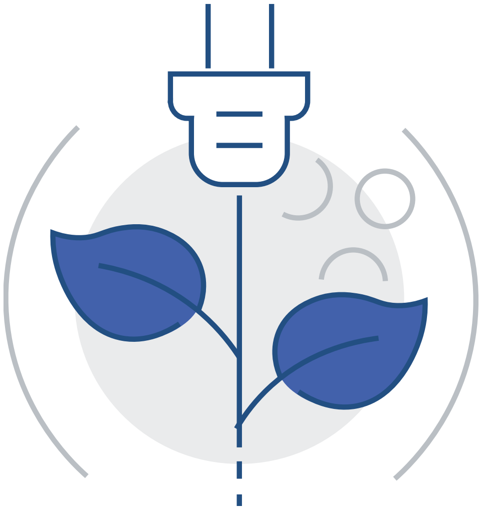


# SECURING OPERATIONAL TECHNOLOGY **IN THE PHARMACEUTICAL AND CHEMICAL MANUFACTURING INDUSTRIES**

## FOUR KEY CONSIDERATIONS

BAYSHORE

# Introduction

A fourth industrial revolution is underway, driven by the interconnection of physical infrastructure and the systems that control it. The Industrial Internet of Things (IIoT), also known as the Industrial Internet and Industry 4.0, is changing how products and services are designed, manufactured, sold, delivered, and operated.

“Industry 4.0 heralds a new age of connected, smart manufacturing, responsive supply networks, and tailored products and services. Through its use of smart, autonomous technologies, Industry 4.0 strives to marry the digital world with physical action to drive smart factories and enable advanced manufacturing.”[1]

Today’s pharmaceutical and chemical manufacturing processes involve standardized, layered systems with in-depth production rules, guidelines, and regulatory oversight. While connecting plant processes, networks, and applications promises to drive significant economic benefits for manufacturers, this interconnection also creates new cyber threat vulnerabilities, including the possibility of safety concerns, operational disruptions and downtime, and costly physical damage to equipment and products.

This whitepaper will examine the growth of IIoT and the concomitant risk of cyber threats in the pharmaceutical and chemical manufacturing industries; opportunities, risks, and challenges created by the convergence of information and operational technology (OT); as well as four key considerations when protecting industrial assets against cyber threats. Lastly, it introduces Bayshore’s Industrial Control Platform, which stops cyber threats before they can damage critical manufacturing assets and systems, and allows secure connection to the industrial internet.

[1] René Waslo, Tyler Lewis, Ramsey Hajj, Robert Carton, “Industry 4.0 and cybersecurity: Managing risk in an age of connected production,” March 21, 2017. https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html

# The Growth of IIoT and Cyber Insecurity

According to Frost & Sullivan, 80% of manufacturing companies around the globe will have adopted the Industrial Internet of Things by 2021.[2] In fact, it is estimated that by 2020, between "30 billion and 50 billion objects will be connected. These connected objects will automate processes, find and self-correct problems, and record and send data to central servers. All of this data can be analyzed to modify and improve products and processes."[3]

The rise of Internet-connected devices on the manufacturing floor yields many benefits, including **business efficiencies** from a digital supply chain and smart manufacturing processes, potential **new streams of revenue** from customized medicine and 3D printed drugs, and the ability to perform **predictive maintenance** on equipment.

For example, pharmaceutical and chemical manufacturers now derive huge amounts of data from Internet-connected sensors and devices on the manufacturing floor and analyze this information to enable more efficient business operations, allowing them to:

- Share and analyze data in real time to optimize manufacturing processes and validate that there have been no modifications
- Enhance and tune systems automatically as needed, without human intervention
- Predict system failures to stop them before they occur, decreasing plant downtime
- Reduce costs and increase profit margin

Sensors detect whether machinery is operating within normal limits as benchmarked against previous performance and when it might need to be worked on. This kind of predictive maintenance enables manufacturers to stay ahead of repair schedules and costs as well as keep systems up and running for optimal productivity, such as in large chemical plants that operate 24x7. This, in turn, enables manufacturers to optimize processes because they can now know when there is a slowdown or less-than-ideal performance through sensor data and analytics, garnered through remote monitoring without the need for massive human oversight.

These benefits, however, are countered by the challenges of securing OT on the plant floor as well as its interconnection with the corporate network. While IIoT "enhances digital capabilities throughout the manufacturing and supply chain processes and drive revolutionary changes to connected devices, it also brings with it new cyber risks for which

[2] Frost & Sullivan, "Cyber Security in the Era of Industrial IoT," sponsored by Bayshore, 2017. https://www.bayshorenetworks.com/cybersecurity-in-the-era-of-industrial-iot

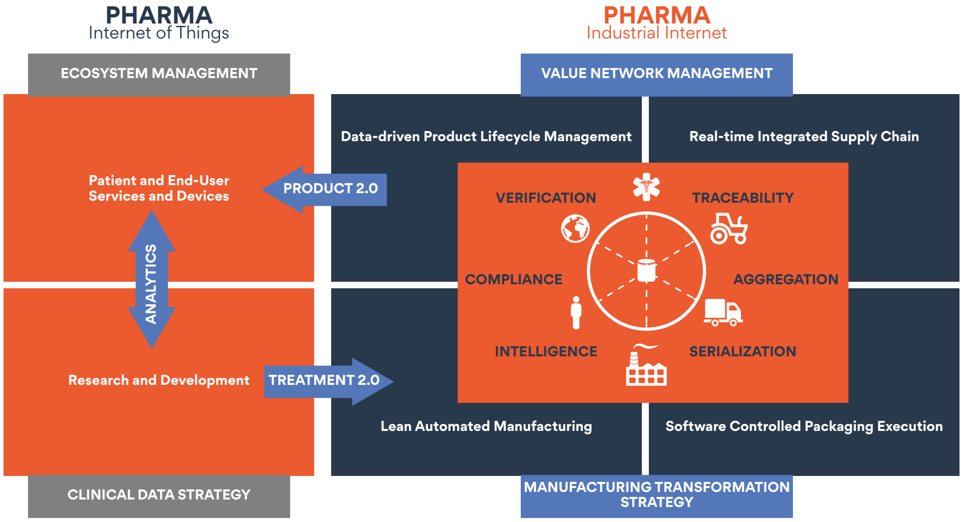
[3] Stefan Guertzgen, "Chemical Industry: 4 Opportunities Provided by Internet of Things," Internet of Things Institute, December 14, 2016. http://www.ioti.com/industrial-iot/chemical-industry-4-opportunities-provided-internet-things

the industry is unprepared."[4] That's because IIoT increases the potential attack surface with billions of interconnected devices, all of which can be searched on dark web search engines for vulnerabilities.

The primary concern in pharmaceutical manufacturing is to ensure that no unknown or unapproved modifications ever happen in the production process and to ensure that all data is recorded for everything that is manufactured. That data must be guaranteed never to be modified; for compliance reasons related to health and safety, if a pharmaceutical manufacturer loses product data, they cannot sell that batch of drugs. "Failure to comply with cGMP [Current Good Manufacturing Practices] can result in regulatory actions taken by the agency, including warning letters, seizure of a product, recalls, and fines."[5] Additional challenges include:

- Internet-connected sensors and devices are built for 24x7 uptime and reliability, not security
- The majority of operational systems is not up-to-date and remain unpatched
- Corporate IT networks can act as a gateway for cyber attackers to infiltrate the OT network through lateral movement
- Different protocols and systems use enterprise networks and the plant's operational technology, making them difficult to secure holistically
- IT and OT staff have different priorities and skill sets, making it challenging for them to align with cybersecurity priorities

These risk and challenges have deep consequences. "When supply chains, factories, customers, and operations are connected, the risks posed by cyber threats become all the greater and potentially farther reaching."[6] These threats include but are not limited to:



- Espionage on corporate systems
- Sabotage of plant systems, leading to overpressure, expansion, explosion, or shutdown
- Physical hazards such as material spills and resulting
- Public and employee health issues

Credit: https://www.linkedin.com/pulse/pharma-digitalization-new-reality-beyond-pill-pasi-kemppainen/

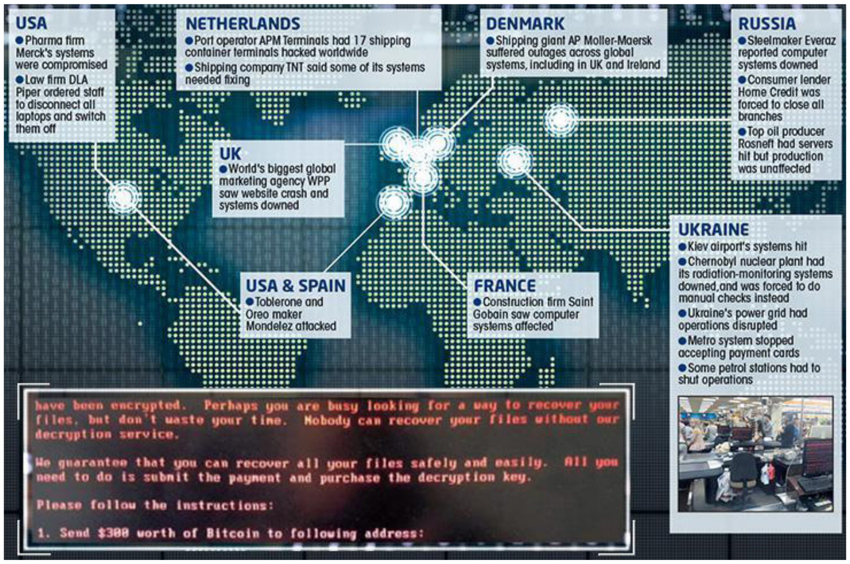
[4] Ibid.

[5] "Measuring Pharmaceutical Quality through Manufacturing Metrics and Risk-Based Assessment," Engelberg Center for Health Care Reform at Brookings, May 2014. https://www.brookings.edu/wp-content/uploads/2014/05/Discussion-Guide.pdf

[6] René Waslo, Tyler Lewis, Ramsey Hajj, Robert Carton, "Industry 4.0 and cybersecurity: Managing risk in an age of connected production," Deloitte University Press, March 21, 2017. https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html

Let's look at these threats, starting with the risk of espionage and loss of intellectual property on the corporate network. "For a manufacturer, the intellectual property it possesses is of the utmost importance.... Unlike the more run of the mill, 'grab-the-loot-and-scram' attacks we see in other verticals, espionage attacks are typically aimed at more long-term results. The criminals want to infiltrate the network, find out where the secrets are kept, and then sit and slowly siphon off the nectar for as long as they can."[7] The 2017 Verizon Data Breach Investigations Report estimates that phishing email that installs malware to siphon secrets represents 73% of the breaches within the manufacturing sector.

Pharmaceutical giant Merck was one of many large global companies affected by the Petya ransomware outbreak in June 2017. "Employees were told to get off their computers and go home, said one scientist who works at a Merck lab in New England....As a scientist, her instruments are connected to a computer, her data is stored on central servers, and the safety data sheets are all online....Beyond the inconvenience of not being able to work, the employee said she fears that critical information tied to Merck drug research could be lost."[8]



USA
- Pharma firm Merck's systems were compromised
- Law firm DLA Piper ordered staff to disconnect all laptops and switch them off

NETHERLANDS
- Port operator APM Terminals had 17 shipping container terminals hacked worldwide
- Shipping company TNT said some of its systems needed fixing

DENMARK
- Shipping giant AP Moller-Maersk suffered outages across global systems, including in UK and Ireland

RUSSIA
- Steelmaker Everaz reported computer systems downed
- Consumer lender Home Credit was forced to close all branches
- Top oil producer Rosneft had servers hit but production was unaffected

UK
- World's biggest global marketing agency WPP saw website crash and systems downed

UKRAINE
- Kiev airport's systems hit
- Chernobyl nuclear plant had its radiation-monitoring systems downed,and was forced to do manual checks instead
- Ukraine's power grid had operations disrupted
- Metro system stopped accepting payment cards
- Some petrol stations had to shut operations

USA & SPAIN
- Toblerone and Oreo maker Mondelez attacked

FRANCE
- Construction firm Saint Gobain saw computer systems affected

```
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:
```

Corporate network attacks like the one at Merck compound cyber threats to the manufacturing processes which could sabotage systems, posing **safety concerns (such as from drug formula manipulation or release of chemicals), operational disruptions and downtime, and costly physical damage to equipment and products.** When operators open up OT networks to let data out, malware such as Havex (aka Dragonfly) can get in; the security perimeter is substantially broken. And that's when the trouble begins. "By breaking into SCADA systems, hackers can find all the information necessary to replicate and reproduce any drug precisely. Worse, they could, without leaving a trail, turn life-saving medicine into poison. Finally, they could hold the entire industrial environment for ransom, cause a system-wide shutdown, or inflict costly damage to manufacturing equipment."[9]

[7] 2017 Verizon Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[8] "Pharmaceutical giant rocked by ransomware attack," The Washington Post, June 27, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/

[9] Yori Shohet, "How Cyber Criminals Could Destroy a Company, or an Industry," Pharmaceutical Processing, September 7, 2016. https://www.pharmpro.com/article/2016/09/how-cyber-criminals-could-destroy-company-or-industry

Unfortunately, those hackers might be third-party contractors. "In most places, the chemical industry self-regulates and the owners of plants take responsibility for their security. By and large, big international companies recognize that the stakes are high and have in-house teams working on cybersecurity. But for smaller companies, the expense makes this unfeasible."[10] For example, chemical manufacturers who cannot afford 24x7 staff rely heavily on third parties, outsourcing/subcontracting parts of their supply chain, which leaves them vulnerable to insider threat. As well, to save costs on plant labor, they rely more heavily on remote technology, which as we've noted isn't built to be secure. Lastly, manufacturers face additional ramifications from compromised corporate and operational networks. "Consequences ranging from stolen IP, repeating clinical trials, litigation, and lost revenue resonate throughout an organization. Although the pharmaceutical industry is lagging behind other industries when it comes to cyber security implementation, there's a new sense of urgency. Because of the impact to share prices and brand image, boards of directors have taken note. As data sharing becomes more prevalent across the industry, companies are starting to grasp that a breach in their network—that subsequently spreads to others—could have significant reputational impact."[11]

## Protecting Against Cyber Threats: Four Key Considerations

So what can pharmaceutical and chemical manufacturers do to secure their systems? What's clear is that enterprise IT cannot be assured by operational technology. A way must be created for data to transit the network securely and be policed at the same time. Identifying and protecting against cyber threats is a mandatory first step **before** connecting plant processes, networks, and applications. Here are four key considerations when assessing potential solutions:

### 1. Improve End-to-End Asset Visibility: You Can't Protect What You Can't See

Ensure your solution continuously maps and monitors industrial traffic, learning as it adapts to observations. You'll want to combine advanced threat intelligence from public and private sources with out-of-the-box policies to establish and maintain a baseline of acceptable behaviors. Look for an approach that helps you optimize and protect your OT environment, including protocols, sources, destinations, manufacturers, models, and anomalies or violations of baseline policies. Also, ensure that the solution can inspect full messages (regardless of protocol) for both content and context at the transaction level and that all reporting can be integrated into your SIEM/SOC and forensic analysis tools of choice.

### 2. Mitigate Cyber Threat Risks: Just Seeing a Threat Won't Stop It

Look for an approach that stops cyber threats in real time, before they can damage your industrial infrastructure or the environment. Look for active alerting and proactive blocking of unauthorized communication and commands, preventing cyber threats from reaching and affecting targeted objects and data. You'll want a solution that operates at line speed, providing protection at a fine-grained transaction level, enabling authorized traffic and standard workflows to continue unimpeded even in the face of ongoing cyberattacks.

[10] Emma Stoye, "Security experts warn chemical plants are vulnerable to cyber-attacks," Chemistry World, June 2015. https://www.chemistryworld.com/news/security-experts-warn-chemical-plants-are-vulnerable-to-cyber-attacks-/8632.article

[11] Booz Allen Hamilton, "Business Insights: 5 Facts about Cyber Security for Pharmaceutical Companies," https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/thought_p/5-facts-about-cyber-and-pharma.pdf

### 3. Provide Managed Remote Access: Protection Means Control Over Access and Actions

Allowing vendors to access industrial equipment for maintenance and troubleshooting remotely offers distinct advantages. Providing industrial data to service providers may help improve business outcomes. However, opening industrial infrastructure to these third parties creates significant risk. Traditional VPNs can help with controlling access, but once a connection is made, manufacturers have no way to know or control the actions that remote users undertake on their open ports. The lack of cyber protection provided by VPNs is just unacceptable in the industrial world. Look for a Managed Remote Access solution that goes far beyond traditional VPNs to create an on-demand, encrypted, policy-protected, bi-directional tunnel between remote users and your industrial infrastructure.

Ensure that every element of communication between you and third parties is verified, managed, and blocked if necessary. Look for Managed Remote Access that enforces authentication, authorization, white lists, and other security controls at the device command and individual transaction level.

### 4. Secure Your Industrial Internet: Protect Your Assets Before You Connect

When you are ready to interconnect your industrial infrastructure and data to take advantage of all the Industrial Internet has to offer, look for a solution that provides bi-directional, access-controlled, and policy-protected tunnels between your organization and your chosen IIoT partners. This means that not only is access limited to specific sources and destinations, but also that content and context is controlled by policy so that every element of communication between the organization and its external IIoT ecosystem can be verified, alerted, and blocked if necessary.

## How Bayshore Networks Can Help

The Bayshore Industrial Cyber Protection (ICP) platform stops cyber threats before they can damage critical industrial assets and systems, and allows secure connection to the industrial internet of things (IIoT).

The Bayshore ICP platform delivers a comprehensive set of capabilities required to protect and defend against sophisticated, complex attack systems. Bayshore empowers industrial enterprises with safe and efficient production, operational insights, and improved business outcomes while blocking cyber threats to industrial plants, machinery, and people. It is designed to support manufacturing customers throughout the entire industrial cyber protection life cycle, leading to improved business outcomes.

The journey begins with mapping networks assets and progresses to identifying anomalies, preventing attacks and incidents, optimizing business efficiencies, and finally, to enabling innovation and digital transformation, such as creating new revenue sources and product markets.

The comprehensive industrial cyber protection platform uniquely offers customers a long-term solution by providing a single, tightly integrated, extensible, and scalable architecture. The benefits of Bayshore's native OT protocol and content-based cyber protection for processing industries include:

- Visibility across global-scale OT infrastructure
- Increased production uptime and reduced downtime
- Enhanced predictive maintenance
- Improved operational efficiency driving increased revenue and reduced OPEX
- Simplified reporting and compliance

## Summary

New cyber security threats targeting IIoT in the pharmaceutical and chemical manufacturing sectors are emerging every day, risking public and employee safety, operational disruptions and plant downtime,  and costly physical damage to plants, machines, and products, in addition to loss of intellectual property via espionage on the corporate network. Identifying and protecting against cyber threats is a mandatory first step before connecting plant processes, networks, and applications.

Bayshore inspects machine-specific industrial protocol traffic, which eliminates cyber threats before they reach critical equipment, protecting OT applications, networks, machines, workers, and the environment. Additionally, Bayshore's Managed Remote Access solution allows manufacturers to grant tightly controlled access to third parties, such as equipment vendors, for maintenance and troubleshooting.

## Next Steps

For more information on the Bayshore Industrial Cyber Protection platform, visit **www.bayshorenetworks.com/platform.**

## About Bayshore Networks, Inc.

Bayshore Networks® is the leading provider of industrial cyber protection. The Company's award-winning technology unlocks the power of the Industrial Internet of Things (IIoT), providing enterprises with unprecedented visibility into their Operational Technology infrastructure while safely and securely protecting ICS systems, industrial applications, networks, machines, and workers from cyber threats. Bayshore's strategic partners include among others Arista, AT&T, BAE, Cisco, Dell, SAP, VMware, and Yokogawa. Bayshore is a privately held company headquartered in Washington, DC and backed by Trident Capital Cybersecurity, Yokogawa, Samsung Next, and BGV Capital. For more information, visit **www.bayshorenetworks.com.**

BAYSHORE

BAYSHORE

www.bayshorenetworks.com