CYBER SECURITY GOLDRUSH

Ilan Barda *reveals what's behind the huge growth in cybersecurity and why people remain the most vital tool in the fight back against attacks*

The global pandemic has hit IT spending with analyst firm Gartner forecasting a 7.3 percent drop this year. However, cyber security spending is still on the rise – and one of the biggest growth areas is cyber security for industrial systems. At the extreme end, Internet of Things (IoT) security spending is expected to increase by 300 percent to $6 billion by 2023, according to a new recent study by Juniper Research.

The growth is due to a myriad of factors including the digitalisation of manufacturing and the opening of utilities to form smart grids; both trends that are exposing industrial systems to connections beyond a traditional air gapped approach to cyber security.

The triple digit growth with this area of cyber security has also led to a swarm of new tech investors piling in, plus the rebranding of IT-centric security tools into products designed for industrial use cases. At the end of 2020, a surge of investment went into security vendors aimed at protecting industrial control systems (ICS).

Analyst firm Valuates Reports estimates that in 2019 the global ICS Security Market size was worth $10,560 million and it is expected to reach $15,120 million by the end of 2026, with a CAGR of 5.2 percent during the forecast period. As to the why, its recent report states that: "Stringent government regulations related to critical infrastructure protection are expected to drive the ICS security market size during the forecast period. Sensitive infrastructure failures, such as the power grid, manufacturing, IT and transportation, significantly affect a nation's economic stability. For critical infrastructure, many governments have developed federal laws and regulations to implement cybersecurity standards. Cybersecurity insurance, grants and tax incentives are also being promoted by governments across different regions to enable companies to invest in critical infrastructure protection."

The fact that OT security is growing faster than IT security – albeit from a smaller starting point, is also attracting a surge of new entrants into the market. In 2018 security vendor McAfee estimated that there were around 1,200 cyber security vendors competing in the market. As of 2021, cyberDB, a service that tries to track cyber security vendors listed over 2,000 on its database – and growing.

On the customer side, the number of security tools in use by each organisation is also remarkably high. However, there is some consolidation. A series of surveys by networking vendor Cisco found that in 2018, one in five organisations had over 20 separate security vendors in use. Yet by 2020, that number had fallen to one in seven – and the trends toward consolidation are continuing.

However cyber security for Operational Technology (OT) has significant differences to its IT counterpart. OT is broadly defined as the hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise, according to Gartner. OT is common in Industrial Control Systems (ICS) such as a SCADA System.

A SHORTAGE OF SKILLS HAS MADE FILLING OT SECURITY POSTS MUCH MORE CHALLENGING

The OT security space has trailed behind IT security in several significant ways. OT networks within critical infrastructure and manufacturing have traditionally been closed environments. Often air gapped to the outside world by design. The digital transformation that has impacted the industrial world – often called Industry 4.0, has exposed these previously closed networks to more external influences – leading to a surge in cyberattacks. This has prompted a traditionally conservative OT security community to embrace cyber security – a surge that has been helped by newer, industry specific compliance frameworks.

The most notable of these frameworks is the ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC). IEC 62443 provides a realistic and workable framework to help address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). The standards core requirements focuses on five phases namely Risk Assessment, Develop/Implement, Counter Measures, Maintenance/Monitoring and finally Modify Procedures, Policies and Auditing.

In some cases it is impractical to shut-down a power station plant that might be experiencing a cyberattack

What makes the standard particularly valuable is its granular approach that includes not just for end users, but through sub-sections such as 3-1 and 3-2 that relate to vendor secure development lifecycle and vendor component specification. This is of vital importance when put in the context of recent supply chain attacks faced by SolarWinds. In this case, attacks actively targeted these weak links in the supply chain to breach better protected end-user targets.

The other major benefit of IEC 62443 is the Security Assurance Levels model that recommends different cyber security controls based on the level of protection needed. This can range from careless employees or contractors (SL1) to attacks by nation-states, using sophisticated means with extended resources, system specific skills and high motivation (SL4). This ability to build protection against the criticality of the infrastructure is a welcomed innovation compared with the almost binary – 'all or nothing' approach of earlier more rigid standards.

However, the interest in cyber security for OT environments is not evenly distributed. For many organisations that are emerging from dark world of air-gapped, closed networks into the light of more digitally connected systems; the biggest challenge is understanding what they have. And establishing where the greatest risk to their operations resides.

This risk assessment phase is time consuming, complex, and challenged by the propriety nature of many industrial control systems. Even though there has been a widespread push towards enabling more IP connectivity across the world of industrial systems, IP does not instantly confer a universal knowledge of a complex OT environment. The command-and-control information following across a network is often highly proprietary in nature. The logic behind industrial systems and changes that need to be made to configurations to elevate security is still a rare skill set – at least in comparison with broad IT infosec skills.

The number that can implement a firewall in a corporate environment is measured in the hundreds of thousands. Compared with the few thousand individuals that understand how to correctly assess the risk around a specialised application layer such as Common Industrial Protocol (CIP) that is prevalent within industrial systems for organising and representing data, managing connections and facilitating messaging on a network.

As such, risk assessment has become one of the fastest growing areas within the OT security landscape and has led to the emergence of new automated risk analysis platforms. There are multiple vendors entering this area but in general these tools follow a similar methodology.

This starts with gaining an understanding of the OT network, which can be gleaned from either a digital twin or through active network probes. Next, an initial risk analysis is conducted to define operational zones according to IEC62443 and the conduits between these zones with the aim of assigning a financial cost or Health-and-Safety-Environment (HSE) value. Next, these automated tools will compare each zone's current and required security level against known vulnerabilities and threats. After this phase, the tool will deliver a detailed report outlining risks and potential mitigation that is ranked against the impact at a monetary or health, safety and environmental level. More recent automated risk tools are staring to use breach and attack simulation (BAS) engines to analyse attack flows and not just vulnerabilities as well as simulate the use of different security controls to help optimise the security road map.

Another major growth area is OT security monitoring. Interest in this area is rising due to several factors. The first is the skills shortage that has meant filling OT security post is challenging – and more so for less intellectually stimulating yet still skilled tasks such as 24/7 monitoring. The other is the constantly changing threat landscape which means that although OT networks are more static than IT, the list of vulnerabilities and attack vectors is constantly growing. Over a typical three-month period, a vulnerability tracking service such as Mitre will post over a 100 new exploits or vulnerabilities that could impact an OT environment.

The last reason why monitoring has seen significant growth is as an aid to better delivering a response to cyberattacks. In an OT environment, attacks are often carried out in various stages that step through reconnaissance, establishing a foothold, lateral movement across the network, more reconnaissance and then attack against a target. And in some cases, extraction of sensitive information. When security monitoring is carried out effectively, the goal is to spot the early stages of an attack and allow operators to act quickly to block an attacker's further progression laterally across the network.

To do this, monitoring needs to be able to detect and alert response teams to anomalies quickly and without generating lots of false alarms. Unlike generic 'IT security systems', more specialist OT security systems are better able to understand the nuances around the operational 'normal' along with often specialist tools that are able to decode and interpret the more proprietary protocols such as ModBus and ProfiNet that are found in industrial systems, but not in the more general IT world.

Almost naturally, the OT world with its skew towards engineering is often focused on technology, tools and automation. However, from speaking to customers, and attending several virtual industry events this year, the impact of COVID-19 has had a knock-on effect on skills training and that also includes developing a response plan.

This is possibly the biggest challenge facing industrial and OT security where – in some cases – it is impractical to simply shut down a power station or sewage treatment plant that 'maybe' experiencing a cyberattack. How to safely isolate systems to pin down a security issue – without forcing a service interruption is a challenging process to define and implement.

Increasingly organisations are having to build more complex risk and response plans that work through several 'What if?' scenarios in simulated environments. In addition, alongside investment in technology that can help automate many of the processes, organisations must not forget that human skills, knowledge and experience must be nurtured as it still offers the best tool to protect against cyberattack. Even as IT vendors pivot into OT security, the industry must recognise that technology is an aid to human expertise and experience and not a like for like replacement ●

Ilan Barda, founder of Radiflow, is a Security and Telecom executive with 20 years of experience in the industry. Ilan has deep experience in developing secure communication equipment from his service in the Information Security division of the IDF.

Risk assessment has become one of the fastest growing areas within the OT security landscape

Picture credit: Siemens