IndustryWeek®

EXECUTIVE SUMMARY

Cybersecurity For Advanced Manufacturing and Critical Infrastructure

Sahil Diwan, Strategic Cybersecurity Consulting, Siemens Advanta
Dennis P. Gilbert, Jr., Founder and CEO, Vector9 Consultants, LLC

KEY TAKEAWAYS

- OT cybersecurity faces challenges from attackers and OT environments.
- OT environments require different approaches to security.
- OT security requires increased cooperation between IT and OT departments.
- Enterprises can take concrete steps to mitigate OT security risks.

in partnership with

SIEMENS

Cybersecurity For Advanced Manufacturing and Critical Infrastructure

OVERVIEW

Digitalization has opened a new world of opportunity for traditional operational technologies. However, these opportunities introduce cybersecurity risks to the OT environment, making it critical for companies to develop OT-focused response plans and security strategies. The historically and fundamentally different sets of physical OT and virtual IT systems require increased collaboration and a holistic approach to cybersecurity.

Siemens Advanta and Vector9 work with OT customers, large and small. As security advisors and solution providers, Siemens Advanta and Vector9 use their considerable industry expertise to meet the cybersecurity needs of an evolving technology landscape, incorporating today's technology integrations and tomorrow's advancements in a holistic cybersecurity practice.

CONTEXT

The presenters discussed the specific challenges to cybersecurity for OT environments and steps that organizations can take to address those challenges.

KEY TAKEAWAYS

OT cybersecurity faces challenges from attackers and OT environments.

Threat vectors have significantly changed over time in response to the increased variation in infrastructure, making it more challenging to discover and counter threats before damage is done. Threat vectors today range from lateral movement in the IT to OT environments, to unauthorized remote access and insider threat, and more.

Many threat actors will use the code of stolen assets to carry out false commands in an attempt to damage systems. Threat actors are frequently professional organizations, investing time and energy to determine attack targets, what it takes to execute the attack, and what capability needs to be used to motivate ransom payouts.

> "Those folks with ransomware groups, sitting around a table, understanding their ROI—they are now targeting the OT environment for that increased opportunity to make some money."
>
> *Dennis P. Gilbert, Jr., Vector9 Consultants*

There is no one-size-fits-all approach to cybersecurity. Regardless of industry, the OT environment is highly complex, with a variety of implementations and needs, including solutions from multiple vendors, hybrid data center configurations, legacy systems that were never meant to be remotely accessed being brought online, and more. Infrastructure varies by company, adding another layer of complexity.

> "Why [is] the simple solution not there? Because it's not simple. It needs to be a bit more holistic, across multiple dimensions."
>
> *Sahil Diwan, Siemens Advanta*

OT environments require different approaches to security.

Today, businesses are most concerned about ransomware in the OT environment, whether via a lateral move from the IT network to the OT network or from direct entry.

- On the **IT side**, risk management and technology availability can be maintained even through upgrades and migrations, as long as configuration and network settings keep data secured.
- However, on the **OT side** an update or change in technology configuration can lead to extensive downtime, which represents significant loss for the business.

While one approach to mitigating risk to the OT environment due to a lateral move is to implement proper segmentation to brick the VPN, routers, or firewalls in the event of ransomware entering the IT environment, restoring system operations post-attack takes a long time. Developing an optimal approach that takes into account both security and availability is top of mind for many enterprises.

> "Attack styles have changed. No longer is it a short-duration attack. Attackers will . . . sit there for months, even a year—they will understand your environment. They will understand how to move laterally. And when everything is set, they will move."
>
> *Sahil Diwan, Siemens Advanta*

.

Because of the differences between the OT and IT environments, one key step to improving OT security is to create a focused incident response (IR) plan specifically for an attack in the OT environment. Just as with an IT IR plan, the OT IR plan should include detailed steps around segmentation, whom to contact, and how to communicate both internally and externally. Although OT risk management is still in its early phases, more solutions or programs will likely become available in the market as the field grows.

OT security requires increased cooperation between IT and OT departments.

Siemens Advanta recommends applying a framework of governance, people, processes, and technology to OT security programs. To operate as efficiently as possible requires bi-directional communications, to both send out performance parameters and receive communications back to control a given unit based on current operational environment. This often translates to an increase in cloud-based solutions across the enterprise; however, securing the full stack now requires cross-department collaboration and cooperation as terminology and processes spread from IT-centric to a shared IT and OT discussion, increasing security effectiveness.

Visibility is critical to risk mitigation. A technology-based solution to track and manage assets provides a foundation for risk management; however, action must accompany the asset information to be effective. Understanding the value being held at risk in the OT environment by bringing together the security team with the owner-operators of facilities will clearly define the impact of threats and vulnerabilities to the OT environment, based on performance and security requirements. Taking technical information and translating it into business impact that can be communicated to the C-suite and board of directors levels supports more balanced, informed decision making.

Other key process areas that contribute to increased OT cybersecurity include investing in security resources for the long term, through hiring or developing specially trained OT security employees, taking time to architect an optimal process and infrastructure design, and involving leadership to build the core areas of security. Executive buy-in and understanding of the fundamental differences between IT and OT environments further support improved enterprise-wide security.

Enterprises can take concrete steps to mitigate OT security risks.

OT security faces challenges of scale at large OT-heavy companies, such as big utilities providers. In the current market, these organizations will benefit greatly from support by consultants, resellers, distributors, and integrators. However, even smaller utilities are advised to invest in OT security.

Although these smaller entities might not see themselves as a target of sophisticated attacks, some threat actors will hone their tactics on smaller municipalities and co-ops to do reconnaissance and map a plan of attack for a larger utility. The risk to not only financial resources, but also to public trust, should not be underestimated.

To protect operations, organizations can undertake three key practices:

- Patch management
- Asset management
- Visibility

Patch management and asset management are close cousins. While there are many solutions, having a solid asset inventory in an operational environment, with relevant data attributes and metadata defined, supports timely patch management. It is important, though, to employ logical segmentation while patching to decrease vulnerability. Robust asset inventory also provides better visibility and improves attack surface management.

As part of risk mitigation strategy across departments, there is also increasing focus on OEMs to participate in the software bill of materials, to ensure that any software being installed into the OT environment does not contain code that is inherently vulnerable. As discussions grow around insider threats, attention on regulations and requirements will also grow.

In fact, increasing attention on cybersecurity at both the federal and state regulatory levels is spurring development of regulations and sector-specific directives. Companies should have access to resources responsible for tracking and helping to deliver on reportability requirements; however, given the longer lead time to develop and publish government regulations, industry guidance tends to be more applicable when implementing strategies to protect against current cybersecurity risks.

> "Staying ahead of the regulations by following industry best practices and standards . . . when the cycle turns . . . and there are new regulations in the market, you're compliant from day one."
>
> *Sahil Diwan, Siemens Advanta*

BIOGRAPHIES

Sahil Diwan

Strategic Cybersecurity Consulting, Siemens Advanta

Sahil Diwan is the lead for Siemens Advanta's strategic cybersecurity consulting practice in North America. Sahil has a wide range of responsibilities at Advanta including steering the development of Advanta's cyber consulting portfolio, managing delivery of large client security transformations, and serving as a sparring partner for our clients' executives.

Sahil has led multiple engagements across different verticals including both manufacturing and critical infrastructure. Sahil specializes in large program transformation through the means of enterprise (including OT) wide program benchmarking and cohesive program design beyond just the technology implementation. Sahil also sits as an advisor to Siemens cyber leadership when it comes to staying ahead of the market conditions and threat landscape.

Dennis P. Gilbert, Jr.

Founder and CEO, Vector9 Consultants, LLC

Dennis P. Gilbert, Jr. has 35 years of leadership experience in cybersecurity, technology, strategic planning, and risk management across both the private and public sectors. He is the founder and CEO of Vector9 Consultants, LLC, a veteran-owned small business (VOSB) that provides strategic cybersecurity guidance for critical infrastructure entities at greatest risk. To stay a step ahead of cyber threats, Vector9 assists entities with innovative solutions to prioritize and protect key IT and operational technology assets, create and execute sophisticated risk management strategies, and develop cyber talent. He is also serving on multiple boards for a variety of small and large cybersecurity-focused businesses.

Between 2014 and 2022, Dennis was the vice president and chief information security officer (CISO) for the two largest energy/utility companies in the US (Duke Energy (Fortune #126) and Exelon Corporation (Fortune #92)). Prior to these two CISO roles, he served as the senior advisor for cybersecurity to the Department of Defense's chief information officer. In 2005, Dennis retired from the USAF, where he held key leadership positions in national-priority programs in cybersecurity, information warfare, satellite communications, and electronic warfare. Dennis received a master's degree in systems management from the Viterbi School of Engineering at the University of Southern California, and a bachelor's degree in management information systems from Louisiana Tech University.