Simon Gawne discusses the need for security teams to expand their remit to include cyber defence as attackers increasingly target vulnerable connected security devices

IS YOUR PHYSICAL SECURITY CYBER SECURE?

©Getty Images

Sony Pictures' movie The Interview was believed to be the cause of a high-profile cyber attack from North Korea

For as long as security has been a professional occupation, the aim of the security director has been to guard the perimeter, identifying and expelling the dangers that threaten the business. That used to be a physical activity – for example, apprehending intruders, ensuring approved entrants aren't carrying concealed weapons or maintaining strong outer walls. The perimeter fence used to be the key concern of the security director, but in recent years the development of digital and systematic threats has caused the 'vulnerable area' of the business to expand exponentially. Now, the perimeter is limitless to all intents and purposes - though physical attackers are far from gone, cyber attacks and system weaknesses are now every bit as dangerous a threat to the business.

The boundlessness that comes with connected technology is also being felt in the physical security sphere, however. Many physical processes such as surveillance and access management are now increasingly being managed from a central control facility with responsibility for multiple sites – which may not even be on the same continent.

While the merging of IT and physical security has undeniably reaped many benefits - including making systems faster, smarter and easier to manage – the downside has been the real and perceived vulnerabilities that come with network-based systems.

Because of the perceived weakness of the virtual network, physical security products are often a target for security researchers, but rarely the end target for a real cyber attack. Cybercriminals come in several varieties – for example, cyber thieves want to make money, state-sponsored attacks intend to cause damage or steal information, while 'hacktivists' try to make a statement. As such, even if a malicious person could play with your locks or watch your video feeds, there's not much value in such an activity.

What an attacker really wants to do is get to something useful or valuable. In this case, security products can often provide the access. So how do you ensure your security products are not the weakest link to your network?

Firstly, it is crucial to ensure a cohesive security strategy within the organisation across both the digital and physical spheres. In this new world, the role of the traditional security director and his or her team remains central, but with new definitions of security that role is now joined by a host of others. In most organisations, professionals from IT and other departments are now in prominent security-related roles.

In many cases it is still true that there is no one in a better position to lead overall security efforts than the experienced security director. However, it is equally true that in order to do so, he or she must now be the leader of a multi-disciplinary team with a group of professionals delivering what might be to them unfamiliar types of expertise. Moreover, that team will likely be located across several different facilities; so effective collaboration and information sharing are essential.

In order to lead these newly expanded teams, many security directors may need to expand their knowledge base first. This does not necessarily mean having to become an IT or cyber security expert, but for many security professionals it will mean gaining a better understanding of the technologies utilised by those disciplines, as well as the language they employ.

This can be done readily through training, and many large organisations in the security industry offer courses that can help close the gaps in a security professional's knowledge. These resources are often especially geared towards the needs of experienced, on-the-job professionals.

But it's not just a case of looking inwards. When evaluating security products before implementation, it is essential that organisations are cyber savvy when it comes to how digital security is built into physical products. When constructing security systems, no matter the facility or size – from small stores to school systems and even the largest government agencies – it is critical to understand how the physical components, such as cameras and video management systems, fit in within those network architectures, and without introducing new vulnerabilities.

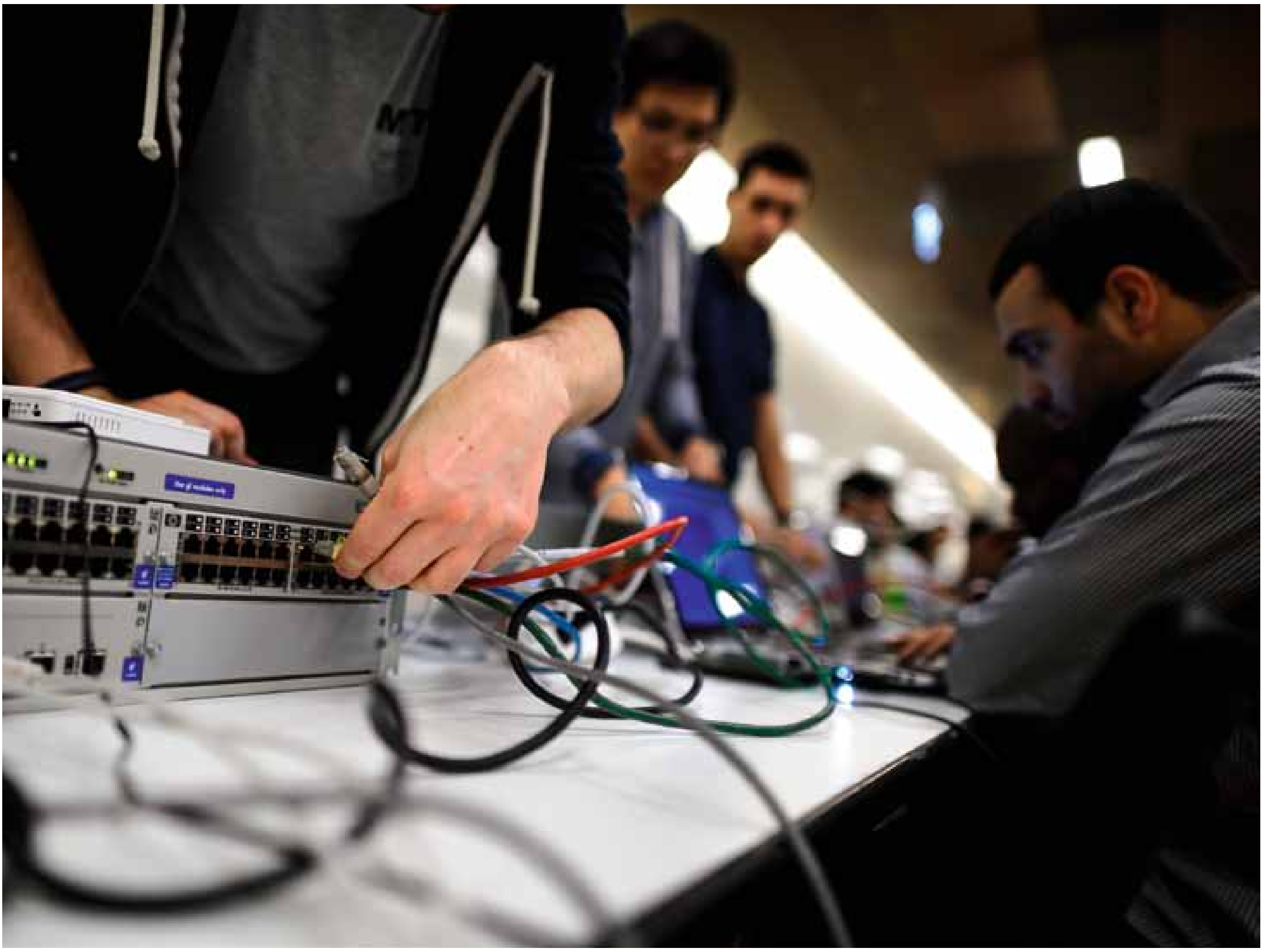
A challenge for all product manufacturers is how to reconcile ease of use with an appropriate level of security. A key selling point for many security products today is that they are easy and fast to install, saving the integrator and the end user valuable time and expense. However, if the trade-off is a lack of authentication or encryption, system vulnerabilities can start to creep in.

As such, the security of the products that make up any IP-based system must be questioned. When security is not a consideration from the start of the process, through the final stages of its creation, it can result in a product that becomes impossible to secure at deployment.

Secure development of a physical product starts with a risk assessment. Organisations must look at whether the key focus areas of confidentiality, integrity and availability have been met. But what does this mean when applied to security products at a very basic level?

Firstly, keeping confidential information out of the hands of those to whom it does not belong. For example, when looking to implement a camera, be sure to consider whether the camera requires authentication to view the video. This is such a simple yet often overlooked step – in fact, there have been websites created that are dedicated to showing the live feeds of security cameras that don't require passwords.

Next, when it comes to integrity of information, access control systems are of vital importance to physical products. The biggest mistake would be allowing changes to the database, which could allow an attacker to gain physical access to the building.



©Getty Images

A participant connects his computer to compete in the ethical hacking contest Insomni'hack in Geneva

Making sure the product is available and continues to function is probably the most important role for security products. While DoS (denial of service) attacks are headline grabbing, functional errors in the product are the most common cause of compromised availability. For example, an intrusion system that fails to detect a sensor going offline, or an access control system that cannot operate during a network or power failure can lead to a security downfall.

Security must always take into account the risk from internal threats as well. A Ponemon Institute study showed that "malicious insiders" were the most expensive form of risk for an organisation when weighted by attack frequency, and were also the longest attack type to resolve. It's therefore important to make sure any products you select can be set up with controls that separate responsibilities for individual users.

Finally, remember to ask about third-party assessments. Does the supplier undergo independent assessments of its products? More importantly – and an often forgotten question – do they then take the proper steps to resolve the issues found?

Ultimately, it must be noted that cyber security is not static. New vulnerabilities and exploits are uncovered every day. A successful product cyber-response plan requires a dedicated, multi-disciplined team with the capabilities to assess and mitigate issues when they arise. When executed properly, the team should be able to respond the same day with an assessment and mitigation plan.

It is, therefore, the security director's imperative to open and hopefully lead the dialogue with IT, logistics and other security-intersecting enterprise operations on how to integrate security applications with the rest of the business, and improve how risk is managed overall.

Security professionals need to take the lead and initiate the discussion. They can offer their security roadmap and business plan to peer leaders in the other departments and see where plans intersect, and how they can work together to provide the best overall security services to the enterprise.

Changing the dynamics of a team to incorporate new skills can seem a challenging prospect to any department, but especially in the essential work of the security team, it is often the price that must be paid for effective service in an increasingly digital world. At the end of the day, if security remains a closeted physical world with no insight into the networks it is designed to protect, then the defence it provides risks being mismatched, outdated and ineffectual. As collaboration and digital activity become the norm, the most successful security directors will be those that take the initiative and gain the digital skills necessary to protect the organisation both from the outside and from within.

Simon Gawne is Director of Integrated Solutions and Innovation at Tyco. He has almost 30 years' business management and R&D experience across a wide range of industries including physical security, cyber security, telecoms and technology. He is based in Tyco's Integration Centre of Excellence in Cambridge, UK.