When did you last update your cybersecurity systems?

Global cyber-crime is on the rise, yet many crucial infrastructure assets remain open to attack. Phillip Corner, industrial cyber-security project manager at Cougar Automation, explains how essential service providers can remain on the right side of the law and minimise their risk.

We're all used to updating the operating systems on our smartphones every month or so to fix bugs, patch security flaws and improve overall performance. Yet when it comes to protecting the cybersecurity of our businesses and critical infrastructures, we are shamefully lax.

In some factories and utilities, software hasn't been updated in more than a decade, leaving systems wide open to attack.

Perhaps we don't think it will happen to us or that it's not worth the investment – but cyber-crime is on the increase and the consequences of a breach can be catastrophic.

Only a few months ago a ransomware infection at aviation component manufacturer ASCO , brought production in four countries to a standstill for an entire week.

Regulatory push

Recognising the increasing threat to important industrial processes, the EU created the NIS Directive, which was intended to identify essential services for society and mandate at least a basic level of cybersecurity protection. This was enacted into UK law in May 2018 as the Security of Network & Information Systems (NIS) Regulations (2018).

Of course, it was not expected that all airports, hospitals, water and energy suppliers etc. install protection overnight, but a year down the line, regulators are now looking to see some genuine progress.

The 'grace period' is likely to end soon and companies that don't meet the requirements of the NIS Regulations' Cyber Assessment Framework could be hit with a fine of up to £17 million.

This may seem like a lot, but compared to the $300 million (£245.6 million) Danish transport and logistics Maersk lost in revenues in the high-profile Petya cyber-attack in 2017, it's a drop in the ocean.

Help at hand

With the help of a control system integration specialist, such as Cougar Automation, robust cybersecurity is not actually that difficult to achieve – although it requires more than simply installing a piece of software.

We work with companies to assess the impact of a potential cyber-attack on their business and introduce cybersecurity in a phased way, according to the budget and risk level.

Cybersecurity is always most effective when designed into the system from the start, but we also help our customers successfully implement robust cybersecurity into existing systems and processes.

In either case, the technical solution is only part of the equation. An overhaul of company procedures may also be required, creating good governance and enforcing policies to support the technical controls.

Something we recommend all our clients to do is appoint a member of the board with responsibility for cybersecurity reporting and make that a regular item for board discussion.

Honest assessment

The first focus should be to undertake an honest assessment of the company's process, evaluating the exposure to threats. When undertaking survey and risk assessment of industrial processes, we often find the reality of the process differs significantly from the customer's understanding of their system. There may be obsolete or unauthorised components or undocumented connections to other systems and the internet.

Much as with any safety management, a detailed and honest assessment enables companies to construct a clear picture of their process, quantify the risk based on the consequences specific to their business, and appropriately target budget and resources to address that risk.

Companies in the essential and digital service industries don't want to fall foul of the law and they certainly don't want to fall victim to what is becoming an increasingly common and dangerous threat. But cybersecurity doesn't have to be a worry.

Wherever you are in your cybersecurity journey – from audit, risk assessment, and developing good governance, to design and commissioning of cybersecurity defences –speak to us and we can help keep your operations running smoothly, safely and securely.

Ends.

Prev

Back to the list