Honeywell
THE POWER OF CONNECTED

Industrial Cyber Security

HELP IN JUSTIFYING CYBER SECURITY

How to Leverage Third Party Security Assessments to Attract the Process Control Network Investments You Need

White Paper

Abstract

Engineers who operate today's industrial control systems are repeatedly asked to do more with less, from recruiting hard-to-find talent to improving production and lowering operational costs. At the same time, there is growing risk of operational disruption from cyber security incidents, driven by factors such as increased plant connectivity, public availability of powerful hacking tools, and active nation state adversaries targeting industrials. From a technology perspective, traditional information technology (IT) in the form of commercial off-the-shelf (COTS) solutions are finding their way into operational technology (OT) settings. This convergence of IT and OT further complicates security, as known IT software vulnerabilities are inherent in COTS equipment such as routers and switches, and legacy OT equipment never designed for connectivity becomes susceptible to hacking.

This whitepaper identifies a path forward for operational engineering teams to attract the business investments they need to modernize their industrial control system environments and reduce cyber security risk. By learning how to use data from objective assessment findings, engineers can address several business outcomes at once and better manage overall cyber security risks. As corporate initiatives such as Industry 4.0 and Digital Transformation place additional pressure on engineering teams, the approach detailed in this whitepaper can help organizations ensure remediation efforts meet a variety of needs.

Table of Contents

Text

From Operations Inhibitor to Enabler

Cyber security has traditionally taken a back seat as organizations have prioritized outputs in refining, manufacturing, or chemical processing. However, pressure from Boards, regulators, and internal security teams to close dangerous security gaps has grown. With this comes an opportunity for engineers to modernize their plants more expeditiously. Just as data analytics has been used to vastly improve business efficiencies and processes, so objective cyber security data can be leveraged to develop a clear picture of necessary infrastructure changes. Without the increased focus on cyber security, such infrastructure changes would be difficult to identify, let alone back up with actionable data.

This section outlines five potential steps to move toward an "enabling" security approach as opposed to viewing security as an operations "inhibitor".

Step 1 – Determine if you have enough OT security information from trusted sources. Before embarking on new data collection, it is useful to not only identify existing data, but assess its validity and relevance to the operations business case. It is worth bearing in mind that insiders may provide only selective data, and external providers may offer only automated data that misses key human observations.

Consider the following:

- Who is regularly providing you with industrial security-related information?
- Who is regularly asking you for such security-related information?
- Has any hands-on human work been done to gain this information, or is it passively reported?
- What automated feeds or security reports are you already receiving? How often?
- Does the information provided relate to your operational network, or only business networks?
- What service providers are handling which portions of your security assessment work? Do you have copies of their last assessments and findings?

- How independent is the security information you are receiving, and does it help you prioritize industrial cyber security work?

- Are you required to share this information with a top level executive? Who receives such information regularly?

A case study: Engineers in Action

Mohammed proactively called in technicians to review several Oil & Gas facilities across his region in the Middle East. Based on two recent cyber security incidents that his colleagues at other companies experienced, he was keen to understand how vulnerable his company was to similar attacks, and to understand further actions he could take. Since he regularly received a network performance report from his service provider, he asked its team to help.

Upon reviewing the assessment proposal, however, he realized the technical team assigned was not deeply familiar with both operational environments and industrial cyber security. Its intent was to perform active scans of his production environment, and most of the work would be focused on hazops, which was not under his purview for remediation.

Based on a visit to a Dubai-based Center of Excellence, Mohammed determined that specific vendor consultants (Honeywell CyberVantage Security Consultants) with experience in control systems and oil and gas facilities would be safer to have on site, and would also ensure his technology warranties remained intact.

Site walk-throughs performed as part of the cyber security assessments revealed that security solutions he thought were in place had in fact not been fully implemented and remained on the shelf. In addition, staff were not well educated about threats such as RubberDucky, and thus lacked any USB security in their local policies or procedures. Mohammed established a yearly cadence for the assessments, and shares the findings with plant managers, CIO, and his direct chain of command.

Step 2 – Assess the situation on your own.

Before calling in any other teams or security partners, articulate your greatest concerns and risks, and where you think you are doing well. Documenting your comments privately early on can help:

- Ensure your experience and judgement are worked into your next steps. Nobody knows your own plant better, and it's important to tap your skills and knowledge as more people become involved with your security processes. Pay close attention to areas where you have no visibility and need it; or where you have visibility and recognize which machines or systems require the utmost sensitivity.

- Draft a rough proposal of what to look for once you do engage experts – your insights might expedite assessments and better enable security experts on the ground. Each process control network has its own unique aspects and diversity of equipment. If you have historically had issues with a brand or equipment type, you may want extra attention for those assets on your network, for example. It might also be important to know physical limitations, so jotting down which areas require special permits or certifications can help as you later as you perform walk-throughs with the security professionals.

- Ensure you don't escalate too early – some security issues can be resolved quickly and internally, before bringing visibility that might cause unnecessary alarm among the higher ranks. For example, an incorrectly placed cable, or non-compliant unsecured control room door, could be simple fixes your own team can perform before a formal review.

- You may also want to remind staff to ensure that no passwords are visible near control stations.

Step 3 – Perform a single plant assessment.

Once you have a basic understanding of your existing security information and your own rough sketch of security status and concerns, it is time to pilot a process for gaining trustworthy, actionable information. Depending on the scope of your organization and physical locations, you may prefer to select a single plant if this is your first cyber security assessment.

- Start with network and cyber security assessments, unless you are planning to expand or introduce any wireless. If you need wireless instrumentation or tools on the plant floor, perform a wireless security assessment as well.

Security is not only about keeping external threats out of your business, it is about making sure the information can be trusted while empowering the authorized users to improve company performance.

- Review the findings yourself. This is an important step, as many assessments uncover surprising information, such as previously unknown connection points, ghost servers, or non-compliant processes. By seeing the information first, you can manage expectations across the organization.

- For issues you find unacceptable based on your own expectations of internal staff, or work you thought was already completed, consider an internal team discussion. Use this to identify if staff bandwidth issues, policy limitations, or other obstacles are getting in the way of your team's ability to perform important security work. Determine what, if anything, should be remediated by your team. For example, your third party assessor may find administrator rights that remain for a fired employee, or uncover a running server that nobody thought still existed. Better for you to know these issues and consider how you want to correct them, before you move to the next step of sharing and leveraging report findings.

Step 4 – Consider corporate support for important security remediation work.
Once you are familiar with assessment findings, and have all available information on hand, determine if your corporate organization can partner with you for broader sweeping upgrades or improvements. In some cases, existing corporate initiatives will overlap with a need for reducing risk, improving productivity, or gaining competitive advantage, and security remediation work defined with these outcomes may be funded.

- Investigate your corporate initiatives to see if security work needed can align with their priorities such as digital transformation, quality improvement, automation, it standardization, performance optimization, or security awareness training programs. Some companies use industry trends to inform their initiatives, so also keep an eye out for Industry 4.0 and IIoT themed initiatives. Any plant improvement effort must include cyber security. Corporate oversight and regulatory bodies will be asking about it.

- Leverage security partner facilities to educate corporate team members regarding the industrial threat landscape, and ideally, ensure they experience a simulated attack relevant to your organization. This live education helps decision-makers better understand the risk and consequences of unfinished security work that might be highlighted in your assessment findings. Providers such as Honeywell offer Industrial Cyber Security Centers of Excellence for these purposes, as well as to validate security solutions. Since increased performance and better functionality is a frequent COTS requirement, consider testing such equipment together with your OT equipment in the safe off-production test bed at such centers.

- Use plant-specific findings to show potential trends or issues that could affect the wider organization. Weak encryption methods, for example, can affect data integrity for any area that data may traverse. COTS-related vulnerabilities will impact any COTS equipment plant-wide. A lack of a secure file transfer capability will impact not only operations, but any teams seeking to share files with operations. Articulating trends and consequences can help find common ground. For example, you may learn that your organization is already seeking remote access tools for efficiency reasons; your need for a secure remote access approach to managing operational technicians and maintenance workers could be an appropriate rationale to fund your secure solution for the division or the entire enterprise.

- Work with your assessment partner to investigate additional funding or budget streams within your organization. For example, if a Secure Network Refresh is underway at another site, see if your network assessment can be packaged into that service, since it will inform and support the refresh. Often, issues such as outdated encryption methods or highly exploitable OS types can be resolved by upgrading to newer equipment that delivers the latest software enhancements. These same security improvements often improve usability and performance.

Case study: Engineers in Action

Jim manages a paper mill in the US Southeast, as part of a larger conglomerate with headquarters far from his location. Corporate repeatedly asks for log data from his operations environment, but Jim has no assigned cyber security staff, nor does he want IT "touching his systems".

When the CIO asked for key information again, Jim presented a proposal from a third party assessor (Honeywell CyberVantage Security Consulting Services) to perform a cyber security assessment. Jim and the CIO decided to split the cost of the assessment, since it supported both teams' needs for objective security visibility. Using the assessment findings, Jim was able to articulate priority actions that the CIO funded, including replacing old switches with known security vulnerabilities. In addition, the findings uncovered additional work that Jim and the CIO agreed should be outsourced in order to expedite execution and keep Jim's team focused on production.

Jim was relieved that his team was not tasked with the work, and the CIO was satisfied that required cyber security diligence was underway. Part of the CIO's rationale for funding the effort was impending regulatory requirements that would force compliance work anyway. The assessment findings allowed the company to reduce risk, meet compliance, and ensure staff productivity, all in one effort.

Step 5 – Develop a consistent, ongoing security program that includes assessments.

With your trusted, objective information and a pilot run of performing assessments, you will be best informed how to develop long-term plans. Recognizing that industrial cyber security is an ongoing practice, not a one-time deployment, is critical for risk reduction success.

The next step is to ensure a formal program is established, with the appropriate stakeholders engaged in a governed program to improve industrial cyber security maturity levels. Such models provide helpful baseline, improvement, and benchmarking capabilities, and help guide the steps to standards implementation. As mentioned, the cyber security checks and actions will also drive toward a more modern, resilient, and high performance process control network as systems and processes are updated.

- If your company does not already have an industrial cyber security program, consider performing cross-facility assessments. Use the findings as discussion points with the varied teams and to push for a centralized governance team that can evaluate and fund future critical security work. Often, once multiple assessments are completed and shared, it is better understood that teams may face similar challenges that can be solved by joint actions.

- If your company does have a program, discuss when and how assessments will be performed, and ensure you are part of receiving or discussing findings. Many organizations learn that multiple teams are performing assessments on an ad hoc basis, but never thought to share findings, or delayed sharing due to reorganizations or changes in personnel. Communicating existing findings, and clarifying a standard timing and approach to assessments, helps ensure you are always ahead of required OT infrastructure changes and can budget accordingly.

- Team up with other plants to fund a standardized approach to required technologies such as USB security management, threat identification, malware prevention, and compliance work and remediation. By simplifying your technology choices across teams, you will be better prepared to assist each other during cyber incidents, and can pursue bulk purchases of equipment or support. In some cases, when an Enterprise-Wide Security Program is in place, you can also influence and help develop top-down policies that specify the technologies you prefer.

Case study: Engineers in Action

Diane runs 8 manufacturing facilities, 2 of which experienced NotPetya-related issues last year. Technical teams from across her facilities lobbied to procure various anti-virus solutions, and others requested a additional headcount for incident response, based on the cyber incidents.

Rather than jumping to conclusions, Diane called in Honeywell CyberVantage Security Consultants as third party assessors to perform both network assessments and cyber security assessments across all 8 facilities.

The findings revealed that despite a sound policy, on-the-ground compliance with that policy was lacking. Specifically, old WindowsXP machines were still in use despite a corporate policy to remove these highly vulnerable systems. In addition, security technology was being applied to low priority assets, with no clear strategy for zoning and segmentation, and no 5-year plan was in place to improve overall cyber security resilience.

Diane leveraged the findings for further discussion with each plant manager, and used the same third party consultants to help educate her staff (who were not cyber security focused). The Honeywell consultants established a security patching process for one of the WindowsXP machines, which had to remain in place temporarily due to the critical processes it ran, while also defining a migration plan to move the processes to a more resilient OS.

Since assessment work was performed across all facilities, Diane was able to work with the consultants further to establish a unified plan and an enterprise-wide security program for ongoing governance and work prioritization. Instead of wasting her limited budget on knee-jerk response purchases that would not lower the organization's risk, Diane was able to gain actionable information that led to efficiencies and ROI-based decision-making. The standardization, enterprise-wide, simplified management and promoted cross-team work, eventually leading to an actively managed Industrial Cyber Security Program.

Knowledge is Power to Fuel Plant Improvements

In demanding roles such as plant and operations management, too many disparate tasks often force security work to the wayside. Viewing security as an enabler for operations instead of an inhibitor, however, not only drives industrial cyber security improvements, but also promotes smarter ways of working.

Industrial cyber security assessments provide objective, actionable information that can justify the required upgrades to your plant infrastructure. Such assessment knowledge is powerful for articulating how cyber security work impacts important initiatives, from quality improvements to digital transformation, and can help meet daily needs, from secure file transfers to credentialed network users.

By using assessment findings to engage cross-teams and corporate decision makers, engineering can document needs and gain the funding needed for important infrastructure updates that improve overall reliability, productivity, and efficiency.

For More Information

Learn more about how Honeywell's Cyber Services can improve your enterprise security, visit becybersecure.com or contact your Honeywell Account Manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road,
Zhangjiang Hi-Tech Industrial Park,
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

WP-18-10-ENG
October 2018

Honeywell