SECURE

THE NEW LIMELIGHT ON
INDUSTRIAL CYBER SECURITY.
ARE YOU READY?

www.becybersecure.com
The attention placed on cyber security at corporate board levels has reached a fever pitch, which has implications for any company managing process control networks (PCNs). These changes have increased the urgency and pressure on leadership teams to address industrial control system (ICS) cyber threats – not only to prevent plant disruptions or safety issues, but also to protect the company against new legal and financial issues. With more than US$12.2 trillion in world trade in manufactured goods, according to the World Trade Organization, a lot is at stake.

This heightened visibility on industrial cyber security reverberates across the entirety of the industrial organisation, impacting both corporate and plant roles.

Dynamics have changed at the business and operational levels regarding ICS cyber security, because of multiple factors. One of these factors is the Cybersecurity Disclosure Act of 2017, which is currently proposed at the US Senate level, and would require companies not only to report the expertise of their board of directors to the US Securities and Exchange Commission (SEC), but also to take steps the company is taking to improve cyber security. The company would report these items to the SEC as part of its annual filings under the bill.

Directors on boards surveyed in 2016 reported more involvement with cyber security than the prior 12 months – and for three years in a row – increasing both the time and money spent on cyber security, according to the 2016 BDO Survey, conducted annually by the Corporate Governance Practice of BDO USA. While they want to know how the company is protecting itself from downtime, they are increasingly worried about legal issues – who is accountable if an ICS cyber attack is successful, and do they have enough measures in place to show they have been responsible in trying to avoid an attack in the first place? What data is available to prove their case?

Most industrial companies are not aware, for example, that a company’s financial credit rating could be impacted by its cyber security resilience status. Standard & Poor’s has already downgraded companies in the financial services sector because they “looked ill prepared” for a cyber-attack. Legal teams are also monitoring related ‘cyber resilience’ cases, as are risk managers and those responsible for negotiating cyber insurance policies. Once these cases run through their respective judicial systems, a precedent will start to set in and make it difficult for industrial companies to lobby for their own desired approach.

These are burgeoning business issues that have pushed cyber security to an urgent state, and now is the time to get ahead of these issues. Yet these are only half the story.

**The plant manager perspective**

On the operational side, cyber security in industrial environments is experiencing new momentum because of the rise in ICS
incidents, up by over 20% from 2014 to 2015 (ICS-CERT). A German steel mill explosion in late 2014 first visualised the consequences of cyber hackers changing a plant’s thermostat controls. Ars Technica reported that 10 turbine control workstations were taken down by USB-borne malware, and that a power plant needed three weeks to restart services after a similar infection. Multiple attacks have been made on the Ukrainian power grid, and recurrences of Shamoon, Dark Energy and other industrial attack campaigns continue.

For operational leaders, there is always the challenge of delivering on production commitments while handling resource-intensive security compliance procedures. They are also under pressure from business leaders to describe infrastructure in newer terms such as the Industrial Internet of Things (IIoT) and digital transformation – but nothing changes the need to deliver on time, and to quality standards. Security has to fit within an already-demanding workload. Add to that a lack of ICS cyber security skills and an average of 7+ different types of control systems in the environment, and it is obvious the plant manager is a busy individual.

What is most important to understand at the C-suite level is that together, these business and operational dynamics are forcing the need to get ahead of ICS cyber security, or face serious fines or impact to the business. This is different than traditional concerns regarding interruptions or downtime. While these are still prevalent and important, the business factors weave in even more reasons to get on top of ICS risk reduction programmes.

**Ready?**

Just five or six years ago, it was common for refineries to hold onto the myth that their operational networks were air gapped. In 2017, the most cyber-aware industrial leaders recognise that digital transformation, remote working, managed services and other trends have changed that reality. Over 50 million industrial devices are now considered ‘connected’, according to IHS Markit research.⁴

One can see leading-edge industrial companies taking advantage of expertise, technical innovations, and change management methodologies to improve their risk reduction measures. Some of the techniques that they use are outlined below.

**Viewing ICS cyber security as a programme**

ICS security programmes include an executive sponsor, defined risk milestones and timelines, budget, and an identified set of resources and processes. By aligning security to their organisation’s specific priorities and technical maturity levels, companies with ICS cyber security programmes are better able to measure and improve risk levels. They are also more likely to be able to implement ICS cyber security standards’ requirements, such as IEC 62443. Such programmes can help leadership teams prioritise and schedule the implementation of new technologies, such as control system upgrades or USB protection systems, which increase cyber resilience. In many critical manufacturing areas, where older systems are still abound, many were designed before the Internet age. As such, they have fatal software vulnerability flaws. As much as safety has been embedded as an important issue, these programmes also raise awareness throughout the organisation for protecting against cyber threats.

**Redistribution of ICS cyber security work**

Considering the lack of consistent in-house cyber security support, as well as newer ICS security automation technologies that are now safer to use across operational networks, some organisations are choosing to outsource ICS cyber security work. There are multiple approaches depending on the company’s geographic locations, legal limitations, internal resourcing levels, and technology types, among other factors. Complete managed security services move all ICS security responsibility to external vendors, including day-to-day management, threat intelligence monitoring and reporting. Hybrid services may allow for deep ICS security technical experts to perform assessments, leaving remediation to internal teams. In whichever combination, these approaches are addressing the cyber security skills gap, while also making it more efficient to implement more threat countermeasures.
Increasing visibility across all networks
In the past, operational networks have been ‘dark’ and difficult to measure in terms of security risk. With less oversight of cyber security and the understanding that any disruption is unacceptable, this blind side was an acceptable risk. Today, amidst the board pressures, both IT and OT networks must deliver increased resilience. New technologies in risk monitoring and management are able to bring safer visibility into the asset inventories and devices in OT networks. In addition, these systems allow for the implementation of comprehensive security policies, together with monitoring risk status in real time. Opportune for seasoned operational managers, these technologies also enable continual improvement by providing baseline and threshold metrics, as well as reporting to prove the incremental risk reduction measures.

Defense-in-depth methodologies
No single technology or process will address all ICS risk. However, establishing a security programme can help layer in countermeasures that, over time, will greatly reduce the highest priority risks. This includes taking a defense-in-depth approach when it comes to people, process and technologies. For example, identifying what systems across the PCN require security patches and on what schedule is a first step, enabling the second step of keeping them up-to-date on time – outdated software and equipment are a common problem in industrial environments and are an obvious risk for any attacker seeking rapid entry into a PCN. Measuring and monitoring such software is an effective countermeasure.

Conclusion
Even for industrial plants that have initiated an ICS cyber security programme, the risks are ever-evolving, and attacks are increasingly targeted. Minimising threats and layering in the latest ICS security innovations, however, represent major steps forward. These are best taken as proactive steps, rather than pressured actions while a cyber-attack is underway. Just ask any plant manager that has had to answer the dreaded question “are we at risk of a cyber security incident?”

References