7 TIPS TO IMPROVE OT CYBERSECURITY FOR LIFE SCIENCES

Honeywell

TABLE OF CONTENTS

2 Executive Summary

3 Map to a Common Framework

4 Prioritize Effective Controls

5 Understand Your Employees and Facility Rhythms

6 Modernize Your Process

7 Remember Compliance

8 Tap into Modernization or “Emerging Tech” Funds

9 Use Technology Providers to Your Advantage

10 Honeywell OT Cybersecurity Specialists and Solutions Can Help

EXECUTIVE SUMMARY

Life sciences companies including pharmaceuticals, medical device manufacturers and biotechnology organizations hold some of the most sensitive data of any industry, including patient information, patented drugs, clinical trials, research projects and manufacturing processes.

This, combined with the direct impact to human health and safety of their products, makes life sciences companies particularly consequential targets for cyberattacks.

This whitepaper draws upon the insights from Honeywell's control system cybersecurity specialists, working in 130+ countries on 7,000+ cybersecurity projects over 25 years. In addition, it taps into Honeywell's extensive experience providing quality management, manufacturing execution systems, distributed control systems and batch historians to life sciences for more than 40 years. By combining these typically distinct views, an operations leader can gain broader context within which to make informed decisions on actions and next steps to improve cybersecurity in operational technology (OT) settings without impacting business operations and production.

MAP TO A COMMON FRAMEWORK

1

OT cybersecurity is competing with other company priorities in terms of funding and backing. Too often leadership teams lack deep technical expertise to understand the importance of investing in OT cybersecurity protections.

From the OT cybersecurity executive sponsor's view within an organization, a significant challenge is weeding through technical detail to determine the criticality or importance of a technology investment.

From the operations leader perspective, mapping their organization's efforts to a framework or model can help streamline funding decisions, and provide a common language for communication around the organization and to peer organizations. Well established frameworks that are developed as collective efforts of different associations and government agencies with input from subject matter experts can provide a systematic approach for assessing risk and implementing cybersecurity programs. Adhering to these frameworks helps with compliance and reduces potential legal and financial risks. Starting with well-established frameworks allows organizations to build a strong foundation by following best practice approach for cybersecurity.

Treating OT cybersecurity as an ongoing practice or cycle of efforts best represents the nature of protecting operational systems, people, and processes. This same view can help prioritize actions and inform how much effort to invest in OT cybersecurity prevention, for example, compared to incident response activities. Similarly, portraying the organization's cybersecurity maturity level can help pinpoint gaps, as well as guide programs and governance efforts to progressively improve OT cybersecurity.

Select frameworks we recommend using:

- National Institute of Standards and Technology's Cybersecurity Framework (NIST)
- Center for Internet Security – Critical Security Controls
- SA/IEC 62443 Series of Standards

PRIORITIZE EFFECTIVE CONTROLS

2

The US Department of Homeland Security warned in 2009 that "standard cyber incident remediation actions deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents"[1] . Yet, 15 years later, a SANS survey revealed nearly a third of organizations lack an OT-specific incident response plan.[2]

The SANS organization created the Five OT Critical Security Controls from enumerating all known past attacks and determining what control areas could have prevented the attack or greatly reduced the impacts.[3] The controls, in order of priority, are:

- OT-specific incident response plan
- Defensible architecture
- OT network monitoring
- Secure remote access
- Risk-based vulnerability management

These security controls may require a significant amount of effort to rollout. For example, creating defensible architecture is part of a zone-conduit assessment described in ISA/IEC-62443. This control segments between IT and OT boundaries, OT systems based on levels of trust, allows for detailed containment actions, and provides data choke points to enable network monitoring. Organizations need to make sure they have the capability to detect and adversary and be ready to respond, which is why creating an OT Incident Response Plan (IRP) is a key control should be prioritized first. The IRP needs to be developed based off known attacks against industry. For the life sciences industry, ransomware is a good starting point.

Another important control tied to incident response is backing up key systems and their respective data. Disaster recovery is increasingly important as ransomware targeting industrial facilities increases.[4] The regular routine of backing up systems using an immutable solution and testing backups, so that if adversaries obtain access and encrypt your systems, you have a mechanism to recover as quickly as possible.

Developing an asset inventory is also a foundational as it helps in understand which systems are critical to operations and supports vulnerability management. SANS control 2, OT Network Monitoring, can support automating asset inventory development, vulnerability management, as well as the primary reason to detect network anomalies and potential advisal activity.

[1] CISA, Developing an Industrial Control Systems Cybersecurity Incident Response Capability: https://www.cisa.gov/sites/default/files/2023-01/final-RP_ics_cybersecurity_incident_response_100609.pdf

[2] SANS, 2024 OT Cybersecurity Survey,https://sansorg.egnyte.com/dl/oq4USL3qoA

[3] Sans, 5 Critical Controls Whitepaper, https://sansorg.egnyte.com/dl/R0r9qGEhEo

[4] ZD Net, Randomsware Attacks Are On The Rise,https://www.zdnet.com/article/ransomware-attacks-are-now-targeting-industrialcontrol-systems/

UNDERSTAND YOUR EMPLOYEES AND FACILITY RHYTHMS

3

In law enforcement, police officers regularly drive or walk around the same locations to patrol a neighborhood. By noticing what is typical, they can more readily recognize abnormal or suspicious behavior.

Operations leaders have an advantage over the analogous police patrol because they have access to system data. Regularly review employee control system log-in and log-out times to note patterns. Check your OT security system dashboards to identify if new assets appeared or an asset's characteristics changed.

We recommend improving OT cybersecurity monitoring and consistency to better notice any anomalies which includes updating and publishing policies.

Establish a USB device policy to know if a personal device is plugged in. When deployed across your various locations, such security controls can collect and log helpful information to pinpoint which users are most prone to infected devices or which locations tend to find more malicious files than others as USB devices are checked in and out of your facility.

Both technical experts and business leaders note the importance of employee awareness efforts to help increase the understanding of cybersecurity noncompliance dangers.[5] Policies can specify each person's role should an attack occur, as well as procedures which detail how teams will work together to expedite remediation.

Third parties can support efforts to reinforce OT cybersecurity awareness. Even physical signage your facility can help keep security top of mind.

[5] Industrial Cyber, Fostering cybersecurity awareness for effective risk management and creating cyber-resilient environments, https://industrialcyber.co/features/fostering-cybersecurity-awareness-for-effective-risk-management-and-creating-cyber-resilient-environments/

MODERNIZE YOUR PROCESSES

4

Particularly as the workforce shifts to younger generations, employees are becoming increasingly tech savvy, and modernizing processes and policies can help mitigate risks that come with new technology.

From the OT cybersecurity perspective, optimizing, monitoring and reworking processes can be as important as modernizing systems to reduce the risks of error or disruption.

Some key process questions to consider in life sciences:

- Do employees and guests alike have the same check-in procedures?
- Are USB devices, such as smartphones or vaping chargers, allowed in the facility areas?
- What is the process for downloading a patch from a vendor and deploying on control systems? In some instances, risk can be introduced if software patches are not verified relative to the exact system configurations of the system upon which they will be deployed.

Not all Windows systems are equivalent, and many industrial instances of an OS have been hardened or otherwise adapted to avoid process interference. Additionally, each facility and its mix of systems and protocols may be unique, requiring workarounds and special configurations. These need to be taken into consideration as patches are reviewed and prepared prior to roll-out.

Another potential need increasingly of concern may be remote access as businesses adopt more high-level executive visibility of operations. Additionally, many

companies have adopted remote or hybrid work policies in recent years. From the OT cybersecurity perspective, though, any connection is a risk and requires compensating controls such as timed sessions, recorded sessions and notifications to management. Reviewing your remote access process is an important step toward

modernization of cybersecurity management as well as overall plant management.

REMEMBER COMPLIANCE

5

Recently, cybersecurity non-compliance penalty fees can reach into the multimillions.[6] As cybersecurity actions are planned and implemented, it is essential to monitor changing regulatory requirements. OT cybersecurity standards and frameworks like those mentioned earlier continue to evolve and can assist in determining minimum requirements for compliance.

To improve overall OT cybersecurity, review the frameworks in context of your company's risk appetite and your operational requirements. In some cases, portions of a standard may not be feasible to implement due to outdated systems or non-existent processes. Identifying these barriers can help plan and budget for necessary upgrades or modernization efforts.

Recommendations may vary, with some industry veterans recommending at least an annual cybersecurity view into compliance status depending on how many regions your company operates.

Despite progress to standardize globally, government regulations differ and may dictate dissimilar frequencies required for cybersecurity compliance documentation.

Those facing an audit need more active management. A five-year plan is often recommended for digital transformation or modernization initiatives that involve cybersecurity, incorporating regular risk assessments performed annually, if not quarterly, across all facilities.

Not all work can be completed instantly, and you may need to balance when and how your company can reach a compliant state. We recommend using automation and efficiency gains wherever possible, understanding that standards implementation and proof of compliance can be manual and time intensive. For example, we suggest using software to automatically report anti-virus or patch deployment status across your operational assets and use automatic reporting from these systems to prepare for compliance reviews or audits.

[6] Irish National Cyber Security Centre, NIS2 Enforcement and penalties, https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_7_ENFORCEMENT.pdf

TAP INTO MODERNIZATION OR "EMERGING TECH" FUNDS

6

Investment and innovation in the OT cybersecurity space is at an all-time high. A 2025 SANS survey found that 60% of medium and large organizations increased their OT cybersecurity budget in the last 2 years,[7] which means new solutions and ideas are appearing constantly.

Many life sciences organizations have established emerging technology funds to allow for ongoing trial and scouting of new technical solutions. In the past, these were reserved for direct application to any products the company was producing. Increasingly, these funds are being allocated to trial or experiment new techniques or processes for digital transformation, modernization or process efficiencies – the hallmarks of differentiation for long-term profitability. Determine if your organization has such a fund and lobby to include new OT cybersecurity technology.

Considering the dynamic level of innovation and the potential savings, from expediting attack forensics to more efficiently closing known vulnerabilities, the investment is directly aligned to competitive survival. We recommend assigning a member of your team as the technical scout to stay attuned to advancements and house offline trial systems and solutions. Another option is leveraging universities, vendors and other well-resourced centers of excellence to learn and apply any new methodologies and technical solutions. Innovations might include software that visualizes overall facility performance to spot areas for improvement, secure data transfer solutions to increase security visibility, edge device monitoring to mitigate risks, and virtual reality cybersecurity training solutions to better prepare staff.

USE TECHNOLOGY AND MANAGED SERVICE PROVIDERS TO YOUR ADVANTAGE

7

With a primary focus on delivering uptime and operational excellence, some organization leaders may not have the incentive or bandwidth to drive top-down change that is needed to support their overall cybersecurity efforts.

Leveraging the resources of global technology and managed security providers such as Honeywell can help solve the resource challenge, as well as the time commitment issues that sometimes prevent leaders from prioritizing cybersecurity programs.

. Aligning the IT and OT teams of an organization around a top five set of cybersecurity objectives can reduce friction and expedite the OT team's day-to-day needs. Often, global technology providers can bridge these groups effectively and drive the meeting schedules, agendas and outcomes necessary for alignment. Several industry leaders suggest that commonalities exist, yet they emphasize the need for each domain technically to perform critical work only with specialized experts. As an example of this IT-OT balance, most organizations are aligned such that the company requires regular cybersecurity risk assessments. Specific tasks, such as a control walk-through or review of the patching process, must be performed by highly specialized teams unique to each domain. Similarly, both organizations need disaster recovery set-up and verification but with collaborative engagement. By leveraging your technology provider's contacts and their incentive to diplomatically unify your company's teams, you can extend your influence and reach without adding excessive workload. As you uncover synergies with IT and common cybersecurity needs for the business, you may find a faster route to new budgets and modernization support that improves OT cybersecurity.

HONEYWELL OT CYBERSECURITY SPECIALISTS AND SOLUTIONS CAN HELP

Honeywell is a leading provider of cybersecurity solutions that helps protect OT-based assets, operations and people from digital-age threats. With more than 25 years of cybersecurity expertise and more than 50 years of industrial domain expertise, Honeywell can help your company make sense of today's IT-OT cybersecurity complexity and reduce your cyber risk. We provide innovative cybersecurity software, services and solutions to protect assets, operations and people at thousands of industrial and critical infrastructure facilities around the world. Our solutions are vendor neutral, meaning they go far beyond Honeywell proprietary devices and assets to help protect assets on your control network. For more detailed and specific technical support of your OT cybersecurity objectives, engage with Honeywell by contacting your local sales representative or visiting www.becybersecure.com.

For more information
visit www.becybersecure.com
or contact your Honeywell
Account Manager, Distributor
or System Integrator.

Honeywell
715 Peachtree Street NE
Atlanta, Georgia 30308
www.honeywell.com

WPR-25-08-EN | 05/25

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell