Cyber-security: the automation sector should lead the debate

Cyber-attacks have been hitting the headlines recently. Victoria Montag*, Gambica's sector head for industrial automation, argues that in an increasingly interconnected world, the risks are increasing and that the automation sector should be taking a lead in moves to tackle the threat.

When the WannaCry ransomware cyber-attack hit hundreds of thousands of systems in 150 countries on 12 May, I was on holiday. I wasn't really following the news and was blissfully unaware that FedEx and Deutsche Bahn had been hit, and that several NHS Trusts had been crippled by the attack.

A day or two later, when I found out about the whole thing, the story had moved on to the finger-pointing and the "heroics" that had stopped the attack. So the full impact of what had happened didn't really hit home. Although lives had been put at risk, luckily, as far as I can tell, no one had died as a result (if that's not a testament to how great the NHS is, I don't know what is). The event seemed as remote as the hacking of the Democratic National Committee emails during the 2016 US presidential election. To be honest, I didn't really give it much thought.

A few days later, it was reported that an 11-year-old, armed with a laptop and a Raspberry Pi computer, was able to "weaponise" an IOT-ready teddy using the hacked Bluetooth-enabled devices of assembled experts at a cyber-security conference in the Netherlands.

It was that that really brought it home.

Unlike the DNC email hack, where the public (me) assumed that there had simply been poor password protection, the WannaCry attacks and Rueben Paul's jaw-dropping demonstration of what an 11-year-old can do, tell us that, as individuals, we can protect ourselves as much as we want – have the best and most secure passwords – but our defence against attacks is only as good as the network and security of every other item on it.

In an age where lightbulbs and children's toys are Bluetooth- and WiFi-enabled, responsibility for cyber-security suddenly becomes a very complex issue. An employee can act in a responsible manner and do everything in their power to ensure that they keep their employer's data safe, but if that employer doesn't make that network safe, you may as well forget passwords altogether. And how many of us connect our smartphones, with their notoriously vulnerable Bluetooth connections, to our work WiFi? Could we be walking vectors?

It is now impossible to talk about automation without talking about cyber-security. But while the automation sector is aware and is discussing cyber-security, writing articles and white papers, and producing guidance documents, the conversation almost feels secondary. Having perused many automation equipment manufacturers' Web sites, I find that you routinely need to search actively to find any information on cyber-security in relation to their products.

As we move into the next era of digital connectivity, now is the time for the automation sector to lead the conversation on cyber-security. ■

"In an age where lightbulbs and children's toys are Bluetooth- and Wifi-enabled, responsibility for cyber-security suddenly becomes a very complex issue."

Cyber-attacks are not just a concern for users of desktop computers. The Stuxnet worm, first identified in 2010, was developed specifically to target PLCs – originally the PLCs that controlled the centrifuges in the Iranian nuclear programme. One fifth of the Iranian nuclear centrifuges were destroyed before the worm was discovered. (I do not make a judgement on whether this is a positive or negative thing, but it does demonstrate how much damage can be caused).

The (Industrial) Internet of Things is not the future, it is happening now. And with cyber-attacks gaining more prominence in the media, the world is becoming increasingly aware of the risk of introducing more and more connected devices into our homes, offices and factories. Soon, these places will be connected to each other by such devices.

*** Gambica is the trade association for the automation, control, instrumentation and laboratory technology sectors in the UK. For more information, please contact Victoria Montag on 020 7642 8094 or via victoria.montag@gambica.org.uk**