cpl.thalesgroup.com

THALES
Building a future we can all trust

Protecting pharmaceutical and life-sciences data against a cyber-attack pandemic

Achieving privacy and IP protection while accelerating innovation

The COVID-19 pandemic has helped bring to the forefront another pandemic: cyber-attacks on pharmaceutical and life-sciences enterprises. Attempts to steal COVID-19 vaccine technology, clinical trial data sets, intellectual property, health records, and disrupt distribution supply chains have rattled the industry and national governments. It is one thing to have a credit card cloned, but it is much more serious when lives are at risk.

Cyberattacks on healthcare facilities have affected 17.3 million people as a result 436 data breaches in the United States alone according to the U.S. Department of Health and Human Services (HHS)[1]. Pharmaceutical and biotech companies suffer more breaches than those in any other industry, with 53% of them resulting from malicious activity[2]. As of result of these threats, the risks to pharmaceutical and biotech organizations include:

- Loss of critical intellectual property (IP) on new treatments, drugs, and research;
- Delays in the production of life-saving drugs and treatments;
- Loss of sensitive personal health information (PHI) and noncompliance with privacy regulations; and
- Brand damage and loss of customer trust.

The end result of these attacks is an average cost of a single data breach in the pharmaceutical industry reaching $5.06 million[3]. However, some attacks can cost much more. One attack on a global pharmaceutical giant is estimated to have cost more than $1.3 billion[4]. However, a successful attack at a life-sciences organization can cost much more than financial losses. Additional impacts can include the loss of years in research and development for life-saving new drugs and treatments or slowing the speed of innovation that is key to the industry.

An industry driven by innovation

Pharmaceutical and biotech organizations rely heavily on innovation in the research and development of complex drugs, treatments, and biotech medical equipment in a highly competitive environment. In the drive to provide better care to patients, cost savings, and faster time-to-market for treatments, they have been adopting new technology platforms at fast pace.

[1] US Department of Health and Human Services (HHS) data breach portal, 2022

[2] Forbes: How The Pharmaceutical Industry Can Secure Networks To Avoid Cyberattacks, Mar 2021

[3] Ponemon Institute and IBM: Cost of a Data Breach Report 2021

[4] Security Magazine: We are at war; a cyber war, 2022

Cloud, Big Data, IoT and more

The cloud is being widely adopted in order to provide the elasticity and flexibility necessary to support a wide-ranging number of new applications and computing resources. 93% to 100% of pharma and 72% to 84% of biotech companies are in the cloud according to IDC, and of those already deployed in the cloud, 42% of pharma and 34% of biotech organizations are using life-science specific apps, including research analytics, clinical analytics, drug safety, and more[5]. The cloud is also essential in the process of collaboration with global third-party suppliers indispensable to the life-sciences business model.

Analytics and Big Data are essential to the task of research and development of new drugs, including the analysis of clinical trial data, identification of trends among large populations, and the ability to personalize and create target medications. Life sciences companies are expected to spend US$18 billion a year in analytics and big data by 2030[6].

The Internet of Things (IoT) is being widely adopted to add new capabilities to operational technology (OT) in manufacturing and to add connectivity to biotech appliances that can even be implanted in patients' bodies to support critical life-preserving functions.

The list of innovations goes on and on, including more mundane topics such as the adoption of digital health records and remote work. But combined, technological innovations are changing the face of the life-sciences industry.

The central role of data

Central to the modern life-sciences enterprise is the role of data. Data is the crucial asset used by scientists to develop drugs, from gene sequencing to the analysis of drug trials. Data captured from IoT sensors and cameras allows remote management of manufacturing at distributed facilities in multiple countries. And data about the performance of drugs, health records, as well as patient and doctor feedback, provide important input to the process of design, delivery, and pricing of drugs and treatments.

As a result, data is now distributed and stored across a variety of cloud environments and internal systems, and accessed by a wide range of applications, devices, and workers. The cyber-security challenge for life-sciences enterprises is that data is also what cyber criminals are after.

Among the petabytes of data flowing through an upgraded and modern hybrid IT systems are volumes of sensitive data that attackers are after. Intellectual property, health records, personal health information (PHI), and personally identifiable information (PII) stored in structured or unstructured data files from databases to email and video, are all targets for attackers. That creates multiple challenges for cybersecurity professionals at these organizations.

Cybersecurity and compliance risks

The growth and sophistication of cyberattacks

In the 2022 Thales Data Threat Report, produced by 451 Research for Thales, 45% of respondents reported seeing an increase in the volume, severity and/or scope of cyberattacks in the past 12 months[7]. The same report also found that 21% of organizations had experienced a ransomware attack. Several life-sciences enterprises have been in the news after major cyber-attacks from cyber criminals demanding ransom, and these are only the ones that were reported.

Furthermore, pharmaceutical and biotech enterprises are high on the target list of well-funded state actors and corporate espionage groups. Those were the cyber criminals trying to get access to COVID-19 vaccine data in 2021. State actors were also the attackers deemed to be responsible for a massive cyber-attack in 2017 that crippled a major drug maker and resulted in over $1.3 billion in damages[4].

[5] IDC: Life Science Market Trends 2021

[6] Precedence Research: Life Science Analytics Market Size to Reach US$ 18.12 Bn by 2030, Feb 2021

[7] Thales Data Threat Report 2022

Cybersecurity complexity

The race to innovate has created a complex Hybrid IT environment to protect. As an example, the 2022 Thales Data Threat Report showed that enterprises use a multitude of cloud services to run their businesses. 72% use more than one Infrastructure-as-a-Service (IaaS) platform and the average number of Software as-a-Service (SaaS) platforms used is 54[7].

The speed of change and the number of new environments and technologies has forced organizations to "bolt on" security point products to meet specific security or compliance requirements on both new platforms and legacy systems that cannot be replaced. Consequently, IT has to manage multiple data security products protecting different cloud and on-premise environments.

The latest Thales Data Threat Report identified that 55% or organizations have five or more key management systems in place. The larger the number of systems, the greater the risk for error and the more time and work required to manage the combination successfully. So perhaps is not a surprise that a majority of organizations (54%) chose to rely on the cloud service provider to manage keys. That eliminates a lot of the key management challenges, but it creates another challenge in terms of compliance and a potential vulnerability, which is the lack of control over keys in the cloud[7].

Third party suppliers and platforms

Distributed manufacturing supply chains are essential to the production of modern drugs. These include a number of third-party suppliers and third-party technology platforms. While the distributed global supply chain may increase efficiency, lower costs, and improve time-to-market for delivery of drugs and treatments, it also creates multiple new vulnerabilities for life-sciences corporations.

Supply chains became the number one target of cyber criminals in 2021. Attackers often figure out they can use a breach in one supplier or third-party platform to spread malware up and down the chain and compromise multiple other enterprises that are part of the manufacturing or software supply chains. Unfortunately, security executives at life-sciences enterprises cannot control security practices performed at third-party vendors; these executives have to trust that best practices are being followed.

IoT and OT convergence

The ongoing transition of OT used at manufacturing facilities from proprietary, firewalled infrastructure, to dedicated connections to the internet has greatly increased the size and complexity of underlying networks while greatly increasing attack surfaces. Suddenly, many systems that were disconnected from the internet and broader IT became available for cyber criminals for attack. And attacked they were.

A survey of 230 healthcare security leaders in China, Germany, Japan, the United Kingdom, and the United States found that 82% of their healthcare organizations had experienced an IoT-focused cyberattack [8]. In addition, a recent research study revealed that 83% of organizations using OT, had at least one OT security breach in the past 36 months[9].

Regulatory challenges and executive orders

Compliance has always been a part of life in healthcare. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States protect critical health patient data, while privacy legislation, such as GDPR and CCPA, broaden the scope to all PII data and levy substantial fines for non-compliance.

Going beyond privacy regulation, governments are now making explicit cybersecurity recommendations. While the May 12, 2021, White House Executive Order on improving the Nation's Cybersecurity is targeted at government agencies, the order and ransomware memo to business leaders explicitly mentions that it provides "the private sector with a template for its response efforts".

[8] Fierce Healthcare: 82% of healthcare organizations have experienced an IoT-focused cyberattack

[9] Skybox Security: 83% of organizations suffered an operational technology (OT) cybersecurity breach in the prior 36 months

Among other directives, the executive order gave civilian agencies 180 days to "adopt multi-factor authentication and encryption for data at rest and in transit..."and"...prioritize identification of the unclassified data considered to be the most sensitive and under the greatest threat".

The challenge for compliance is a big one, because in order to properly protect sensitive and regulated data organizations need to know where their sensitive data resides. However, only 56% of respondents in the 2022 Thales Data Threat Report were very confident or had complete knowledge of where their data was being stored, and only 25% of all respondents said they could classify all their data[7]."

Thales cybersecurity recommendations

To face these challenges, life-sciences organizations need to implement solutions that allow them to identify sensitive data, protect it based on policy rules, simplify compliance, and maintain the speed of transformation.

Discover and classify all sensitive data

The first step in a process to protect the "crown jewels" of an organization – be it IP, PHI or PII – is to know where the crown jewels reside. CIOs must adopt solutions that provide complete visibility into sensitive data with efficient data discovery, classification, and risk analysis across heterogeneous data stores including the cloud, big data, and traditional environments.

Protect data at rest, in motion and in use across Hybrid IT

The target of almost every attack is data, especially sensitive data that include personal, financial information or intellectual property. The number one priority of cyber security is the protection of this data at rest, in motion, or in use in applications. Security should be attached to the data itself in addition traditional endpoint or perimeter security measures. Both structured and unstructured files must be protected with technologies such as encryption and tokenization, and access to repositories protected with strong authentication and key management.

All sensitive data stored in the cloud should be encrypted and control of keys should be maintained by the owner of that data, separating the roles between storage administration and security administration. A number of security methodologies are available that perform much better than native encryption, including bring your own key (BYOK), hold your own key (HYOK), and most important bring your own encryption (BYOE). Sensitive structured data shared with third parties in situations where you can't control encryption can be de-identified using tokenization, so that even if the data is captured, it will be useless to attackers.

In addition, all sensitive data in motion should be encrypted, including network traffic between data centers and the headquarters, and data flowing between facilities and shared with third parties, whether on premises or in the cloud. This will allow enterprises to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception.

Automate and simplify data security governance in a single pane of glass

Every data security regulation and mandate requires organizations to be able to monitor, detect, control, and report on unauthorized access to data and encryption keys. In addition, each regulation may require the protection of specific datasets such as PHI and PII in specific circumstances in different geographies, adding enormous complexity to compliance by global enterprises.

Automation of data security governance simplifies compliance with privacy legislation, data sovereignty regulations, and government or industry mandates. It is essential to centralize security governance in a single pane of glass. The organization needs to automate the protection and access to data based on granular security policies. The automated solution should centrally manage encryption keys and configure access policies, so organizations can protect and control access to sensitive data in the cloud, on-premises, and across hybrid environments.

Organizations should consider platforms that can deliver the core components of discovery, classification, protection and user access controls in an automated fashion to reduce the complexity of managing security across hybrid environments. In fact, according to Gartner, 30% of enterprises will adopt a data security platform by 2024, up from less than 5% from 2019[10].

Protect IoT devices

In an age when an IoT device can be a pacemaker implanted in someone's body, IoT security is paramount. Each IoT device needs a unique, cryptographically based identity that is authenticated when a connection is attempted to access data or update software. Organizations should be able to track each device throughout its lifecycle, communicate securely with it, and prevent it from executing harmful processes. All this should be based on a secure root of trust for secure key management and authentication.

Adopt a zero-trust model

CIOs need to adopt a zero-trust model for their organizations' security architecture. Access should be given on a "least privileged basis" and multi-factor authentication (MFA) should be adopted across the organization to prevent unauthorized access. Identity management and access control rules for all platforms should be centralized and should be determined by a dynamic policy, enforced on a per-session basis, and updated based on information.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

[10] Gartner, 2022 Strategic Roadmap for Data Security Platform Convergence, September 28, 2021