Unlocking data is the silver lining in revamping OT security

John Swanson, Global Security Portfolio Lead, Uvance

There's an upside to everything. The silver lining of implementing much-needed revamps to OT security is how it opens new horizons, creating actionable insights from fresh data sources.

In the world of operational technology (OT), evolution happens slowly. Many OT control systems like SCADA (Supervisory Control and Data Acquisition), PLC (Programmable Logic Controller) and DCS (Distributed Control Systems) have been running flawlessly for years, if not decades.

OT systems are also in focus for the next round of digitalization, now that 5G and network-edge technologies are mature enough to provide the connectivity for manufacturers and utilities. However, a significant factor has been holding them back. Many have inherent, well-documented security vulnerabilities which cannot simply be patched. Therefore, exposing these systems to the internet is an inherently bad idea, as it creates a new attack vector. This has, of course, been a major deterrent.

The proper controls are a must-have to unlock the benefits of rich OT data

Solving this challenge is important. OT data describes what is actually happening inside manufacturing operations. It therefore contains the rocket fuel that powers digital and sustainability transformation.

No OT/IT convergence means no data, and that means no transformation.

There are now, fortunately, ways to reconcile this dilemma and safely open up the valuable data inside OT systems to the data analytics that IT offers.

Putting in place boundary controls is just one of these. They help to block and prevent known exploits and other attack methods. But, in an age where ecosystems of partners in a value chain are strategic differentiators, there is potential dissonance between powerful network boundaries and "the borderless enterprise".

A different approach to security is required. While a perimeter- and network-based approach is part of the solution, security needs to be 'architected-in' with other key facets. These include inventorying assets and understanding overall topology to increase visibility.

The overall approach should be a strategic and prioritized maturity viewpoint – whether that is through network segmentation, hardening, utilizing threat intelligence or other means — rather than simply adopting ever more secure point solutions. An equally key aspect is to address organizational silos to underpin overall resilience.

The effort is well worth it. One outcome, for example, is a remote, consolidated dashboard showing the performance of site machinery across multiple locations. And for manufacturing and utilities, many of these locations are well off the beaten track. Remote access to OT data means operators can move from planned to predictive maintenance – and save money in the process. They can also speed up the diagnosis and resolution of ongoing issues, as it's possible to consult logs of what happened before a machine malfunctioned to at least narrow down the cause of failure – and get spares on the way in short order.

However, despite the appropriate security safeguards now being available, some 60% of companies are still at what analyst firm Gartner describes as the "baseline" awareness stage regarding their Operational Technology security.

It's time to protect, connect and transform

Fujitsu has introduced security maturity assessments enabling manufacturers and utilities to accelerate the modernization of their OT estates. With the goal of protecting, connecting and transforming, we take a non-judgmental look at critical vulnerabilities, the overall security posture and longer-term operational goals. This creates a blueprint for sustainable transformation and starts to increase operational resilience.

We break it down into three phases. The first is baselining by analyzing existing networks, identifying gaps in compliance, and establishing the overall risk profile. The second is applying priority remediations based on the baseline findings. And the third is a 24/7 service identifying anomalous behaviors across OT environments.

Fujitsu is well-placed to offer these services, as a leading cyber-security provider to Critical National Infrastructure, an acknowledged expert in implementing Artificial Intelligence-powered solutions, and on top of that, a global manufacturer.

Putting the appropriate controls in place and preparing for an ongoing monitoring and response regime mean it's also easier to make a compelling business case for investment. It's possible to quantify the balance between risk and gain in the world of OT. Organizations usually know how much their manufacturing plant costs per hour to run and are fully aware of the health and safety risks – and the costs – of a system failure.

For suppliers, protecting the end-to-end supply chain is more than critical

Protecting the end-to-end supply chain is important for manufacturers and even more critical for utilities like gas, water and electricity providers. Any manufacturer or supplier which suffers an outage causing their customer to suspend production is likely to lose their contract, or to be hit with a heavy financial penalty for failing to adhere to a service level agreement. And nobody wants to be without gas, water or electricity.

As I mentioned, the silver lining is that OT transformation unlocks data points that were previously out of reach. Systems can be connected, end to end. Data can be captured, analyzed and leveraged to improve processes or smooth peaks and troughs. Fujitsu's tried-and-tested operational framework for OT Cyber Security gives manufacturers and utilities access to their live OT data, delivering enhanced visibility of their estate, and protecting their network. This data not only benefits security teams; it can benefit operations, engineering and maintenance functions by enabling, for example, operational effectiveness, resilience and predictive maintenance.

Over time, OT system transformation is about accelerating the implementation of sustainability strategies. It's also about convergence with IT systems – which starts by connecting data and then analyzing this to create actionable insight. On the back of that, strengthening operations and accelerating toward sustainability goals is essential.

According to management consultancy firm McKinsey, "Doing so promises to accelerate in-flight use cases, democratize access to data and technology across the value chain, launch new use cases that utilize cloud-native capabilities, and improve frontline decision-making by using data from both IT and OT systems."

Ultimately, this approach both increases production efficiency and reduces waste by preventing issues from arising in the first place. Which is truly the silver lining for investing in revamping your OT security.

To find out more, visit: https://www.fujitsu.com/global/themes/security/

John Swanson
Global Security Portfolio Lead, Uvance

John has fulfilled many Information Security leadership roles across Public and Private sectors including security programme and capability leadership, consultancy (advisory and delivery), Security Operations Centres and Security Pre-sales functions.

He is responsible for developing Fujitsu's compelling Cyber security go to market propositions, which also underpin Fujitsu's wider Applications, Hybrid IT, Digital Workplace and Industry Sector aligned propositions. John focuses on the business aspects of Information Security and how Fujitsu can help clients enhance the strategic and operational maturity of the information security capabilities within their organizations.