ARC VIEW

SEPTEMBER XX, 2021

Close Your OT Cybersecurity Gaps Now

By Sid Snitkin

Keywords

Industrial/OT Cybersecurity, Risk Management, IEC-62443, Radiflow

Summary

Industrial companies need stronger OT cybersecurity programs to deal with today's sophisticated threat environment. The risks of serious industrial cyber incidents have grown significantly. Industrial companies have become prime targets for ransomware and sophisticated attacks on critical infrastructure. Digital transformation efforts are proliferating new attack pathways through connectivity with cloud services, vendors, and remote workers. IoT devices are bringing more vulnerabilities into critical control systems.

The risks of serious industrial cyber incidents have grown significantly. Advanced attacks and digital transformation demand more advanced cybersecurity strategies that can anticipate threats and rapidly respond to suspicious behavior.

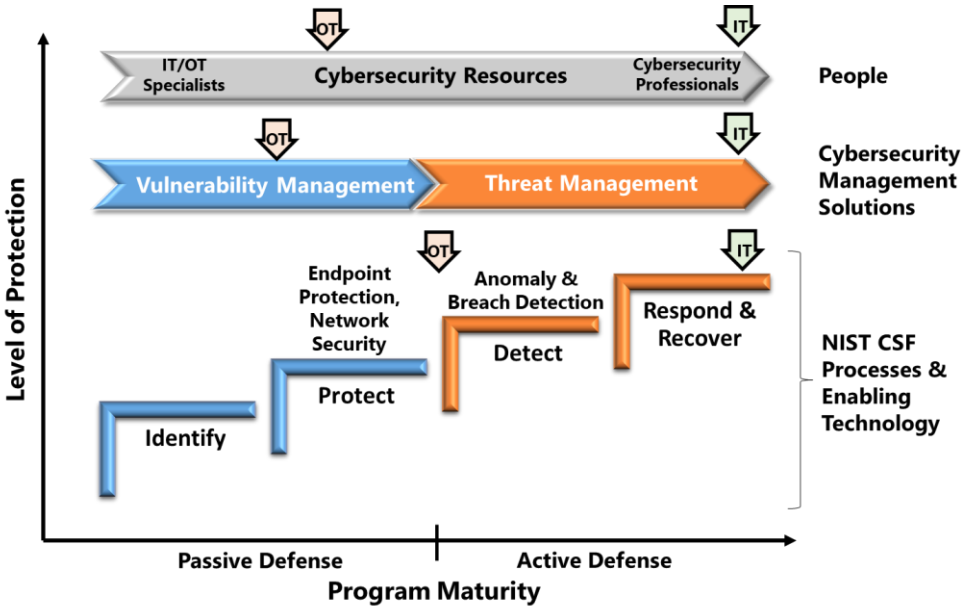
While industrial companies have invested heavily in cybersecurity, the bulk of spending has focused on IT defenses. Most OT systems only have basic capabilities that address yesterday's threat environment. Advanced attacks and digital transformation demand more advanced OT cybersecurity programs that can anticipate threats and rapidly respond to suspicious behavior.

Recently, ARC Advisory Group discussed the OT cybersecurity situation with executives from Radiflow. This company has extensive experience protecting critical OT systems and a portfolio of products to deal with the new threat environment. A brief overview of their security offerings is included in this report.

Industrial Cybersecurity Today

ARC's Industrial/OT Cybersecurity Maturity Model provides a useful tool for analyzing the status of industrial cybersecurity programs. This model

extends NIST cybersecurity framework recommendations with an investment roadmap for the associated security technologies, cybersecurity management solutions, and human resources. A key feature of the model is how it highlights the need for maintaining alignment of people, processes, and technology investments. The colors in the model distinguish basic passive defensive measures, which protect systems against conventional hackers, from the active defense capabilities needed for sophisticated attacks.



ARC Cybersecurity Model Shows Current State of Industrial Cybersecurity Programs

As the figure shows, industrial IT cybersecurity programs are significantly more mature than those for OT. IT security programs include passive and active defenses. They also have teams of cybersecurity professionals equipped with advanced cybersecurity management solutions that help them maintain security posture and rapidly respond to suspicious events.

Typical OT cybersecurity programs only have passive defenses and many lack the people and security tools needed to manage vulnerabilities effectively. Few companies have invested in active defense capabilities needed to detect and manage ransomware and sophisticated attacks. They likewise lack the resources and expertise to ensure secure deployment of new digital transformation efforts.

OT Cybersecurity Requirements Have Changed

Sophisticated attacks on manufacturers and critical infrastructure operators have changed security requirements. Yesterday, most industrial facilities could get by with basic OT cybersecurity programs designed to protect operations from general hackers and malware floating around the internet. Today, every facility needs an OT cybersecurity program that can deal with ransomware and targeted attacks by sophisticated adversaries.

Companies need OT cybersecurity programs that can deal with ransomware, sophisticated attacks, and digital transformation security issues. No company should accept the risk of incidents that may jeopardize worker safety, product quality, regulatory compliance, or operational continuity.

Digital transformation is another development that requires better OT cybersecurity. Operators, inspectors, and maintenance personnel are demanding direct access to engineering systems, cloud analytics, and third part web sites. Vendors are demanding service access for robots, autonomous vehicles, and packaged systems. Increased demands for access to OT data and new IoT sensors are expanding network technologies and protocols. COVID-19 accelerated these efforts and added the challenge of supporting more remote workers and vendors. These developments are improving efficiency, effectiveness, productivity, process consistency and are vital for company survival. But they are increasing the risks of cyber incidents that can impact safety and business continuity.

Industrial companies can be excused for the fact that initial OT cybersecurity investments did not anticipate these developments or the rapid pace of technological change. But there is no excuse for continuing to operate with weak OT cyber defenses. A single incident could jeopardize worker safety, product quality, regulatory compliance, and operational continuity.

Addressing OT Cybersecurity Gaps

Changes occurring in industrial facilities are creating OT security environments that are similar to what IT cybersecurity teams face. So, OT security teams need comparable defensive capabilities. As ARC's model illustrates, this requires improvements in people, security management tools, and security technologies.

People

Lack of OT cybersecurity professionals is often cited as the major reason for the low maturity of OT security programs. When security teams can't keep

up with vulnerability alerts, patches, and product updates the effectiveness of security technologies erode. Adoption of advanced cybersecurity technologies is also impeded when facilities lack people with OT security expertise.

Resource issues are hard to resolve. Few managers can justify the costs of adding expensive cybersecurity professionals to their staffs. But some companies are overcoming this hurdle through IT-OT cybersecurity convergence programs. Others are leveraging third party cybersecurity service providers.

Security Management Solutions

Addressing resource issues is critically important, but not enough to ensure good security. The continuous stream of vulnerabilities and threats can overwhelm even large security teams. System changes, for digital transformation and unexpected events like COVID-19, likewise create a constant stream of new security issues that need to be addressed in a timely manner.

Security professionals need cybersecurity management tools to manage workloads and maintain focus on the most critical issues. In the OT world, cybersecurity management solutions should include capabilities that:

- Automate time-consuming activities like asset inventories, compliance reporting, and evaluations of vulnerability advisories.
- Contextualize security alerts and enable fast triaging of potential security threats.
- Facilitate rapid blocking of known threats, implementation of "kill chain" actions to stop active attacks, isolation of compromised assets, and remediation of systems.
- Continuously analyze risks based on new vulnerabilities and threats and ensure that security teams have the guidance they need to focus efforts on the most critical and immediate issues.
- Support for planning of cybersecurity investments to address new security challenges.

Security Technologies

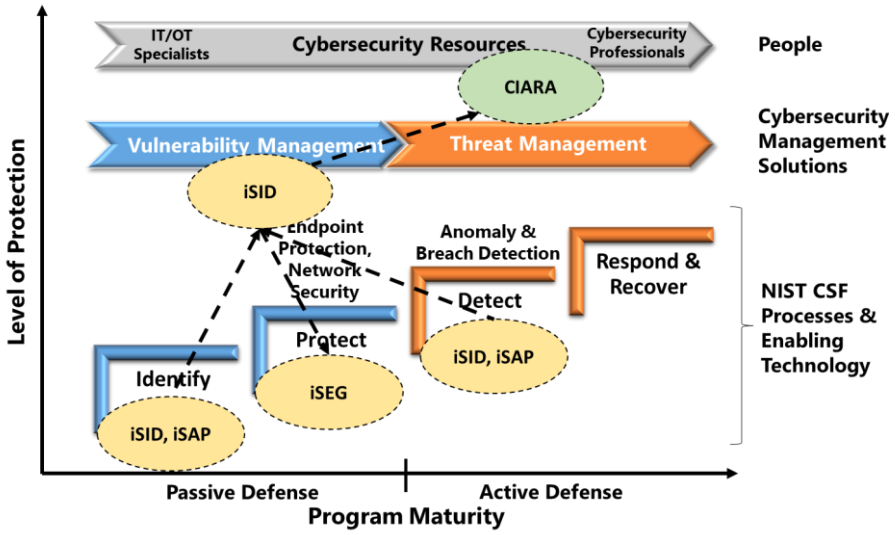
Passive defenses can never stop all attacks, regardless of how well they are maintained. Companies need Anomaly and Breach Detection solutions that rapidly detect intrusions and give defenders time to respond before attackers

wreak havoc. Companies should have solutions that detect anomalous behaviors within assets and network communications.

Radiflow Can Help Companies Close OT Security Gaps

Radiflow was founded in 2009 and has a team of professionals with diverse backgrounds, including people from elite military units, automation vendors, and global cybersecurity vendors. According to the company, Radiflow products are being used by major industrial enterprises and utilities, protecting more than 5,000 critical facilities worldwide.

ARC's discussions with Radiflow executives demonstrated their understanding of OT cybersecurity challenges and commitment to helping industrial companies protect critical ICS and SCADA systems. Their iSID and CIARA products provide the functionality needed to close some of the major cybersecurity gaps described above.



Radiflow Cybersecurity Solution Portfolio

iSID

iSID provides automated asset inventories and data flows; vulnerability management workflow support; and detection of anomalous system behaviors. It uses deep packet inspection (DPI) passive network monitoring to develop a digital image of a system's assets and communication patterns. This digital image contains the detailed information users need to efficiently manage vulnerabilities and evaluate security advisories. iSID also supports

use of passive network monitoring and the digital image to address a variety of other security needs that can arise in OT environments:

- **Network Visibility –** automatic detection of changes in system networks and behaviors (e.g., new devices, new connections, new sessions.).
- **Cyber Attacks –** continuous monitoring of network traffic for known threats to industrial networks, including PLCs, RTUs and industrial protocols.
- **Policy Monitoring** - Monitoring of network traffic for user-defined policy violations. This includes things like valid commands (e.g., "write to controller") and valid operational ranges (e.g., "do not set turbine to above 800 rpm.")
- **Maintenance Management –** Monitoring networks for erroneous commands that occur during system maintenance activities. This is driven by user-defined work orders for specific devices and time slots and includes logs of all maintenance activities that can support compliance reporting and troubleshooting.
- **Anomaly Detection –** Network messages are compared against the digital image to detect abnormal behaviors, considering things like device sampling time, and changes in operational values.
- **Operational Behavior Monitoring –** auditing of devices (PLCs, RTUs, and IEDs) at remote sites and alerting on any firmware changes or configuration modifications (e.g., software updates or turning edge devices on or off) and activity logging.

iSID can be deployed at a central location, locally at each remote site, or a combination of both (for larger facilities that require on-site threat monitoring). Radiflow also offers additional products that extend iSID capabilities. This includes a central management console that aggregates information from multiple sites (iCEN), smart probes that collect network information from remote sites (iSAP), and a DPI gateway to enforce NERC CIP and IEC-62443 zoning requirements (iSEG).

CIARA

CIARA is Radiflow's newest product. It provides a sophisticated risk simulation capability that companies can use to guide mitigation efforts and plan

security investments. CIARA's simulation uses a wealth of information about the system, known vulnerabilities, current security controls, and known threat actors, to generate a detailed, system-specific evaluations of security risks. ARC received a demo of this product and was impressed with its comprehensiveness and decision support capabilities. CIARA's risk assessment process consists of four steps that were designed to meet the recommendations specified in IEC-62443-3-2:

Step 1 – Learning the Network

Risk assessments begin with the creation of a digital image of the system that identifies all of the assets, vulnerabilities, connections, and protocols that an attacker might leverage in an attack. This image can be obtained from iSID or through integrations with other network monitoring solutions.

Step 2 – Network Definition and Initial Risk Analysis

The image is analyzed to identify security zones and conduits. Asset types are used to establish recommended target security levels for each zone (which can be adjusted by the user). Industry and geography are used to assess the relevance of known threat actor groups and their associated techniques and tactics are identified using the MITRE ATT&CK framework, Mandiant, and other information sources.

All of this information is used to drive simulations of attacks that generate estimates of the likelihood of successful compromises. Initial estimates are performed on unmitigated systems to get a solid security baseline. This step is repeated whenever a user wants to assess the risks after changes in the system or threat landscape. In these cases, the simulation considers all of the security controls that are in place.

Step 3 – Analysis of each zone's foundational risk and security gaps

The system provides users with radar charts showing the security status of each zone relative to its security level target value. It also provides lists of security controls that can be used to mitigate unacceptable risks. Users can selectively apply these security controls and see their risk reduction impact. CIARA also has the capability to automatically recommend controls on the basis of what can have the greatest risk reduction benefits. These recommendations can also consider budget constraints.

Step 4 – Finalize Mitigation Plan and Apply Controls

Users update CIARA as each security control is applied to gain an ongoing assessment of system security status. CIARA is a unique product that can help industrial companies manage security throughout a system's lifecycle. Consultants can use it during security assessments to identify risks and recommend security investments. Owners can use it to periodically assess the risk implications of proposed system changes and to identify actions needed in response to changes in the threat landscape. MSSPs can use CIARA to understand the significance of system alerts and develop security recommendations for clients.

Conclusion

Threats to industrial operations have outpaced the capabilities of most OT cybersecurity programs. Many facilities lack the security resources, technologies, and cybersecurity management tools to defend operations against ransomware and sophisticated attackers. They also lack people and expertise to ensure security of digital transformation efforts and expanded use of remote workers. Today's OT security team is facing the same security challenges as their IT counterparts, and they deserve to have comparable capabilities. No company can afford to ignore the growing risks of serious cyber incidents.

This report highlighted the major differences between industrial IT and OT cybersecurity programs and outlined the improvements that should be made to ensure the security of critical ICS and SCADA systems. The review of Radiflow's products show that there are solutions available that can help companies overcome their critical OT security gaps. So, the biggest risk to OT security is lack of user urgency in addressing these critical issues.

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.