Picture credit: Ukraine MOD

# STAKES ARE HIGH

**Rob Demain** *considers resilience and recovery in modern IT/OT environments*

**Imagine a world without the modern conveniences of clean running water, reliable electricity and working traffic lights. From struggling with basic hygiene and hydration to living in dark, uncomfortable homes, life would instantly become more difficult. We rarely think about these invisible systems, and yet we'd notice their absence within seconds given their importance within our daily routines.**

Today, operational technology (OT) underpins many of these essentials – digital solutions that interface with the physical world, with examples including Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). Protecting these technologies is absolutely vital. While cybersecurity has long focused on IT systems (and centred around the confidentiality, integrity and availability of data), OT security is now an equally urgent priority. The focus is different and significantly more far-reaching in its consequences. OT security is often associated with reliability and safety, namely because of the clear physical dangers and damages that could arise with OT failure or malfunction.

By infiltrating the OT systems behind water treatment systems, a threat actor could tamper with nationally critical processes and leave entire communities without access to clean drinking water. Similarly, if they were able to hack into power grid systems, they could potentially enforce widespread power outages. In other words, the stakes are incredibly highly when it comes to OT and cybercriminals know this. These are systems and technologies that have become foundational to the operational of critical national infrastructure (CNI), forming the backbone of services that people have come to rely on heavily on a daily basis. That reality has only galvanised threat actors in going after them – be it foreign adversaries, activists or otherwise.

According to PwC, OT has become a major target in geopolitical cyber conflicts and several recent attacks reflect this. Back in September 2024, the US Cybersecurity and Infrastructure Security Agency (CISA) made a statement announcing that it was continuing to: "respond to active exploitation of internet-accessible operational technology (OT) and industrial control systems (ICS) devices, including those in the Water and Wastewater Systems (WWS) Sector". The war in Ukraine has repeatedly involved the use of OT-centric attacks. In one example, the Russia-backed threat group known as Sandworm used a novel OT threat technique to enforce power cuts that coincided with missile strikes on CNI across the country.

**Russia-backed threat group Sandworm enforced power cuts in Ukraine that coincided with missile strikes on CNI across the country**

More recently, in March 2025, Jaguar Land Rover made headlines after it was hit by a cyberattack that forced it to halt production for weeks on end, impacting more than 200,000 supply chain jobs. In the aftermath, the Cyber Monitoring Centre (CMC) model estimated that the event caused a UK financial impact of £1.9-billion and affected over 5,000 different UK organisations.

## NUMBERS GAME

The statistics also speak for themselves. Palo Alto Networks findings show that three in four organisations have experienced a cyberattack on their OT environment, with ransomware-driven shutdowns and IT-borne intrusions continuing to dominate.

This uptick isn't a coincidence. For threat actors, the appeal is clear. Whether financially motivated, politically motivated, military motivated or otherwise, the impacts of OT attacks – particularly in relation to CNI – can be significant. For security teams, it is therefore critical to boost the resilience of OT environments. Yet this has its challenges.

Many operational technologies were created with the purpose of providing operational efficiencies. Security was not necessarily a priority in their creation and many legacy systems now lack the cybersecurity maturity required to stand up to modern threats.

In some cases, OT environments are managed in separate domains that are subordinate to IT environments, which can lead to uneven security safeguards. The situation also isn't helped by the continual convergence of IT and OT systems, which has the potential to introduce new pathways for IT-based threats to reach critical OT assets (and vice-versa), without adequate segmentation, visibility or protection.

It's not just the convergence between IT and OT that can expand the OT attack surface, but also the growing role of third-party integrators, vendors and maintenance providers in supporting these technologies and networks. Indeed, high-profile incidents such as SolarWinds and MOVEit have clearly shown how attacks on a single vendor – be it a software provider or otherwise – can have severe repercussions for several downstream organisations.

OT environments are not immune to this. In the case of SolarWinds, the supply chain attack compromised the Orion network management platform, enabling the threat actors involved to push malicious updates to thousands of organisations, including US government departments. That backdoor had the potential for threat actors to potentially access, manipulate, or disrupt OT systems by bridging IT networks with industrial environments.

In this sense, the very technologies that are being used to modernise industrial operations are becoming their Achilles heel. So much so, that the European Network for Cyber Security (ENCS) recently warned that increasing interconnectivity within renewable energy assets has made substations and distributed control systems more exposed to cyber threats than ever before.

Given the growing focus of threat actors on OT and the growing attack surfaces that are surrounding these critical systems, it is vital that organisations spend the necessary time evaluating and implementing the necessary controls, safeguards and security protections.

Unfortunately, this process again has its complications. While regular updates and vulnerability remediations can take place with relative ease in IT environments, traditional approaches to OT patching require systems to be taken offline. In tightly regulated, always-on industries, even a short shutdown can present major issues and/or be significantly expensive.

## OT HAS BECOME A GROWING TARGET IN MANY GEOPOLITICAL CYBER CONFLICTS

Consider utilities: applying patches might require turning off water treatment systems which could disrupt supply to thousands of homes. Similarly, updating traffic-light controllers could mean taking junction systems offline, creating congestion.

In this sense, in OT environments, even brief downtime can impact public safety and cause serious knock-on effects. It's a catch-22 – downtime if you do patch and potentially even longer downtime resulting from OT attacks if you don't. Both can be problematic, but the latter will likely be much more damaging and dangerous, with downtime driven by malicious intent that could endanger lives, rather than in prepared environments with controlled timeframes.

Therefore, it's important to find ways to detect, withstand and recover from cyber compromises, ideally without resorting to disruptive shutdowns, as we continue to become ever-more dependent on OT.

To achieve this, a strategy built on visibility, unified monitoring and sensor-driven intelligence is required. Currently, many OT applications face practical constraints. From old manufacturing lines that don't support agent-based tooling to facilities that can't accommodate new hardware without engineering changes, OT sensors can make a massive difference by providing passive, low-impact monitoring capable of operating even in bandwidth-restricted or safety-critical locations.

Rather than relying on intrusive security scans, OT sensors can observe traffic patterns and control commands that provide a more practical route to visibility that doesn't have any impact on operations and production.

Metadata is collected from sensors, which in turn can be streamed directly to the Security Operations Centres (SOCs), where analysts can correlate vital OT insights with IT intelligence and threat models. Establishing that comprehensive and unified view removes any guesswork. It's an approach which ensures potential attacks or threats are identified and remediated accurately and at speed, ideally before

they result in major OT impacts and operational shutdowns. It's also important to note that resilience is not only about preventing attacks, but also about shortening recovery windows when incidents do occur.

Here, OT sensors can also play a key role. By identifying suspicious behaviour at the earliest stage, sensors can help SOC teams to flag issues and alerts to OT operators who may then collaborate with security teams to assess the situation, and ascertain the best way in which to resolve the issue or reduce the impact of a potential attack.

## EVEN BRIEF DOWNTIME CAN IMPACT PUBLIC SAFETY AND CAUSE KNOCK-ON EFFECTS

Implementing OT safeguards such as these is not only a question of security, but also one of compliance. Indeed, CNI organisations typically must adhere to a multitude of cybersecurity regulations, demonstrating best practices so as to avoid potential legal repercussions or penalties.

Regulations are starting to rapidly catch up with the realities that are facing operational technology. In the EU, NIS2 stands as a prime example, mandating controls for CNI organisations, as well as incident reporting timelines and executive accountability. In the US, meanwhile, CISA, TSA and EPA are introducing OT-specific expectations for resilience and incident response.

In the UK, the Cyber Security and Resilience Bill was also introduced into parliament last year. This could expand on the scope of cyber regulations to include managed service providers, data centres and critical suppliers. If approved, it may also require faster incident reporting and stronger security practices across supply chains.

### NEW PATHWAYS

Ultimately, the direction of travel is clear. OT systems that were once isolated now operate in complex environments, with cybercriminals and nation-state actors actively targeting them with growing frequency. The convergence of IT and OT is creating new pathways for potential compromise, and third-party dependencies are introducing risks that extend beyond the digital walls of any organisation.

It is within this context that resilience becomes a strategic imperative. Continuous OT visibility, unified monitoring and proactive detection are now needed to not only prevent attacks, but recover from them at speed, with minimal OT disruption.

This is what the current regulatory trajectory recognises. These OT capabilities could be the key to keeping water flowing, power grids stable, manufacturing lines running and communities safe. Legislative requirements across the EU, US and UK shouldn't be viewed as burdens. They reflect what is now necessary. Indeed, as dependence on OT grows, so too must the commitment to protect it ●

**Rob Demain** is CEO at e2e-assure.

**Updating traffic-light controllers could mean taking junction systems offline, creating chaos**

Picture credit: AdobeStock