An open target

Despite progress in corporate cybersecurity, life sciences operational technology is still vulnerable to increasingly sophisticated threats
Since patient data and intellectual property (IP) have been chief targets of cybercriminals, life sciences’ cybersecurity functions have been focused on corporate information technology (IT). Attacks on these systems can cause potential harm to patients, loss of trust, reputational damage, business disruption, and regulatory penalties—negative outcomes that are very serious and very real.

On the other hand, there is a growing threat that is receiving limited focus, and that is the threat to operational technology (OT)—the technology that runs the manufacturing floor and distribution centers, as well as R&D facilities and labs. In the past, these industrial control systems (ICS), which include critical supervisory control and data acquisition (SCADA) functions, were outside the realm of cybersecurity concern, as they were siloed from corporate networks.

However, things have changed with the introduction of the industrial internet of things (IIoT) and interconnected factories, i.e., factories that connect to the corporate environment and other factories and that involve enhanced internal connectivity between systems. While extraordinarily impactful in terms of productivity and business analytics, these technological advances dramatically expose OT environments to attack.¹

Following are some examples of potential OT cyber threats that could put the viability and integrity of both medical device and pharmaceutical manufacturing at risk:

— Malware specifically designed to cause disruption to ICS, e.g., by targeting safety systems that prevent overflows or triggering manufacturing systems to shift into high-alert mode
— Faults forced into the quality assurance (QA) process, which can have dangerous impacts on the long-term functioning of postmarket medical devices, e.g., pacemakers, insulin pumps, etc.
— Compromise of programmable logic controllers (PLCs), exposing industrial system data, and raising the risk of programming alterations, all of which could cause significant damage to connected equipment
— Theft by state-sponsored criminals of valuable intellectual property utilized in the manufacturing process, e.g., parts schematics, product recipes, and processes.

An expanding risk landscape

Given the intense focus on cybersecurity programs to protect IT, why has there been so little emphasis on securing OT environments? The answer is that cybersecurity budgets have traditionally excluded funds for OT, as addressing the risks correctly and at scale were viewed as prohibitively expensive.

By contrast, today’s organizations are making the argument to corporate boards, committees, and other decision makers that it is critical to invest in OT cybersecurity measures due to the seriousness of the risks if this environment is exposed. Specifically, they are driving awareness of how certain market, operational, and regulatory factors are contributing to a wider risk landscape. For example:

1. The industry’s growing focus on consumer needs and preferences

   The increasing shift from blockbuster drugs to smaller patient cohorts, specialty drugs, and personalized medicine means that valuable—and vulnerable—patient data is needed on the manufacturing floor to customize products and delivery systems. While segmented supply chains and contract manufacturing are necessary to support rapid shifts in product focus, additional players in the supply chain could increase the attack vectors for harmful malware to infiltrate the OT environment. Further, as organizations seek to expand or rationalize their product portfolios, many are turning to partnerships and alliances with technology- and consumer-focused life sciences and healthcare companies, which brings additional third-party risk.

   The shift to consumerism and specialized drug development requires access to previously siloed patient data and IP during production.
2. Increasing digital disruption

Disruptive digital technologies from blockchain to predictive analytics to artificial intelligence (AI) and the IIoT are playing an increasingly important role in expediting not only the life sciences manufacturing process, but also supply chain management, compliance operations, clinical trials, drug discovery, and continuous quality assurance.\(^2\) For example, industrial robots offer manufacturers a way to streamline production lines, increase productivity, and optimize workflows from assembly to inspection and packaging. Motion control systems are used to assemble and move medical devices. Control sensing and vision-guided systems monitor product safety by scanning and verifying barcodes.\(^3\)

Although these innovative technologies are integral to ensuring patient safety and elevating quality, they are so complex that, if a cyberattack were to disrupt their operation, it would be difficult to bring them back online and costly to rebuild or replace them. Further, IIoT in particular renders traditional mitigating controls like firewalls obsolete, as these technologies bridge OT assets to corporate networks via cellular connectivity and cloud services. Further, even if a facility doesn’t have 24-hour operations, IIoT is always on, leaving the organization open to attack on any day and at any time.

---


3. Outdated legacy systems and undefined roles

Despite incredible innovation on the product front, some life sciences organizations are still operating with outdated technologies. Such organizations run on infrastructures that include a significant number of legacy systems, which leave the OT environment vulnerable to unmitigated cyberattack. Further, in many legacy OT environments, users still share passwords with others on their rotation shifts—although this is a complex issue given the fact that forcing a user log-out deprives the operator of visibility into the system during the time offline.

In comparison to the more granular roles in corporate IT, the manufacturing floor is less structured with plant managers overseeing a variety of locations and lacking assigned OT responsibilities, including management of security and incident response. There is also very little crossover between IT and OT functions, leaving the issue of who is responsible for OT equipment procurement and configuration unclear. Although companies are starting to give designated individuals in the OT environment specific cybersecurity responsibilities, the lack of a formalized cybersecurity infrastructure will likely hinder an expeditious response in the event of an attack.

Life sciences organizations need to balance clinical product innovation with modernized methods of protecting that innovation.

---

4. Emerging data privacy regulations

As patient data is known to be more valuable than financial data on the black market, there is a continuing movement throughout the world to take information protection to a new level. A number of recently enacted regulations—some of which originated in the European Union (EU)—are complicating life sciences’ decision-making about how to maintain data privacy while taking advantage of the enormous competitive advantages such data has to offer. For example, the General Data Protection Regulation (GDPR) in the EU has restricted the use of health data to situations where there is individual consent or where the data significantly benefits the public good. This, of course, puts some constraints on how life sciences organizations can utilize non-clinical-trial data—some of which may come from third-party vendors—in the manufacturing process.

When it comes to supply chain practices, organizations are subject to the FDA’s Drug Supply Chain Security Act (DSCSA), which mandates the electronic documentation of products’ journeys from the manufacturing floor to the patient. Finally, the draft guidance entitled “Data Integrity and Compliance with CGMP Guidance for Industry” seeks to ensure that accurate and reliable data is used across functions that impact drug safety and quality. In addition to potentially sustaining tens of millions of dollars in penalties, organizations that fail to comply with regulations designed to secure patient data can face serious reputational and financial damages from patients who may be affected.

How to help minimize the risk

1. **Identify the risks and develop a roadmap.**

Before organizations can begin to institute formal OT cybersecurity programs, they must first identify where the greatest risks reside. Based on our experience across industries, the following is a step-by-step approach to risk identification:

- Determine the scope of OT assets, as well as inbound and outbound connectivity points to the OT environment
- Specify potential threat actors and attack vectors
- Determine the factors affecting the likelihood of a threat event (e.g., threat actor proximity, required skill level)
- Articulate the possible impacts resulting from a threat event (e.g., operations are halted, operational safety is compromised)
- Calculate risk levels utilizing the attack vectors, threat likelihoods, and expected impacts.

**In summary:** Before life sciences organizations can protect themselves from attack, they must identify and prioritize the most significant risks they face.

Further, before life sciences organizations can begin to institute cybersecurity controls in the OT environment, they must define a target state and determine how to get there. Based on our experience, following are the steps organizations should take:

- Document a target state, including prioritized capabilities
- Establish a detailed network diagram and visibility into the data flows permitted into, out of, and within the OT environment
- Develop a cybersecurity framework and ICS/OT controls to mitigate risks to an agreed upon, acceptable level
- Enable the success of the framework with a governance model that includes ICS/OT vendor risk management
- Begin to enable the business to comply with and support cybersecurity measures through awareness programs, education, and people and change initiatives
- Sustain progress by putting all newly introduced technologies through the lens of this framework and ensuring that there are solid business continuity and disaster recovery programs in place.

**In summary:** Cybersecurity programs in the OT environment cannot be established overnight. They must be addressed via incremental, multiyear initiatives.
Segment risks introduced by advanced connectivity.

With today’s shift toward consumerism and specialized drugs, product formulations and medical device configurations are often stored in the OT environment. Further, the manufacturing process is employing increasingly disruptive technologies, from blockchain for supply chains to predictive analytics in quality control functions to AI to accelerate identification of potential new products. While all of this innovation is critical to advancing production speed and quality, these technologies can raise the risk that threat-induced failures in one area will have a snowball effect throughout the entire life sciences value chain.

With biologic drugs, IP and trade secrets are particularly valuable, and their formulas can be discerned by hacking into development processes on the manufacturing floor. Cyber threat actors know this and devise ways to infiltrate OT systems to steal IP or cause disruption in the manufacturing process. Life sciences organizations know it too, but many are tackling the problem using the same solutions they use to protect IT, e.g., antivirus software, firewalls, and role-based access controls (RBAC). Instead, they should be employing tools and processes that are specific to the OT environment and that can detect security anomalies in these sensitive networks.

Most critically, all of this connectivity requires layers of segmentation to limit compromise and keep potential threats localized. In most cases, this will mean North/South segmentation, i.e., minimizing and strictly controlling connectivity between corporate networks and OT. Although less common, some organizations will also implement East/West segmentation, i.e., segmentation between separate operational functions like production and quality control. Finally, there are cases where organizations will want to consider micro-segmentation, i.e., abstraction of asset ID and authentication from traditional networking into overlays capable of covering a variety of OT assets via dedicated hardware or software agents.

In summary: Organizations should identify jumping off points from the corporate network into the OT network and assess segmentation device configuration to identify potential risk areas that could be leveraged by an attacker.
Expand cybersecurity awareness enterprise-wide.

Since many cyberattacks stem from human susceptibility to social engineering ploys, raising awareness of cybersecurity throughout an organization is critical. In addition to intensive training programs to encourage vigilance for potentially suspicious activity, steps should be taken by senior management to foster a culture of cybersecurity, supported by dedicated champions throughout the organization.

As an organization’s cybersecurity initiatives mature, there should be personnel assigned to strategy, design, and implementation of cybersecurity programs for each of the following areas: AI, cognitive computing, blockchain, IIoT, cloud, and mobility. In the future, organizations will likely require hybrid roles, e.g., R&D researchers with cybersecurity skills, but this won’t happen overnight. In the meantime, organizations need to acknowledge the convergence of IT and OT and establish an enterprise-wide governance structure with clearly defined roles and responsibilities that are accepted by stakeholders.

In summary: Document policies related to the direction of the organization, the scope of protected information, and, most important, roles and responsibilities.

Tighten data access controls as part of compliance efforts.

A critical measure for securing patient data and complying with increasingly stringent regulatory mandates is addressing loose access management policies. Attribute-based access control (ABAC) should be instituted, since accessing the front of a system can create an entry point to the entire system. Access management policies should cover remote access, which could be necessary if analytical data is needed to address problems in real time. At a minimum, secure remote access should require two-factor or multifactor authentication through a firewall.

It is critical to ensure that third-party vendors comply with the same level of cybersecurity rigor as the organization. Without their support, it will be more difficult to adhere to requirements and update/maintain cyber capabilities with any degree of continuity. On this point, assessing vendors and scanning their mobile devices (e.g., laptops) is particularly critical to maintaining some degree of assurance that malware is not being introduced from the outside. There must be strict control over the parts of the system that are accessible to vendors, all of which must be spelled out in the vendor contract or SLA.

In the short term, organizations should make the shift to directory services with granular individual rights and RBAC for particular users, e.g., R&D personnel can only see the back-end systems needed to access data that is pertinent to their function. Looking forward, organizations should work toward developing comprehensive identity management policies and procedures that include ABAC for all individuals using the network.

In summary: Ensure that the organization understands current and impending data privacy regulations and how they may impact the use of data in the manufacturing environment.
In conclusion

The life sciences industry has entered a time of incredible innovation—with drugs that significantly prolong lives, treatments that cure diseases, and customized medications and medical devices that meet consumers’ health and lifestyle needs.

These advances depend upon equally groundbreaking connected technologies that enable accelerated, cost-effective, and customized production. Continuing to innovate on all these fronts is critical to a thriving and productive industry. This will require bringing OT and IT cybersecurity to parity and staying several steps ahead of threat actors whose actions could bring innovation to a halt. Life sciences organizations have made significant progress when it comes to protecting IT networks and critical data in the corporate environment. The same attention must now be paid to the OT environment. The future of life sciences innovation depends on it.
How KPMG can help

KPMG’s Cyber practice assists organizations from pre-breach to post-breach with an eye to transforming their security, privacy, and business continuity controls into business-enabling platforms. Our philosophy is that security is a process and not a solution. Therefore, safeguarding IT and OT networks and sensitive data from electronic attack and exposure is a constant endeavor.

Our teams have significant on-the-ground credentials in the cybersecurity space, having been retained by some of the world’s largest organizations in life sciences, healthcare and other industries. Our work runs the gamut from strategy and governance, to large-scale security transformation programs, to a full range of cyber-risk and response services, including on-demand malicious code analysis, host- and enterprise-based forensics, network forensics, threat intelligence, and expert testimony.

KPMG’s operational technology compliance and transformation team has helped its clients plan for and design essential IT-OT interoperability, appropriate resilience mechanisms, and prioritized, risk-focused enhancement programs across a range of industries. We leverage technology to support true protective mechanisms, continuously measure OT security capabilities, and enable significant operational improvements, allowing our clients to better compete in the modern world. Services include:

- Security program strategy design
- Security process engineering and operational transformation
- Network architecture strategy and segmentation
- Asset inventory/management, intelligence enablement, and event correlation
- Technology integration and logical design
- Industrial internet of things security and architecture.
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

cpmp.com/socialmedia