HONEYWELL FORGE

7 TIPS TO IMPROVE OT CYBERSECURITY

Whitepaper

MANAGEMENT SUMMARY

Extensive material has been published to advise operational leaders on cybersecurity issues and concerns. What is lacking, however, is a holistic view of the situation, as research suggests that technology alone cannot adequately manage cybersecurity risk[(1)].

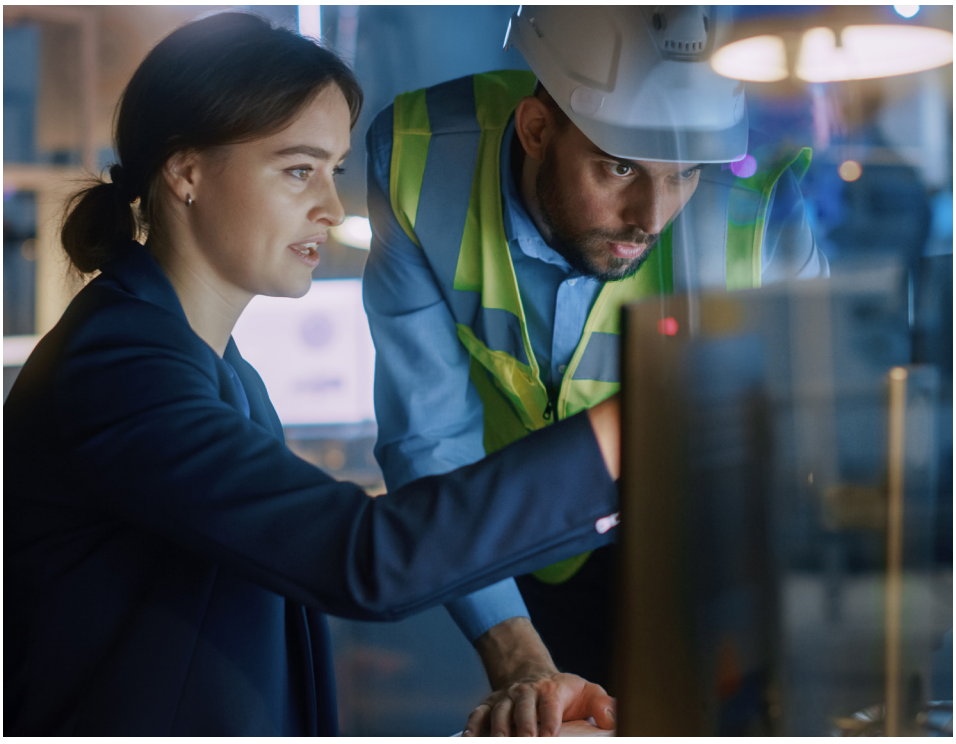
This whitepaper draws upon the insights of multiple Industrial Control System (ICS) cybersecurity specialists from Honeywell, working in the industry for over 15 years. In addition, it taps into Honeywell's extensive experience working with executive management across global organizations, to provide related commentary and perspective. 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. For recommendations or data points sourced outside of these Honeywell industry veterans and stakeholders, footnotes are included.

COMMUNICATE WITH A FRAMEWORK OR MODEL

1

OT cybersecurity is competing with all other company priorities in terms of funding and backing, and too often leadership teams lack deep technical expertise. 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, using a framework or model to communicate needs and actions can help streamline funding decisions, as well as clearly map the ups and downs prominent in any risk management endeavor. Visualizing OT cybersecurity as an ongoing practice or cycle of efforts may best represent the nature of protecting operational systems, people, and processes. This same view can help prioritize OT team actions and consider how much effort to invest in OT cybersecurity prevention, for example, compared to response activities. Similarly, portraying the organization's maturity level of cybersecurity can help pinpoint gaps, as well as guide programs and governance efforts to progressively improve OT cybersecurity. Another approach to simplify a shared understanding of OT cybersecurity needs is to categorize technical steps within a defined set of controls, using common language as descriptors, such as "Inventory and Control of Hardware Assets." Viewing the full set of controls, and the organization's progress aligned to these categories, can streamline joint efforts to manage OT risks.



SELECT EXAMPLES OF FRAMEWORKS:

- NIST Cybersecurity Framework
- Center for Internet Security - Controls

TRIPLE CHECK OT CYBERSECURITY BASICS 2

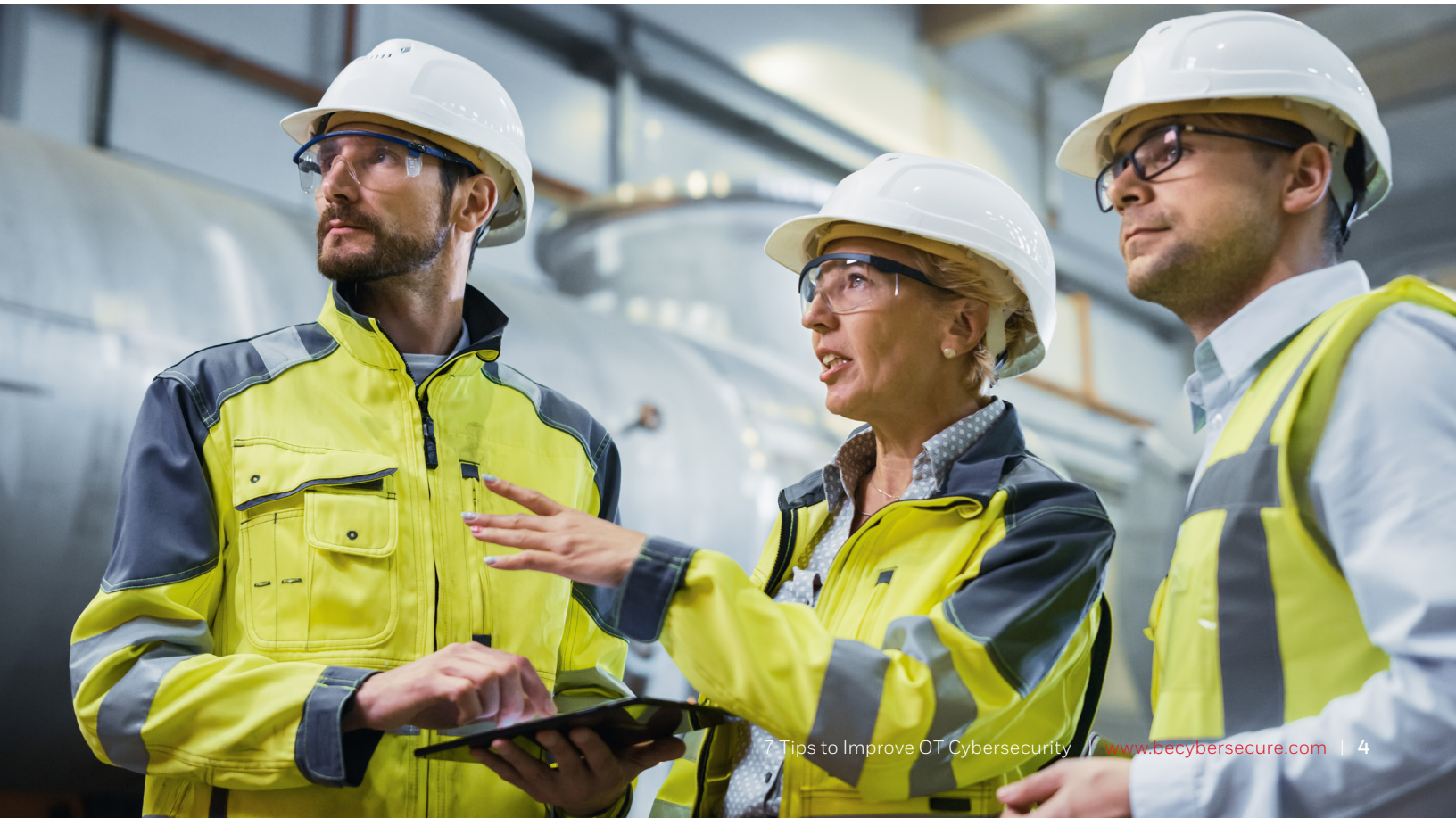
Despite recent training and education regarding the need for OT cybersecurity and the impact of ongoing ICS threats, industry still lacks some of the fundamental safeguards relative to the level of threat.[2]

At the most basic level:

- Understand which systems are critical to operations and inventory them
- Across these critical systems, know their OS specifics and what protocols are normal for the system's vintage
- Check that these systems have been hardened and do not, for example, still use the default passwords initially delivered with the solution
- Walk through your facility to ensure these systems do not show passwords on sticky notes or paper nearby; experts note that this is unfortunately a common and basic cybersecurity issue that can also trigger regulatory non-compliance

Other basic steps, based on Honeywell's OT cybersecurity team inputs, include segmenting your assets, monitoring them, and of course, backing up key systems data. Disaster recovery has become increasingly important as ransomware targeting industrial facilities has increased.[3] The regular routine of backing up systems, and ensuring the backups are functional, ensures that if hackers obtain access and encrypt your systems, you have a mechanism to recover as quickly as possible.

Finally, note the importance of performing regular risk assessments. In some cases, these have turned up surprising findings in organizations, such as remote access connections that are unmonitored and other out-of-policy concerns. (Such findings are not typically publicly disclosed, yet veterans working within industry often cite active connections as an issue, and thus we include the mention here.)



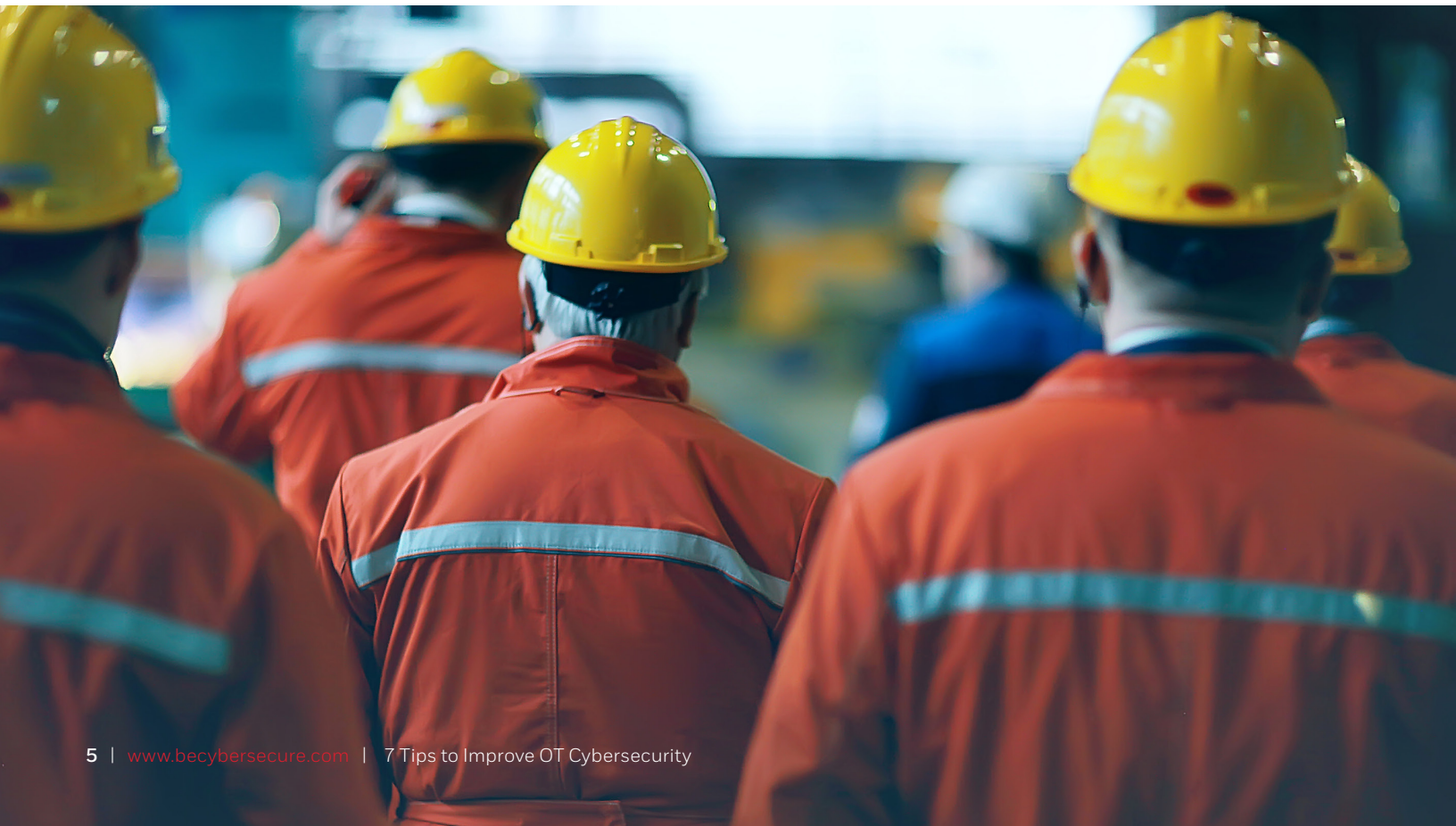
KNOW YOUR EMPLOYEE AND PLANT RHYTHMS

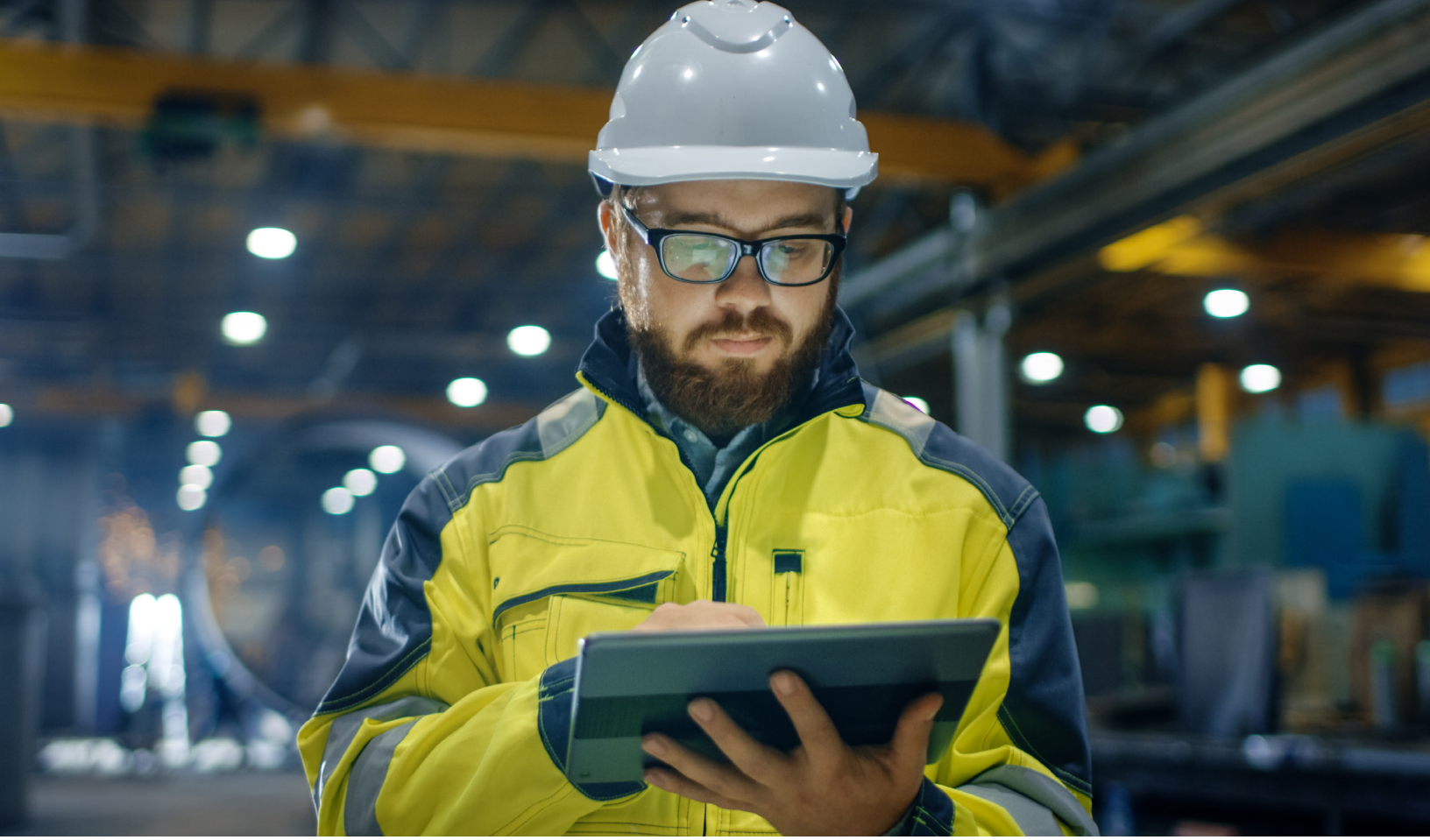
3

In law enforcement, police officers regularly drive or walk around the same locations to patrol a neighborhood. Becoming familiar with the usual neighborhood activity allows the officer to recognize suspicious behavior quickly. Operations leaders have an advantage over the analogous police neighborhood check because they have access to system data. Review employee control system log-in and log-out times to note patterns. Check your OT security system dashboards to identify if new assets have appeared or an asset's characteristics have changed.

Experts from Honeywell recommend improving OT cybersecurity monitoring and consistency to better notice any anomalies, and this includes updating and publishing policies. Establish a USB device policy to know if a personal device is plugged in. When deployed across your various plant 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 plant.

Both technical experts and business leaders note the importance of employee awareness efforts to help increase the understanding of cybersecurity noncompliance dangers. 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 your efforts to reinforce OT cybersecurity awareness. The simple act of posting a sign or notice at your facility can help keep security top of mind, for example, ICS Security posters from SANS.





MODERNIZE YOUR PROCESS 4

Particularly as the workforce shifts industrial facilities employees are becoming increasingly tech-savvy, the importance of reviewing processes and policies increases. Bullet proofing both can help mitigate risks, according to Honeywell experts. From the OT cybersecurity perspective, processes can be as important as systems for optimizing, monitoring, and reworking to reduce the risks of error or disruption. Do employees and guests alike have the same check-in procedures? Are USB devices, such as smartphones or vaping chargers, allowed in the control room? What is the process for downloading a patch from a vendor, and deploying on industrial 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 plant and its mix of systems and protocols may be unique, requiring particular workarounds and special configurations. These need to be taken into consideration as patches are reviewed and prepared prior to roll-out.

Another common need that often requires regular review is remote access. Innovations in remote monitoring of facilities, from offshore platforms to oil refineries, have resulted in more specialized expertise becoming available from a distance. This avoids hazardous travel by technicians to remote locations and can more rapidly support teams on the ground. From the OT cybersecurity perspective, however, any connection is a risk and requires compensating controls such as timed sessions, recorded sessions, and notifications to management. Honeywell experts in ICS also note that increasing cybersecurity will enable enterprises to train more staff. Recordings of remote access sessions can be replayed to learn troubleshooting, for example. Reviewing your remote access process is an important step toward modernization of cybersecurity management as well as overall plant management.

REMEMBER COMPLIANCE 5

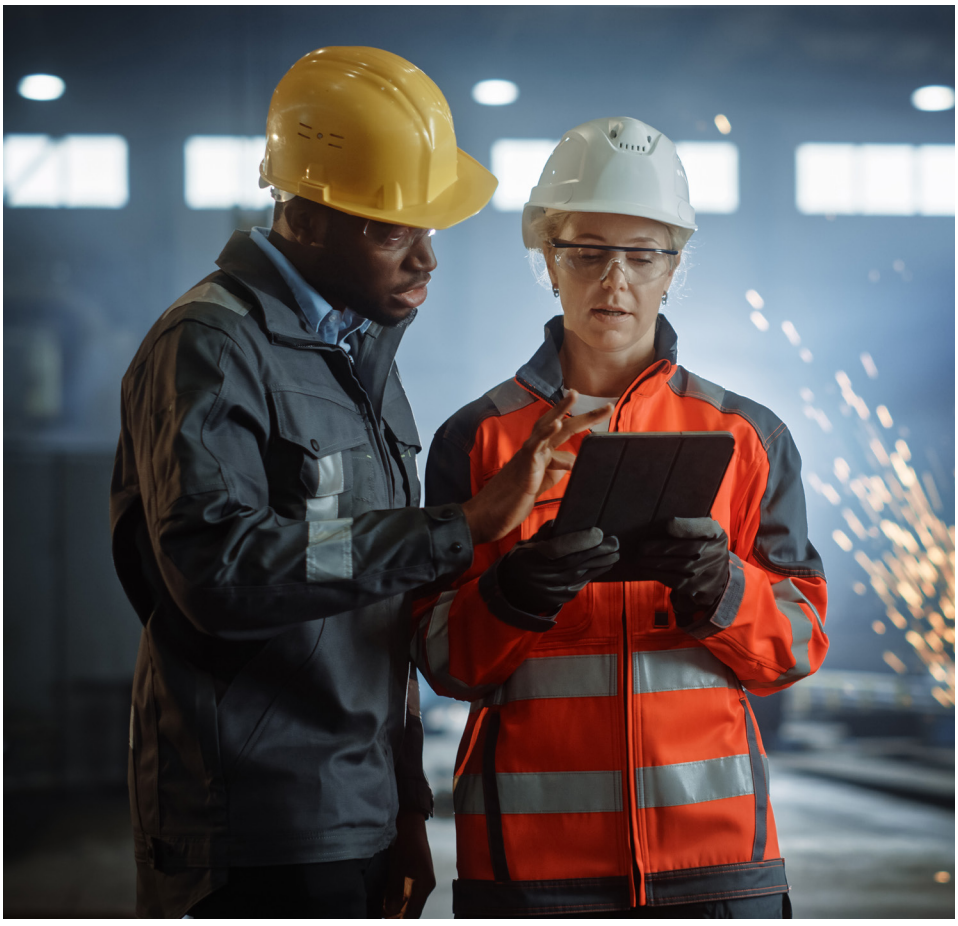
Recently, cybersecurity non-compliance penalty fees have reached into the multimillions (USD). As cybersecurity actions are planned and implemented, it is essential to monitor regulatory requirements. OT cybersecurity standards have evolved globally and can assist in determining minimum requirements for compliance.

To improve overall OT cybersecurity, review the standards 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 vary, with some industry veterans recommending at least an annual cybersecurity view into compliance status depending on how many regions your company operates in.

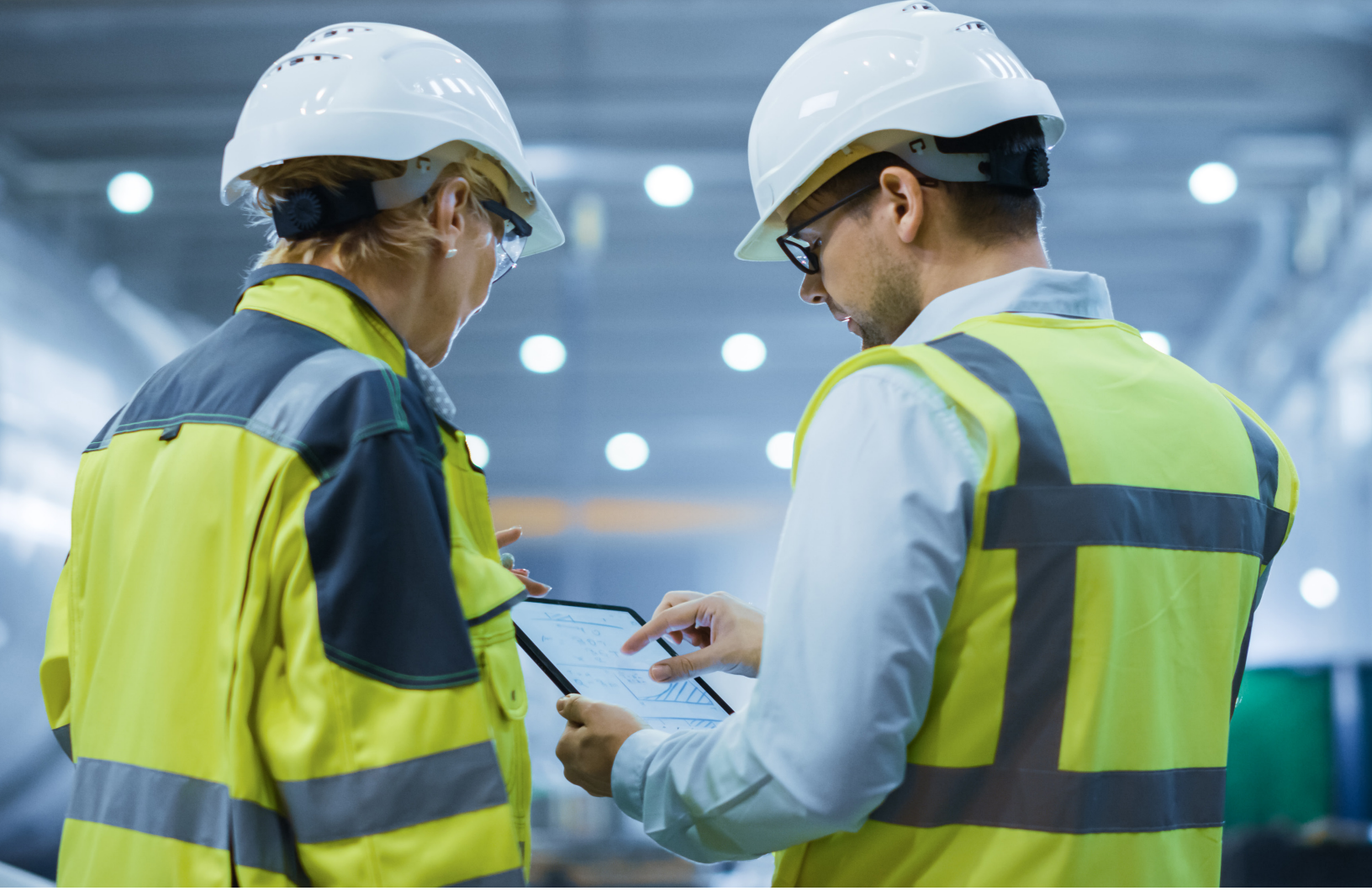
Despite progress to standardize globally, government regulations still differ and may dictate dissimilar frequencies required for cybersecurity compliance documentation. Those facing an audit obviously need more active management. A 5-year plan is recommended by some experts for digital transformation 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. Industry experts also recommend using automation and efficiency gains wherever possible, understanding that standards implementation and proof of compliance can be manual and time intensive. For example, use 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.



SELECT EXAMPLES OF KEY STANDARDS BY INDUSTRY

- ISA/IEC 62443 – industrial control system security
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) - utilities
- Nuclear Energy Institute (NEI) 08-09 - nuclear



6 TAP INTO MODERNIZATION OR EMERGING FUNDS

Investment and innovation in the OT cybersecurity space is at an all-time high, growing more than 30 times in 13 years,[4] which means new solutions and ideas are appearing constantly. Many industrial 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 (such as adhesives or coatings for paper and pulp products). 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 OT cybersecurity domains. 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.

Some experts recommend assigning a newer member of your team as the technical scout, to stay attuned to advancements and house offline trial systems and solutions. Others recommend 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 plant 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, for example.

USE TECHNOLOGY PROVIDERS TO YOUR ADVANTAGE 7

With a primary focus on ensuring uptime and operational excellence, some industrial 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 providers such as Honeywell can, in fact, swing momentum in an OT security improvement direction. This can help solve the resource challenge, as well as the time commitment issues that sometimes prevent OT leaders from forging these lateral or upward facing alliances.

For example, 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 veterans have suggested 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 room walk-through or review of the patching process, however, 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 AND SOLUTIONS

Honeywell is the leading provider of cybersecurity solutions that help protect OT-based assets, operations and people from digital-age threats. With more than 15 years of industrial 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 1000's 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 all assets on your ICS 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.

SOURCES:

1. Gartner: The 2019 CIO Agenda: Securing a New Foundation for Digital Business by Andy Rowsell-Jones, et al.

2. Honeywell OT cybersecurity research based on over 500 projects delivered in 2017. See also prior publicly published research at LNS Research: https://www.honeywellprocess.com/en-US/news-and-events/Pages/pr-12062017-honeywell-survey-shows-low-adoption-ofindustrial-cyber-security-measures.aspx

3. ZD Net: https://www.zdnet.com/article/ransomware-attacks-are-now-targeting-industrialcontrol-systems/

4. TechCrunch: https://techcrunch.com/2019/10/03/cybersecurity-is-a-bubble-but-its-notready-to-burst/

Honeywell Connected Enterprise
715 Peachtree St NE
Atlanta, GA 30308
www.becybersecure.com

Whitepaper | V2 | 07/21

THE FUTURE IS WHAT WE MAKE IT

Honeywell