CYBERSECURITY - WITH A MORE CONNECTED INDUSTRIAL WORLD, HAVE YOU EVERYTHING IN PLACE TO MITIGATE THE RISK OF A CYBER-ATTACK?

We explore cybersecurity and what you can do to protect your business.

The industrial world has increasingly become more interconnected, implementing smart technologies through Industry 4.0 and IIoT to drive efficiencies and productivity. These technologies rely on heavily populated networks, which open us up to the risk of cybersecurity attacks with every device that's connected.

Scarily, a 2017 survey conducted by Kaspersky1 discovered that on average one out of three internet connection sharing (ICS) computers, who experienced a cyberattack, were part of an industrial automation system.

With cyberattacks on the increase and the need to apply the same principles to operational technology (OT) as we do with information technology (IT), we take a look at how to start with the simple things to protect ourselves.

Often how systems can be attacked and infected can be misunderstood. We're all aware of viruses and malware associated with our personal PCs and likewise with more industrial smart devices, this has led to more access points onto the networks. This means more potential for an attack through any unprotected access point – something, which in theory, could bring a whole industrial system down.

There is a lot of information that can be accessed on unprotected control systems that could be useful to a competitor, or someone wanting to infiltrate a network – sounds like something from a Bond movie, doesn't it? But, if the information is out there, all they need is to find out where to access it.

More and more businesses are taking out cybersecurity insurance, but this can be deemed void or impact your claim if simple processes, such as updating firmware or assessing your vulnerabilities aren't followed.

Start with the basics

Best practice starts with basic checks – for instance, something as simple as restricting access to your control cabinets and making sure that they are locked. How easy is it for someone to walk unchallenged around your facility? That in itself is a vulnerability.

We've all heard of spam and phishing attacks, often in the form of very professional looking emails, all targeted to get you to click on or download something. They mimic an organisation to convince you to click on a link – a link that asks you to input details – to capture your data. They can then go on to sell that data or use it elsewhere.

Common sense can often help here by asking the right questions: Are you expecting an email from that organisation? Do you know that person? Does the email address look right? – often these are totally different or only slightly different to the organisation they are trying to mimic.

The same with attachments that don't look genuine - it's important that your people know not to open it, as once open the damage is done. There are tools that can help check out any link, website, attachment and scan it to help mitigate against tricks to manipulate and infect your system. One such example that is free and open source is totalvirus.com.

You don't have to be a master criminal or technical expert to find a way to infiltrate systems, there are websites that exist that can search the internet to check for an open IP address or if a system is vulnerable. An example of a site is 'Shodan', which recognises unprotected targets globally and can filter down to country. It will tell you exactly what protocols are open, i.e., no level of security on that system – which makes it a target.

Why do these types of websites exist? One reason is to allow manufacturers to see how far their products have gone, what markets have they penetrated or need to work on. Secondly, they've been developed so cybersecurity specialists can see what's being exposed on their IP address. They can see if a port is exposed and what software is at risk, however, it's also showing hackers what your vulnerabilities are as well. These sites can be an important tool to show you what's exposed on your IP address.

In essence, the industrial world, especially those with industrial automation systems and IIoT networks are susceptible to four main types of cybersecurity threats:

- **Malware**, which is a broad category of malicious software including viruses, adware, spyware, ransomware, Trojans, worms, bots, mobile malware, fileless malware, and rootkits. Malware can originate from external attackers on the internet or personnel who either accidentally or knowingly click a malicious link or connect infected removable media and other external hardware to the system.

- **Denial of Service Attacks**, which is when hackers overload your internet-connected network with vast amounts of bogus traffic to prevent legitimate users from accessing internal or external resources.
- **Intrusion**, which is when an attacker gains unauthorized access to network systems and infrastructure. Intrusions can originate from hacked applications in the production environment, extranet, or cloud. Remote access solutions, which are increasingly popular in Industry 4.0 environments due to persistent labour shortages and skills gaps, are particularly vulnerable. Another common threat is unauthorized smart devices that connect to production networks via a wireless local area network (WLAN) interface.
- **System Exploitation**, which is when hackers attack IT systems based on outdated and un-patched hardware and software by leveraging the inherent vulnerabilities of inadequately protected technologies.

What should you do if you think you have an open network?

If you have an open network, the first thing that you need to do is take stock of all the assets on there and cross-reference with your vulnerabilities within that network. From there it's a case of patching all the relevant systems up to date and mitigating access to the network. This could apply to IPCs, HMIs and always having user interfaces that require credentials to be input to gain access. In fact, the more layers of security controls to protect networks, devices and other applications the better, as each act as another obstacle to help prevent hackers from getting through and causing mayhem.

Here are some essential Cybersecurity solutions to consider:

- **Keeping your systems updated** - Outdated systems are at extreme risk of exploitation and will only grow more vulnerable with time.
- **Managed Ethernet Switches** - Managed switches facilitate communication between Ethernet devices and allow users to configure, manage, and monitor traffic on a local area network (LAN), control how data travels over the network, and who can access it. They also offer security features that unmanaged switches can't, including 802.1X authentication, port security, and private VLANs to help control who can access the network, monitor for attacks, prevent infected hardware from transferring malware to the network, and help rectify any breaches.

- **Network simplification and segmentation** - Eliminating gratuitous connections and splitting large networks into smaller segments using VLANs or firewalls makes it easier to control data exchange between various zones, like the factory floor (OT) and the corporate office (IT), and limits vulnerabilities to outside threats.
- **Secure WLAN password assignment**
- **Encryption** - Use firewalls to connect your automation equipment to the internet and encrypt your wide-area connections. Firewalls restrict incoming and outgoing traffic to authorized connections and encryption, which can be accomplished using virtual private networks (VPNs) and internet protocol security (IPsec), can prevent criminals from accessing, altering, erasing, or stealing your data.
- **Secure remote access** - To prevent unauthorized access to your machinery and ensure that any system changes made from a remote location are made to the right machinery, encrypt outbound equipment communications.
- **Secure Industrial Routers** - Industrial routers equipped with integrated security features like configurable firewalls, secure VPN connections, and access control lists help protect industrial networks from cybersecurity threats. For example, Phoenix Contact's FL mGuard security routers facilitate efficient and secure communication with the local network and provide a flexible and scalable solution for network infrastructure management.

- **Secure Protocol Converters** - Protocol converters, which are also called protocol or IoT gateways, enable interoperability between devices or systems with incompatible communication protocols by converting one communication protocol to another. They're essential for bringing legacy production equipment into IIoT networks and supporting predictive maintenance strategies but could introduce serious vulnerabilities into production networks if they're not equipped with integrated security features.

As smart manufacturing continues to grow, so should the concerns for Cybersecurity. Driven from the top down within the organisation, it's crucial to protect the business from the devastating costs and irreparable damage to reputation that could result, if not taken seriously.