WRITEN BY

TAMAS BUZGO
Senior Manager
PwC

FOLLOW THE THREADS IN CYBER THREATS

Advancements in the digital world are moving forward at an unprecedented rate—but are the industries aware of the threats that come with them? While industry leaders often claim their facilities and systems are well-protected, the sole realization that they could unknowingly become a digital aggressor's next target often comes all too late.

As digitalization across industries strides forward, it creates risks of tripping itself up due to cyber attacks. This fact alone should make industry giants want to stay protected—now more so than ever. Predictions show that the demand for operational technology (OT) integration will have increased by a whopping 8.17% by 2026.

But what is the impetus and what does employing operational resilience really accomplish? The fact is, industries are beginning to understand the dangers that come with these "unwelcome outsider attempts."
As part of OT, control systems such as Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) are, therefore, nowadays being introduced to a wider spectrum of the industrial environment.

If we take a peek back to history, we can pick out 2010's *Stuxnet* from the malicious crowd—a computer worm initially aimed at the Atomic Energy Organization of Iran, later "morphing" itself into a rummaging assailant targeting power plants and energy facilities. And it didn't stop just there, as a few years later, the computer worm's "sons" targeted the safety systems at a petrochemical plant—which could have ended in disastrous consequences had the final payload been delivered.

Undeniably, the most prevalent source of attack possibilities comes from a sense of delusion, disbelief, lack of knowledge and inadequate preparation. Statements like "we're not even connected," or "our systems pack a next-gen firewall," or even the classic "hackers don't know a thing about ICS/SCADA" have no place in 2022. And just like industries like to increase their financial gains and efficacy by introducing new technology into their environments, attackers continue to hone their sophisticated methods—called "attack vectors"—in parallel.

From the perspective of OT, industries are best off when employing verified security strategies consisting of policies (management statements), standards (mandatory controls) and step-by-step procedures. Being devoid of these creates excellent opportunities for attackers to gain a foothold inside the victim's systems. The primary "point of entry" can be traced to deficiencies in OT processes, security policies, patch management (with system updates being out-of-date for up to ten years) and even a lack of security features whatsoever (outdated antivirus databases, no USB restrictions). Sadly, many utilities and water companies still employ obsolete and unsecured OT protocols, such as *Modbus* and *DNP3*, which represent a significant threat due to their lack of security features.

> **...one must incorporate the most rudimentary security measures — analyze, discover and maintain.**

Talking cross-industry, RATs (Remote Administration Tools) are utilized to remotely operate Human-Machine Interfaces (HMIs) from operator and engineering workstations, to control SCADA from an operator side, to cross-connect multiple operators and even remote-control workstations to check emails or work with software applications, for instance. However, this has created fertile soil for attackers—especially today, during the long-lasting (but hopefully soon-ending) pandemic which has made a lot of employees across industries work exclusively from home. As expected, this opened the gates for many ransomware attacks. If we look at recent deficiency discoveries by Mandiant, such ransomware attacks have already resulted in numerous confidential documentation and design leaks.

Imagine governments having their intelligence records erased; hospitals full of patients, dependent on interconnected devices, having their systems fried by an outside attack.

IN TIMELY DETECTION LIES POWER

So, how does a power plant or a hospital prevent hackers from delivering devastating payloads and endangering the continuity, safety and integrity of their systems? There are several methods to establish full operational control and "plug" the sinkholes—but to do that, one must incorporate the most rudimentary security measures—analyze, discover and maintain.

First off, we have *Asset Discovery*. Before any assessment is made, the environment we work with needs to be fully explored. This is a critical activity, as it's a starting point for the vulnerability management process. Whereas one might think that a one-off asset list is enough, assets need to be monitored and cataloged regularly.

Another crucial aspect comes from *Vulnerability and Risk Assessment*. Besides detecting infrastructure weaknesses inside systems, networks and applications, this detection form also puts an emphasis on other assets at risk—people and physical security. The results deliver a better understanding of assets, vulnerabilities, and the risk that may be presented to the facility—all while solidly diminishing chances an attacker could breach the facility's security barriers.

Finally, we arrive at *ICS Penetration Testing*, a.k.a. "pen test" or "ethical hacking." While this assessment method cannot be utilized in all environments (shouldn't be done on critical and online systems) and requires a high level of expertise, it represents a realistic analogy to how hackers would try to access the systems, utilizing real hacking tools and valid exploits.

Acknowledging the growing influence of IIoT (Industrial Internet of Things), the interconnectedness of industry systems is at an all-time high, with many believing IIoT applications are essential to sustainability. But without proper analytics, protection infrastructure and management systems, industries can be easily endangered by those who might want to steal data, disrupt systems or even commit acts of terrorism.

All there is to do now is continue strengthening cyber resilience across the industries.