Gallagher

Insurance | Risk Management | Consulting

RESILIENCE IN THE FACE OF RISING CYBER RISKS

A guide for life sciences companies

Adopting the right processes and technologies can help life sciences organisations innovate and become more competitive. However, in an evolving digital landscape, companies must be able to collect, share and analyse data while navigating the security challenges around personal information and intellectual property.

Over the last decade, digitalisation has enabled the life sciences sector to make significant improvements, providing a platform for transformational changes in how companies undertake drug discovery. However, as technology becomes more sophisticated, so do cybercriminals. Cybercrime is growing across the world and is a major threat for many companies.

Digital interactions have increased between companies, their supply chain and partners, ranging from email communication and video conferencing to sharing of commercially sensitive data. And, for entrepreneurs in the life sciences ecosystem, the advent of Artificial Intelligence (AI), wearable technology, analytics and real-world data has created a huge growth opportunity.

Through all of this change and innovation, life sciences companies find themselves balancing the need to move quickly and the need to operate safely.

The effect of COVID-19 on digital transformation

The COVID-19 pandemic accelerated the pace of digital transformation in the sector, with new norms emerging within a short space of time, such as home working and remote clinical trials. However, for life sciences companies, the fast pace of progress also had several side effects.

Before the pandemic, big pharmaceutical companies had already taken steps to protect themselves against cyber threats by investing heavily in cyber defences, cyber insurance and risk management, but were still comparatively slow on the uptake compared to other industries.

In its 2020 Annual review, the National Cyber Security Centre stated that at the peak of the pandemic, cyber attackers based overseas were targeting the life sciences sector using a variety of tools and techniques to gain access to intellectual property — ranging from formulation of products through to mechanisms of manufacture.[i]

The threats are not new but have intensified, and with all eyes on this sector at a critical time, it has affirmed these companies and their research work are critical to our national pandemic response infrastructure.

287 days

The average time it takes to identify a data breach.[ii]

80 days

The average time it takes to contain a data breach.[iii]

88%

The percentage of data breaches caused by **employee mistakes.**[iv]

17%

The percentage of **life sciences organisations** that we quoted purchased cyber insurance by quarter 4 of 2021.[v]

Companies can lose sight of their intangible assets such as data and intellectual property, and may not seriously consider the impact a cyber event would have on the company until it happens.

Clinical data — a valuable asset

Clinical trial data is one of the most critical forms of intellectual property generated by life sciences companies and is closely associated with a company's value. Therefore, protecting this data asset is of paramount importance.

At one end of the life sciences sector spectrum, large pharmaceutical companies retain control over many in-house functions governing IT services, data collection, specialist research and development services, and analytics. However, at the other end of the spectrum, start-up and early stages companies are reliant on a large number of third parties. This means that the smaller life sciences companies depend on systems and data that they themselves do not completely control, making them more vulnerable to a cyber event and putting their clinical trial data at risk.

What we have also seen is that smaller life sciences companies focus their budgets on acquiring talented staff and physical assets such as lab equipment and computers, while neglecting intangible assets such as data. This can lead to a 'cyber gap' in business continuity planning, with little or no protection against data breaches and other damaging cyber events.

In view of the importance of clinical trials data and the drive to digitise it, a company should consider the implications of the data being stolen or compromised following a cyber event to the extent that clinical trials will have to be repeated.

The consequences of a cyber incident

The disruption to a company's operations resulting from a data breach can be catastrophic — including interruption of research and development work, the loss of data or intellectual property, and regulatory fines for the organisation.

Theft of funds by electronic means is also on the rise, and increasingly, the subject of cyber claims. It can cause severe project delays as well as presenting the issue of having to explain the situation to your investors. Any kind of disruption, whether financial or operational, can have a knock-on effect on pre-agreed milestones, which are key drivers to securing ongoing funding.

Reputational damage can last far beyond any operational disruption, and so your company's preparedness for dealing with the fallout from a cyber event can be crucial to maintaining trust.

The importance of specialist cyber insurance

Cyber insurance is designed to provide financial protection from data breaches or cyber-attacks, and provide specialist support when a business needs it most, enabling companies to carry on operating with minimal disruption.

Historically, many general business insurance package policies contained a small but useful level of cyber insurance cover. However, as the threat landscape has evolved and the insurance market conditions hardened, many insurers have taken action to exclude all cyber-related losses from such package insurance products. Today, life sciences companies must purchase standalone dedicated cyber insurance policies in order to mitigate cyber-related threats.

With cyber insurance claims increasing in both frequency and severity, purchasing appropriate cyber insurance cover is now an essential part of successful business planning. Having this cover in place may prove vital in saving money and helping to safeguard your company's operations in the event of a cyber-attack or data breach.

How a cyber insurance policy works

Cyber insurance policies are typically divided into three sections: First Party, Third Party, and Cyber-crime. Most policies will cover Third Party, but there is usually the option of purchasing First Party and Cyber-crime cover. Here, we examine what cover each section might include, along with some examples.

First Party

This section of a cyber policy covers your company's own losses that arise from a cyber event, where this is typically defined as unauthorised system access, electronic attack or data breach. It includes the following:

- **Incident response costs:** This is a key cover consideration from a GDPR responsibility perspective and it covers the cost of responding to an incident in real-time, including forensic IT investigations, legal advice regarding data breaches, and the costs of notifying individuals whose data may have been compromised. Critically, the cover provides access to specialists, and it pays for the services they provide to the company in support of the incident response.
- **Cyber extortion:** This covers the company in the event a hacker steals data from your systems and then demands a ransom to prevent them from leaking the information. It includes reimbursement for any ransom payment made. Ransomware attacks are one of the fastest-growing forms of cyber-crime.
- **Operational risks:** Cyber Business Interruption covers the lost income as a result of a network disruption to your systems. Digital Asset Restoration covers the costs incurred by the company to restore affected data (classified as Digital Assets), after a breach or security compromise. Cyber Reputation Business Income Loss covers earnings loss or increased cost of working due to the loss of current or future customers within 12 months from the data breach or network interruption event.

First Party examples:

Company A: A cyber-attack led to the loss and corruption of research data held on company A's servers. As the company's backups were not segregated from the network, these were also compromised. The insurance policy paid the cost of a forensic investigation service and the cost for the research team to rework R&D project data.

Company B: Company B, a small clinic, discovered that an unauthorised third party had gained remote access to a server that contained electronic medical records. The third party posted a message on the server stating that the information on the server had been encrypted and could only be accessed with a password that would be supplied if the clinic made a ransom payment.

Company B worked with law enforcement and determined that the payment should be made. The payment constituted Cyber Extortion Monies under the cyber insurance policy and the ransomware sum was reimbursed to the clinic by insurers.

Company C: Company C discovered that an unidentified third party had uploaded files to their system, which allowed them to corrupt the company's information files. Data obtained included private, personally identifiable information, including credit card information. The third party made fraudulent charges on multiple accounts, and Company C was required to notify the affected individuals.

Given the discovery of the fraudulent charges, Company C offered affected individuals an opportunity to obtain credit monitoring. They also wanted to manage the breach in the media to demonstrate decisive, responsible action, so a public relations expert was brought in to assist.

The costs related to all of the above were covered under the Breach Response Costs section of Company C's cyber insurance policy.

Third Party

This covers liability where a legal action is brought against your company by a third-party that claims to have been adversely impacted by a cyber event emanating from your network.

Third Party example:

Company D: Company D suspected that its network had suffered a cyber-attack following a network outage. One of its employees casually shared this information with a third party that the company was collaborating with on an R&D project. Within a few days, the third party issued legal action against Company D for breach of confidentiality, alleging that they had failed to protect commercially sensitive information belonging to the third party, which it had shared with Company D as part of the R&D project.

The insurance policy paid the cost of a forensic investigation service, which demonstrated that there had not been a cyber-event and no confidential information had been shared outside of its protected network. It was established that the outage was in fact caused by an employee who had accidentally pulled out a cable in the server room. The third party legal action was retracted.

Cyber-crime

This covers the theft of your funds or assets through the manipulation or misuse by a third party of computer hardware, software programmes or systems.

It also extends to cover the theft of your company's funds or assets resulting from your company, or any financial institution acting on your company's behalf, having transferred the funds or other assets based on fraudulent electronic or telephonic communications that purport to have been communicated or sent by company employees, directors, customers or suppliers.

Cyber Crime example:

Company E: The finance officer of Company E received multiple emails and calls in quick succession — including emails from what appeared to be the company CEO – telling them to transfer funds to various accounts for the acquisition of another company. Pressured into acting quickly, the employee transferred the funds, losing the company thousands of pounds.

Whilst Company E had an operative cyber insurance policy, it did not purchase the cyber-crime extension, which is optional. Therefore, the claim was ultimately uninsured and their bank was also unable to recover the funds.

If the cyber-crime extension had been operative, Company E's claim could have been covered in full.

Improving your company's cyber resilience

It is important for life sciences companies to address the contrast between investment in science innovation and investment in the protection of data and intellectual property. Strengthening an organisation's digital armour means developing a greater understanding of cyber risk and how to reduce exposure to cyber threats.

Here are some key action points to help your company improve its cyber resilience:

1. Purchase a Cyber Insurance policy.
2. Evolve the role of the Chief Information Security Officer within your company.
3. Enable Multi-Factor Authentication across all email accounts for remote access.
4. Implement an ongoing staff cybersecurity training regime.
5. Know your operations — understand how to back up and restore critical data at speed and scale across the business, and strive for continuity of operations.
6. Establish a robust recovery plan and test it at regular intervals.
7. Undertake regular network resilience testing for greater response speed and agility.

How Gallagher can help

Gallagher's Cyber Risk Management Practice can support you throughout the entirety of the cyber resilience journey, which starts with a free 30-minute consultation.

We use a multi-faceted strategy to ensure your company is armed against cyber threats. This typically begins with an audit of your company's IT infrastructure to identify weaknesses or vulnerabilities and how to remedy them. This is a comprehensive overview to help you have the confidence to what risks are known. The benefit of this insight is that your organisation can gain clarity on what to do next.

Our aim is to improve your cyber strategy, defences and ability to recover from a cyber event. We do this through the implementation of processes and procedures, such as the design of board-level reporting templates.

We also help organisations gain information security standards such as Cyber Essentials, Cyber Essentials Plus and IASME Governance.

Would you like to talk?

Rebecca Lambton-Heys

Business Development Executive – Life Sciences Practice

D: +44 (0)207 375 9102
M: +44 (0)784 961 4383
E: Rebecca_LambtonHeys@ajg.com

[i] https://www.ncsc.gov.uk/news/annual-review-2020
[ii] https://www.ibm.com/security/data-breach
[iii] https://www.varonis.com/blog/data-breach-statistics/
[iv] https://www.influencive.com/human-error-is-still-the-number-one-cause-of-most-data-breaches-in-2021/
[v] Gallagher benchmarking data collected between 01.01.2021 – 30.09.2021

ARTUK-2952

Gallagher
Insurance | Risk Management | Consulting