AN IDC INTERVIEW WITH

Jamie Wilkie

Director for Industrial Security Offerings, Europe, Fujitsu

by Stefanie Naujoks, Research Director, IDC Manufacturing Insights EMEA

We had the great pleasure to exchange views with our partners at IDC European Manufacturing Executive Digital Summit 2021. The following interview was conducted by Stefanie Naujoks, Research Director, IDC Manufacturing Insights EMEA and Jamie Wilkie, Director for Industrial Security Offerings, Europe, Fujitsu

Stefanie Naujoks: *Why are we hearing more about OT security now?*

Jamie Wilkie: Operational technology controls some fundamental aspects of our lives – which are literally matters of life and death. Water treatment plants must add just the right amount of chlorine to our drinking water. Too little and we get sick. Too much and we die. These are vital matters, and we tend to assume everything will continue to be okay.

But times change. Operational Technology (OT) used to be completely separate from other aspects of enterprise IT – software like ERP, databases that contain the information generated in operations and enable operations to become more effective, and the networks carrying data to and from where it's needed. However, OT is no longer air-gapped from IT in the way it once was – and there are consequences to that. Cyber criminals have woken up to the potential to exploit OT in recent years and manufacturers and providers of critical national infrastructure now find themselves in the front line of the cyber war.

Naujoks*: Is this affecting businesses in the real world?*

Wilkie: Absolutely. Digitalization is charging ahead across all sectors of business. In the future, those not pursuing it will only be relevant in business school case studies of missed opportunities.

Organizations on their DX journeys have to get rid of the idea that their OT environments are air-gapped. That is a dangerous illusion because you have to get data out of your production environment. It's simply too valuable to leave isolated. You need it to identify and harvest new efficiency opportunities, for example. Or as an essential tool to meet the sustainability and net-zero goals that will be imposed across all industries in the next decade. How can you meet your carbon goals if you don't know how much carbon you are currently emitting?

This urgency means manufacturers have limited time to align their OT and digitalization security strategies. Opening up OT to digitalization exposes it to unchartered risks. Even at the most basic level, vulnerable OT security is bad business news. Security breaches decrease the value of companies in due diligence. FM Global - a major US business insurer – now issues guidelines that stipulate its customers have to have industrial control systems (ICS) evaluations to obtain the best insurance coverage and rates.

Bad things are already happening. Let's take the single example of ransomware. It was widely reported that the world's biggest meat processor paid an $11m ransom after a cyberattack shut down its operations a few months ago. And examples like this are just the tip of a massive and rapidly expanding iceberg.

This all comes together in terms of business value – senior management seeks to create manufacturing strategies that are fit to play in digital value chains. Fujitsu is working with a manufacturer of paper pulp and cardboard boxes – not, you perhaps think, the most glamorous end of the business world. However, its most important customer is Amazon, which dominates one of the world's most important value chains. The CEO of this company does not ever want to be on call to Jeff Bezos to explain why a Wannacry stoppage meant Amazon could not fulfill its Black Friday orders.

Simply ignoring what's on offer from digitalization is not an option for manufacturers. Improving production and supply chain efficiencies with smart sensors and sophisticated analytics bring OT into the 21st century. But organizations should do this in a controlled way – building in cyber security right from the start to minimize the danger of cyber threats.

***Naujoks**: Where does OT security currently stand in comparison to IT?*

Wilkie: It's not a question of a race or someone being behind. IT and OT are starting from different places.

IT cares about "CIA" – the confidentiality, integrity and availability of data. OT cares about physical processes and safety – like in the chlorine example I mentioned earlier. IT has highly detailed procedures to cover all circumstances and some extremely rigorous protocols for incident response. OT understands that system failure can be fatal.

The reality is that the two are still not fully aligned and work is needed to bring them together – adopting best practices from each. When it comes to OT security, there are some essential models and standards in place. However, most manufacturing organizations are still beginning security journeys to address OT/IT integration. They need to take stock of where they are, what they have and what they will need to secure operations into the future.

***Naujoks**: Where and how does that journey start?*

Wilkie: Assessment. Most manufacturers still need to start there. Usually, in our experience, this is prompted by a breach – ransomware perhaps, but hopefully something less serious - that triggers awareness that there is a problem.

There are agreed international standards that help here, for instance, NIS-D for regulated Critical National Infrastructure or industry standards such as IS027001 and IEC 62443. Achieving compliance with regulations may well bring additional business benefits such as better coverage from industrial insurers.

The first requirement is to stop the bleeding, deal with the crisis. But then, step back and see the bigger picture. Think about your overall digital transformation goals and how you will lay the foundations for your data-driven strategy. Fujitsu sees connecting, protecting, and managing digital assets as a good way of building the foundations.

The first phase is all about visibility. Use assessment to understand your current OT security posture and how it relates to business risk. Does the vulnerability you have identified impact your coffee machines or your furnace if you are a ceramics company? One has a higher business priority than the other.

- An assessment should look at people – their roles, responsibilities, and training. It's not good when an operator decides one late night shift to insert a USB stick of family photos into a SCADA controller.
- The assessment should look at processes. Does an incident response process exist for OT? What if something goes wrong on the shop floor at 2 am on Sunday? Who gets the phone call?
- And it should look at technology to reveal the networked assets in use in OT. All this information drives the security analysis but can also be used for other management purposes.

After a thorough assessment, you are in a position to conduct any necessary point-in-time improvements – for instance, ensuring there is proper segmentation between your IT and OT networks and that there are controls on remote access to your plants. For example, nearly all manufacturers enable remote access to their networks so that key equipment suppliers can monitor when maintenance is needed. But few, in our experience, know exactly how many suppliers have network access.

Now move on from there to introduce continuous visibility with a managed monitoring security service that alerts you to changes and abnormal behaviors in the network, such as an unscheduled installation that might be the precursor to a cyberattack.

You also need to create the necessary processes to support OT security, such as incident response for OT and align your IT and OT security within a single Information Security Management System. Consider security automation with SOAR (Security Orchestration, Automation and Response). This is an incredibly powerful tool to assess and prioritize cyber threats and simplify the incident response process. SOAR capabilities enable constantly evolving approaches as a means of achieving enhanced security. Other options include further security controls, such as secure remote access, vulnerability management and identity and access management (IDAM) for OT.

***Naujoks**: Is there a connection between OT security services and OT asset management?*

Wilkie: Yes, OT assets are at the heart of OT processes. Knowing what those assets are and what state they are in is the first step to extracting valuable data from them and actively managing their availability.

The asset discovery, which is typically part of a security assessment, as mentioned before, produces asset data that can feed an asset database in a configuration management database (CMDB). Assets can be discovered by manual inspection and by passively listening to the OT network using appropriate technological tools.

Asset discovery sounds simple but needs preparation: First, access must be provided to the network and then time is needed to analyze the data which emerges. This is especially true when an OT network is not separated from the IT network, when there may be many assets discovered that are not part of OT.

Once the initial work has been done, it is possible to use a continuous security monitoring service to provide regular updates on the equipment attached to the network.

***Naujoks**: Thank you – that's comprehensive. Is there an even more advanced platform for OT security beyond what you have described?*

Wilkie: For anyone who reaches the level I've described here, the next steps would be to consider additional layers of AI for threat identification and response acceleration, and the use of digital twins to model and isolate impacts.

In the case of manufactured goods, management should also consider the security of those goods to avoid claims and reputation damage. But these are all steps for when you have the foundations right. The top priority is to ensure your operations are as safe as you can make them.

***Naujoks**: Thank you very much for the interview, Jamie.*

Stefanie Naujoks

Research Director, IDC Manufacturing Insights EMEA