cognizant

Microsoft

AI-driven cybersecurity in life sciences

Protecting the asset that powers innovation and defines advantages

Introduction

The pharmaceutical manufacturing landscape is evolving rapidly—driven by the need for greater efficiency, accelerated drug development, improved quality and stronger regulatory compliance.

As digital transformation reshapes operations, robust cybersecurity has become essential to protect sensitive data, ensure system integrity and safeguard increasingly complex, interconnected global supply chains. In this landscape, secure digital foundation has become one of the most critical enablers of innovation and resilience.

AI: Securing your manufacturing data

Today's cybercriminals are more sophisticated than ever, using advanced attack techniques like ransomware, as well as AI technology, to steal data, cripple operations or both. As attackers get more digitally ambitious and set their sights on bigger targets, the question is: **Are life sciences companies moving fast enough to protect themselves?**

AI has a vital role to play in life sciences—not just in unlocking the value of data, but also in protecting it. From detecting and responding to cyberattacks in real time to proactively identifying and addressing system vulnerabilities, AI can help companies protect their most valuable asset and ensure the overall health of their business.

Data is life sciences companies' most critical asset. Patient records, research breakthroughs and intellectual property (IP) fuel innovation, create blockbuster drugs and define competitive advantage. But what makes this data so valuable also makes it a prime target for cyberattacks.

Problem

Protecting your business from a $5.10M million threat

$5.10M

average cost of a pharma data breach in 2024[1]

85%

of cybersecurity professionals attribute the increase in cyberattacks to the use of generative AI by bad actors[2]

85%

of stakeholders believe AI tools are needed to detect and stop AI-generated threats[3]

The pharmaceutical industry has significantly improved its data protection and cybersecurity posture in recent years, but since 2022, the average cost of a pharma data breach has increased from $4.45 million in 2023 to $5.10 million in 2024[4].

Detection and containment times must improve, now averaging 213 days, more than the average of 194 days across other industries[5].

Widening the lead means understanding how attackers operate. Malicious attacks remain the leading cause of breaches (51%), however human error (26%) and IT failures (23%) are also common attack avenues, as threat actors exploit vulnerabilities to access systems and dwell undetected.

1 https://www.ibm.com/reports/data-breach (2024 statistics)

2 https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/

3 https://www.darktrace.com/resources

4, 5 https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry

While public cloud environments often present the highest risk and breach costs due to their shared infrastructure and broader attack surface, it's important to recognize that vulnerabilities also exist in non-cloud-based systems. Data stored locally on PCs, analytical instruments and site-based physical servers can be equally susceptible to threats such as unauthorized access, malware and physical damage if not properly secured. On-premises storage and private cloud solutions generally offer greater control and can be more secure when robust access controls, encryption and monitoring are in place. However, the complexity of managing hybrid environments—including combinations of cloud, local and instrument-based data—requires a comprehensive cybersecurity strategy tailored to the unique risks of each storage modality.

What's at stake for pharma companies during a cyberattack?

Manufacturing disruptions

Product distribution delays

Theft of sensitive data and IP

Lost revenues

Regulatory fines

Reputational harm

Cybersecurity and compliance: Unlocking the power of AI

For life sciences companies, cybersecurity is also a matter of compliance.

The pharmaceutical industry faces stringent regulatory requirements for data protection and privacy, including Good Manufacturing Practices (GMP) and 21 CFR Part 11, EU Annex 11, GAMP 5, the EU's General Data Protection Regulation (GDPR) and the US Health Insurance Portability and Accountability Act (HIPAA).

A single cybersecurity breach can lead to regulatory noncompliance, triggering legal action, hefty fines and reputational damage. HIPAA penalties alone average $1.5 million, with violations ranging from $137 to $68,928 each, depending on severity[6].

In Europe, the stakes have also risen. As of October 2024, EU Member States are subject to an enhanced directive on network and information security (NIS). The measure, Directive (EU) 2022/2555, strengthens cybersecurity requirements for both public and private entities operating in "essential" or "important" sectors, including healthcare and pharmaceuticals. Noncompliance could result in fines of up to €10 million or 2% of global annual revenue for essential entities, and up to €7 million or 1.4% for important entities—whichever is higher.

Advanced and intelligent technologies, including AI, have a role to play in helping companies defend against costly cyberattacks and mitigate their far-reaching consequences. Yet integrating AI into a cybersecurity strategy is not without its challenges. Working with expert digital transformation partners is essential to ensure companies have access to the latest innovations, and that these tools are effectively integrated into their existing infrastructure for maximum impact.

[6] https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

What AI can do and how

The future of data protection is AI-enabled

The cybersecurity landscape is being shaped by a new generation of generative and agentic AI tools. These tools, often used in combination with machine learning (ML) and automation, can analyze vast amounts of security data across systems in real time, providing precise, actionable recommendations to strengthen human decision-making or even taking action without the need for human intervention.

The use of these tools enables a dynamic, proactive approach to threat detection and risk mitigation, helping companies detect and respond to threats faster and with greater accuracy—while also optimizing limited human cybersecurity talent.

Below we outline five key use cases for AI within cybersecurity for life science organizations and the benefits of this technology as compared to traditional methods:

Unlocking the power of AI in cybersecurity

Strengthen the security postur

Reduce the risk of data breaches

Maintain regulatory compliance

Securing the future of pharma manufacturing

Pharmaceutical companies face a range of cybersecurity risks that can disrupt operations and compromise safety. Here we highlight several key challenges within pharma manufacturing and how AI can help mitigate them.

Issue	Security challenge	AI-enabled solution
Globalized and fragmented supply chains	Expansive supplier and distribution networks increase the number of cyber threat entry points, raising the risk of breaches and operational disruption.	AI can enhance supply chain visibility and detect anomalies in real time, improving end-to-end security and resilience.
Aging infrastructure and legacy systems	Outdated IT and OT systems lack interoperability and robust security, making them prime targets for cyberattacks.	AI-powered analytics can identify vulnerabilities, prioritize patching and recommend modernization pathways to strengthen defenses.
The shift to Industry 4.0	As pharmaceutical manufacturing embraces Industry 4.0, the rise of IoT and connected devices, including manufacturing and analytical equipment, expands the digital footprint and the cyberattack surface.	AI can help secure this smart infrastructure by enabling real-time monitoring, threat detection and automated response.
Emerging attack vectors	Misconfigured cloud platforms and unsecured IoT devices introduce new cyber risks across manufacturing environments.	AI can monitor cloud and IoT ecosystems continuously to detect misconfigurations, flag unusual behavior and automate responses.
Insider threats	Employees or contractors with access to sensitive systems can unintentionally or maliciously cause breaches, often via phishing or negligence.	AI-driven behavior analytics can detect insider anomalies, while intelligent phishing filters and personalized training improve employee cyber hygiene.

Manufacturing sites and lab compromise	Attacks on ICS and OT systems can compromise product quality, halt production or introduce safety risks.	AI can monitor production systems for irregular patterns, support predictive maintenance and isolate potential threats before they impact operations.
Increased outsourcing	Partnering with CDMOs expands the cybersecurity risk surface across third-party ecosystems.	AI can automate third-party risk assessments and monitor data sharing to enforce secure, compliant collaboration.
Talent shortages	A lack of skilled cybersecurity professionals leaves organizations vulnerable to growing threats.	AI-enabled cybersecurity platforms reduce reliance on manual oversight, offering intelligent automation and augmenting lean security teams.

Five key AI use cases for life sciences in cybersecurity

1. **Enhancing threat detection**

   For an industry where data is both the lifeblood and the most coveted asset, incorporating AI into a comprehensive cy strategy is the key to resiliency and security.

   Traditional cybersecurity tools, which rely on static rules and known attack signatures, often struggle to keep up with fast-evolving tactics. This creates vulnerabilities that can jeopardize data integrity, regulatory compliance and business continuity.

   AI, including generative and agentic AI, is offering companies a more autonomous and adaptive approach for detecting, preventing and predicting cyber threats. Unlike conventional systems, AI- and ML-powered defenses can analyze massive streams of data in real time to uncover subtle patterns and anomalies that may signal an emerging breach, allowing teams to act before major damage occurs. [Agentic AI builds on these capabilities by autonomously assessing situations, prioritizing actions and even executing predefined countermeasures, reducing the burden on human operators.]

   AI also brings powerful predictive capabilities to cybersecurity. By mining historical data and spotting trends, generative AI tools can estimate the likelihood and potential impact of future attacks, pinpointing likely targets and timing. This foresight equips pharmaceutical and biotech companies to proactively shore up defenses, optimize their security investments and minimize risk exposure.

2. **Automating routine security tasks**

   For pharmaceutical companies, sprawling, complex IT ecosystems can create security vulnerabilities if routine tasks, like updates and patching, aren't executed consistently and expeditiously.

   Advanced AI—especially agentic AI with its autonomous decision-making capabilities—helps automate many of these critical but repetitive activities, such as monitoring network traffic, updating security protocols and managing access controls.

   Automating these functions not only eases the burden on overstretched cybersecurity teams, but also reduces the risk of human error, one of the most common causes of breaches.

3. Optimizing the protection of IP and patient data

Advanced AI tools, particularly generative and agentic AI, are proving invaluable in elevating data protection for life sciences companies. Beyond employing strong encryption and secure storage solutions, AI-powered systems autonomously oversee and regulate access to sensitive information, continuously verifying that only authorized users can view or modify it.

This level of intelligent, proactive oversight helps pharmaceutical organizations stay aligned with demanding regulations like GDPR and HIPAA, while also protecting against breaches and other attacks.

4. Sharing threat intelligence

Through advancements in generative and agentic AI, the pharmaceutical industry can now share threat intelligence more effectively than ever. This collaborative intelligence helps organizations remain alert to emerging threats and adopt proven strategies from across the industry. Moreover, AI streamlines the standardization of threat intelligence formats, making it easier to share and act on this critical information seamlessly.

5. Augmenting workforce capabilities

In 2024, the demand for skilled cybersecurity professionals continues to outpace supply, with an estimated global shortfall of 4.8 million professionals needed to adequately secure organizations[7]. This talent gap makes building and retaining an in-house security team both costly and challenging.

AI offers a powerful way to close this gap by enhancing the effectiveness of existing security teams. AI-driven tools deliver actionable insights and guidance, enabling less experienced personnel to make smarter, more informed decisions.

Generative AI, in particular, can strengthen training efforts by simulating realistic cyberattack scenarios and providing engaging, interactive learning experiences. Meanwhile, agentic AI can be used to automate routine tasks or take predefined actions when threats are detected.

[7] https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

At a glance: How AI can help life sciences companies strengthen cybersecurity

Intelligent threat detection

Spot and predict attacks in real time, reducing risk and strengthening defenses before damage occurs.

Routine task automation

Handle repetitive security activities with little or no human intervention according to predefined rules, easing staff workload, minimizing human errors and improving speed.

Advanced data security

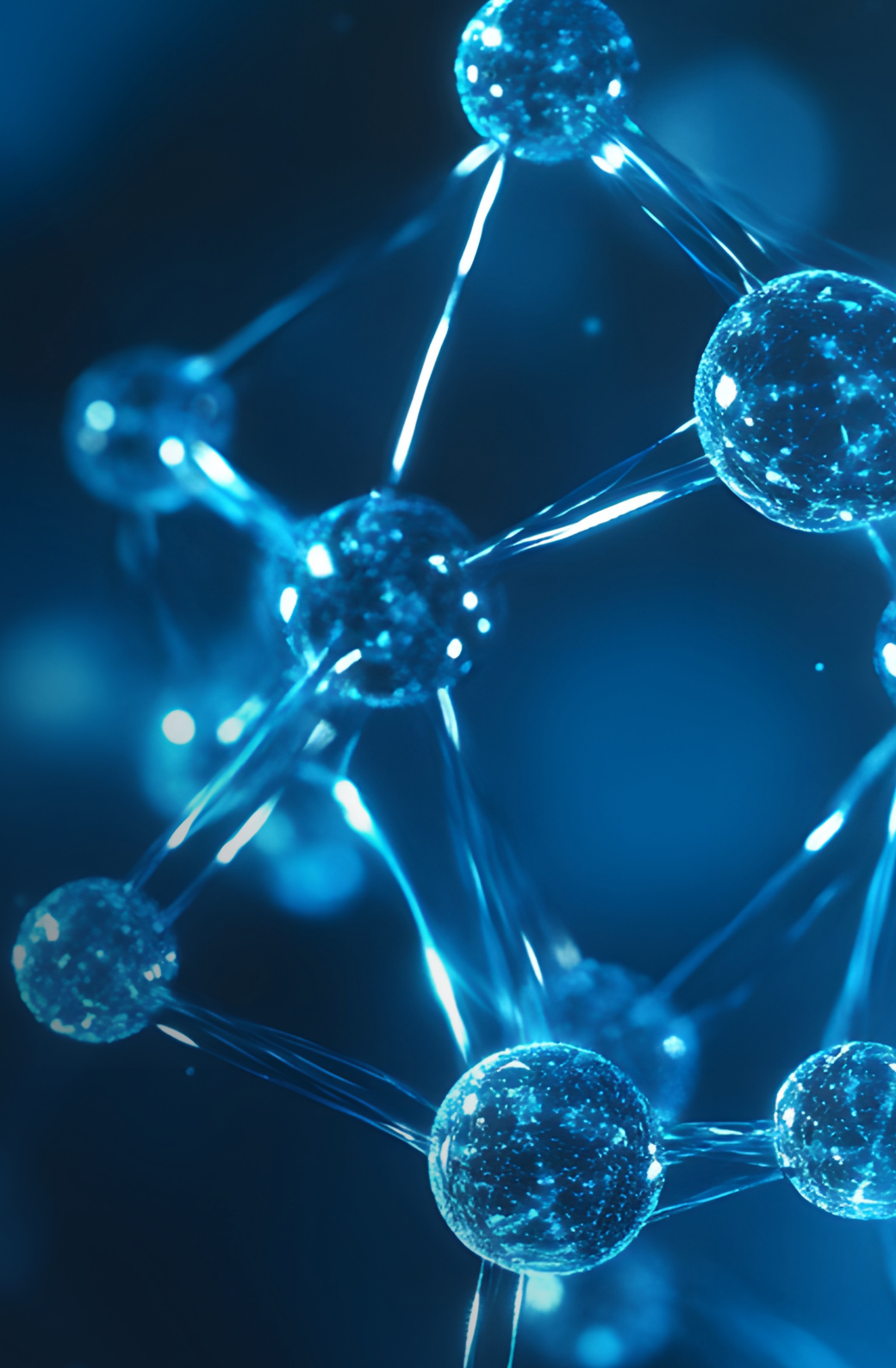
Safeguard IP and patient information through robust data access measures and advanced encryption.

Seamless intelligence sharing

Standardize and share threat insights, keeping teams and organizations across the industry informed and aligned against emerging risks.

Human augmentation

Close the cybersecurity skills gap with AI-powered training, augmentation tools and automated actions that enhance team performance.



Best practices

Five best practices for overcoming AI implementation challenges

Embracing AI-driven security comes with challenges, but the payoff is clear: faster, more accurate threat detection, greater operational efficiency and lower long-term costs that far outweigh traditional methods.

Here our experts offer five key recommendations to help life sciences companies build a robust cybersecurity system:

1. **Review data availability and quality at the program outset**

   Low-quality or fragmented data can compromise AI effectiveness, leading to missed threats or excessive false alarms. This is especially relevant in pharma, as data is often scattered across departments and kept in legacy platforms, making it harder to consolidate and analyze holistically. Engaging specialists at the outset to audit data sources and make targeted investments to ensure data is current, complete and reliable is the key to properly training AI models and operating a high-impact AI-powered cybersecurity strategy.

2. **Create a comprehensive integration strategy**

   Pharmaceutical companies often rely on a mix of legacy and modern IT systems, making it difficult to integrate AI-based cybersecurity tools. Older systems may lack compatibility or require significant customization and expensive upgrades. To avoid inefficiencies and unforeseen costs, integration needs should be assessed early in the project to ensure the final solution is both effective and aligned with the existing infrastructure.

3. **Confirm regulatory compliance**

   AI cybersecurity solutions, including generative and agentic AI tools, must meet the strict requirements of GDPR, HIPAA and other industry regulations. While this process can be both complex and time-consuming, failing to comply risks hefty fines, legal consequences and reputational harm. Engaging experts early can help ensure the system remains compliant while keeping implementation efficient and cost-effective.

4. **Engage employees to leverage new AI tools**

   Successfully implementing AI-driven cybersecurity requires a workforce skilled in both AI technologies and security best practices. Upskilling team members early ensures they have the knowledge to use the system effectively. Early involvement also builds trust and acceptance, addressing common skepticism among stakeholders about the reliability of AI tools. Including employees in planning and deployment helps them understand how the solution protects critical data and enables them to be more effective in their roles.

5. **Stay ahead of evolving threats**

   As cybercriminals constantly develop new tactics to bypass defenses, AI systems must adapt just as quickly. Regular training and updates of AI models are essential but can also be resource-intensive. Planning early for ongoing reviews and updates helps optimize resources and ensures sustained protection.

Key benefits of AI-powered cybersecurity in pharma

Enhanced threat detection
Real-time monitoring and predictive analytics help identify and prevent breaches before damage occurs.

Improved data protection
Safeguards sensitive IP and patient data while ensuring compliance with GDPR and HIPAA.

Increased efficiency
Automates routine tasks to reduce workload, minimize errors and enforce consistent security.

Collaboration
Shares and standardizes threat intelligence for stronger, industry-wide defenses.

Workforce optimization
Augments human teams, closes the skills gap and enhances training through simulations.

Reduced costs
Lowers long-term costs by streamlining operations, minimizing breaches and optimizing resource allocation.

Why us?

Embracing OT security in an evolving world with Cognizant and Microsoft

With over 25 years of life sciences expertise, Cognizant is your trusted digital transformation partner and cybersecurity advisor. We help companies harness advanced digital solutions and build the foundation for secure, sustainable adoption across all sites.

To better support life sciences organizations, the Cognizant and Microsoft partnership offers fully-fledged frameworks to help get things done – from getting small pilot projects off the ground to embedding larger, full-scale systems that make protection a priority.

Together, our proven frameworks, robust infrastructure and intelligent cyber solutions help organizations rapidly assess current capabilities, identify areas for improvement, develop an AI-driven security strategy and scale the use of new tools.

What we do

Cognizant's OT/ICS security practice offers life sciences companies a portfolio of tailored services and accelerators, including:

- Robust advisory services to help clients pilot projects, deploy new solutions and operate at scale
- Digital supply chain capabilities including cyber risk assessment and mitigation
- Cyber risk protection as part of the overall supply chain risk management plan
- Security control assessment, recommendations and implementation to reduce risk of cyberattacks on the IT/OT layer

The future

Faster, stronger, smarter: Outpace cybersecurity adversaries with AI

By 2027, 17% of cyberattacks are expected to employ generative AI[8]. As adversaries weaponize advanced technologies to outpace traditional defenses, it is critical for life sciences organizations to keep pace to protect sensitive patient data, intellectual property and critical operations.

In this rapidly evolving landscape, companies must take proactive steps today to integrate AI, including generative and agentic AI, into cybersecurity strategies. By acting now, pharmaceutical and biotech companies can position themselves to not only meet today's threats but also repel those of tomorrow.

To learn more about how your organization can enable faster threat detection, stronger response, more resilient operations and enhanced compliance with AI, contact our experts today.

[8] https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

Authors

Juan Jose Lopez

Associate Director of Cybersecurity Architecture and Governance – UKI
Cognizant

Simon Hukin

Data & AI Life Sciences Lead – Northern Europe
Cognizant

Revelino Boera

Senior Manager OT Cybersecurity Program, OT Architect – DACH
Cognizant

Rohit Dayama

Life Sciences Market Leader and Global Client Partner – UKI
Cognizant

Cognizant (Nasdaq-100: CTSH) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. Together, we're improving everyday life. See how at www.cognizant.com or follow us **@Cognizant.**

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

280 Bishopsgate
London
EC2M 4RB
England
Tel: +44 (01) 020 7297 7600

India Operations Headquarters

5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096 India
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters

1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower, Singapore 138542
Phone: + 65 6812 4000

WF 4217200