



DRAGOS

Dave Kang

ADVISORY
SOLUTIONS
ARCHITECT



ROCKWELL
AUTOMATION

Kamil Karmali

SENIOR GLOBAL
COMMERCIAL MANAGER,
CYBERSECURITY
SERVICES

Understanding the OT Threat Landscape Helps Manufacturers Improve Cybersecurity

The level of sophistication and frequency of cyberattacks on manufacturers keep increasing, making readiness and incident response capabilities imperative. To explore the latest trends and what they mean for manufacturers, I spoke with two experts on the topic: Kamil Karmali, Senior Global Commercial Manager, Cybersecurity Services at Rockwell Automation and Dave Kang, Advisory Solutions Architect at Rockwell Automation Technology Partner Dragos.

Theresa: Why is the industrial control system (ICS)/OT community especially vulnerable to cybersecurity threats?

Kamil: I think insufficient workforce skills and awareness of security hygiene prioritization are the core challenges. In manufacturing, the top most critical goal has been to keep the production environment up and running. Suddenly, workers who were focused primarily on quality, efficiency and profitability are now the first line of defense against nation-state

actors and skilled attackers — without having the proper skills to identify risk and design, implement, and execute a holistic cybersecurity strategy.

Another weakness is when the manufacturing install base is old and in need of modernization, so there are increasing unknown vulnerabilities, making driving cyber investment a challenge due to competing priorities.

Dave: There is a historical aspect as well. In the late 1990s through the early 2000s, as IT networks evolved and threats grew, cybersecurity began to mature. But we in OT are just seeing that now because traditionally, OT has trailed 15 to 20 years behind IT technologies.

Theresa: How did the OT threat landscape change in 2023?

Dave: The growing number and scope of vulnerabilities is impossible to ignore. For example, according to our recently released report, "OT Cybersecurity: The 2023 Year In Review" (<https://tinyurl.com/5n6uxdnw>), there was a near 50% increase in

ransomware attacks against industrial environments last year, with 70% of all attacks targeting manufacturing entities.

It's why cyber is becoming a board-level objective, especially for companies driven by regulatory compliance, and why vulnerability and risk management are moving very quickly to the top — especially in industries with large, disparate install bases such as oil & gas, mining and chemicals.

Theresa: What do you consider to be the greatest vulnerabilities today?

Kamil: To me, critical infrastructure continues to have the greatest threat vulnerability. Attackers are positioned on that industry segment because of its potential for human loss-of-life casualties or disruption; it's the simplest and quickest way to create harm or malice.

Another aspect is what I call "scaling of size." A large manufacturer may have sites around the world at different stages of cyber maturity or

In 2023, there was a near 50% increase in ransomware attacks against industrial environments, with 70% of all attacks targeting manufacturing entities.



security hygiene, using decades-old automation assets that weren't built for security. This is a vulnerability, especially considering how many companies still struggle with the basics around patch management.

Dave: Inertia is another one, the idea being, "We've gone this far without anything going wrong, so why don't we just continue to press forward and take that risk?"

Also, the disparate nature of manufacturing environments and all the growth — by acquisition, organically or just expansion — increases the attack surface and companies aren't prepared to defend against that.

Theresa: Why is having a unified, risk-based response important? What does that look like?

Kamil: A risk-based approach is knowing your vulnerabilities, how to manage them, and how to right-size your investment. What's most important is to never build a strategy purely based on technology.

Rather, what's beautiful about standards like NIST or other governing cyber frameworks is that they allow you to think both proactively and reactively — identify, detect, protect, respond, recover, and governance.

Naturally, every manufacturer is in a different state of their cyber maturity journey, and many are reactively trying to figure out where to start. Companies like Dragos and Rockwell Automation try to put them on a proactive journey, using a framework to help tackle one step at a time.



Theresa: What types of cybersecurity controls are most critical to securing OT?

Dave: First and foremost, based on my experience, you need an incident response plan, and not just "restore from backups." Things like tabletop exercises can really bring to light how ahead or behind any organization might be in terms of responding to an incident.

The response plan will be your stopgap or buffer while you put other controls in place, such as a risk-based OT vulnerability management program for timely awareness of key vulnerabilities and how best to mitigate them.

You'll also want to validate controls from a segmentation basis, examine firewall rules, ensure that your architecture is defensible and deploy some method to monitor traffic for threats.

Kamil: We also see companies moving towards a true security operations center (SOC) provider, or augmenting to a hybrid SOC model,

when their operators lack the right skill sets or when IT doesn't know what alerts mean in OT.

Theresa: What key takeaways do you want our readers to remember?

Dave: Don't buy into the fear, uncertainty and doubt. The fact of the matter is this: Defense of your industrial network is possible, and the greatest risk is just doing nothing. Start with the foundational components, which are the most important, rather than striving for perfection. And consider this: if you can stop any one of the stages in a cyberattack kill chain, you have effectively nullified the attack.

Kamil: I would add that you are not alone in this. There are experts who can help you, so if you don't have the right workforce skill set, look to outside partners to help build the cyber journey with you. |

Q DRAGOS Rockwell Automation Technology Partner Dragos provides ICS/OT cybersecurity solutions for hundreds of industrial organizations. In addition to technology and service offerings, the firm offers threat intelligence to provide organizations with in-depth visibility of threats targeting industrial environments globally and the defensive recommendations to combat them. Learn more at www.dragos.com.