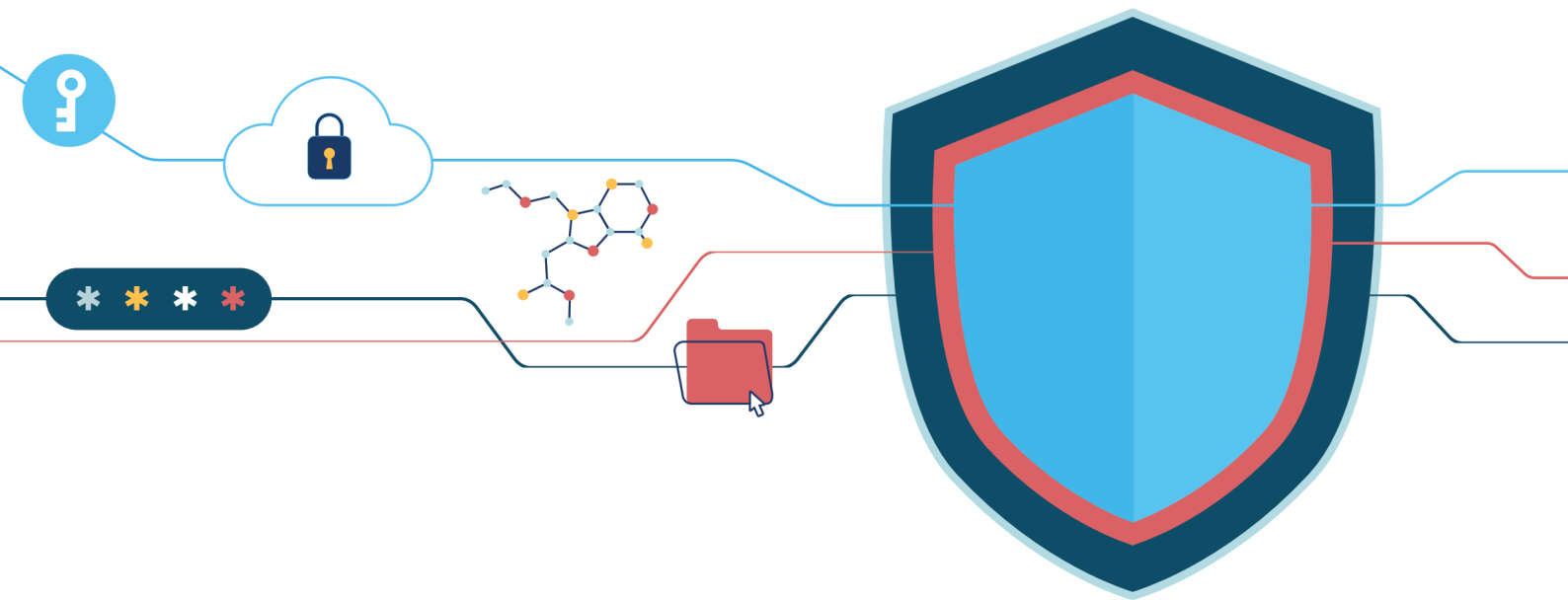


Whitepaper

Information Security Management at Discngine



SUMMARY

Information security is of utmost importance in today's digital age. Pharma and life science organizations handle particularly sensitive and confidential data on new molecules design and discovery, which makes them prone to cyber-attacks. To keep the data within their organizations safe, research-driven companies implement strict protection systems by setting up processes, enhancing technologies, and training people.

However, collaborating with third-party service providers (e.g., for R&D, supply chain, or manufacturing operations) and sharing data externally increases cyber risks. Although the third-party provider's security assessment is a crucial part of the deal-closing process, often information on their data management and security systems is incomplete or the

procedure takes a lot of time. This can ultimately have serious consequences for their clients.

The question is: How to ensure your company's data protection from potential breaches from third-party service providers?

The ISO/IEC 27001 certification grants organizations a systematic and proactive approach to information security. It defines a comprehensive set of controls and policies to help protect critical assets and ensures that client data and information remain confidential, available, and secure. Working with ISO 27001-certified organizations guarantees that all the shared sensitive data is kept safe.

The scope of the whitepaper:

Trends and challenges in information security	2
Cost and number of data vulnerabilities.....	2
Information security challenges for pharma and life science businesses.....	4
Third-party vendor-related risk	4
The "Dragonfly attack" scenario.....	5
Information security management system and ISO standard.....	6
Understanding ISO/IEC 27001	6
The scope of ISO/IEC 27001 at Discngine	7
The benefits of ISO/IEC 27001 Certification for Discngine clients	7

TRENDS AND CHALLENGES IN INFORMATION SECURITY

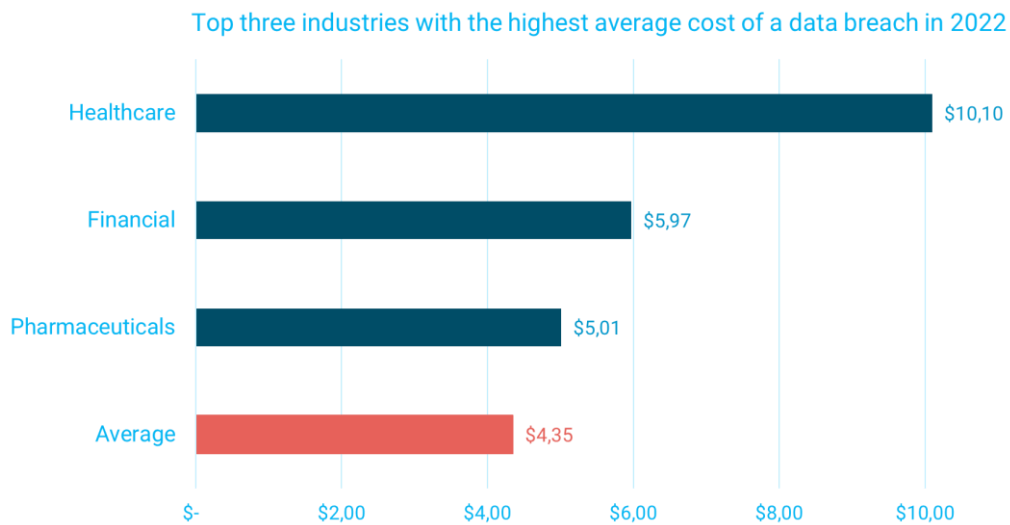
Pharma and life science industry is a popular target for hackers that wish to access sensitive information like research data, patents, and patient information. Research-driven organizations, therefore, face a complex landscape of security risks, including cyberattacks, data breaches, and unauthorized access to confidential information. The impact of these threats can be severe, ranging from financial losses and reputational damage to intellectual property theft.

In the following section, we will highlight the significance of cyber-attacks based on the multiple data reports that account for the cost and number of data breaches.

Cost and number of data vulnerabilities

To give some perspective, the *Panemon institute and IBM Security®* did an extensive report on data breaches in 2022, collecting data from 550 organizations from 17 countries impacted by those accidents. Based on their findings, **the average cost of a data breach worldwide was \$4,35 million (USD) in 2022**, reaching an all-time high. This figure represents a 2,6% (4,24 million) and 12,7% (3,86 million) increase from 2021 and 2020, respectively.

The healthcare industry is highly targeted, with a 42% increase in the cost of a breach since 2020. For the 12th year in a row, the **healthcare industry had the highest average data breach cost of any industry** averaging \$10,10 million. After healthcare and financial services (\$5,97 million), **the pharmaceutical industry has the third highest cost – averaging \$5,01 million**, 1,2 times the global average.¹



Based on the IBM report "Cost of a Data Breach Report 2022. Numbers are measured in USD millions.

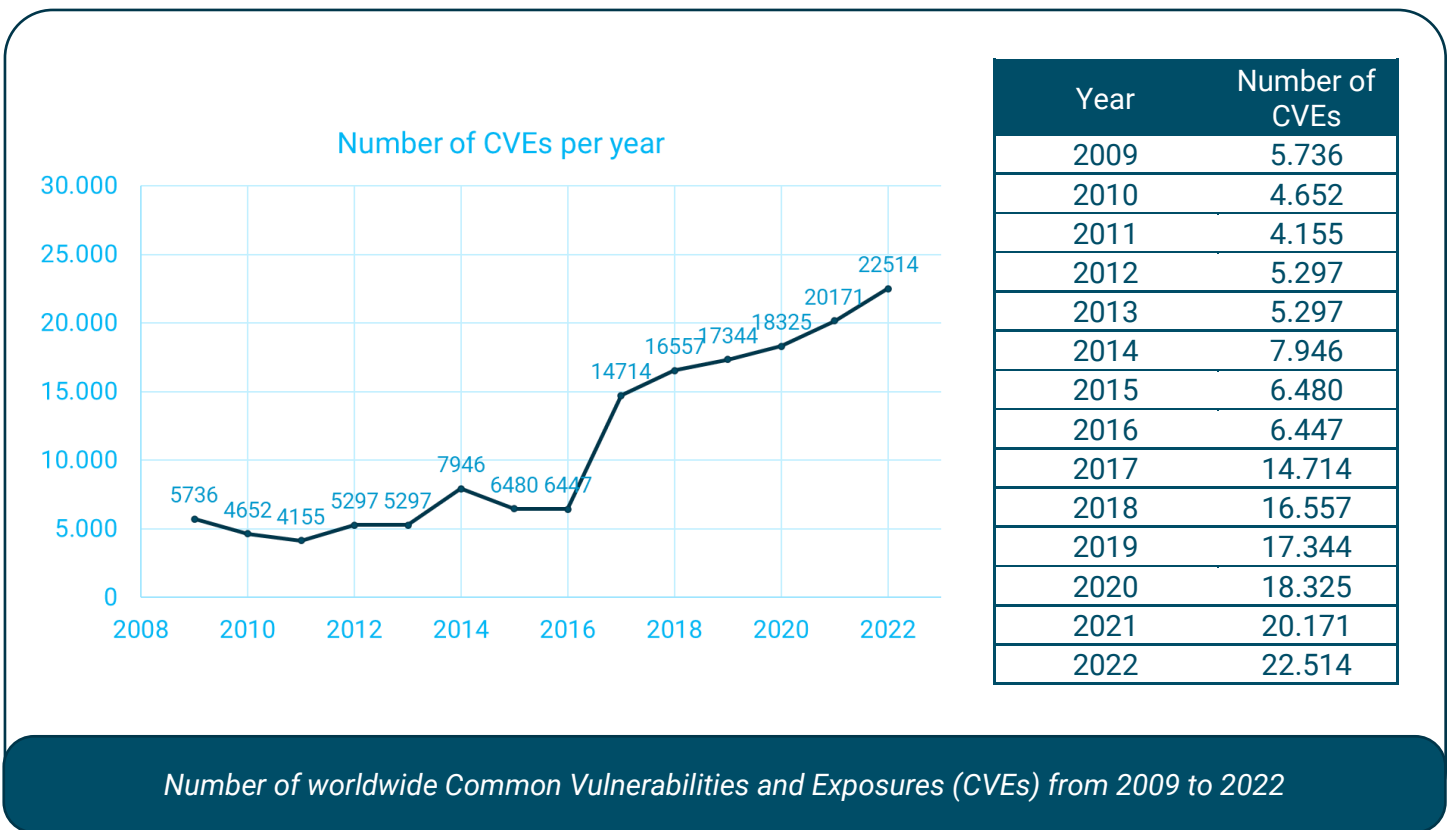
1 - Cost of data breach report 2022, IBM Security®; <https://www.ibm.com/downloads/cas/3R8N1DZJ>

In addition, the size of the global cybersecurity market is booming. According to Cybersecurity Ventures, during the next five years, the cost of the cybercrime market will increase by 15% per year, reaching **\$10,5 trillion annually by 2025**. This presents an immense 300 percent increase from 2015 when the cost was \$3 trillion.

However, it is essential to highlight that as enormous and frightening as those numbers are, they are most likely just the tip of the iceberg of reported cyber attacks. Namely, due to the reputation damage, embarrassment, and belief that law enforcement is powerless to intervene, only around 10% of all cybercrimes are reported yearly.²

Along with the cost, the number of attacks is growing drastically. Statista reports worldwide Common Vulnerabilities and Exposures (CVEs) numbers from 2009 to 2022, with a record-high number in 2022 being 22.514.³ The Check Point Research (CPR) release trends indicate that the **education and research industry had an average of 1.463 attacks** per organization per week in 2022, a 74% increase over the previous years.⁴

All these insights clearly show that there are increasingly expensive security breaches, with life science and pharmaceutical organizations being one of the main targets.



Number of worldwide Common Vulnerabilities and Exposures (CVEs) from 2009 to 2022

2 - Morgan. Steve. "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics", Cybercrime Magazine, 19 Jan., 2022, [Link](#)

3 - Statista, [link here](#)

4 - LePree Anderson. Joy. "Global cyberattacks increased 38% in 2022", Security Magazine, [Link](#)

INFORMATION SECURITY CHALLENGES FOR PHARMA AND LIFE SCIENCE BUSINESSES

The upward trend of security risks is perhaps not that surprising, considering the data digitalization in life science companies, remote work, and the high number of internet-connected devices and services, to name just a few. While **digital innovation** enables efficiency improvement across all areas in the pharma sector (from R&D to supply chain and operations), it causes exposure to new data-related risks.

In fact, the pharma and life science industries face several unique challenges when it comes to data security, such as:

Protection of sensitive data, including research data, intellectual property, and clinical trial data, which safety is critical to maintaining the trust of patients and partners.

Regulatory compliance, such as FDA regulations and GDPR, requires implementing appropriate security measures to maintain compliance.

Insider threats mean anyone with access to sensitive data (e.g., employees, contractors, vendors) must be adequately trained to prevent

unauthorized data breaches and accesses.

Data integration because the life science industry often deals with a large amount of complex data from multiple sources, and it isn't easy to secure all of it properly.

Partners and Third-party service providers can mainly introduce cybersecurity risks if their security measures are not taken care of.

Even if these are only one portion of the challenges industries face, the positive aspect is that security professionals in research organizations have implemented **data security strategies**. They consist of keeping the software up to date, educating staff, and implementing zero-trust platforms; yet, the concern remains: the number and cost of data breaches continue to increase.

In the following section, we will focus on the third-party provider risks and why choosing a partner and company vendor with a strong data protection system is important.

Third-party vendor-related risks

While organizations are making big efforts to establish cyber security within their four walls, it is challenging to determine the risks of the external cyber environments. Many life science companies rely on third-party vendors and partners for critical aspects of their operations, giving them access to their own internal data. Such exchange is often risky because the company is not completely aware

of the third-party provider's vulnerability to data breaches. These third-party vendors may not have adequate security measures in place, or they do not follow industry best practices for security. If victims of cyber-attack, they can cause severe consequences for their clients and represent a risk management blind spot.

For example, life science companies may rely on third-party vendors to develop software and other technologies. If these vendors don't have an information security system in place, they could [introduce vulnerabilities into the life science companies' systems and compromise sensitive data](#) (see scenario below). This is why the best third-party vendors are those that take all necessary security measures to keep their clients safe.

The "Dragonfly attack" scenario

Between 2011 and 2014, a group of cyber attackers infiltrated the computer systems of several large pharmaceutical companies through their third-party vendors. First, the

group used a variety of tactics (e.g., spear-phishing attacks and malware-infected websites) to collect data about the company's third-party suppliers. They attacked the supplier's software by sending trojan viruses and other malware. Once inside, they gained access to intellectual property related to developing new therapies, which could have been used to establish fraudulent medications. As a result, many pharma clients were forced to postpone their drug discovery processes.

The attacks were discovered by cybersecurity researchers in 2014. They caused significant concern among the affected companies and government officials, who feared that the stolen data could be used to develop copycat drugs or create other national security risks.⁵

Since the Dragonfly attacks, there have been several other high-profile cyber-attacks targeting pharmaceutical companies, highlighting the ongoing need for effective cybersecurity strategies.



The "Dragonfly attack" scenario:

1. *The hackers used phishing to collect data about the third-party providers of the pharma company*
2. *They sent malware to those companies and gained access to their systems*
3. *This allowed them access to sensitive information in drug development and the intellectual property of the pharma companies. The information was used to create counterfeit drugs*

5 - Millar. Abi., "Five pharma cybersecurity breaches to know and learn from", *Pharmaceutical technology*, 17 Sept., 2021, [Link](#)

INFORMATION SECURITY MANAGEMENT SYSTEM AND ISO STANDARD

To mitigate the third-party provider's risk and gain client trust, third-party providers must adopt a [robust information security management system \(ISMS\)](#) that protects their clients' data and information from unauthorized access and other cyber threats. They must ensure privacy and confidentiality and provide a secure environment for storing, exchanging, and processing sensitive information – both its own and its clients.

This is where [ISO/IEC 27001 standard](#) comes into play. The ISO certificate guarantees that data access, sharing, and manipulation are secure because the client is aware of all the processes in implementing and maintaining the third-party vendor's information security. Besides, pharma companies can apply and get ISO certification themselves and secure their internal data and valuable information.

Understanding ISO/IEC 27001

ISO/IEC 27001 is an international standard for ISMS that provides a framework for protecting sensitive information and ensuring compliance with industry standards and regulations. It is a globally recognized standard that defines best practices for information security and offers a systematic

approach to managing confidential information.

The certification process for ISO/IEC 27001 includes a thorough assessment of an organization's ISMS by an independent certification body. The assessment covers the organization's policies, procedures, processes, and physical and technical controls to ensure they meet the standard's requirements. Upon successful completion of the assessment, the certification body issues a certificate of compliance.

The standard requires organizations to implement security controls, such as:

- [access control](#)
- [encryption](#)
- [backup and recovery](#)
- [incident management](#)
- [security awareness training for employees](#)

These controls aim to ensure information confidentiality, availability, and integrity. The standard is flexible and scalable, allowing organizations of all sizes to implement the appropriate controls and policies for their specific needs.

All in all, ISO/IEC 27001 provides a comprehensive framework for information security management. The standard covers all aspects of information security, including physical security, access control, network security, and incident management. The certification process offers organizations the assurance of information security and improved risk management to prevent security incidents.

The scope of ISO/IEC 27001 at Discngine



In the field of life science, Discngine helps researchers to discover new active molecules. Its IT software and service solutions are used in the pharmaceutical, cosmetics, and agrochemical industries. Since 2015, the company has started its **cloud shift** and now offers solutions in the SaaS environment on the cloud. Therefore, delivering solutions in the cloud, on top of accessing the sensitive data of pharma clients, was a game changer in cybersecurity for Discngine and **having a robust ISMS in place became paramount**.

Consequently, the company was recently certified under ISO/IEC 27001, demonstrating its commitment to providing secure and reliable IT services and SaaS solutions. The standard is integrated into various aspects of Discngine operations, including **software-as-a-Service (SaaS) development, customer support, and SaaS hosting**.

In software development, Discngine increased a range of security controls over the development cycles to ensure the confidentiality, integrity, and availability of customer data. This includes security assessments, code reviews, and vulnerability assessments to identify and mitigate security risks.

Discngine implemented robust information security controls **in customer support** to protect customer information, including access control, encryption, and secure data storage. All customer support staff receive extensive training on information security to ensure that customer data is managed securely.

Discngine SaaS hosting services are also certified under ISO/IEC 27001, providing customers with a secure environment for their critical information. The company implemented technical controls, such as firewalls and strict access control measures to prevent unauthorized access to customer data.

Every employee at Discngine has been involved in this collective effort by going through extensive education and practical training. Implementing strict information security policies and processes took months of intense work and collaboration. The driving force for obtaining the certification was ensuring its information security management system was comprehensive and robust.

The company undergoes yearly surveillance to ensure its compliance with the standard.

The benefits of ISO/IEC 27001 Certification for Discngine clients





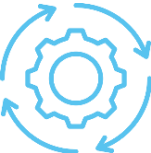
With the ISO 27001 certification, Discngine assures potential and existing clients that the organization is following information security best practices. It gives clients **peace of mind**

that they work with a third-party provider company whose security risks are being treated effectively and that their sensitive data and intellectual property is protected and managed securely.

The certification also allows Discngine to meet customer security requirements and [speed up the security assessment stage](#) in the

customer journey. The security assessment can take up to 12 months with some of Discngine pharma clients. ISO 27001 speeds up the response time with systems already in place and brings the scientific applications sooner to the researcher.

The summary of benefits is listed below.

Benefits for research-driven organizations that work with Discngine regarding data security		
	<p>Data protection</p>	<p>ISO 27001 certification ensures that Discngine has implemented robust and thorough security measures to protect sensitive information, including research data and intellectual property. This can provide peace of mind for research-driven organizations that their valuable data will be protected against unauthorized access, disclosure, or loss.</p>
	<p>Compliance</p>	<p>Research organizations often work with sensitive information that must be protected under strict regulations such as GDPR, and FDA. An ISO 27001-certified company can help to ensure compliance with these regulations, reducing the risk of fines and penalties for non-compliance.</p>
	<p>Risk management</p>	<p>ISO 27001 certification requires Discngine to conduct regular risk assessments and implement measures to mitigate identified risks. This means that our customers can be confident that Discngine has identified and is proactively addressing any potential security threats related to their data.</p>
	<p>Confidentiality</p>	<p>An ISO 27001-certified company is required to implement confidentiality agreements and NDAs to protect the sensitive information of their clients. This provides an extra layer of protection for Discngine customers, ensuring that their confidential information is protected and not disclosed to unauthorized parties.</p>
	<p>Continuity</p>	<p>ISO 27001 certification ensures that Discngine has implemented a business continuity plan to ensure that the organization's critical processes can continue to operate in the event of an incident. This helps minimize disruptions and ensure that research projects can continue even in the face of unexpected events.</p>

CONCLUSION

Companies working with valuable and sensitive data in pharma and life science industry are attractive target for cyber attacks. The cost and number of data breaches is drastically increasing year by year, which means that critical actions are needed to establish advanced protection systems.

Special attention is required when there is a collaboration with third-party providers, since companies are not sure how are their sensitive data protected once shared externally.

ISO27001 is a certified standard that allows third-party vendor companies to ensure the complete trust and transparency with its clients by knowing how to manage their data and protect from breach attempts.

To give its clients a piece of mind and have seamless collaboration, Discngine has obtained ISO 27001 certification. Discngine operations including software development, customer support, and SaaS hosting are following the ISO27001 guidelines. It is a proof that client's sensitive data in Discngine solutions is kept safe and secure.

Resources

- Website:
[ISO27001 at Discngine](#)
[About Discngine](#)
- Information security at Discngine [FAQs](#)
- Contact us: contact@discngine.com