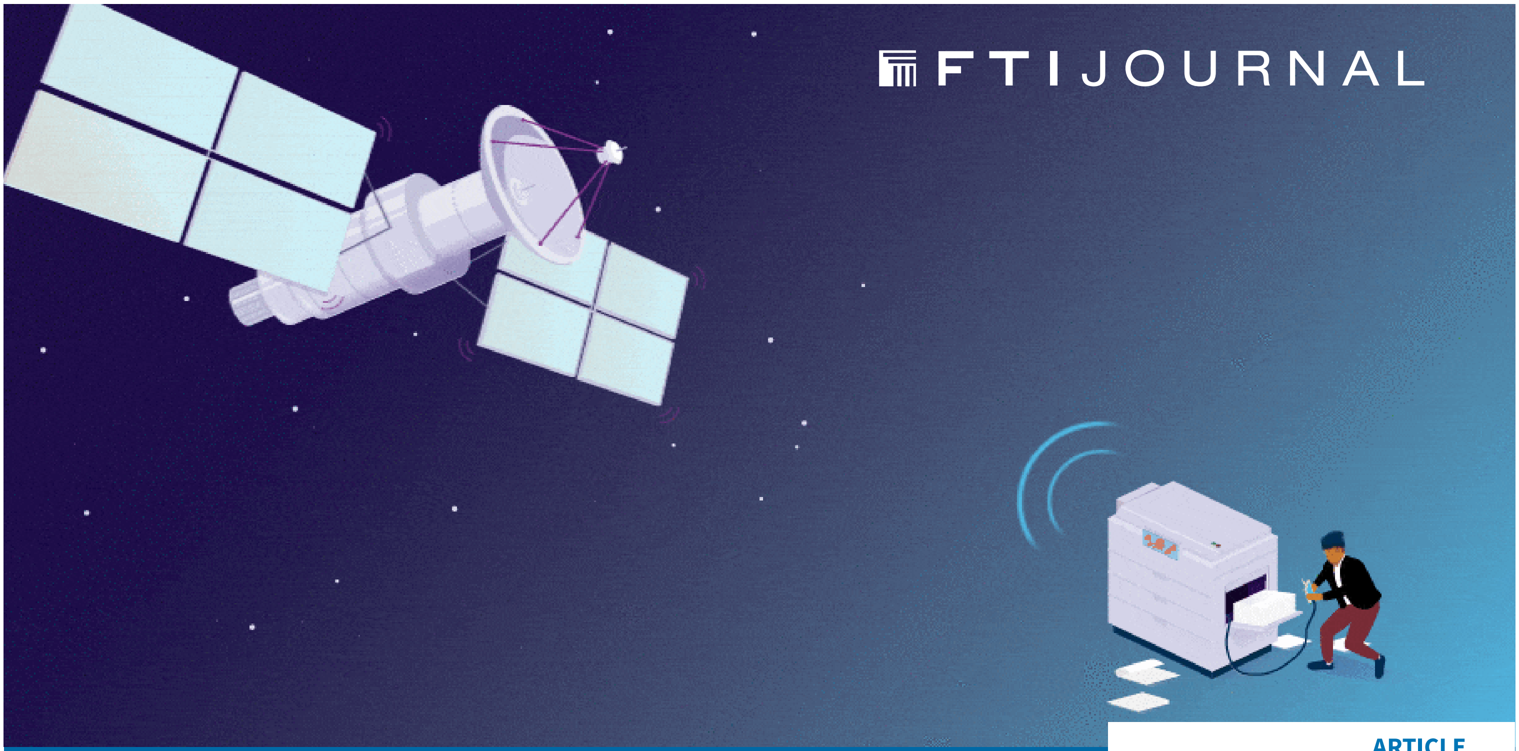
FTI JOURNAL



ARTICLE

Five Steps to Secure Operational Technology in an Evolving Threat Landscape

October 2020

In a world where hackers can change a satellite's orbit, or youngsters honing their cyber skills can cause huge disruptions, organisations need to be more vigilant than ever when protecting operational technology. Here are five ways an organisation can remain resilient and keep its OT secure.

Imagine you are the CEO of an organisation storing highly confidential intellectual property on a private, on-premise server. One day, the temperature in the office starts to rise — slowly at first, but gradually it becomes dangerous. Emergency services arrive and your entire staff is asked to evacuate the building. Thirty minutes later, you are allowed to re-enter only to find that your company's data has been breached. This is what a coordinated cyber attack may look like.

Operational technology (OT) — the hardware and software used to change, monitor or control physical devices — is increasingly being targeted by hackers. In the last decade, we have seen a growing number of attacks rise especially across the industrial sector, with targets ranging from dams to satellites to commercial property, and this is now bleeding into connected devices in offices and, indeed, in homes.

This surge paints an alarming picture of tomorrow — one where hackers could hold an entire city's water supply hostage from across the globe. Now more than ever, it's crucial that organisations consider the vulnerabilities within their systems to avoid becoming the weakest link in a larger chain.

Secure by Design

Organisations no longer need to be the target of a cyber attack to feel its impact. If effective security hygiene is not hard-baked into operations from the start, the organisation runs the risk of being disrupted when a third party, for instance, experiences a cyber attack. Thus, all organisations need to constantly ensure that they have designed, and are redesigning, their OT infrastructure with security front of mind.

The United States Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) offer a comprehensive set of guidelines to help companies secure their credentials. These practices range from having a resilience plan for OT to implementing a continuous and vigilant monitoring program.

By hardening their network, organisations can proactively protect their OT. However, there is an order in terms of priorities: Organisations should first secure their legacy systems, and then immediately focus on future-proofing their operations.

Exorcise Your Ghosts

One issue many organisations face is that their vision is fixed forward — on the future, the customer journey, or disrupting the marketplace. As such, these organisations fail to secure their legacy tails.

That is to say that many overly complex systems are built atop older technologies that no longer have the ability to support an organisation. This leads to a foundation consisting of fading building blocks — the proverbial castle made out of sand. Further, as these building blocks grow older, they become more foreign to members of the organisation.

Eventually, the mindset becomes one of deferment. The legacy tail becomes more vulnerable as the case for investing in an outdated system becomes much harder to sell. That is why organisations should make a point of explicitly understanding the infrastructure that underpins their OT.

Look Beyond Tomorrow

Once an organisation has successfully and comprehensively secured its legacy tail, it can begin to invest in future-proofing. Unfortunately, most organisations only think about the immediate future of their business.

One way to do this is by being innovative and disruptive — not only in the marketplace, but in the organisation's thought process. Where is the industry going? How is the landscape evolving? Who will be the dominant player 10 years from now? This is a fine balancing act versus overstrategizing and actually enacting change and activity, but it is important to refocus priorities on the journey.

While there is no way to predict the future, organisations can successfully protect themselves by embedding agility and flexibility throughout the enterprise. In so doing, they will position themselves to quickly respond as the cyber threat landscape continues to evolve.

Consider Your Connections

Without a doubt, connectivity is at the heart of the world we work and live in today. From sprawling networks that reside in the cloud to an interest in smart refrigerators, the Internet of Things has never been more extensive — or vulnerable.

It is important to remember that nearly every device is connected. Consider a commercial printer. Most likely it contains memory that has stored images of documents recently scanned. In the wrong hands, that information could prove dangerous. Organisations should take stock of what information is most important to them and work meticulously to ensure that information's security constantly evolves to the threat landscape.

This extends beyond the organisation to third parties as well. Due diligence can no longer be a "one and done" instance. Companies must constantly revisit their agreements with suppliers, scrutinize their relationships and reevaluate their risk appetite. In doing so, they can not only secure their OT but build a stronger, more secure partnership with third-party providers.

Engage in Intelligent Sharing

Organisations should remember that despite competing with other businesses, the best way to secure their OT is by working alongside others in their network. Should an organisation receive notice that there's a potential attack on the horizon, or become aware of malicious activity, it would benefit everyone to share that information — competitor or not.

By working with other organisations, businesses can create a series of layered defense mechanisms, otherwise known as defense by depth. They can also foster a collective defense, where an attack on one is considered an attack on all.

Despite our digital progress, there has never been opportunity without obstacle. The promise of OT and intelligent operations comes with the challenge of defending it first. As businesses continue to move the needle forward and as cities adopt more connected technologies, robust due diligence and collaboration will be instrumental in securing the collective future.

© Copyright 2020. The views expressed herein are those of the authors and do not necessarily represent the views of FTI Consulting, Inc. or its other professionals.

PAUL REILLY
Managing Direction, Cybersecurity
+44 20 76325013
paul.reillyname@fticonsulting.com

FTI™ CONSULTING