded).

From our experience, to supplement any detailed policy document, organisations should ensure that they have a short "grab sheet" of no more than a couple of pages that documents the key information. This should set out contact details of who forms the initial response team - including details of external third-party specialists, such as forensic IT consultants and legal advisors – and a prioritised checklist of actions to initiate. This will ensure that the "first responders" can be mobilised quickly, and critical containment activities can be implemented without delay.

Bringing all of this together, set below are our top tips for incident response planning:

- produce a grab sheet, keep it updated, and keep it to hand;
- set up notification email addresses – one for reporting potential incidents, and one to cascade internal notifications;
- build a good relationship with an IT consultancy business that can deploy forensic IT specialists on immediate notice to assist with initial investigations and containment activities;
- engage external legal counsel on a retainer – you need to know a trusted legal advisor who can step in and support on critical incidents (and you don't want client/matter onboarding admin to delay their ability to respond and advise);
- ensure you understand any legal reporting obligations, such as to the Information Commissioner's Office (and other data protection regulators), including applicable timescales;
- raise awareness of cyber risks across the organisation by ensuring everyone has participated in relevant on-going training;

- ensure key stakeholders, and in particular those listed on the grab sheet, are trained on handling a cyber incident; and
- understand the terms of any insurance cover, including breach notification requirements (which should be noted on your grab sheet).

We are here to help

Cyber risks will continue to evolve at a rapid pace, and the risk levels in the UK are likely to remain high for the immediate future. Organisations in the life sciences sector therefore need to maintain their resilience to cyber-attacks, and ensure that their internal controls, governance, and planning are up-to-date and fit for purpose.

Should you wish to discuss any of the matters raised in this insight, or require assistance with reviewing and updating your organisational cyber security measures and response plans, please contact one of our experts and we will be happy to discuss further.

Our cyber security services

- Regulatory guidance
- Supply chain audits and risk mapping workshops
- Policy reviews and updates
- Bespoke training sessions
- Response planning – grab sheets and containment plans
- Incident management
- Advice on regulatory notifications

Simon Bollans
Partner
Commercial, Outsourcing & Technology
T: +44 20 7809 2668
E: simon.bollans@shlegal.com

STEPHENSON HARWOOD