Insider Secrets From a Front-Line Industrial CISO

Times of significant change often amplify challenges within organizations — especially when it comes to blending business-critical operational technology (OT) with information technology (IT).

During the third installment of Recorded Future's executive dialogue series, Recorded Future's chief operating officer, Stu Solomon, joined Satish Gannu, chief security officer and chief technology officer digital at ABB, to discuss the fast-converging worlds of IT and OT, along with new remote work challenges, and explore why OT and IT leaders must band together to tackle growing cybersecurity risks.

Don't miss their insightful discussion on demand here, and read on for some of our favorite highlights from the conversation.

Setting the Record Straight on OT, IT, and IIoT

Even within the cybersecurity community, many people are fuzzy on how OT and IT intersect. Then there's this whole other beast: The industrial internet of industrial things (IIoT). Where do they all converge?

"OT can be broadly defined as the manufacturing and delivery of things, whether they are objects or critical services like power generation or water transportation," explains Gannu. "Many OT systems have been around for years, even decades, and as the world evolves, they are becoming interconnected and getting IP addresses in the process."

These OT systems are rapidly converging with IT, bringing the promise of improved efficiency and new business models enabled by the industrial internet of things (IIoT). However, the promise of greater connectivity comes with greater risk.

Comparing Apples to Oranges?

OT has evolved at a much slower rate than IT, and for good reason. Gannu says, "When you buy equipment to set up a cement plant, it runs nonstop for seven years. Some transformers are even built to last 40." In the world of OT, availability is king, and keeping systems up and running to avoid devastating power outages or water shortages is critical. "If something is running, that means the plant is operating, and you don't touch it," he says. This also means that change across OT systems, processes, and operators happens gradually, in stark comparison to the dynamic, fast-paced world of IT. You can easily patch a software bug. It's something entirely different to upgrade an OT system.

Separating IT and OT Is No Longer an Option

Due to the critical nature of OT systems, IT and OT have historically been kept apart to minimize risk. Additionally, there's often a level of mistrust for IT on the OT side, which hinders collaboration and convergence. Gannu says this needs to change.

"The 2001 Stuxnet attack showed us that isolation doesn't work. There are different mechanisms threat actors can apply to attack critical systems," explains Gannu. Just because systems are separated doesn't mean a malicious insider can't walk in with a USB stick to launch an attack, for example.

Applying IT Learnings to Tackle OT Challenges

With 30-plus years of leadership experience in both IT and OT, Gannu hasled large-scale convergence initiatives across processes, data, and physical systems.

During the discussion, he describes his approach for effectively communicating with line-of-business owners, helping them understand how to apply learnings from IT to address OT challenges. For example, anomaly detection techniques are widely used in enterprise security programs to establish a baseline of traffic and understand what's normal, and what's not. From micro-segmentation to behavior analytics, there are many examples like this. "Just because OT is a different environment, doesn't mean we should forget the basic blocking and tackling that makes a good security program effective in the first place."

This is particularly true in the wake of COVID-19, as many employees continue to work from home. There's much to be learned from IT about rapidly scaling infrastructure and establishing new policies to enable remote access to critical systems.

The Critical Role of the CISO

More than ever, this pervasive question urgently demands an answer: Who is responsible for mitigating cybersecurity risk across OT systems, as they become increasingly connected as part of IIoT?

Organizations are increasingly focusing on security as a key business enabler. While OT and IT leaders across the business are collaboratively addressing evolving challenges and threats, CISOs are uniquely positioned to lead because they understand the context in what they're seeing, especially from an anomalous perspective. And, Gannu notes, since most of their careers follow the IT path, "Who knows better than the CISO?"

Collaborating and Sharing Information to Evaluate Risk

It's clear that IT and OT network environments will continue to merge, so how can organizations build the right security monitoring and detection controls to effectively manage them?

Gannu urges CISOs to focus on the fundamentals first. Discover what you're actually responsible for — where IoT-connected devices exist across OT and IT environments. As you discover assets, you'll also discover vulnerabilities and want to patch them. Resist this urge, Gannu says. "Before patching, do a vulnerability analysis to see how bad things are. Don't just patch, patch, patch." It's important to understand the risk of the vulnerability in relation to the organization so you can prioritize efforts and keep critical systems up and running, he notes.

Gannu also encourages information sharing and industry-wide collaboration. "The best way to learn is through your peers," he says. In security, while the impact always feels personal, the reality is, someone's probably been there before. "Bodies such as the OT Cybersecurity Alliance are helping to build a community of knowledge, guidance, and resources to help organizations mitigate cyber risk in the digital world.

Watch this executive dialogue now to dig further into these topics.