backbone secure

Life science real estate

Data security and cyber security in life sciences buildings

2024 white paper supported by Backbone secure

simplybackbone.co.uk

Life science real estate -
Where science meets real estate

At Life Sciences Real Estate, we are dedicated to bringing science and real estate closer together. Our expertise lies in delivering independent research, insightful market analysis, and cutting-edge data tools to empower decision-making.

What we offer:

- Biweekly research and market analysis: stay ahead with our exclusive, subscriber-only biweekly reports, offering the latest insights and trends in life sciences real estate.
- Premier events: our journey began with the inaugural event at Leiden Bio Science Park on 8 November 2022, followed by successful gatherings at Potsdam Science Park on 9 May 2023, in London on 24 May 2023, and in Leeds on 7 November 2023. This White Paper was launched at our event in London on 24 October 2024.
- Innovative data tool: unveiled in August 2024, our groundbreaking data tool illuminates over 700 life sciences real estate deals across the UK and Europe, providing unparalleled insights and analytics for industry professionals.

> The consequences of a cybersecurity breach in the life sciences sector are profound, with potential damages reaching into the trillions.

backbone secure

Contents

Executive summary

The life sciences sector, encompassing research, production, distribution, and point of care facilities, is at the forefront of global innovation but also faces significant risks in terms of data security and cybersecurity.

As the sector undergoes rapid digital transformation, the volume and complexity of data generated, stored, and transmitted across multiple platforms, including public clouds and IoT devices, have dramatically increased. This heightened complexity introduces substantial vulnerabilities that can be exploited by malicious actors, making robust cybersecurity and data protection strategies critical for the sector's resilience and long-term success.

Life sciences buildings house the critical infrastructure and personnel that manage and utilise sensitive data, such as intellectual property (IP) and patient health records. These facilities contain the networks, devices and possibly the on-site servers where this data is stored, accessed, and protected. These types of data are prime targets for cyberattacks. The theft or manipulation of this data can lead to severe financial losses, compromised research integrity, and significant disruptions in healthcare delivery. For instance, the unauthorised access to a new drug's chemical formula can result in counterfeit production, undermining years of research and investment and causing reputational damage.

Moreover, the sector's propensity for mergers and acquisitions (M&A) often leads to the accumulation of legacy systems, which may further complicate the security landscape by introducing outdated or incompatible technologies into critical environments.

The consequences of a cybersecurity breach in the life sciences sector are profound, with potential damages reaching into the trillions. The healthcare and pharmaceutical industries experience higher than average breach costs (according to IBM Security[1]).

Key cybersecurity threats in the sector include disruption, sabotage, data theft, and system manipulation. Many of these breaches involve shadow data - information that exists outside the central data management framework - making it a particularly insidious threat due to its often unmonitored and unprotected status.

To combat these threats, life sciences organisations should implement a comprehensive cybersecurity strategy that includes both preventive and responsive measures. These strategies should encompass data encryption, access controls, regular security audits, and employee training to mitigate human error, a common cause of breaches. Additionally, organisations should invest in advanced cybersecurity tools, such as Security Information and Event Management (SIEM) systems, to monitor and respond to threats in real-time.

In conclusion, the life sciences sector should prioritise cybersecurity as an integral part of its operations. By adopting a proactive and layered security approach, organisations can protect their critical data, maintain regulatory compliance, and safeguard their reputation and financial stability in an increasingly connected and digital world. The stakes are high, and the cost of inaction could be catastrophic, not only for individual organisations but for the broader healthcare ecosystem and society at large.

Introduction

> "There are two types of companies: those that have been hacked, and those who don't know they have been hacked."
>
> **John Chambers**, former CEO of Cisco Systems

Business background

Digital transformation increases the need for robust data governance as enterprises create and store more data across complex environments, including public clouds and Internet of Things (IoT) devices. This complexity raises the risk of cyberattacks and complicates monitoring and security. Rising consumer awareness and privacy regulations, such as GDPR, underscore the importance of data protection, and non-compliance can result in significant fines. Protecting trade secrets, intellectual property and personal data is crucial for ensuring profitability and maintaining consumer trust.

The life sciences sector has two features that increase vulnerability:

1. M&A activity[2]
2. Tendency to outsource

M&A activity: mergers and acquisitions are very common but also pose a major risk to confidential data if the process is not managed effectively. Common risks involved during a merging/ acquisition process include:

- Integrating separate IT environments is a complex process that requires careful planning and due diligence. Poorly executed integrations can create vulnerabilities in the IT infrastructure, creating opportunities for cybercriminals to strike.
- Merging different companies creates new compliance risks and data protection considerations as different companies may have different procedures or be less up to date with regulatory requirements than the other.
- Mergers may also run into cultural differences when it comes to differing cyber security postures and approaches to risk management[3].

Outsourcing: life sciences companies are working with external organisations in important areas such as research and development, manufacturing (i.e. CDMOs/CMOs), supply chains, clinical trials and more. This increases the vulnerability to attack because these organisations may have access to areas in the company's systems4. Increase in third-party service providers, including law firms, accounting firms, and IT service providers. These external parties may have access to sensitive data, creating additional cyber security risks.

How bad could the damage be?

To the question, how bad could it be the answer is "very bad indeed". The magnitude of the disruption cause by a systemic cyberattack in the pharma sector is estimated in the trillions and considered worse than a financial crisis, according to McKinsey[5]. In the World Economic Forum's survey of global risks[6] by severity over the next two years, cyber security is ranked fourth, ahead of interstate armed conflict which is ranked fifth.

Figure 1 Global risks ranked by severity over the short term (two years).

1. Misinformation and disinformation
2. Extreme weather events
3. Societal polarisation
4. **Cyber insecurity**
5. Interstate armed conflict

(Source: World Economic Forum)

Data breaches and failure to comply with regulatory requirements can all result in reputational damage, compromised intellectual property, loss of revenue, and fines for noncompliance. Under the European Union General Data Protection Regulation (GDPR), data breaches can lead to fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher)[7]. The EU Network and Information Security Directive (NIS-2) is also relevant. It became

applicable from 18 October 2024 and allows fines of €10 million or 2% of annual worldwide turnover (whichever is higher). Under NIS-2, certain kinds of incidents within much shorter deadlines than GDPR, in some cases within 24 hours. The UK Government has also announced that it will be strengthening its cyber laws and will soon put forward the Cyber Security and Resilience Bill. It aims to reduce the impact of cybersecurity issues within the healthcare supply chain.

A cyber lockdown of drug manufacturing facilities or medical device commercial operations could irrevocably cripple competitiveness of an organisation[8].

The attack surface for attacks on personally identifiable information (PII) has expanded recently by the industry's efforts to improve the patient experience with wearable medical technology devices and personalised, smart medication. This type of attack can leave a life sciences enterprise reputationally injured and potentially subject to financial loss associated with damage to the corporate brand, regulatory fines, restitution and legal fees[9].

The total cost of a data breach is increasing, according to IBM Cost of a Data Breach Report 2024 (released in August 2024) and now stands at $4.88 million. Organisations using multi-cloud environments are the least secure, with breaches in these environments being the costliest[10].

There are four cost components: lost business cost (30%); detection and escalation (33%); post-breach response (28%); notification (8%)[11].

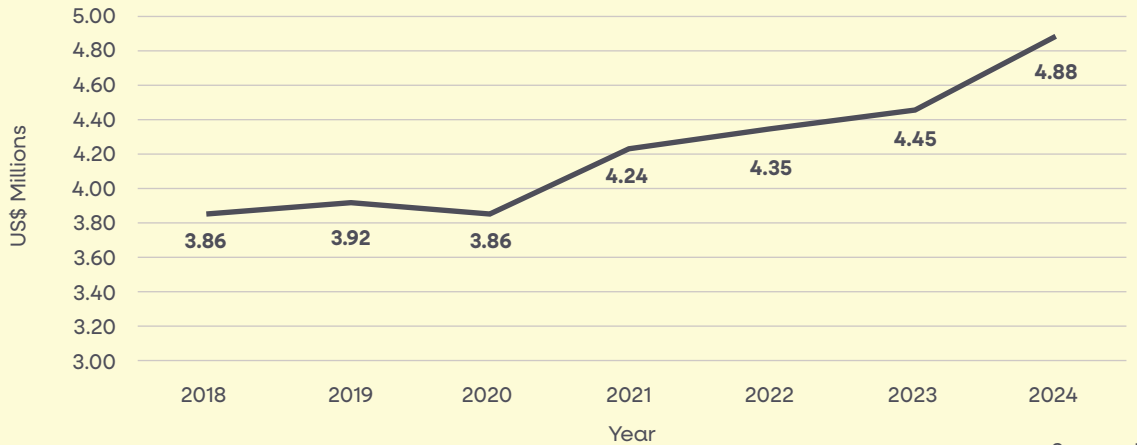
Customer data and intellectual property are the most frequent data targets[12]. 35% of breaches involve shadow data (any organisational data that exists outside the centralised data management framework. This includes data that has been copied, backed up, or stored in a manner outside the framework. This elusive data may not adhere to access control limitations or be visible to monitoring tools. Shadow data is the ultimate 'known unknown'. You know it exists, but you don't know where and what it is exactly[13].

There are six distinct types of threat[14]:

1. Disruption: intentional temporary impairment of the accessibility of data, information systems or information services.
2. Sabotage: intentional and very long-lasting impairment of the accessibility of data, information systems or information services, possibly resulting in destruction.
3. Data manipulation: impairment of the integrity of information by means of the intentional editing of data.
4. Data theft: impairment of the confidentiality of information by means of the copying or removal of data.
5. System manipulation: impairment of information systems or information services targeting the confidentiality or integrity of these systems/services. These systems or services are subsequently used to conduct other attacks.
6. Breakdown/failure: impairment of integrity or availability due to natural causes, technical difficulties or human error.

As the cost of breaches increases, the value of cybersecurity software increases too; Google is eyeing a $20+ billion investment in a cybersecurity startup called Wiz[15].

Figure 3: The components of data security and ccyber security



Source: IBM Security

Life sciences buildings

> "In life sciences, cyberattacks can have consequences far beyond financial loss - they can undermine the trust and safety of entire healthcare systems."
>
> **Theresa Payton**, former White House CIO and cybersecurity expert

Buildings in the life sciences sector fall into four distinct categories: research and development (R&D), production, distribution, and point of care. Each category requires specific types of facilities that support their unique functions.

R&D

Research and development facilities are the backbone of innovation in the life sciences sector, focusing on the creation and validation of new products and technologies. These facilities include biotech and pharmaceutical laboratories, university research labs, clinical trial centres, and diagnostic laboratories. They are designed to support scientific research, product development, and clinical testing.

For instance, BioNTech's lab in Mainz, Germany is renowned for its groundbreaking work in mRNA technology, particularly in the development of the COVID-19 vaccine. Similarly, the Medical University of Vienna, one of Europe's oldest medical schools, exemplifies the role of academic institutions in pioneering medical research. Drapers Yard in Leeds, operated by Fortrea, is a key example of a clinical trial centre, while Diagnostyka in Poland stands out as the largest network of medical labs in the country, performing millions of analyses annually.

Production

Production facilities are dedicated to the manufacturing of life sciences products, including pharmaceuticals, biologics, and medical devices. These facilities are equipped with production lines, clean rooms, and quality control areas, adhering to stringent regulatory standards.

For example, GSK's plant in Dungarvan, Ireland, is where Panadol, a widely used pain relief medication, is produced. In Switzerland, Lonza Biologics in Visp specialises in the production of biologics, including cell and gene therapies. Medtronic's manufacturing plant in Mirandola, Italy, is another notable facility, focusing on the production of kidney care devices.

Movianto's distribution warehouse in Warrington, UK (source: Movianto)

Distribution

The distribution phase involves specialised facilities that ensure the safe and efficient movement of life sciences products from manufacturers to the point of care. These facilities include cold-chain distribution centres, medical supply warehouses, and pharmaceutical logistics hubs, all of which are essential for maintaining the integrity of products, especially those requiring temperature control.

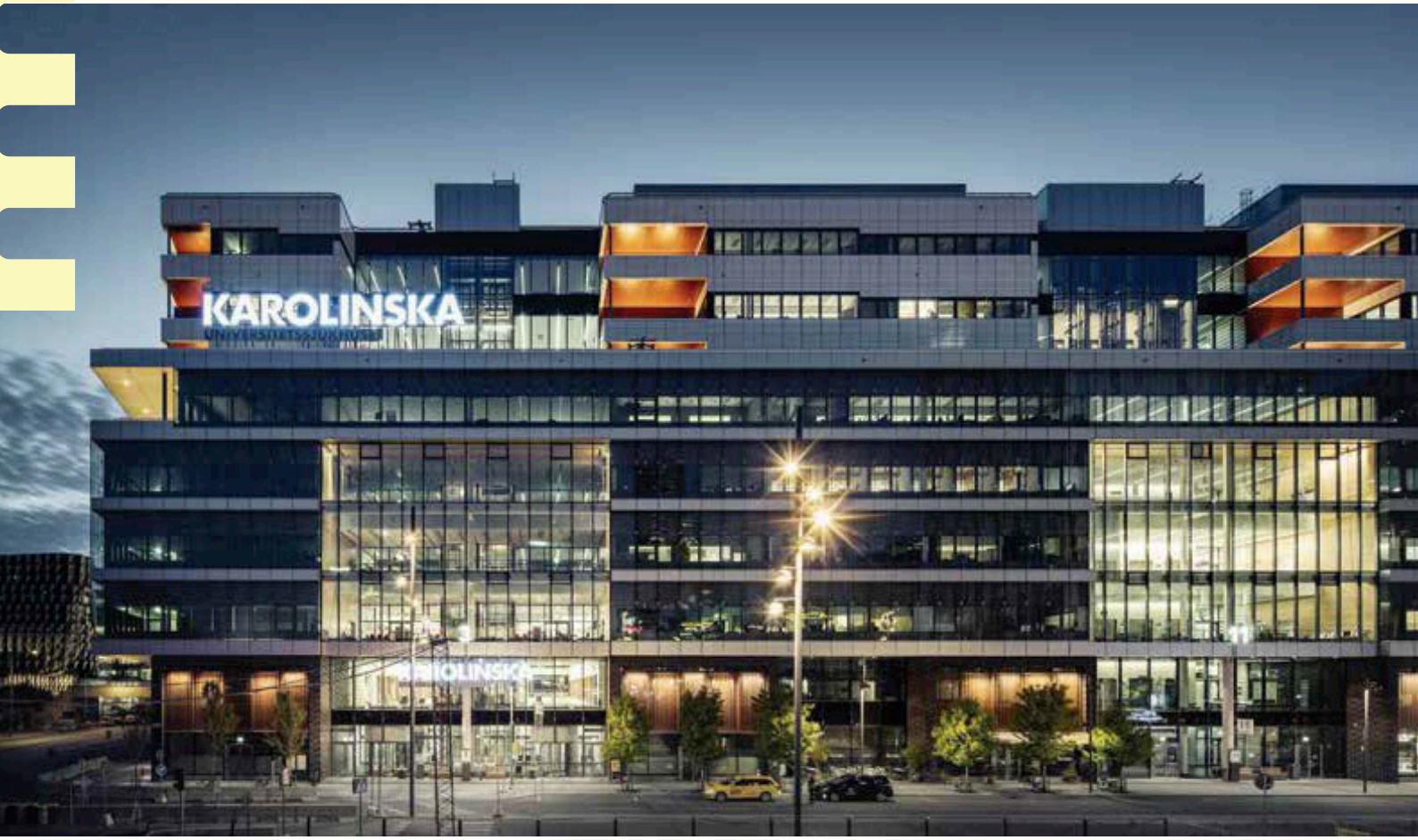
Logistics4Pharma in Frankfurt is an example of a cold-chain distribution centre, providing advanced temperature control at Frankfurt Airport. Movianto in Warrington, UK, serves as a critical supply chain partner for the pharmaceutical and biotech industries, while UPS Healthcare's hub in Roermond, Netherlands, offers extensive storage capabilities for pharmaceuticals, particularly those needing strict temperature management.

Point of care

Point of care facilities are where direct healthcare services are provided. These facilities are equipped with clinical spaces, patient care rooms, and dispensing areas, and they play a crucial role in delivering healthcare directly to patients.

Karolinska University Hospital in Stockholm, for example, is known for its advanced medical treatments and research collaborations. Clinique du Parc in Lyon offers outpatient surgery and medical imaging services, demonstrating the importance of outpatient care centres. Boots is the UK's largest pharmacy chain with over 2,000 outlets, of which 70 have a reinvented healthcare area16. (In the UK, people with seven common ailments such as earache can now go into a chemist to be assessed, rather than making an appointment with their doctor.)17

These examples from across Europe illustrate the diversity and specialisation of facilities within the life sciences sector, each contributing to the overall healthcare ecosystem by supporting the lifecycle of life sciences products from inception to patient care.



Karolinska University Hospital in Stockholm (source: White Arkitekter)

The need for data and cyber security

A shocking “near miss” in Florida in 2021 illustrates the need for security. A hacker got inside a water treatment system and adjusted the level of sodium hydroxide, or lye, to more than 100 times its normal levels. The breach could have been catastrophic had it not been caught in time18. Outmoded tech can provide hackers with an easy entrance point onto an otherwise sophisticated network. In this instance, an old PC running Windows 7 with no firewall enabled a hacker to gain access. This is just one of many examples: the 12 most common types of cyberattack are listed here19.

Here are examples from the four different types of life science building:

R&D examples[20]

Dr. Reddy’s Laboratories (2020): during the COVID-19 pandemic, Dr. Reddy’s Laboratories experienced a significant cyberattack, forcing the shutdown of data centres and production facilities globally. The attack targeted clinical trial data for the Sputnik V COVID-19 vaccine. Dr. Raddy’s is a multinational pharmaceutical company based in Hyderabad.

Irish health service: on 14 May 2021, the Irish health service was the victim of a nationwide ransomware attack. Patient care was disrupted across 4,000 locations, including 18 cancer clinical trials units. The effect of the attack on referrals and enrolment to trials was marked, resulting in a drop of 55% in recruitment of volunteers[21].

UK Government Survey (2024)[22]: higher education institutions are frequently targeted by cyberattacks, including unauthorised access, denial of service attacks, and ransomware. 97% of higher education institutions identified breaches or attacks in the last 12 months, compared with 50% for all UK businesses[23].

Production

Pfizer/BioNTech and AstraZeneca (2020): both companies were targeted by cyberattacks during their COVID-19 vaccine development efforts. The European Medicines Agency reported unlawful access to documents related to the Pfizer/BioNTech vaccine, and North Korean hackers attempted to infiltrate AstraZeneca’s systems.

Merck (2017): the NotPetya malware attack spread through Merck’s network, disabling around 30,000 computers and halting operations for weeks. The estimated damage was around $870 million.

Cencora Cyberattack (2024): in February this year, Cencora, Inc. suffered a cyberattack impacting at least 27 pharma and biotech clients, leading to data exfiltration and significant disruptions for companies including Bayer and Novartis[24]. Cencora is drug wholesaler company and contract research organisation (CRO).

Distribution

Truepill (2023): personal and sensitive health information was stolen during a cyberattack at Postmeds, the parent company of online pharmacy startup Truepill. The online pharmacy fulfilment company fills prescriptions for bigname telehealth services and other pharmacies and mails medications to their customers[25].

To quote Dutch cold chain experts: “The risk that a European cold storage business might face a fire incident is 1 in 8,000, the risk of being burgled is 1 in 250, but the chance of being subjected to a serious cyberattack is 1 in 5.”[26]

Point of care

In June 2024 major hospitals in London declared a critical incident after a cyberattack a cyberattack on Synnovis, a provider of pathology services, led to operations being cancelled and emergency patients being diverted elsewhere.

UnitedHealthcare (2024)[27]: pharmacies across the United States experience disruptions following a hack at UnitedHealth's (UNH.N) technology unit, Change Healthcare. A ransomware gang took files containing personal data and protected health information. The company said that the attack may "cover a substantial proportion of people in America."[28]

Canadian pharmacy London Drugs had to shut its outlets for several days following an attack earlier this year[29].

The bad actors and their actions

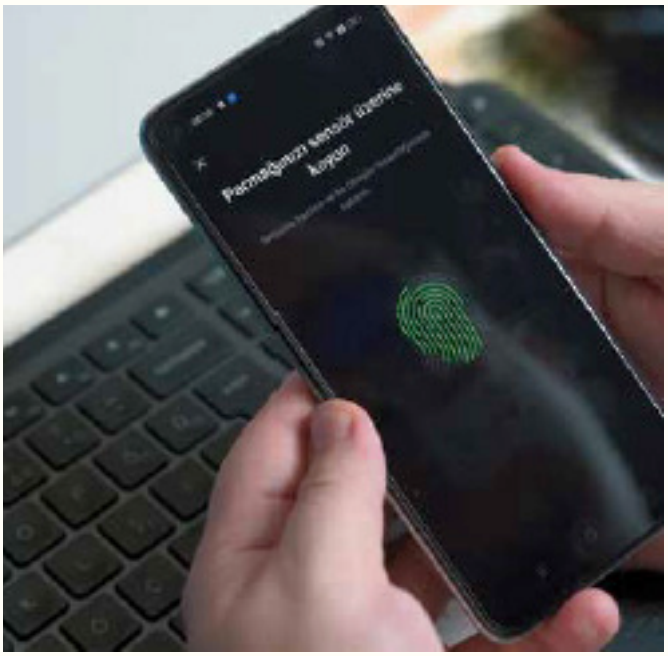
Across all sectors, external actors were responsible for 83 per cent of breaches, while internal ones account for 19 per cent[30]. Internal actors are not only responsible for intentional harm in these cases, but they are also likely to be responsible for errors. The most expensive data breaches are caused by malicious insiders[31].

Classification of cyber threat actors

In contemporary cybersecurity, threat actors are typically categorised into three main groups: external threats, internal threats, and strategic adversaries.

1. External threat actors originate from outside an organisation, lacking insider access. These include cybercriminals motivated by financial gain and hacktivists using cyberattacks for political or social causes. These threat actors often employ widespread attacks to exploit common vulnerabilities.
2. Internal threat actors come from within an organisation, either intentionally or unintentionally. These include disgruntled employees who misuse access for personal gain or revenge and negligent user who compromise security through carelessness or lack of training. Internal threats are dangerous due to their authorised access and insider knowledge.
3. Strategic adversaries are sophisticated actors engaged in long-term, targeted campaigns. These include corporate espionage groups who seek to steal intellectual property for market advantage. Characterised by patience, resources, and advanced techniques, these adversaries pose significant challenges to defend against.

Understanding these categories helps organisations develop comprehensive cybersecurity strategies addressing the full spectrum of modern digital threats.



How do they get in?

The top access routes[32] are:

1. Web application
2. Email
3. An unprotected device

For the attack on Ireland's health system in 2021 (mentioned above under R&D), the source of the cyberattack was an employee opening an Excel file that was attached to a phishing e-mail sent two months before. The workstation's antivirus software was set to monitor mode and consequently did not block the malicious commands. The attack triggered the critical incident process within the health system resulting in the shutting down of all HSE connected devices - over 1,000 applications.

What do they do when they are in?

1. Basic web application attacks: these attacks are against a Web application - "get in, get the data and get out" pattern.
2. Denial of service: these attacks are intended to compromise the availability of networks and systems.
3. Lost and stolen assets: where information goes went missing, whether through misplacement or malice.
4. Miscellaneous errors: incidents where unintentional actions directly compromised a security attribute of an information asset fall into this pattern.
5. Privilege misuse: unapproved or malicious use of legitimate privileges.
6. Social engineering: the psychological compromise of a person to alter their behaviour into taking an action or breaching confidentiality.
7. System intrusion: complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying ransomware.

R&D and production

R&D and production facilities in the life sciences sector are highly targeted by cybercriminals due to the sensitive and valuable data they handle, including intellectual property and production processes. These facilities are particularly vulnerable to system intrusions, where attackers exploit network vulnerabilities to gain unauthorized access. Such breaches often lead to ransomware attacks, with critical data encrypted and held hostage until a ransom is paid.

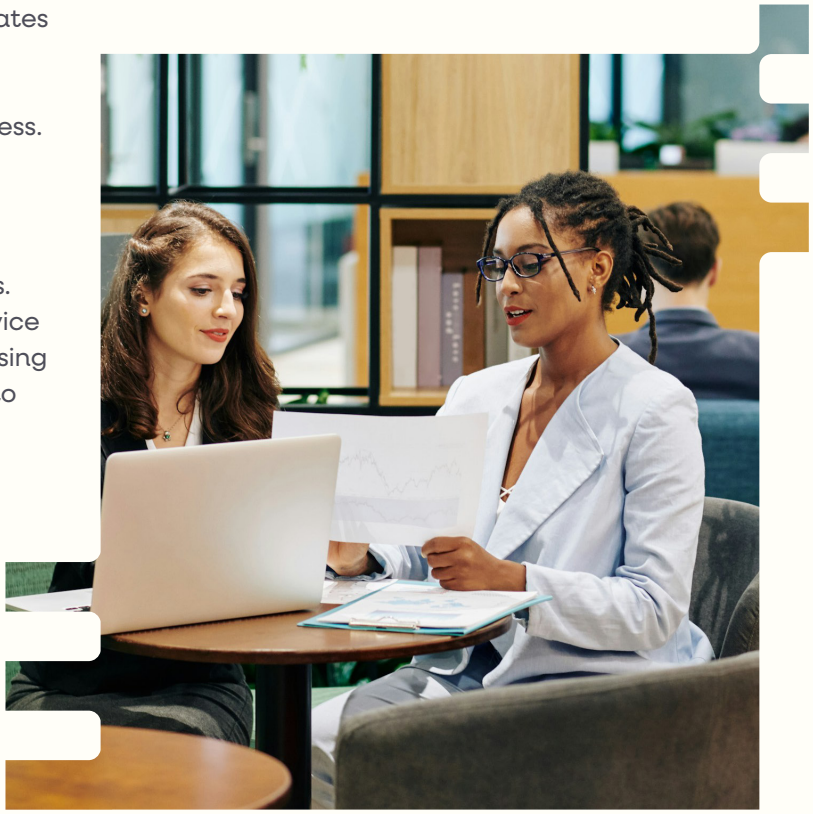
Basic web application attacks are also common, targeting the software platforms used for research collaboration in R&D and for managing production schedules. These attacks can disrupt operations, steal data, or serve as entry points for further exploitation. Social engineering further exacerbates these threats by manipulating employees into revealing credentials or executing malicious software, granting attackers deeper system access.

External actors, primarily motivated by financial gain, are the main culprits, though espionage is a significant concern in R&D, where intellectual property theft can have profound consequences. Additionally, the growing threat of Denial of Service (DoS) attacks in production highlights the increasing risk to operational continuity, as attackers seek to disrupt manufacturing processes.

Distribution

The distribution phase, involving warehouses and logistics hubs, mirrors the broader supply chain in its cybersecurity vulnerabilities. Ransomware attacks are particularly dangerous, with cybercriminals encrypting critical systems and demanding ransom, which can severely impact the delivery of sensitive products like vaccines. Attackers may also compromise less secure parts of the supply chain - such as suppliers or logistics providers - to gain access to more secure core systems.

The reliance on IoT devices33 and automation in distribution centres introduces new vulnerabilities, where hijacked devices can disrupt operations or serve as entry points for broader cyberattacks.



Point of care

Healthcare facilities, including hospitals, clinics, and pharmacies, are frequent targets due to the sensitive personal and medical data they handle. System intrusions, particularly ransomware, are the most common method of attack, where patient data is encrypted and ransom demanded for decryption. Basic web application attacks exploit vulnerabilities in clinical systems, while miscellaneous errors like incorrect delivery or insider misuse also pose significant risks.

Healthcare facilities face specific threats from internal actors, who may inadvertently or maliciously compromise patient data. While financial motives dominate these attacks, some breaches are driven by ideological or personal motives, such as disgruntled employees seeking revenge.

These overlapping threats across different types of life science building highlight the need for robust, integrated cybersecurity strategies for each stage of the product lifecycle.

Figure 3: The components of data security and ccyber security

The components of data security and cyber security[34]

In life sciences buildings, both data security and cyber security are critical to safeguarding sensitive information, ensuring uninterrupted operations, and maintaining trust between research institutions, healthcare providers, and patients. Data security encompasses the full spectrum of practices and technologies designed to protect digital information from unauthorised access, corruption, theft, or loss throughout its lifecycle. These measures include physical and administrative controls, as well as technical solutions like data encryption and backup strategies, all aimed at ensuring data integrity and confidentiality.

Security management: aligning people and processes to enhance security posture, foster maturity and ensure business resilience.

Identity protection: verifying identities to track data access and usage. Multi-factor authentication password-less access and single sign-on access controls limit the blast radius of attacks.

Threat defence: proactively safeguarding endpoints, applications, identities and data, while continuously monitoring for and responding to threats.

Data security: understanding data usage and implementing measures to prevent data loss and ensure compliance.

Device compliance: ensuring all devices accessing data, whether personal or company-owned, comply with security standards and providing secure access.

Network security: securing connections within the business and safeguarding data flow across networks forming the backbone of overall security.

In summary, while data security zeroes in on protecting information, cyber security is a broader concept that extends to shielding networks, systems, and applications from a wide range of potential threats.

Strategy for managing the risks

> "The biggest cyber risk businesses face is not from hackers outside of their company, but from complacency within their company."
>
> **John Edwards,** UK Information Commissioner[35]

Eight essential guidelines

The data and cybersecurity needs in R&D, production, distribution, and point of care buildings in the life sciences sector, while distinct, share significant overlap. The eight-point unified strategy below outlines essential measures to protect these critical environments.

1. Adopt a zero-trust cyber environment

Always verify access, all the time, for all resources[36].

2. Improve staff cybersecurity literacy

Education and training: equip staff with cybersecurity knowledge beyond compliance, focusing on proactive threat identification and response.

Regular updates: ensure all devices, particularly those involved in remote work, are consistently updated with the latest security configurations.

3. Use advanced cybersecurity technologies

AI and predictive analytics: use AI to detect anomalies and predict potential cyber threats, especially in distribution networks.

Smart technologies: deploy secure RFID, blockchain[37], and IoT solutions to enhance visibility and traceability across all facilities.

4. Enforce strict access controls

Mandatory multi-factor authentication (MFA): implement MFA across all systems to safeguard access, especially with the rise of remote work.

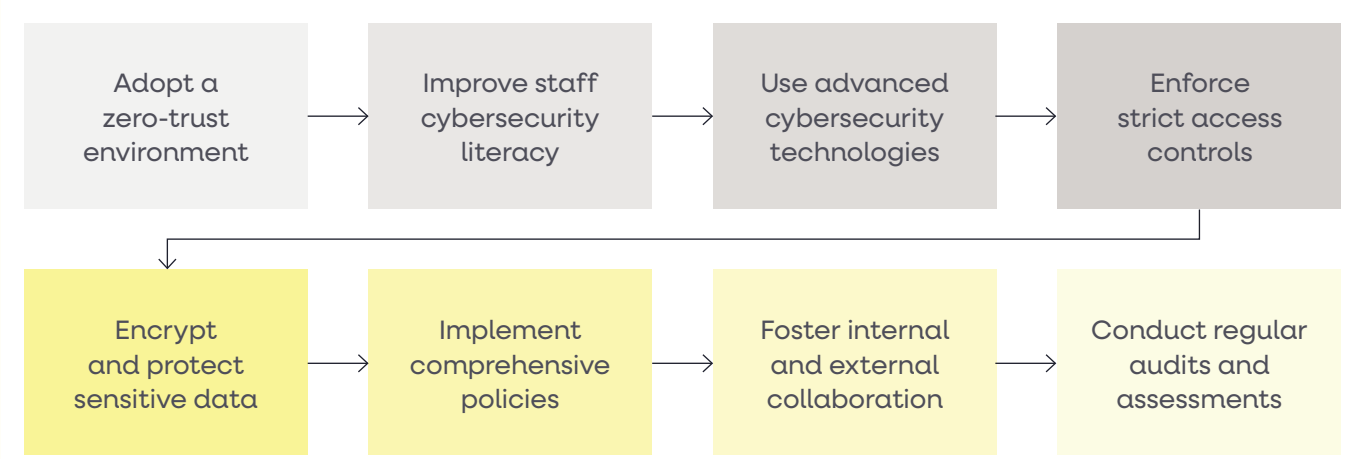
Device management: authenticate and monitor all network-connected devices, ensuring secure updates and preventing unauthorised access.

5. Encrypt and protect sensitive data

Data encryption: encrypt all sensitive data, including genomic and patient information, during transmission and storage.

Regulatory compliance: align with evolving cybersecurity regulations, ensuring prompt application of security patches without compromising product quality.

Figure 3: The eight essential risk management guidelines



6. Implement comprehensive cybersecurity policies

Clear policies: establish and enforce robust policies on log-in protection, password management, and incident reporting across all facilities.

Incident response: maintain a well-communicated and regularly updated incident response plan to handle breaches effectively.

7. Foster internal and external collaboration

Internal collaboration: foster coordination between IT, cybersecurity, and operational teams to embed cybersecurity into daily operations.

External collaboration: engage with suppliers, manufacturers, and regulatory bodies to uphold shared cybersecurity standards.

8. Conduct regular audits and assessments

Audits: conduct regular audits to identify and address vulnerabilities.

Continuous risk assessments: adapt to emerging threats through ongoing risk assessments, ensuring the cybersecurity strategy remains robust and effective.

By implementing these strategies, life sciences buildings can better protect against data breaches and cyber threats, ensuring the security of sensitive data throughout all stages of operation.

The eight guidelines need to be applied in an adaptive way, one that can be flexed

as a company's operations grow rather than one that is brittle and designed to tackle a particular incident in the past.

Speed of detection and response is of the utmost importance. There is a "golden hour" between the moment a threat actor gains access and before the attack can break out from one single device to infect the wider system. This can be compared to a race to the finish line between the intruder and the security team[38].

SOC it to me

A security operations centre (SOC) is considered the gold standard in cyber security. This centralised facility employs cyber security engineers and automated technologies to monitor, detect and respond to incidents and threats. It brings a unified and proactive approach to cyber security – offering the highest level of protection. However, it can be difficult and costly for regulated industries to bring the right specialist talent in-house and build the IT infrastructure required. Some may be caught in a 'halfway house', trying to do their best in-house while not reaching the cyber security maturity demanded by their sector.[39]

Who are the good guys?

Every team member has a role but security teams (internal or otherwise) and senior management are particularly important.

"Globally, security teams are doing a much better job of detecting and containing breaches, despite a stubborn skills shortage"[40], a notable result given that burnout in cybersecurity teams is seen as an issue[41].

Senior management has a key role to play too. A 2023 article from Harvard Business Review42 emphasises the crucial role of senior management and the board in effectively governing cyber risk, especially in light of new SEC cybersecurity rules. It highlights that as technology becomes more integrated into organisations, the complexity of cyber threats increases, making it essential for boards to actively engage in cybersecurity governance.

The SEC mandates that companies disclose their cyber-risk governance, which includes board oversight and the role of management in handling cyber risks. The article outlines four key areas where boards should focus: aligning cyber risk management with business needs, continuously monitoring cyber risk capabilities, proactively anticipating changes in the threat landscape, and positioning cybersecurity as a strategic business enabler. These guidelines ensure that cyber risks are not only managed effectively but also aligned with the company's overall strategic objectives, thereby safeguarding both short-term and long-term shareholder value.

Conclusion

The intersection of life sciences and real estate presents unique challenges, particularly in the realm of data security and cybersecurity. As the life sciences sector continues to innovate and expand, it faces an increasingly complex threat landscape that demands robust and adaptive security strategies. The four categories of life sciences buildings - R&D, production, distribution, and point of care - each play a critical role in the lifecycle of scientific products and services, and each has its own specific vulnerabilities that must be addressed.

The eight-point strategy outlined in this paper provides a comprehensive approach to managing these risks, emphasising the importance of a zero-trust cyber environment, enhanced cyber literacy, and rigorous access controls. These measures are not just theoretical; they are practical steps that can be implemented across all types of life sciences facilities to safeguard against a wide array of cyber threats.

For R&D buildings, the focus on strengthening access control and authentication is particularly critical. These facilities are the epicentre of innovation, handling sensitive intellectual property that,

if compromised, could lead to significant financial and reputational damage. Multi-factor authentication, secure device management, and network segmentation are essential in ensuring that only authorised personnel have access to critical data and systems.

- In production facilities, the need for enhanced cyber literacy and proactive measures cannot be overstated. The production phase is where the theoretical becomes tangible, and any disruption here can have cascading effects across the entire supply chain. Employees must be trained not just to follow protocols but to actively identify and mitigate potential threats. A compliance-driven approach is no longer sufficient; the dynamic nature of cyber threats requires a proactive stance.
- Distribution and warehouse facilities, meanwhile, should leverage advanced technologies and AI to maintain the integrity of the supply chain. These facilities ensure that products reach their destination intact and on time. By implementing smart technologies such as RFID, IoT, and predictive analytics, these facilities can pre-emptively address potential cybersecurity risks.
- Finally, point of care facilities should develop and implement comprehensive cybersecurity policies. These are the frontline of healthcare delivery, where patient data is most vulnerable. Clear policies on data handling, access control, and incident reporting are essential to protect sensitive information and maintain patient trust. Additionally, regular training and drills are necessary to ensure that all staff are prepared to respond to potential cyber threats.

The stakes in the life sciences sector are high. A breach in any one of these facilities could have far-reaching consequences, not just for the organisation involved but for the broader healthcare ecosystem and society at large. As such, cybersecurity should be treated as a top priority, integrated into every aspect of life sciences operations. By adopting a proactive and layered security approach, life sciences organisations can protect their critical data, maintain regulatory compliance, and safeguard their reputation and financial stability in an increasingly connected and digital world.

In summary, while each category of life sciences buildings faces distinctive challenges, the strategy outlined in this paper offers a cohesive framework for mitigating these risks. By giving special attention to the specific needs of R&D, production, distribution, and point of care facilities, the life sciences sector can build a resilient defence against the ever-evolving threat landscape, ensuring the security and success of its operations now and in the future.

Glossary

1. **Attack surface:** refers to the total sum of all the points where an unauthorised user (the "attacker") can try to enter data to or extract data from an environment. This includes all hardware, software, networks, and external services that interact with your environment, which could be potential targets for cyberattacks.
2. **Basic web application attack:** an attack that targets vulnerabilities in web applications. These attacks aim to steal data, disrupt services, or gain unauthorised access to systems.
3. **Brute force:** a method used by attackers to gain unauthorised access to a system, account, or network by systematically attempting all possible combinations of passwords or encryption keys until the correct one is found. It is a trial-and-error approach that rapidly generates and tests multiple possible combinations.
4. **CISO:** chief information security officer
5. **CMO:** Contract Manufacturing Organisation, an organisation that provides manufacturing services.
6. **CDMO:** Contract Development and Manufacturing Organisation, an organisation that provides development and manufacturing services.
7. **Data liquidity:** the ease with which data can be securely exchanged between different systems, applications, or organisations. High data liquidity implies that data flows smoothly and efficiently, while low data liquidity indicates barriers or challenges in sharing and accessing data.
8. **Denial of service (DoS):** an attempt to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests, which prevents legitimate requests from being fulfilled.
9. **Endpoint detection and response (EDR):** a cybersecurity solution that monitors and responds to potential threats on endpoint devices such as computers, mobile devices, and servers. EDR tools collect data from endpoints and analyse it for suspicious activities, allowing security teams to detect, investigate, and respond.
10. **Espionage:** the practice of obtaining confidential information without the permission of the owner.
11. **IoT devices and automation:** Internet of Things (IoT) devices are physical objects embedded with sensors, software, and other technologies that connect and exchange data with other devices and systems over the internet. Automation refers to the use of these devices to perform tasks without human intervention, often in industrial or logistical settings.
12. **Malware:** malicious software designed to disrupt, damage, or gain unauthorised access to a computer system. Types of malware include viruses, worms, Trojan horses, ransomware, and spyware.
13. **Mean time to contain (MTTC):** a metric used in cybersecurity to measure the average time it takes to contain a security incident after it has been detected.
14. **Mean time to identify (MTTI):** the average time it takes to identify that a security incident has occurred.
15. **Miscellaneous errors:** in cybersecurity, miscellaneous errors refer to unintentional actions that result in security incidents. These can include incorrect delivery of sensitive information, misconfigurations, or other human errors that inadvertently expose data or systems to risk.
16. **Personally Identifiable Information (PII):** any data that could potentially identify a specific individual such as names, social security numbers, addresses, and phone numbers.
17. **Phishing:** a type of social engineering attack where an attacker sends fraudulent messages (usually emails) designed to trick individuals into revealing sensitive information such as passwords or credit card numbers. These messages often appear to be from legitimate sources.
18. **Ransomware:** a type of malware that encrypts the victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Ransomware attacks are typically carried out via phishing emails or by exploiting vulnerabilities in software.

19. **RFID:** radio frequency identification, a wireless communication method that uses electromagnetic waves to identify and track tags attached to objects, people, or animals.
20. **Security Information and Event Management (SIEM):** a set of tools and services offering real-time analysis of security alerts generated by applications and network hardware. SIEM systems are used to detect, monitor, and respond to security incidents within an organisation.
21. **Shadow data:** data that is stored, processed, or transmitted in an organisation without the knowledge of the IT or security teams. This data often resides in unsanctioned cloud services or devices, posing significant security risks as it is often unprotected.
22. **SOC:** security operations centre, a centralised function or team responsible for improving an organisation's cybersecurity posture by preventing, detecting, and responding to threats.
23. Social engineering: the psychological manipulation of people into performing actions or divulging confidential information. Unlike technical hacking techniques, social engineering exploits human trust and error to gain access to secure systems or data.
24. **System intrusions:** unauthorised access to a computer system or network. This can occur through various methods, such as exploiting vulnerabilities, brute-force attacks, or gaining access via stolen credentials. Intrusions are often the first step in more extensive attacks, such as ransomware deployment.
25. **Zero-day vulnerability:** refers to a software security flaw that is unknown to the software vendor or developer. Since the vendor is unaware of the vulnerability, no patch or fix exists at the time the vulnerability is discovered.

References

1 Cost of a Data Breach Report 2024 by IBM Security (henceforth COADBR 2024)

2 The average number of M&A deals in the global healthcare sector is 2,640 per annum from 2007 to 2023 inclusive, according to PitchBook's 2023 Annual Global M&A Report

3 https://www.littlefish.co.uk/insights/cyber-security-inpharmaceutical-industry/

4 https://intersys.co.uk/2024/02/12/pharmaceutical-cybersecurity-the-threat-the-solution-and-the-need-for-a-specialistprovider/

5 https://www.mckinsey.com/industries/life-sciences/our-insights/four-ways-pharma-companies-can-make-their-supply-chains-more-resilient

6 World Economic Forum Global Risks Perception Survey 2023-2024

7 https://www.oracle.com/security/database-security/what-isdata-security/

8 https://isg-one.com/articles/life-sciences-2022-2023-part-1-cybersecurity-threats

9 https://isg-one.com/articles/life-sciences-2022-2023-part-1-cybersecurity-threats

10 https://securityintelligence.com/articles/cost-of-a-databreach-2023-pharmaceutical-industry/ See also https://www.cloudwards.net/cloud-computing-statistics/

11 COADBR 2024. Does not sum to 100% due to rounding

12 COADBR 2024

13 https://www.sentra.io/blog/securing-shadow-data

14 https://www.ncsc.gov.ie/pdfs/National_Cyber_Emergency_Plan.pdf

15 https://www.economist.com/business/2024/07/18/googlewants-a-piece-of-microsofts-cyber-security-business

16 https://www.boots-uk.com/about-boots-uk/our-purpose-andvalues/boots-in-numbers/

17 https://www.bbc.com/news/health-68139870

18 https://www.historyhit.com/the-biggest-cyberattacks-in-history/

19 https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

20 For clinical trials specifically, see: How Cybersecurity Protects Participants in Clinical Trials and https://www.centerwatch.com/articles/25180-clinical-trials-need-to-be-on-high-alert-forcybersecurity-threats

21 https://ascopubs.org/doi/10.1200/CCI.22.00149 The Impactof a National Cyberattack Affecting Clinical Trials: The Cancer Trials Ireland Experience

22 https://www.gov.uk/government/statistics/cyber-securitybreaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex

23 https://www.gov.uk/government/statistics/cyber-securitybreaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex Figure 2.1

24 https://techcrunch.com/2024/05/24/cencora-americanshealth-data-stolen-breach-cyberattack/

25 https://techcrunch.com/2023/11/18/postmeds-truepilldata-breach-pharmacy-millions/

26 https://www.gcca.org/magazine-article/are-your-systemscybersecure/quoting Techniek Nederland

27 https://www.reuters.com/business/healthcarepharmaceuticals/change-healthcare-network-hit-bycybersecurity-attack-2024-02-22/

28 https://techcrunch.com/2024/04/22/unitedhealth-changehealthcare-hackers-substantial-proportion-americans/

29 https://bc.ctvnews.ca/london-drugs-stores-remain-closedfor-4th-straight-day-after-cybersecurity-incident-1.6868920

30 Data Breach Investigations Report (2023) by Verizon

31 Costing $4.99 million versus average of $4.88 million, according to COADBR 2024

32 Verizon 2024

33 https://www.linkedin.com/pulse/securing-cold-chain-dataiot-cybersecurity/

34 https://www.ibm.com/topics/data-security

35 https://ico.org.uk/about-the-ico/media-centre/news-andblogs/2022/10/biggest-cyber-risk-is-complacency-nothackers/

36 https://www.crowdstrike.com/cybersecurity-101/zero-trustsecurity/

37 https://www.skycell.ch/news/big-data-pharma-cold-chainlogistics/

38 Joe Bertnick of Backbone. See also https://intersys.co.uk/2024/02/12/pharmaceutical-cybersecurity-the-threat-the-solution-and-the-need-for-aspecialist-provider/

39 https://www.crowdstrike.com/cybersecurity-101/zero-trustsecurity/

40 Cybercrime Trends 2024

41 Four Areas of Cyber Risk That Boards Need to Address by Sander Zeijlemaker, Chris Hetner, and Michael Siegel. June 02, 2023

backbone connect

General enquiries

+44 (0) 203 9557 100

hello@simplybackbone.co.uk

simplybackbone.co.uk

© 2024 Life Sciences Real Estate Limited. All rights reserved. Registered in Ireland No. 713479.

This document is for information purposes only. Whilst every care has been taken to confirm the accuracy of the information presented, Life Sciences Real Estate Limited cannot accept any liability arising from any use of this document.