FALSE SENSE OF SECURITY

Stuart Jubb *explores the multifaceted challenge of addressing cybersecurity in critical national infrastructure and what the chief information security officer can do*

The Russian invasion of Ukraine began in cyberspace. According to UK intelligence services, Russia was almost certainly responsible for an attack on a Ukrainian communications provider an hour before the invasion and cyber attacks have continued since. These attacks, and others going back as far as 2017, attributed to Russia by the CIA, have shut down airports, banks, government ministries and even radiation monitoring at the Chernobyl nuclear power plant. They are a chilling reminder of the damage a determined state actor can cause to critical national infrastructure and the depth and breadth of the threats that cybersecurity professionals across every sector are up against.

Major services such as power generation, telecoms, payments, water supply, public health systems and less obvious ones like traffic lights or petrol pumps are vital to keep a modern country running. They rely on complex and often rather old systems, and because there are so many of them, there is an asymmetry when defending such services from cyber-attack. We have a lot to protect against highly motivated adversaries.

So are we doing enough to fend off attacks – and what else could we be doing? This is a regular topic for discussion at Crossword with clients and partners, and came up recently in conversation with Professor Raj Muttukrishnan, director of the Institute for Cyber Security at London's City University and Professor Tim Watson, director of the Cyber Security Centre at WMG, University of Warwick, as we drafted our recent report, Strategy and collaboration – a better way forward for effective cybersecurity.

The future is self-healing systems that can detect unusual behaviour as soon as it occurs and take action to prevent it becoming an incident

Of the many areas of concern, here are three that come up often, and which also chime with our research. Firstly, as Prof Muttukrishnan says, even where systems are well-built: "problems come with inexperienced employees, who might misconfigure a new product and create a vulnerability". Our survey collated insight from over 200 senior cybersecurity professionals and we found an industry that is overstretched, making it more likely that mistakes will happen. Rather than being able to plan for potential threats, the professionals we spoke to were trapped in fire-fighting mode, constantly responding to the latest crisis.

Secondly, critical national infrastructure often relies on legacy systems, some of which date back to the Seventies. These might run on an obsolete programming language or use hardware which is difficult to repair or replace. As a result, it is becoming harder and more expensive to find people with the expertise to work on these systems. For example, many COBOL software developers are now reaching retirement age and the programming language is not widely used enough for younger developers to learn it. In addition, these systems were not designed to connect to new online systems and are now being exposed to new threats. Finding – and fixing – vulnerabilities in these older systems will be increasingly difficult.

But a third question is whether those who manage the systems have the incentive to fix them at all. Many systems, such as those used in power generation, are in the hands of private companies. In many companies, risk management still lacks the priority it deserves, and cybersecurity teams must constantly lobby for the budget and tools that are too often seen as an avoidable cost providing no financial return. Professor Tim Watson says: "They answer to shareholders and they might not see it as financially worthwhile to go beyond the minimum where cybersecurity is concerned".

EVEN IF ATTACKERS CAN GET IN, THE AIM IS TO ENSURE THERE IS LITTLE THEY CAN DO ONCE THERE

Despite these vulnerabilities, it is possible to defend against attack. Russia, with all its resources, has caused online disruption in Ukraine, but hasn't brought the country's IT infrastructure to a standstill. That is partly because Ukraine, with the support of Western cybersecurity firms, is quickly identifying vulnerabilities and rolling out upgrades to fix them.

This is one advantage that defenders have over attackers. As Prof Watson says: "An attacker might need to hold on to a vulnerability for a long time and, at any moment, it can be fixed with an update; sometimes an update intended to fix something else closes the vulnerability by chance. Updates happen all the time, so there's no guarantee that an attacker has a working vulnerability to hand."

Smart security experts are constantly working to make systems more resilient, so that even if attackers can get in, the aim is to ensure there is very little they can do once there. Prof Muttukrishnan notes: "The future is self-healing systems that can detect unusual behaviour as soon as it occurs and take action to prevent it becoming an incident – all without involving a person."

Many cybersecurity tools now employ automation and AI, which reduce the burden on cybersecurity teams by detecting and acting on security alerts without any human intervention. This means teams don't need to deal with false positives, but it also means legitimate threats will be dealt with more quickly.

It would be easy to think that if you have great technology and staff then everything will be OK, but this is never the case. As with any aspect of a business, a false sense of security (if you'll pardon the pun) can develop from the comfort of the status quo. Over time bad habits can develop, processes become broken, and if a cyber team is very insular, a fishbowl mentality that 'everything is OK' can persist and this is perhaps the greatest threat of all.

A new mindset and approach to cybersecurity is needed that takes into account the scale of the threat. This must be mandated from the top of an

organisation, but not be limited to it, and include each company's complete supply chain and associated third parties. This should include training, processes and policies for employees and suppliers that focus on reducing cyber risk.

Managing cybersecurity successfully requires several things: budget, support and the right culture. Without sufficient budget, nothing can be done. I've heard of instances where the board will see security purely as a cost and resent paying for it. At the same time, they sometimes think that what they are paying for is a guarantee of never being attacked. A big part of the CISO's job, therefore, is communicating the balance of risk, mentioned above.

FINDING – AND FIXING – VULNERABILITIES IN OLDER SYSTEMS IS INCREASINGLY DIFFICULT

That isn't always easy. The board is still likely to be dominated by people who did not grow up in a world where cyber risk was a business concern. They don't necessarily understand the language of cybersecurity or how the CISO is trying to manage it. Contrast this with the CFO, for example. Most boards are very comfortable with financial language.

Staff should understand that security is everyone's responsibility. There are several ways to build a culture. Simulated cyber incidents are one of them, allowing everyone involved to understand just how quickly and completely a cyberattack can paralyse the organisation. But nothing beats support from the top. If the CEO puts cyber at the heart of the organisation, then the culture will change.

Whatever the culture, the CISO must make their strategy clear and then execute it. The strategy defines the process for incident response and policies for adopting technology such as IoT. Across an organisation it must be clear to people how they can identify a business need, find the right technology to meet it and deploy that technology, all with security in mind. The CISO can easily be viewed as a blocker to new initiatives in a company, but it's always better to ensure that security is considered from the outset because adding security afterwards is much more complex, and can be more expensive too.

This kind of complexity is what can lead to constant firefighting, which the CISO must avoid being drawn into. Getting caught up in the detail is a guaranteed way to stall strategic progress. Instead, the CISO needs to focus on the big picture while a trusted team manages day-to-day challenges. It requires good management skills and the ability to delegate.

Without that, the CISO will burn out. It's a high-pressure job and even good managers can be worn down by the intensity of the role. Many CISOs find it hard to switch off, but it's essential to have some downtime each week and the confidence to hand over to the team at least long enough for a holiday.

Beyond their team and the wider organisation, CISOs will also find support from other CISOs, particularly in critical national infrastructure where the benefits and collective aims are the same – to keep everything working and safe. They are working together against a common enemy, so building that network is vital. CISOs warn each other of emerging threats and share experiences to learn from past mistakes. It's a very valuable resource.

These aren't the only relationships to maintain. It's important to be on good terms with the relevant regulators, such as the Information Commissioner's Office and the UK Cyber Security Council. Most of them are helpful and will offer guidance on doing things the right way. A good relationship also makes things run more smoothly if and when an attack occurs.

Cyber criminals and nation-state attackers are constantly looking for weaknesses and updating their methods, so the CISO's job will never be an easy one. But with the right structure in place, they can at least ensure sound defences and a solid strategy that will give them the best chance of securing critical national infrastructure and its supply chains.

To succeed, an organisation's overall aim must be to ensure that cybersecurity professionals are no longer trapped in fire-fighting mode. They need to be prepared and, if an attack comes, we need them to be alert and ready to react ●

Stuart Jubb is Group Managing Director at Crossword Cybersecurity.

Critical national infrastructure often relies on legacy systems dating back to the Seventies