



Building Cybersecurity Immunity in Pharma: A Strategy for CISOs

Keep the Operation Running



Contents

Executive Summary	4
Introduction	6
Overview of Cyber-Physical Systems in Pharmaceutical Manufacturing	7
Advancing Towards Automation: Continuous Manufacturing	8
Digitalizing the OT Environment: Enhancing Efficiency, Tackling Risks	10
Cross-Environment Data Sharing	11
Pharmaceutical Cyber Threats: Real-World Case Studies	13
Ransomware	13
Threats to OT/ICS Systems	15
IP Theft in OT Environments	16
Supply Chain Attacks	17
Good Practices for the Pharmaceutical Sector	19
Strengthen OT Cybersecurity Governance	19
The Key to Implementation: Assemble a Cross-Functional Team	20
Establish Security Architecture for IT and OT	20
Enhance Security with Rigorous Maintenance Tracking	23
Develop a Rapid Response Capability for Cyber Incidents	24
Conclusion	26
Reference	27

Executive Summary

In today's rapidly evolving pharmaceutical landscape, Chief Information Security Officers (CISOs) face an unprecedented confluence of challenges. Accelerated digital transformation, driven by technological advancements and the exigencies of the COVID-19 pandemic, has significantly expanded the cyberattack surface. The industry's shift towards hybrid work models, increased reliance on automated systems, and extensive supply chain integrations have further compounded cybersecurity risks.

Cybercriminals are targeting pharmaceutical companies at an increasing rate, spurred on by the high value of their intellectual property and sensitive data. The sector's complex ecosystem, characterized by a mix of legacy systems and new technologies, creates numerous vulnerabilities. Cyber threats have evolved, with attackers now focusing on data theft and system manipulation rather than merely deploying ransomware.

The consequences of successful cyberattacks are severe, impacting drug formulations, intellectual property, clinical trials, company reputation, and revenue. As such, pharmaceutical companies must adopt a holistic cybersecurity framework that encompasses not just information technology (IT) but also operational technology (OT) and supply chain partners. This publication explores the critical threats and challenges that CISOs must address to safeguard the networks, data, and operations of their organizations.





01

Introduction

The pharmaceutical industry frequently handles vast amounts of sensitive data, including patient information, proprietary formulations, and clinical trial data. To maintain a competitive edge, continuous innovation in new drugs, treatments, and therapies is essential. Consequently, research and development (R&D) data are highly valuable targets for cybercriminals. The most notable example is the launch of COVID-19 vaccines and other breakthroughs in life sciences, which have significantly increased the risk of cyberattacks on the pharmaceutical sector. Attackers may attempt to steal critical research data or disrupt production processes during the vaccine development and distribution phases.

Pharmaceutical companies are advancing toward continuous manufacturing to enhance production efficiency and quality control. They now rely on highly integrated automated systems and data analytics tools, including Manufacturing Execution Systems (MES), public cloud services and interconnected manufacturing environments on the shop floor. This connectivity not only adds potential entry points for cyberattacks but also requires systems to operate continuously and remain highly stable. Any system failure or malicious attack could disrupt continuous production, leading to product quality issues and supply chain interruptions, ultimately resulting in significant losses.



Given the direct impact of pharmaceuticals on human health, governments worldwide impose stringent regulations on drug development and production. In the U.S., the FDA's 2002 "Pharmaceutical cGMPs for the 21st Century" introduced the concept of risk management, emphasizing that regulatory and control measures should be proportional to the level of risk to ensure drug quality and safety. It also stressed the need for pharmaceutical companies to establish comprehensive quality systems, not only to meet current Good Manufacturing Practice (cGMP) requirements but also to continuously improve manufacturing and quality management processes. Furthermore, it encouraged the adoption of Process Analytical Technology (PAT) and Quality by Design (QbD) concepts for real-time process monitoring and control to ensure product consistency and quality.

This paper aims to investigate the unique cybersecurity issues pertaining to pharmaceutical manufacturing, particularly those arising from the widespread adoption of personalized medicine, automation technologies, and continuous manufacturing processes. It includes an exploration of integrated protections for OT and IT systems and proposes specific measures and strategies to address the increasingly sophisticated cyber threat landscape.

02

Overview of Cyber-Physical Systems in Pharmaceutical Manufacturing

In the modern pharmaceutical industry, the advancement of Industry 4.0 has driven widespread adoption of digitalization and automation, significantly enhancing production efficiency and product quality. However, these technological advancements also introduce complex cybersecurity challenges. To effectively address these challenges, it is crucial to understand the architecture and importance of each manufacturing process and equipment. ^[1]

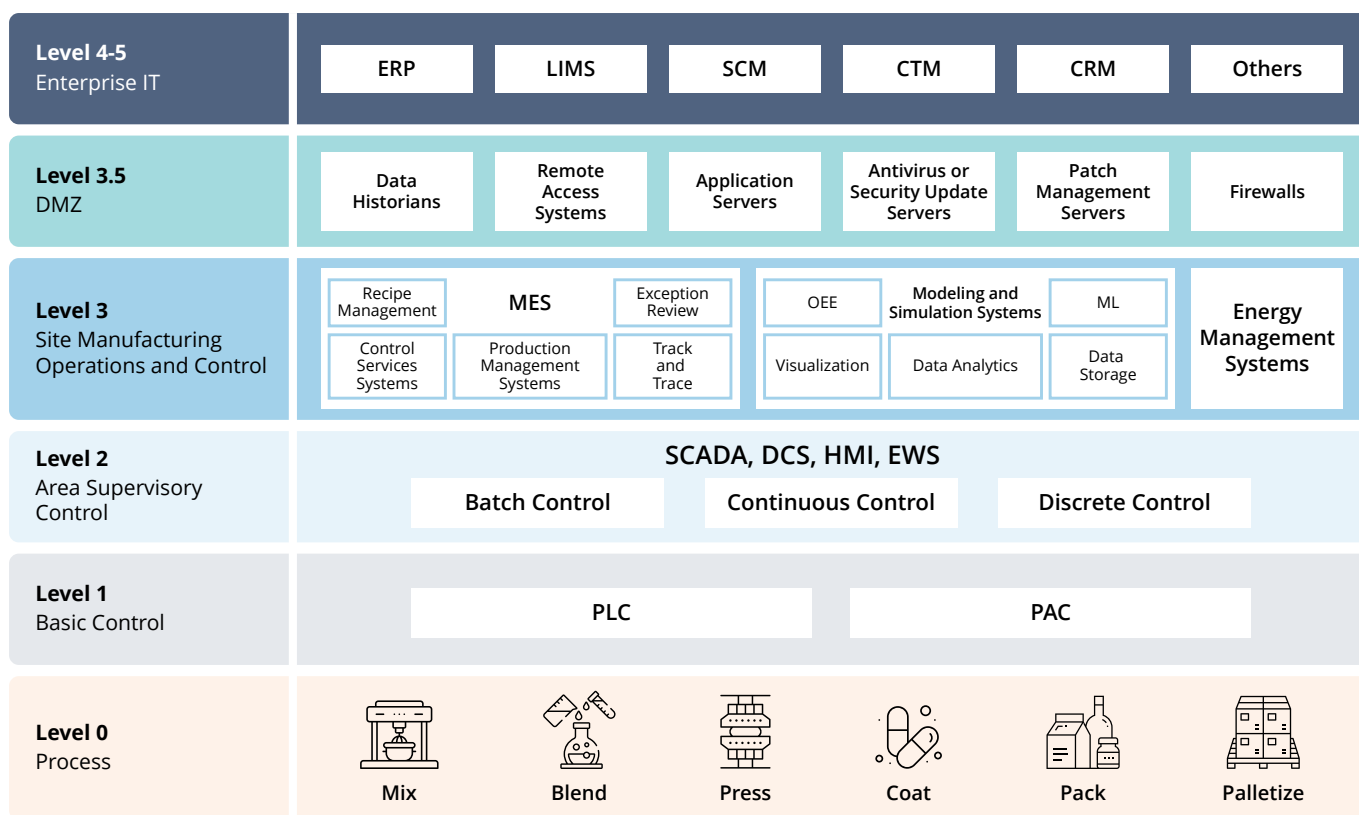


FIGURE 1. Example of CPS Architecture in Pharmaceutical Manufacturing Processes

Advancing Towards Automation: Continuous Manufacturing

Recently, the pharmaceutical industry has been moving towards continuous manufacturing. Compared to traditional batch processing, continuous manufacturing offers higher production efficiency and improved process control. This method allows for uninterrupted production, effectively reducing manufacturing time and costs. However, the implementation of continuous manufacturing relies heavily on highly integrated automated systems and data analysis tools that must operate around the clock and maintain high stability. In the context of Industry 4.0, continuous manufacturing involves several defined steps, each playing a critical role in producing pharmaceuticals.^{[2][3]}

1. Synthesis:



This stage is where chemical reactions produce active pharmaceutical ingredients (API). Continuous reactors ensure that these chemical reactions occur under optimal conditions without interruption, while Process Analytical Technology (PAT) systems continuously monitor reaction conditions and product quality to maintain consistency. Any deviation can impact subsequent steps and compromise product safety.

2. Crystallization:



Following synthesis, the API typically undergoes crystallization, separating the API from the solution and forming solid crystals. Continuous crystallizers maintain optimal conditions, and PAT systems monitor crystal size and shape in real-time, affecting the drug's solubility and bioavailability.

3. Blending:



The crystallized API is mixed with other excipients to form a homogeneous mixture. Continuous blenders ensure the even distribution of ingredients, which is critical for dose accuracy and consistency in oral medications.

4. Granulation & Particle Size Control:



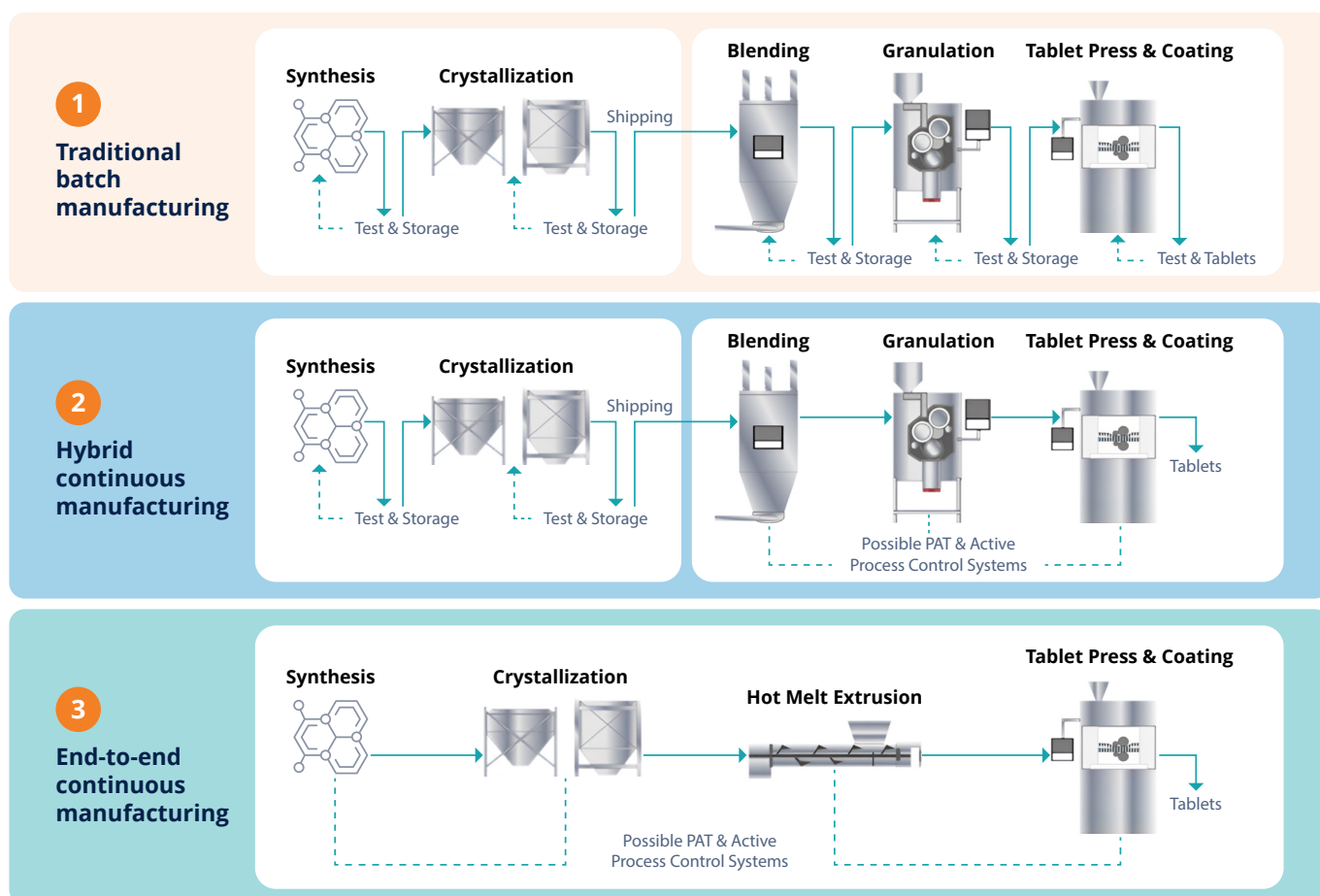
The blended mixture is then granulated, forming granules with controlled size and shape, which are crucial for the drug's dissolution rate and stability. Continuous granulators and particle size controllers unify granule size, enhancing product quality and performance.

5. Tableting & Coating:



In the final step, granules are compressed into tablets and coated as needed for protection, controlled release, or improved taste. Tablet presses and coating machines in continuous manufacturing determine the tablet's appearance, release characteristics, and stability, ensuring high production efficiency and consistent quality.

PROCESS ANALYTICAL TECHNOLOGY (PAT) FOR PHARMACEUTICALS MANUFACTURING LINE



Note: Retrieved from Muzzio, F. J. (n.d.). Continuous manufacturing [Lecture material]. Department of Chemical and Biochemical Engineering, Rutgers University, New Jersey, USA.

FIGURE 2. Pharmaceutical Manufacturing Process

Operational Challenges in Continuous Production

Although the above processes have improved production efficiency and product quality, the heightened connectivity also creates more attack vectors. Each stage of the highly automated pharmaceutical process can become a target for attacks, from data tampering to equipment failures. Pharmaceutical companies' biggest challenges stem from OT systems that are either nearing end-of-life (EOL) or were built without security by design—these are the systems most vulnerable in practice. If the vulnerabilities of process equipment are exposed, PAT systems, continuous reactors, and crystallization equipment may face cyber threats, severely impacting product quality and safety. If data from the blending process is stolen or altered, it could result in the leakage of drug formulas or incorrect ingredient distribution. Similarly, if the control systems of tablet pressing and coating machines are attacked, it could halt the manufacturing process and compromise product quality.

OT cybersecurity is critical here, as any system failure or malicious attack can disrupt continuous production, leading to significant losses. Pharmaceutical companies need to implement comprehensive OT/ICS cybersecurity strategies, particularly to protect critical shop floor assets and maintain product quality.

Digitalizing the OT Environment: Enhancing Efficiency, Tackling Risks

In pharmaceutical factories, the integration of IT and OT is crucial for enhancing production efficiency and product quality. However, this integration also introduces several cybersecurity risks, including vulnerabilities in remote monitoring systems, production management data protection, energy management stability, control system security, and the reliability of modeling and simulation systems.^[4]

TABLE 1. Common Industrial Control Systems (ICS) Used in Pharmaceutical Factories

Purdue Model		Description
Level 3	Site Manufacturing Operations and Control	Systems at this level manage comprehensive manufacturing processes, including Manufacturing Execution Systems (MES), Recipe Management, Exception Review, Track and Trace, and Energy Management Systems. These functions not only ensure production efficiency but also maintain product quality control and compliance. For example, MES manages production planning and operations, while Energy Management Systems help facilities effectively manage energy consumption.
Level 2	Area Supervisory Control	At this level, SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems), HMI (Human Machine Interface), and EWS (Engineering Workstations) provide monitoring and data management for the entire production process. These systems can be categorized into Batch Control, Continuous Control, and Discrete Control, ensuring that production processes in each area operate according to specified parameters.
Level 1	Basic Control	The Basic Control level consists of PLCs (Programmable Logic Controllers) and PACs (Programmable Automation Controllers) used to monitor and control Level 0 production equipment. These controllers execute real-time control logic, such as starting and stopping machines, controlling production parameters, and ensuring safe equipment operation.
Level 0	Process	This is the foundational level that directly interfaces with physical production equipment and processes, including manufacturing operations such as Mix, Blend, Press, Coat, Pack, and Palletize. Equipment at this level includes sensors, actuators, and other control elements responsible for executing specific process operations.

Cyber Risks Specific to Pharmaceutical Research Environments

Remote monitoring systems rely on network connections, making them vulnerable to cyberattacks. Attackers can infiltrate these systems to steal or alter data, or even take control of the equipment. Cyber intrusions targeting laboratory equipment and facility control systems can access sensitive scientific and commercial data, including intellectual property. Cyber-biosecurity vulnerabilities can lead to data breaches, denial-of-service attacks, and malware introduction, severely damaging the organization's reputation and finances, and ultimately threatening its survival.

Additionally, if the laboratory is involved in biopharmaceutical product development, changes in the temperature and humidity of the housing environment can cause stress or death to research animals, which are often expensive and vital to research. Cyberattacks on connected lab tools, such as refrigerators and incubators, can result in the loss of essential chemicals and microorganisms in ongoing research. These cybersecurity risks can cause irreversible damage to principal investigators and the entire organization. Public trust among stakeholders such as students, employees, and investors may diminish, directly threatening the survival of the life sciences industry.

Cross-Environment Data Sharing

During the pandemic, cross-cloud, on-premises, and edge data sharing has facilitated accelerated collaboration to address complex and urgent health issues. This may involve utilizing external-facing applications or even migrating certain functions to public clouds to support core functions critical to competitiveness and market responsiveness. By leveraging cloud and on-premises collaboration, pharmaceutical factories can enhance production efficiency, ensure product quality, and maintain a competitive edge. For example, Pfizer and BioNTech utilized Amazon Web Services (AWS) cloud computing capabilities to accelerate the development of the COVID-19 vaccine and rapidly scale up production, achieving the unprecedented goal of producing billions of doses.^{[5][6]} By processing vast amounts of research data and setting up digital operation centers to monitor production in real-time and resolve issues, they achieved a 20% increase in production capacity.

TABLE 2. Common IT Layers in the Pharmaceutical Industry

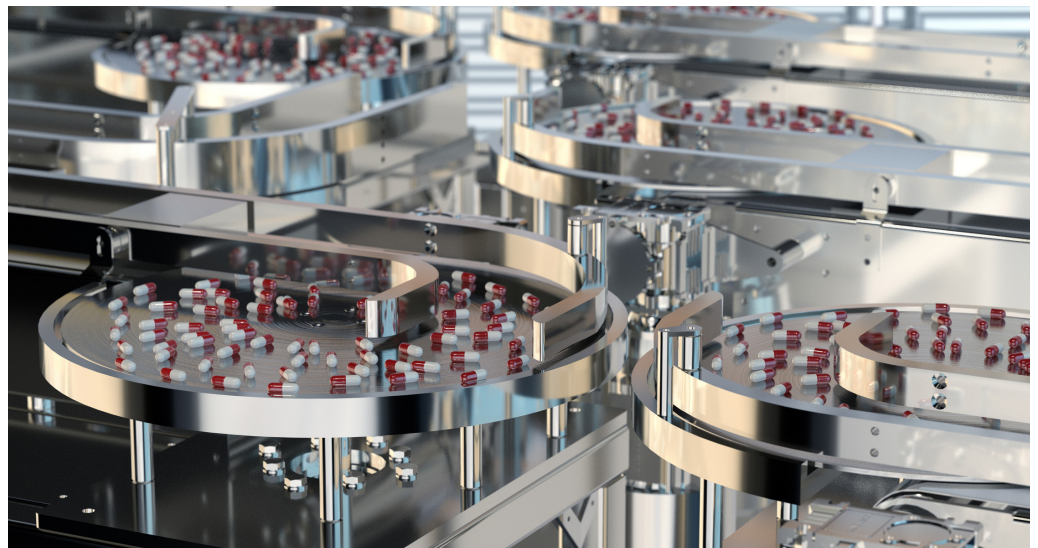
Purdue Model		Description
Level 5	Cloud Services	This architecture represents an enterprise-scale cloud services platform, designed to facilitate strategic decision-making, advanced analytics, and cross-regional collaboration. The adoption of cloud technologies empowers pharmaceutical enterprises to efficiently process substantial data volumes, optimize resource utilization, and drive innovation initiatives.
Level 4	Enterprise IT	The enterprise layer encompasses critical business systems including ERP (Enterprise Resource Planning), LIMS (Laboratory Information Management Systems), SCM (Supply Chain Management), CTM (Clinical Trial Management), and CRM (Customer Relationship Management). These integrated solutions provide comprehensive oversight of production, logistics, financial operations, and sales activities, optimizing enterprise resource allocation. As an example, ERP systems unify multiple business functions, maintaining end-to-end control from raw material procurement through final product delivery.
Level 3.5	DMZ	This level is dedicated to safeguarding information exchange between OT and IT systems. It encompasses data historian systems, remote access infrastructure, application servers, and security update and patch management servers, all working to maintain data security and integrity during cross-network communications.

Cybersecurity Concerns for Pharmaceutical Data Protection

With the advent of personalized medicine, pharmaceutical companies are shifting towards more flexible production modes to meet individual patient needs, particularly in gene therapy and precision medicine. Technologies like synthetic biology and DNA databases are crucial for developing new treatments based on genetic characteristics. However, this involves handling vast amounts of sensitive patient data, making security and privacy protection paramount. This sensitive data includes clinical trial results, proprietary formulas, and patient information. Data breaches can lead to intellectual property loss, legal liabilities, and a trust crisis, threatening the long-term viability of the company.

Recently, several cybersecurity incidents have occurred, the most common being the leakage of sensitive data such as formulas, clinical trial data, and patient information from public cloud systems. Due to the stringent regulatory environment of the pharmaceutical industry, this data has become a primary target for hackers.

Additionally, integrating some companies' cloud applications with IT and OT systems in pharmaceutical factories increases the complexity and potential security risks. The supply chain of cloud systems is extensive, and any security vulnerability in any part of the chain can be exploited. Therefore, choosing compliant cloud providers, managing supply chain security, and implementing secure system integration are critical to the safety and stability of manufacturing processes.



03

Pharmaceutical Cyber Threats: Real-World Case Studies

Ransomware



From a pharmaceutical manufacturing perspective, ransomware is a highly targeted form of malicious software designed to encrypt or block access to critical production systems and data until a ransom is paid. The pharmaceutical industry relies on stable and continuous operations to ensure the development and production of drugs, making ransomware attacks particularly devastating. These attacks are often highly sophisticated, with attackers frequently employing social engineering techniques to obtain employee login credentials, which are then used to infiltrate the factory's network. Once inside, the attackers deploy ransomware to encrypt essential production data. Recent observations indicate that ransomware groups are increasingly leveraging Initial Access Brokers (IABs) to gain entry into organizational networks, thereby enhancing the efficiency of their attacks.

Case Study: Ransomware Attack on Merck (2017)

In 2017, the NotPetya incident struck approximately 40,000 Merck computers, destroying data and forcing a months-long recovery process. This attack impacted thousands of multinational companies, including FedEx, Mondelez, Saint-Gobain, and Maersk, resulting in an estimated \$10 billion in total damages.^[5]

The NotPetya malware initially gained access through the update process of the Ukrainian tax software MEDoc. It then exploited the EternalBlue SMBv1 vulnerability to spread across networks by attacking machines. Additionally, it employed other propagation techniques to infect even patched machines, such as using a modified version of Mimikatz to extract user passwords from the Local Security Authority Subsystem Service (LSASS) process. The malware was designed to spread rapidly across networks without user interaction, sometimes shutting down computers within minutes.^[6]

Once executed, it overwrote the master boot record, preventing the system from booting. Although a ransom note demanded payment for decryption, NotPetya's true intent appeared to be pure destruction. The damage it caused was irreversible, permanently wiping files with no hope of recovery.

Impact on the Pharmaceutical Industry

The NotPetya cyberattack caused significant losses to pharmaceutical giant Merck, leading to a major legal dispute. Merck filed claims of up to \$1.4 billion with its insurance providers, reflecting the severe financial impact of the attack. This case, which was heard by the New Jersey Supreme Court, garnered significant attention due to its potential far-reaching implications for the cyber insurance industry.^[7] When critical production systems are encrypted, multiple production lines may be forced to shut down. This not only directly disrupts the production and supply of medicines but also triggers a series of dire consequences. For instance, core intellectual property, such as research data, production formulas, and clinical trial results, may face the risk of permanent loss, profoundly affecting the company's new drug development pipeline and existing drug production. Additionally, large-scale data recovery efforts and system reconstruction usually come at a high cost.

- **Supply Chain Attack Vectors:** The initial spread through infected Ukrainian accounting software updates highlights the importance of supply chain security checks and software update management.
- **Destructive Ransomware:** NotPetya's primary objective was destruction, not ransom. This means that even if a ransom were paid, the data would not be recoverable. Pharmaceutical companies must prioritize prevention and rapid recovery capabilities, as the option of paying a ransom may not even be available—making the worst-case scenario far more severe than a financial loss.
- **Rapid Lateral Spread:** The exploitation of the EternalBlue vulnerability emphasizes the importance of network segmentation, particularly the segmentation of OT from IT.
- **Credential Extraction Capability:** Techniques similar to Mimikatz attacks were used to extract credentials from LSASS, highlighting the need for enhanced identity authentication and the implementation of privileged access management.
- **Vulnerabilities in OT Systems:** The outdated systems in pharmaceutical production environments are particularly susceptible to attacks, potentially leading to production disruptions. This calls for dedicated OT security strategies, including the protection of industrial control systems.

Threats to OT/ICS Systems



In the pharmaceutical industry, OT and ICS are crucial for the smooth operation of manufacturing processes, from maintaining precise environmental conditions to ensuring the integrity of production lines. However, modern programmable logic controllers (PLCs) are highly interconnected and integrated, supporting multiple communication protocols such as Ethernet/IP, Modbus, and Profinet, particularly in conjunction with Supervisory Control and Data Acquisition (SCADA) systems. Additionally, remote monitoring and maintenance are key features, and with the help of Internet of Things (IoT) technology, PLC systems can enable remote monitoring, fault diagnosis, and maintenance, thereby enhancing production efficiency and equipment uptime.

Due to the limitations of legacy equipment or resource constraints, many security measures common in IT environments (such as EDR and access control) are challenging to implement in OT environments. The unique demands of operational environments make regular software updates impractical, or even impossible, as this could mean halting production. Attackers typically exploit vulnerabilities to gain access to devices, then use SSH to establish a connection and tunnel into internal systems. Once inside, they deploy malware that sends attack commands to proprietary controller network communication protocols like Modbus and Profinet. For pharmaceutical companies, such attacks pose a serious threat. The disruption of industrial sensors could lead to catastrophic failures in production, such as incorrect dosage formulations, contamination risks, and complete shutdowns. Furthermore, since many pharmaceutical companies' CISOs traditionally focus on IT assets, overlooked OT systems may become a vulnerable entry point for cybercriminals. This not only results in operational downtime but could also lead to regulatory violations, product recalls, and severe reputational damage.

Case Study: EKANS Malware Targeting OT/ICS

EKANS was first discovered in late 2019 and is a type of ransomware specifically targeting industrial control system (ICS) environments.^[8] The emergence of this malware marks a turning point where cybercriminals began to focus attacks on OT environments. EKANS contains a hardcoded list of processes specifically targeting ICS-related software. By terminating these processes, EKANS can cause industrial control systems to lose their monitoring and control capabilities, significantly impacting system operations. In addition, EKANS uses RSA and AES encryption schemes to encrypt files, appending the ".ekans" extension to the encrypted files, further compounding the damage to victims. After the encryption process is completed, EKANS leaves a ransom note on the victim's desktop demanding payment. Unlike some other ICS malware, EKANS does not possess self-propagating worm capabilities, meaning that attackers may need to manually deploy or use other methods to spread the ransomware across networks.

Impact on the Pharmaceutical Industry:

EKANS malware poses a significant threat to the pharmaceutical industry, as attackers could forcibly shut down or damage equipment, steal intellectual property, and even cause major health and safety risks. The unique nature of pharmaceutical manufacturing means that any system failure could have severe consequences.^[9] Issues ranging from incorrect dosage formulations to complete production line shutdowns and potential contamination risks not only threaten the financial health of the company but also jeopardize the strict regulatory environment. In the pharmaceutical industry, where continuous production must comply with current Good Manufacturing Practices (cGMP), Good Automated Manufacturing Practices (GAMP), and Federal Regulation Title 21 (CFR21), such issues could result in regulatory penalties and reputational damage.

IP Theft in OT Environments



In the pharmaceutical industry, intellectual property (IP) theft has traditionally been seen as a primary risk within enterprise IT environments. However, as digital transformation deepens, trade secrets utilized in OT networks may encompass a wide range of sensitive data, including processes, operational documents, and experimental results.^[10] For instance, in the biopharmaceutical industry, the explosive growth of biologics over the past 20 years has created highly valuable information. These drugs are difficult to manufacture, making companies eager to protect their intellectual property and trade secrets. If this information is compromised by hackers or exposed publicly, it could result in the loss of first-to-market advantage, decreased profitability, or even the takeover of entire business lines by competitors or counterfeiters.^{[11][12]}

Furthermore, due to the high costs of the machinery and operational expenses required in pharmaceutical manufacturing, some biotech companies outsource drug production, forcing them to share proprietary secrets with contract manufacturers. To safeguard company interests, contracts should stipulate the confidentiality obligations of the manufacturing facilities and require them to establish control mechanisms to prevent data leaks.

Case Study: The EMA Covid-19 Data Leak

In December 2020, COVID-19 vaccine data from Pfizer and German biotech company BioNTech was accessed following a cyberattack on the European Medicines Agency (EMA) in Amsterdam, Netherlands. During the pandemic, cyberattacks targeting healthcare institutions and pharmaceutical companies became more frequent, with hackers—including state-sponsored spies and cybercriminals—seeking to capture the latest information related to the pandemic.^[13]

Implications for the Pharmaceutical Industry

The pharmaceutical industry handles highly sensitive and valuable information, including trade secrets, intellectual property, personal health data, and confidential research data. In the context of IT/OT convergence, major concerns include:

- **Strengthening LIMS and R&D Equipment Security:** Laboratory Information Management Systems (LIMS) and R&D equipment store highly sensitive data, including experimental results, intellectual property, and proprietary research. Enhancing the security of these systems is crucial to protecting this valuable data from cyber threats.
- **Data Classification and Access Controls:** Implementing strict data classification categorizes information based on its sensitivity and criticality. Access controls ensure that only authorized personnel can access sensitive data, reducing the risk of data breaches or leaks. This is a standard best practice in cybersecurity.
- **Protecting OT Systems with Critical Parameters:** OT systems that manage production processes, such as Batch Record Systems and Manufacturing Execution Systems (MES), are essential for maintaining product quality and consistency. Securing these systems helps prevent disruptions that would otherwise lead to costly production errors.
- **Change Management Processes:** Implementing change management processes ensures that any modifications to critical production parameters are documented, reviewed, and approved. Monitoring and auditing these changes are vital to prevent unauthorized or incorrect adjustments from disrupting production or compromising product integrity.

Supply Chain Attacks



Supply chain attacks pose a significant cybersecurity threat to the pharmaceutical industry, as threat actors target third-party entities to indirectly access core operations. These attacks often exploit vulnerabilities in the supply chain, such as compromised software suppliers or service providers, to introduce malware or other malicious code into a company's systems.

For example, an attacker might infiltrate a pharmaceutical company's software supplier, embedding malware within a routine software update. When the update is distributed, the malware is introduced into the pharmaceutical company's network, potentially compromising sensitive data, disrupting manufacturing processes, or tampering with critical research and development information.

Case Study: SolarWinds Supply Chain Attack

The SolarWinds hack in December 2020 is a prime example. In this case, hackers targeted the software update mechanism of a third-party supplier, embedding malware that ultimately spread to multiple U.S. government agencies. This type of attack highlights the vulnerabilities in extended supply chains, particularly in complex operational environments like those in the pharmaceutical sector, where multiple third-party vendors and suppliers are often involved.^{[14][15]}

Impact on the Pharmaceutical Industry

Supply chain attacks in the pharmaceutical industry can lead to catastrophic consequences, including the theft of intellectual property, disruption of drug development and production processes, and potential harm to patient safety. The complexity of pharmaceutical supply chains, coupled with their reliance on numerous third-party suppliers, creates multiple points of vulnerability that can be difficult to secure.

A successful attack can undermine the integrity of research data, delay product launches, and result in regulatory penalties, not to mention significant reputational damage. It is crucial to assess and monitor the IT/OT security posture of partners, such as Contract Research Organizations (CROs) and Contract Manufacturing Organizations (CMOs), and establish secure data-sharing mechanisms, particularly when involving regulatory bodies.

As the pharmaceutical industry continues to advance technologically, the importance of securing the entire supply chain—particularly software and service providers—cannot be overstated. Robust vetting processes, continuous monitoring, and strong cybersecurity practices across all supply chain partners are essential to mitigating these risks.



04

Good Practices for the Pharmaceutical Sector

Pharmaceutical companies must adhere to regulations set by organizations like the U.S. Food and Drug Administration (FDA), European Medicines Agency (EMA), Good Manufacturing Practices (GMP), or Good Automated Manufacturing Practice (GAMP), while also protecting themselves from various cyber threats. TXOne Networks recommends the following good practices and secure operations with asset-centric lifecycle protection to mitigate potential threats that pharmaceutical factories might face.^[16]

Strengthen OT Cybersecurity Governance



Robust OT cybersecurity governance is crucial in the pharmaceutical industry, where precision, safety, and compliance are paramount. OT systems manage key aspects of drug manufacturing, such as temperature regulation, mixing processes, and quality control. Disruptions or failures in these systems can compromise product quality, lead to regulatory breaches, and cause significant financial losses. Implementing OT cybersecurity governance establishes structured risk management and maintains cybersecurity measures that align with industry standards and regulatory requirements.

- **Develop an OT Cybersecurity Plan**

Gaining management support for OT cybersecurity initiatives is key to ensuring long-term commitment and resource allocation. Start by identifying business objectives and demonstrating how the cybersecurity plan reduces risks and protects these objectives. The business value of the plan should align with the concerns of senior management and include performance metrics to showcase the plan's impact.

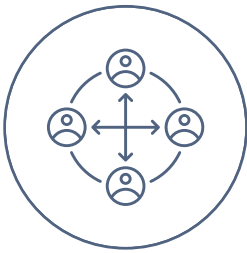
- **Integrate with Enterprise Risk Management**

Any compromise in OT systems can lead to significant operational downtime, product recalls and even patient harm due to compromised drug quality. By adopting a structured risk management framework (RMF) specifically for OT, pharmaceutical companies can proactively identify, assess, and mitigate cybersecurity risks, ensuring the continuous and safe operation of their manufacturing processes.

- **Develop Comprehensive Policies and Procedures**

It is essential to define OT-specific policies and procedures. This can be done by a) incorporating regulatory requirements from bodies like the FDA and EMA into security policies, b) ensuring that OT security measures align with GMP and GAMP 5 standards, and c) establishing data lifecycle management policies to ensure the security of production systems. This is how pharmaceutical companies can safeguard their production environments against evolving cyber threats and operational risks.

The Key to Implementation: Assemble a Cross-Functional Team



Enhancing OT and supply chain cybersecurity requires a cross-functional team that should include key members such as the Chief Information Security Officer (CISO), plant managers, and procurement managers. Ideally, this team would function as follows: The IT department, led by the CISO, would provide critical support for OT security through its cybersecurity experience. Despite the significant cultural differences between control engineering and IT, their integration is essential for creating effective security designs and smooth operations. The involvement of plant managers and OT professionals in the security team would help identify network vulnerabilities and their potential impacts. They would be able to define cybersecurity roles, manage OT security programs, and develop network mitigation measures based on OT design and security insights.

Meanwhile, the procurement department would address cybersecurity threats before products enter the plant by reviewing and evaluating vendors' information security practices, establishing clear cybersecurity roles and responsibilities for third party providers. Their risk assessments would also promote supply chain cybersecurity awareness and support compliance with cybersecurity controls. Through this cross-departmental collaborative effort, each department's function would be fully utilized, collectively reinforcing a successful OT security program.

Establish Security Architecture for IT and OT



Unlike traditional IT systems, any disruption in OT systems can lead to severe product quality issues, regulatory violations, and threats to patient safety. Therefore, establishing a dedicated OT security defense framework has become an urgent priority. At the core of this framework is the implementation of an asset-centric strategy to protect the production environment from evolving cyber threats and operational risks.

Proactively Identify Cyber Risks

Effective cybersecurity risk management is a critical component of OT protection. Regular assessments of the enterprise's OT system operations, data processing, storage, and transmission can significantly reduce cybersecurity risks related to OT operations, assets, and personnel. This management framework includes several key aspects:

- **IT/OT Asset Management:** Implementing a comprehensive and precise IT/OT asset inventory is the foundation for effective risk management in the OT environment. Accurate asset information supports multiple risk management objectives, including threat assessment, vulnerability management, and legacy asset tracking.
 - ✓ **Hardware Asset Management:** Track computing and networking equipment within the OT environment, including detailed information and location of each device.
 - ✓ **Software and Firmware Asset Management:** Track software and firmware installed on OT components, including version numbers, location data, and Software Bill of Materials (SBOM).

- **Threat and Vulnerability Management:** All machines and equipment must undergo threat and vulnerability scans before deployment, with any identified security issues documented. All known security issues must then be resolved before deployment. For example, the severity of vulnerabilities, calculated using the Common Vulnerability Scoring System (CVSS), must be below the acceptable residual risk level in the product's security environment.
- **Supply Chain Security Management:** Require product suppliers to manage security risks through supply chain contract management, making it a criterion for future equipment procurement evaluations.

Zero Impact Network Defense

OT network defense utilizes network segmentation, access control, virtual patching, and enhanced intrusion detection to prevent vulnerable assets from leading to large-scale disasters. This approach not only simplifies monitoring processes but also makes it more difficult for hackers to gather information or move laterally within the OT network. Recommended OT network deployments include:

- **Network Segmentation:** Divide the network into internal zones and micro-segments based on technology, bandwidth, and communication protocols. Micro-segmentation allows users to narrow the protection scope to specific areas or even individual assets, ensuring industrial network visibility and protocol filtering without altering the existing network architecture.
- **Virtual Patching Technology:** Implemented through OT Intrusion Prevention Systems (IPS) or network IPS, these devices filter packets to defend against known vulnerabilities without forcing endpoint security updates, circumventing the need for system reboots and production line downtime.
- **Network Allowlisting:** Supports deep analysis of various ICS protocols and L2-L7 network traffic, enabling the creation and editing of protocol commands and endpoint connection whitelists. All hardware protection devices can be visually monitored and managed through a central control platform, reducing risk by enforcing the principle of least privilege.

The Edge solution suite proactively protects OT assets and eliminates malicious activities during critical production phases, ensuring the reliability, safety, and availability of industrial processes and infrastructure in pharmaceutical plants. TXOne's unique automatic rule generation feature within Edge offers a significant advantage for pharmaceutical companies and organizations. It drastically reduces the months-long preparation time typically needed for effective network segmentation in OT environments, allowing operations to continue smoothly during cybersecurity incidents.

- **Efficient Network Segmentation:** Network segmentation is crucial for controlling and mitigating the impact of security incidents. However, because each network segment involves different applications, software, and hardware, creating network rules is often time-consuming and costly. The TXOne Edge V2 engine simplifies this process by automatically generating and learning network rules.

- **Virtual Patching Technology:** The Edge solution also offers in-line virtual patching capabilities, enabling proactive defense against vulnerabilities without downtime. It provides flexible deployment options, supports a layered defense strategy, and allows for deep analysis across various network protocols.
- **Intelligent OT Protocol Allowlisting:** Edge features an operationally focused OT network visualization and advanced intelligent OT strategy deployment mechanism. Organizations can utilize Edge to analyze network traffic and automatically generate OT protocol allowlists tailored to their specific infrastructure.

All-in-One Endpoint Protection

TXOne Networks offers a next-generation cybersecurity solution designed for critical OT assets, utilizing Cyber-Physical Systems Detection and Response (CPSDR) technology to prevent any unintended system changes from affecting operations. It is the first solution to simultaneously provide both seamless protection and comprehensive oversight for both legacy and modern OT assets.

- **Industrial-Grade Next-Generation Antivirus:** TXOne Stellar supports malware scanning for network drives and removable media, significantly enhancing security and reducing infection risk.
- **Operational Behavior Anomaly Detection:** Uses advanced algorithms and analytics to identify and block any abnormal behavior in system operations in real-time, providing protection against fileless malware attacks.
- **Application Lockdown:** This cutting-edge feature prevents any unauthorized activities within the system, ensuring operational integrity, reducing downtime, and lowering recovery costs, making it especially valuable for "unpatchable" systems.
- **Trusted Peripheral Control:** TXOne Stellar's USB vector control feature primarily blocks unauthorized use of external storage media. However, it can be configured to allow specific external storage devices based on device identification parameters such as vendor ID, product ID, or serial number, granting access only to trusted devices.



Enhance Security with Rigorous Maintenance Tracking

In the pharmaceutical industry, security in the Operational Technology (OT) environment is not a one-time implementation but a dynamic, ongoing process of continuous improvement. To adapt to the ever-evolving threat landscape, companies must regularly review and update their security measures. This approach not only enhances security performance but also ensures compliance, which is particularly crucial in the highly regulated pharmaceutical sector.

Continuous Security Improvement Strategy

- **Resource Allocation:** Companies should allocate dedicated resources for regular security reviews and updates.
- **Regular Assessments:** Conduct routine evaluations of security effectiveness, including vulnerability scans and penetration testing.
- **Adaptive Adjustments:** Adjust and enhance security measures promptly based on assessment results and emerging threats.
- **Maintenance Log Management:** Maintain detailed logs of maintenance activities to support audits and compliance checks.

Application of Innovative Security Tools

The use of innovative tools is essential for conducting effective security checks without disrupting production. TXOne Networks' Portable Inspector is one such advanced tool designed specifically for OT environments.

Features and Benefits of TXOne's Portable Inspector

Portable Inspector is designed as a USB flash drive that can scan and remove malware from assets without requiring software installation. This feature is particularly valuable for pharmaceutical companies, as it allows malware detection without altering complex manufacturing equipment, ensuring compliance with industry regulations such as FDA's CFR Title 21 Part 11.

Key benefits include:

- **Minimized Impact:** Reduces the impact of third-party software on production equipment, avoiding violations of vendor warranty terms.
- **Offline Scanning Capability:** Offers offline malware scanning, even in air-gapped environments.
- **Rapid Inspection:** Quickly inspects electronic devices from personnel and vendors, automatically performing cleanup or quarantine operations if necessary.
- **Asset Data Capture:** Records asset information during each scan and transmits it to a central management console for review and archiving.
- **Secure Data Transfer:** AES-256 hardware encryption secures data transmission, protecting files and maintaining data integrity.

By combining stringent maintenance strategies with advanced security tools like Portable Inspector, pharmaceutical companies can significantly enhance the security of their OT environments while ensuring continuity and compliance in their production processes. This approach not only addresses current security challenges but also lays a strong foundation for future threat defense.

Develop a Rapid Response Capability for Cyber Incidents



In the pharmaceutical industry, the impact of cybersecurity incidents can be far more severe than in other sectors. Even minor system disruptions can result in significant consequences, including substantial financial losses, stringent regulatory penalties, and risks to patient safety. Therefore, establishing a swift and effective incident response capability is a critical task for pharmaceutical companies. A comprehensive incident response strategy not only enables the rapid containment and mitigation of cyberattacks but also minimizes downtime and prevents security breaches from escalating into more serious crises.

To achieve this, SageOne offers a multidimensional cybersecurity posture visualization platform, providing pharmaceutical companies with a comprehensive and detailed security perspective. This solution is particularly suited to the fast-paced incident response needs of the pharmaceutical industry, with key features including:

1. CPS Attack Surface Management: In the OT environment of the pharmaceutical industry, visibility is the cornerstone of cybersecurity. SageOne offers an overarching view of the security posture, helping to identify security focal points within the OT environment by:

- **Displaying the ratio of protected to unprotected assets**
- **Monitoring asset health and detect anomalies**
- **Assessing asset exposure levels**
- **Providing an overview of the asset lifecycle**

Through this comprehensive visibility, pharmaceutical companies can quickly identify potential threat entry points, prioritize high-risk areas, and enhance the efficiency and accuracy of incident response.

2. Integrated Lifecycle Protection: In the complex pharmaceutical production environment, centralized management is crucial for simplifying cybersecurity governance and achieving coordinated defense. SageOne acts as an abstraction layer, streamlining data contextualization and integration across multiple products by:

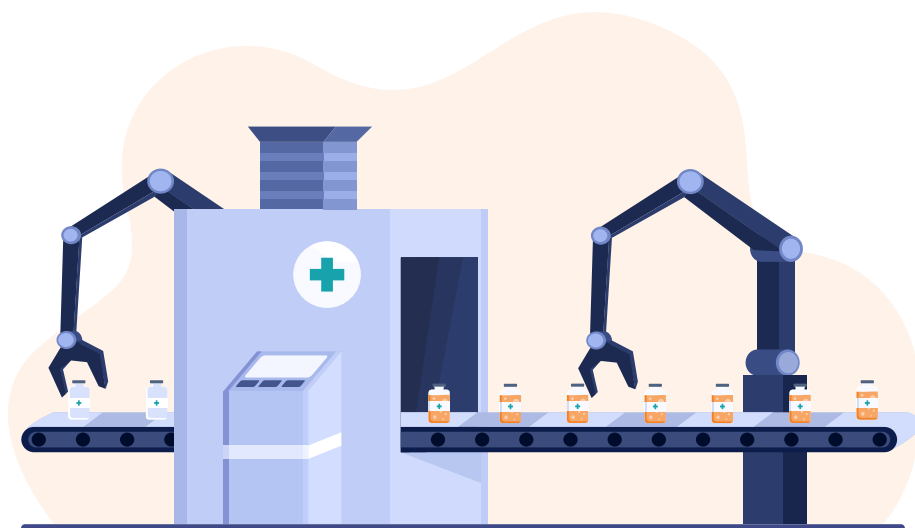
- **Providing customized, mission-driven dashboards for executives, security personnel, and plant leaders**
- **Simplifying cross-departmental security collaboration, ensuring rapid and unified incident response**
- **Optimizing resource allocation to improve response efficiency**

This integrated approach enables pharmaceutical companies to quickly mobilize and coordinate resources in the face of cyber incidents, leading to more effective responses.

3. CPS Threat Detection and Response: In the dynamic threat environment of the pharmaceutical industry, addressing both known and unknown threats is crucial. SageOne provides comprehensive support in this area by:

- **Compiling security insights from multiple solutions**
- **Proactively scouting potential risks to provide early warnings**
- **Initiating rapid response mechanisms when necessary**

Through this comprehensive threat intelligence and response capability, pharmaceutical companies can more quickly detect and respond to various cybersecurity threats, whether they are targeted attacks on production systems or widespread threats impacting the entire supply chain.





Conclusion

Pharmaceutical companies are navigating an era of rapid digital transformation driven by the adoption of advanced technologies such as AI, IoT, and robotics. These technologies, while enhancing operational efficiency and innovation, also introduce new cybersecurity vulnerabilities. A unified platform approach that provides end-to-end protection and visibility is essential to mitigate these risks. This approach should cover data, remote devices, network infrastructures, and the entire ecosystem to ensure compliance and rapid response to cyber threats.

The future of cybersecurity in the pharmaceutical industry lies in the establishment of an integrated IT and OT security architecture. This security architecture is designed to leverage asset-centric lifecycle protection for security inspection, endpoint protection, network segmentation, anomaly detection, access control, and comprehensive incident response plans. By understanding and addressing all potential threat vectors, pharmaceutical companies can build a secure and mature cybersecurity posture, ensuring the protection of their critical assets and maintaining a competitive edge.

Reference

- ^[1] Ingrid Carla Reinhardt, Dr. Jorge C. Oliveira, Dr. Denis T. Ring, "Current Perspectives on the Development of Industry 4.0 in the Pharmaceutical Sector", *Journal of Industrial Information Integration*, 2020.
- ^[2] Roger van den Heuvel, Chris Stirling, "Pharma Outlook 2030: KPMG Pharmaceutical Industry Perspective", KPMG, 2024.
- ^[3] Lee, S.L., O'Connor, T.F., Yang, X. et al. Modernizing Pharmaceutical Manufacturing: from Batch to Continuous Production. *J Pharm Innov* 10, 191–199, 2015.
- ^[4] N. Sarah Arden, Adam C. Fisher, Katherine Tyner, Lawrence X. Yu, Sau L. Lee, Michael Kopcha, "Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future", *International Journal of Pharmaceutics*, 2021.
- ^[5] Jen Frost, "Merck and insurers settle \$1.4 billion NotPetya cyberattack case", *Insurance Business Asia*, Jan. 09, 2024.
- ^[6] Andy Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history", *Wired*, Aug. 22, 2018.
- ^[7] David Jones, "Merck reaches settlement in closely watched NotPetya insurance case", *Cybersecurity Dive*, Jan. 08, 2024.
- ^[8] Dragos, Inc., "EKANS Ransomware and ICS Operations", Dragos, Feb. 03, 2020.
- ^[9] Trend Micro, "New Critical Infrastructure Facility Hit by Group Behind TRITON", *Trend Micro*, Apr. 11, 2019.
- ^[10] John Norman, Patrick Duxbury, "Combatting cybercrime: critical for life science companies", *European Pharmaceutical Review*, Apr. 24, 2017.
- ^[11] Pfizer, "Shot of a Lifetime: How Pfizer and BioNTech Developed and Manufactured a COVID-19 Vaccine in Record Time", *Pfizer.com*, May 24, 2022.
- ^[12] Amazon Web Services, "Pfizer accelerates innovation with AWS cloud services and generative AI", *Amazon.com*. Accessed Aug. 20, 2024.
- ^[13] Abi Millar, "Pharma cyber attacks: the growing threat", *Pharmaceutical Technology*, Nov. 22, 2022.
- ^[14] Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations", Dec. 17, 2020.
- ^[15] U.S. Senate Select Committee on Intelligence, "Hearing on the Hack of U.S. Networks by a Foreign Adversary", Feb. 23, 2021.
- ^[16] Stouffer, Keith, Joe Falco, Karen Scarfone, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. *Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82r3*. National Institute of Standards and Technology, 2023.

