ARC VIEW

JANUARY 25, 2024

Industrial Operations Need Mature OT Cybersecurity

By Sid Snitkin

Keywords

OT Cybersecurity, Honeywell

Summary

Cybersecurity has never been more important or more challenging for manufacturers and critical infrastructure operators. These organizations have become prime targets for ransomware and sophisticated nation-state attacks. Many are facing more stringent security compliance requirements. Most have limited security resources and struggle to maintain defenses and keep up with new risks being created by digital transformation efforts.

Cybersecurity has never been more important or more challenging for manufacturers and critical infrastructure operators. Industrial companies need a new approach that delivers mature defenses with less people, less complexity, and lower costs.

Cyber incidents, like Colonial Pipeline, show the devastating costs of disruptions to industrial operations and the sophistication of today's attacks puts every industrial operation at risk. Small companies in industrial supply chains have also become pawns in efforts to cripple operations in critical industries. No company can afford to operate with the risks of such attacks. Every industrial company needs a mature cybersecurity program to deal with these challenges.

Most large industrial companies have made significant investments in cybersecurity but lack the resources and integrated solutions to achieve required maturity levels. Cybersecurity costs and complexity have left smaller industrial companies with little or no protection. All industrial companies need a way to achieve maturity with fewer people, less complexity, and lower costs.

This ARC View discusses how industrial companies can effectively leverage third party support to achieve these goals. A review of Honeywell's cybersecurity offerings is included to show how one supplier is helping industrial companies build the maturity required for today's world.

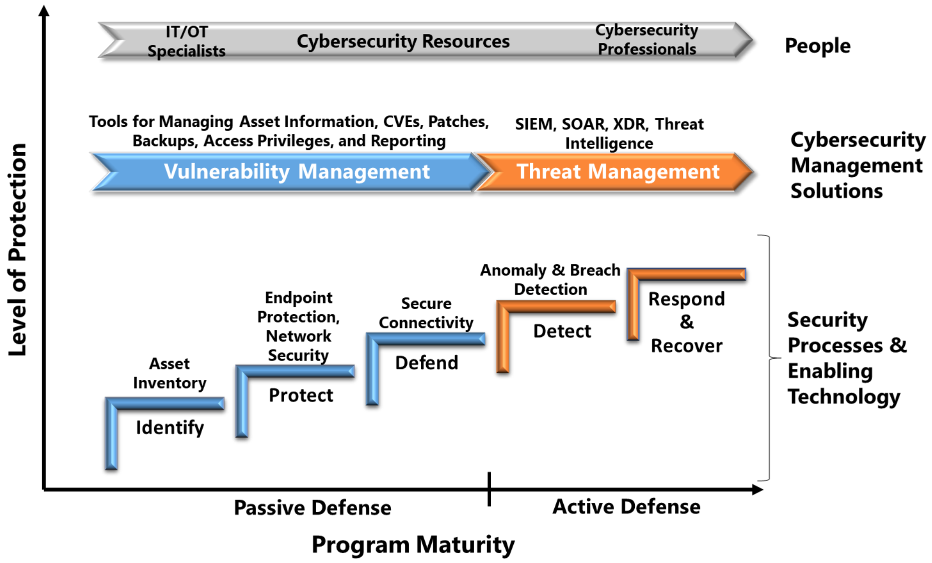
Navigating the Evolving Cyber Threat, Governance, Risk, and Compliance Landscape

Today, cyber threats are a critical concern for organizations of all types and sizes. Industrial companies are particularly concerned, as they operate in an extremely treacherous cybersecurity landscape, with threats evolving at an alarming rate. Not surprisingly, there is deep concern about the potential for significant financial losses, operational disruptions, and reputational damage that a cyberattack can cause.

These worries stem from a convergence of factors, including the growing complexity of industrial systems and the convergence of IT and OT (operational technology) networks, which have created more interconnected systems increasing the attack surface and making it more difficult to defend against cyberattacks. There is also a growing number of cybersecurity regulations and compliance requirements. This includes 52 current or proposed U.S. Federal cybersecurity regulations and 156 countries have enacted cybercrime regulations that impose significant burdens on companies and require them to continuously update their security posture.

Cybersecurity Maturity Requires Capability Alignment

ARC's Industrial/OT (Operational Technology) Cybersecurity Maturity Model provides a useful tool for understanding and building an effective industrial cybersecurity program.


IT/OT Specialists
Cybersecurity Resources
Cybersecurity Professionals
People
Tools for Managing Asset Information, CVEs, Patches, Backups, Access Privileges, and Reporting
SIEM, SOAR, XDR, Threat Intelligence
Vulnerability Management
Threat Management
Cybersecurity Management Solutions
Level of Protection
Asset Inventory
Identify
Endpoint Protection, Network Security
Protect
Secure Connectivity
Defend
Anomaly & Breach Detection
Detect
Respond & Recover
Security Processes & Enabling Technology
Passive Defense
Active Defense
Program Maturity

ARC Industrial/OT Cybersecurity Maturity Model

This model provides a roadmap for implementing the people, processes, and technologies needed to support the NIST cybersecurity framework recommendations.

The steps at the bottom of ARC's model reflect the sequence that companies should follow in security technology investments. Following these steps ensures that foundational capabilities are always in place to support the requirements of subsequent steps. The colors in the model distinguish passive defensive measures that are needed to protect systems against conventional hackers and malware, from the active defense capabilities needed for today's more sophisticated attacks and ransomware.

Alignment across cybersecurity people, processes, and technology investments is essential for effective, sustainable OT cybersecurity. But choosing the right technologies, processes, and human resources is equally important. Companies need to be sure they have the expertise and required level of cybersecurity experience to make these decisions.

The bars above the technologies show the people and processes needed at each step to ensure the associated security technologies can be properly maintained and effectively utilized. The effectiveness, or maturity, of a cybersecurity program is determined by the category (people, processes, and technology) with the lowest maturity score.

Cybersecurity Effectiveness Is More than Alignment

Alignment across cybersecurity people, processes, and technology investments is essential for effective, sustainable OT cybersecurity. But choosing the right technologies, processes, and people is equally important. Requirements vary significantly across different industries and regions and here are some recommendations for things companies should consider in their cybersecurity investments:

Technology

- **Endpoint Protection** – Can the solution protect all your OT assets against malware? Does the solution also protect the loss of any critical data you may have in the assets? If not, what compensating controls can you use to address unprotected OT assets?

- **Network Security Solutions** – Does the solution limit external access to all critical systems and devices? Does the solution enable segmentation of critical and non-critical control areas? Can the solution support rapid, selective isolation of compromised assets?

- **Secure Connectivity** – Does the solution protect OT systems from unauthorized external access? Does the solution provide security for communications with remote assets, mobile devices, cloud apps, third party sites, and connected workers?

- **Vulnerability Management** – Does the solution include all the tools to enable efficient and effective maintenance of all security defenses? Does it support asset inventories' information across your entire control system and collect all the information you need to identify and classify all your assets? Does the solution support assessment of security risks, evaluation of vulnerability alerts, management of patches and AV updates, maintenance of system backups, and management of user privileges?

- **Threat Management** – Does the solution include all the tools to enable efficient and effective detection and response of potential security threats? Does it include passive monitoring for anomalous behavior within OT devices, networks, and user actions? Does it have the tools needed to analyze alerts, integrate threat intelligence, and help defenders investigate, isolate, remediate, and restore systems?

Human Resources

Companies need the right human resource plan to ensure effective cyber defenses are built and sustained. The right plan includes qualified people with the OT and cybersecurity expertise to support the full range of cybersecurity activities throughout an OT system's lifecycle. These activities include:

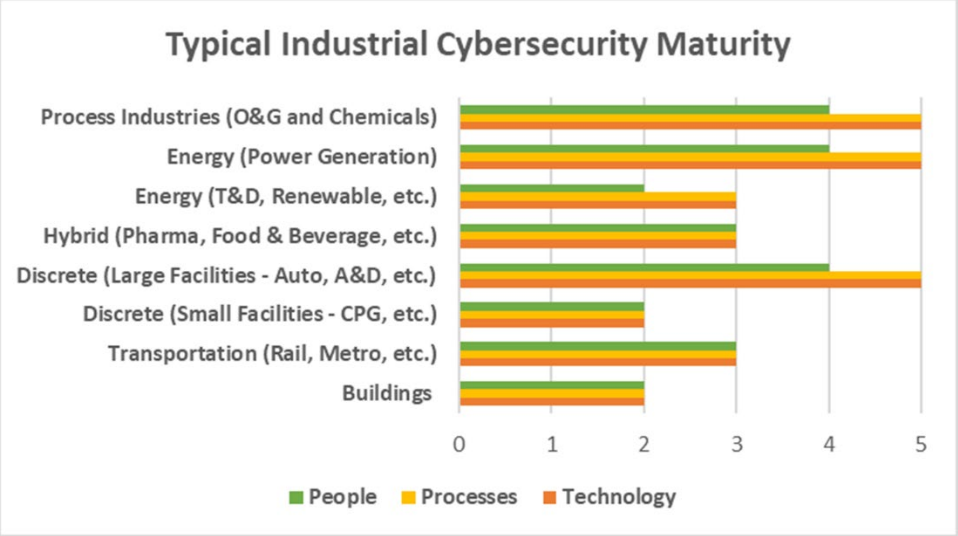
- **Assessments and Audits** – Performing periodic assessments of the cyber risks within system architectures, devices, people, and processes and developing recommendations to mitigate risks that are unacceptable. Assessments can also include periodic audits to ensure that system defenses and policies are being maintained and working as expected.

- **Design & Implementation** - Managing the selection, implementation, configuration of new cybersecurity hardware and software solutions. Developing security policies, procedures, and incident response plans. Training people in the use and maintenance of all security defenses.

- **Security Management** - Performing the many different kinds of system maintenance tasks that are needed to sustain the effectiveness of the cybersecurity program. This includes monitoring and evaluation of vulnerability and threat intelligence, implementation of security patches and product upgrades, analyzing and responding to system security alerts, and managing active cyber-attacks and cyber incidents, and restoring systems to operational status.

Most Industrial Companies Face Serious Cyber Risks

ARC's research shows wide variation in the maturity of today's industrial cybersecurity programs. Major process, power and large discrete manufacturers have invested extensively in security technologies and processes, but many still lack the human resources to manage vulnerabilities, threats, and digital transformation initiatives. Cybersecurity programs in many other industries have only basic passive defenses managed by plant personnel on a part-time basis with limited time and cybersecurity expertise.



Industrial Cybersecurity Maturity Levels (Relative to Steps in ARC's Model)

This situation is leaving many industrial operations at risk of serious cyber incidents. Recent incidents demonstrate that cyber criminals and unfriendly nation states have the capabilities to penetrate even mature security programs. They are also disrupting critical infrastructure through attacks on smaller, weaker partner systems that companies need for meaningful operations. These attacks show why every industrial operation needs to ensure their cybersecurity programs achieve maximum maturity.

Overcoming Cybersecurity Obstacles

Closing cybersecurity program gaps is challenging for many companies. A complete portfolio of cybersecurity management tools and a full-time staff of OT cybersecurity professionals are expensive and hard to justify, especially in companies that have not yet experienced a significant cyber-attack. Finding ways to reduce software and cybersecurity resource costs is the only way to overcome these obstacles.

Many large companies are addressing these issues internally, through programs that converge global IT and OT cybersecurity programs. But the only option for smaller companies is to use third party cybersecurity services providers that offer the resources and expertise they need. Large companies are also finding that they need third party support to address regional and plant specific security needs.

Use of a third party cybersecurity service provider ensures a way to overcome financial constraints, as they can leverage their investments in people and technologies across many clients. But their impact on cyber risk reduction depends on their ability to support specific systems. Many companies offer third party cybersecurity services, but few are experts in protecting critical industrial OT systems. Choosing the right third party cybersecurity service provider is critically important, and ARC recommends that companies consider the following kinds of issues to select the right third party cybersecurity service provider:

- Does the provider have people who are familiar with your OT system technology and operating processes?
- Can they support all your facility's assets, regardless of supplier and vintage?
- Do they have the global resources and expertise to ensure that cyber risks are minimized in all your facilities?
- Do they have the tools and processes in place to deliver quality services remotely and minimize the downtime of any cyber incident?
- Do they understand your operations enough to help you ensure that they are resilient to cyber-attacks?

Honeywell Understands Operations & Industrial Cybersecurity

Honeywell is a company that meets ARC's requirements for a strong industrial cybersecurity provider. The company has been one of the leaders in industrial control for over fifty years, and over the past two decades, has built a robust cybersecurity offering including cybersecurity software, managed security services, industrial security consulting services, and integrated security solutions—all tested and tailored for the OT environment. Their global team, of over 500 cybersecurity professionals, provides services to help protect essential operations across various industries. And many of these capabilities are delivered on a 24/7 basis through a global network of managed security service centers, cybersecurity customer innovation centers, and cybersecurity development centers.

Honeywell's OT cybersecurity offerings are designed to help customers facilitate the following outcomes:

- **Risk Reduction** - Through integration of threat intelligence and in-depth defense strategies, organizations can implement Honeywell cybersecurity offerings designed to preemptively neutralize potential threats. Honeywell cybersecurity assessment services help companies understand their threat landscape and vulnerabilities. Honeywell can then design and build services to help them deploy and configure the appropriate passive and active defenses to manage these risks.

- **Operational Safety -** Honeywell's Cyber Insights and Cyber Watch software solutions, part of the Honeywell Forge Cybersecurity+ platform, are designed to provide real-time threat detection and risk-based intelligence that companies need to improve the safeguards for operational processes and employee safety. These measures are designed to help customers preempt disruptions and hazards, fostering an environment where safety protocols align with security operations.

- **Compliance** - Monitoring compliance status and analyzing site security metrics are essential for maintaining your GRC (Governance, Risk, and Compliance), regulatory adherence, and identifying security gaps. Honeywell's Cyber Watch is designed to provide an automated compliance dashboard that gives organizations a comprehensive view of their OT compliance across multiple sites.

- **Business Continuity** - Proactive detection and prevention of cyberattacks are integral to maintaining profitable operations. Honeywell's Managed Security Services (MSS) and Advanced Incident Response (AMIR) solutions are designed to help companies maintain security hygiene and rapidly detect and respond to new threats.

- **Workforce Development:** Honeywell offers a variety of cybersecurity training services to empower the facility's workforce. This includes certifications and tabletop exercises and helps cultivate a proactive security culture that can significantly increase the effectiveness of OT cybersecurity programs.

Based on decades of experience in process automation, Honeywell offers cybersecurity services designed to help customers protect the availability, safety, and reliability of their industrial assets worldwide. Honeywell's Cybersecurity+ software solutions extend this capability and help reduce the growing risks of cybersecurity attacks on industrial operations and are backed by Honeywell's GARD Threat Intelligence and vertical-specific security content.

Many of Honeywell's cybersecurity offerings are designed to offer these capabilities for Honeywell and many non-Honeywell assets. ARC has also been advised that over 50 percent of Honeywell's current cybersecurity customers have a blend of automation supplier equipment.

Conclusion

Today every industrial operation needs a mature cybersecurity program. Cyber-related disruptions of critical infrastructure are too costly to ignore, and society is demanding that every company address these risks. Filling resource gaps with the right products and services from knowledgeable OT cybersecurity professionals is essential for rapid detection and response to every suspicious event. Interoperable solutions are needed to reduce the costs and complexity of cybersecurity. ARC's analysis of Honeywell shows that Honeywell's cybersecurity offerings include many end-to-end capabilities that are designed to help end users achieve their required level of OT cybersecurity maturity. The biggest risk to end users is to not avail themselves of a company like Honeywell that has such capabilities and to ignore the critical issues outlined in this report.

For further information or to provide feedback on this article, please contact your account manager or the author at SRSnitkin@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.