Radiflow

A 2020 View of Industrial Cyber Security: Predictions for Upcoming Trends and Changes in the OT Security Landscape

CIARA, THE FIRST OT-BAS PLATFORM

THE RADIFLOW CYBER-RESEARCH TEAM

A 2020 VIEW OF INDUSTRIAL CYBER SECURITY

The next 12-to-24 months will see major changes in industrial cyber security strategies.

The last few years have witnessed a rise in targeted cyber attacks, along with increasing recognition from governments and the industrial sector that more must be done to protect operational systems from sustained cyber-attacks ranging from hacktivism, ransomware and state-sponsored actors.

From the regulatory side, new EU laws such as NIS and more active national regulators have aligned with high profile incidents that have spooked the industry to do more. At a time when more organisations are exploring and pursuing greater automation as well as newer technologies such as IOT and AI to gain operational benefits, the corresponding increase in connectivity and process-control software has led to a greater attack surface and elevated risk.

Here are out prediction for the 2020s, based on recent trends:

FUELED BY ITS EXPANDED ATTACK SURFACE, PROCESS MANUFACTURING IS SET TO BECOME THE FASTEST GROWING SEGMENT FOR OT SECURITY ADOPTION

Over the last decade, Industry, including manufacturing and operators of essential services, have moved away from the notion that air-gapped infrastructure will protect them from cyber-attacks. The reality is that the benefits of modern IT systems and connectivity are too seductive to ignore and consequently, attacks are occurring more frequently and across a wider front.

As a result, demand for dedicated Industrial Cyber-Security Solutions is increasing rapidly. But the prediction is that this will expand past the realm of regulated industries and larger manufactures into the numerous tier-2 process manufacturing enterprises that have overlooked active cyber security in the past.

Based on the many projects we have conducted over the past 12 months, process manufacturing will become the fastest growing segment for OT Security adoption. This prediction is supported by industry research: IDC has concluded that alongside the central government sector, utilities and manufacturing will see the highest growth in security spending, at 7.8% CAGR between 2017 and 2022.

GLOBALISATION AND GEO-POLITICAL INSTABILITY WILL LEAD TO A 'DOMINO' EFFECT CAUSING MAJOR INCIDENTS IN "SURPRISINGLY" NEUTRAL LOCATIONS

This expansion into the mid-market is reinforced by wider societal trends, including globalisation. This is especially relevant to multinationals, subsidiaries and partner networks that operate in geo-politically sensitive countries and regions that are at higher risk of cyber-attack: these organisations' activities in sensitive countries may present risk to their entire network, including sites located in areas which are not the immediate target of the attackers.

The risk is especially high for industrial enterprises, whose facilities are typically tightly connected. Left desegregated, malware in one site can easily propagate to other sites. Unfortunately, Radiflow has witnessed this lack of inter-site segregation in our vulnerability assessments in multiple enterprises over the past months.

The knock-on effect of a distant attack rippling back to impact a critical system in another country is yet a bolder, albeit realistic prediction that organisations should take into account when evaluating their cyber security strategy. An example of this domino effect was witnessed in 2018 when Italian energy contractor Saipem S.p.A suffered a targeted Shamoon malware attack that was originally believed to have targeted the company's interests in Saudi Arabia, but eventually impacted servers in India, Aberdeen [Scotland] and Italy.

GROWING DEMAND FOR OT-CYBERSECURITY CONSTRAINED BY HUMAN RESOURCE LIMITATIONS WILL BOOST MSSP ADOPTION

As in all economic models, demand drives supply and unfortunately, cyber security is still heavily driven by expertise. The recognised deficit in trained cyber-security personnel is compounded by the extent of specialisation needed to manage industrial control systems. The skill sets required by an "industrial" Infosec team spans the worlds of IT and SCADA, and appropriately-skilled individuals are just not entering the sector in the numbers required.

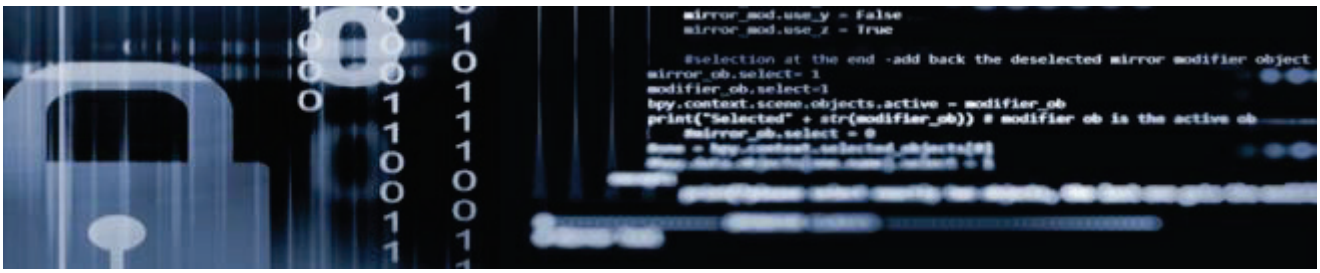
As a result, our next prediction is the increased adoption of managed security services and outsourcing. This trend has already been observed in broad IT and is picking up pace in industrial security, but we predict it will greatly accelerate in the next year, as tier-2 industrial enterprises start to double down on cyber security compliance.

It is unlikely that very large organisations will move immediately to fully managed cyber security services, but smaller organisations faced with the same human resource burdens, but with tighter budgets, will take the leap, followed by larger organisations. This is evident by the rapidly increasing number of Radiflow MSSP partners across the US and Europe, who now offer cloud OT-monitoring services to their existing install-base of utilities, building owners and industrial enterprises.

VALUE-ADDED FUNCTIONALITY WILL HELP ENTERPRISES JUSTIFY THEIR INVESTMENT IN ICS SECURITY SOLUTIONS – VENDORS THAT CAN'T SHOW MORE VALUE WILL WITHER!

As more customers realise the need for OT cyber-security to protect against potential attacks, it would become imperative to gain value-add features that would ultimately "pay" for the new investment. Our main prediction for the OT security industry is that these systems must evolve to offer some kind of value add – and those that don't will ultimately fall by the wayside. Therefore, alongside OT security, the same systems should be able to deliver monitoring of the operational health of devices for inventory purposes along with key metrics for system availability, maintenance and capacity planning. An example of this trend is the recent technology partnership between Radiflow and Asset Guardian, launched in October 2019, which has already gained traction among multiple customers globally.

A BUSINESS-DRIVEN, RISK-ORIENTATED CYBER-SECURITY STRATEGY MUST BECOME A CORE REQUIREMENT IF ORGANISATIONS ARE TO EFFECTIVELY COMBAT CYBER ATTACKS



In many industrial organisations, especially those that still operate systems that are over a decade old, the process of strengthening the organisation's cybersecurity will uncover vulnerabilities and weaknesses that would need to be addressed. Knowing that a problem exists and having the resources to fix it will become a significant challenge across the entire sector.

As a result, both the vendors and the users of cyber security technologies will shift towards business-driven, risk-oriented systems. This approach must be at the core of any OT security strategy and is a shift away from the current Industrial Cyber Security thinking that is very much focused on visibility, hygiene and threat monitoring. While

admittedly vital, a reactive response within the impact assessment process could generate a firehose of alerts that could overload and overwhelm cyber security analysts. This is particularly true of low-maintained SCADA networks.

To optimally handle events and recommendations, the monitoring systems must provide risk-oriented prioritization of threats, vulnerabilities and mitigation measures. However, risk is not a one-size-fits all; it must be modeled against several criteria such as business interruption, safety, environmental impact or violation of regulations. Any method of prioritization must consider the different threats, business processes and of course, the probability and potential impact of every cyber event.

Without a risk-orientated approach, there is a danger that Infosec teams will waste valuable and finite resources fixing potential problems that have little material impact on critical systems, while more dangerous vulnerabilities remain. Considering that ICS CERT will typically add between 100-150 new entries each quarter that are relevant to ICS/SCADA environments, the ability to categorise systemic risks effectively should be the most vital consideration for every organisation in 2020.

ABOUT RADIFLOW

Radiflow develops trusted Industrial Cyber-Security Solutions for critical business operations. We offer a complete portfolio of game-changing solutions for ICS/SCADA networks that empowers users to maintain visibility and control of their OT networks, including an Intelligent Threat Detection tool that passively monitors the OT network for anomalies, as well as Secure Gateways that protect OT networks from any deviations from set access policies.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global industrial vendors and operators.

Founded in 2009, Radiflow's field-proven solutions, validated by leading research labs, currently secure thousands of customer facilities. For more information visit www.radiflow.com.