INTEGRATED SECURITY

Ian Robinson *thinks we've been talking for too long about integrating security and that it's now time to implement it*

There was a definite shift at this year's IFSEC event, moving from purely physical-based security to an integrated event, incorporating the latest in cyber defence technologies and showcasing how digital and physical security can be intertwined. It was good to see this, but again we heard the same messages about integrated security, avoiding security silos and taking a multi-disciplinary approach. This is no fault of the organisers – obviously it's a message we need to keep hearing because I'm not seeing the evidence that it's happening on the ground.

Besides, I am doing exactly the same – another self-proclaimed industry veteran banging the same drum that everyone else has for 20 years or so. Except, the tune has changed in the past few years, hasn't it? The world has changed. Terrorism targets have changed. Terrorist tactics have changed. Our tactics have also changed. The problem is these changes have largely been dictated to us – we've been reactive not proactive. I fear we are making the same mistake with integrated security.

But why do we need to move to integrated security? The threat we now face around the world is multi-faceted – our people, our buildings and our data are all at risk. But the threat is not always a physical one nor is it always direct; cyber attacks on our public infrastructure don't just affect the buildings or the infrastructure themselves, but the people they exist to support.

The WannaCry cyber attack that affected Britain's health service and organisations around the world in 2017, resulting in appointment and surgery cancellations and much more. The perpetrators may have been criminals trying to hold firms to ransom rather than terrorists, but it showed the world how vulnerable a country's infrastructure could be.

When it comes to security cameras, consideration needs to be given to lighting

STAYING SAFE

Hospitals provide an excellent example where integrated security is of the utmost importance. They are large targets usually in urban areas where a complex system of physical security is not logistically realistic (employees need to get to work, patients need quick access). Nor is it desirable – we want hospitals to be safe, but they should also be a pleasant place to be for recovery.

But hospitals need to know who is coming in and out and why they are there. Not to mention the vast quantities of medication, equipment and data stored on site. We should be asking harder questions of our security processes and ourselves. The right data in the right place can be a huge step in the right direction.

Take existing HR software that shows which personnel are accessing the facility or logging on to valuable commercial data. This could be completely harmless and appropriate, but it shouldn't be taken as a given. Should that employee be there? Should they be accessing and importing files and documentation?

If the answer is "No", can existing security systems be integrated to provide a method of control, such as doors being remotely locked, alarms activated and security staff notified?

Moving to an integrated approach to security does not solve all of these issues, but, by integrating IT, HR and physical security measures that share information and automatically raise alerts based on the assumed threat level, it does enable rapid and intelligent responses to potential security breaches. We need to move to an approach that detects risks at an early stage whereby the system can intervene or alert the relevant personnel or team.

THE BIGGER PICTURE

Integrated security does not mean we neglect physical measures, but we need to think of the bigger picture. Security is the job of planners, architects, construction firms, IT businesses, HR departments, and front-of-house personnel. This requires an integrated approach and an integrated platform.

For years we have managed perfectly well to protect our buildings, infrastructure and people with a mixture of security solutions that were often intelligent, innovative or well designed, but rarely have those been part of what I'd describe as a holistic, intelligent security system.

Currently, security solutions are developed in silos built as proprietary software packages or physical devices. This means that it is impossible to create an integrated solution. In addition, most general security solutions tend to rely on email or web reporting that then alarms an individual to deal with any potential threats.

Of course, this might prove to be sufficient in some circumstances, but the reliance on an individual in a singular team or department without any communication to other relevant personnel is laden with risk.

INTEGRATING IT, HR AND PHYSICAL SECURITY MEASURES ENABLES A RAPID RESPONSE

As Jasvir Gill, CEO of AlertEnterprise, Inc, notes: "You can never be safe if you put three locks on one door and leave the other doors wide open".

There are plenty of security solutions out there, but we need to begin implementing singular platforms that can manage those systems and interpret the data they output.

These platforms will act as an interpreter, analysing the incoming data, looking for any abnormalities and then delivering the relevant information to the right people.

REDUCING THE BURDEN

Artificial intelligence will also mean more advanced and complicated decisions can be taken by the platform itself – again, further reducing the admin burden on humans who can look after the more nuanced decisions that need to be taken. It might seem complex now, but once we begin implementing this approach, it will become much more simple.

But how can we make the shift? Security is a design issue that must be incorporated at the initial concept design phase. Traditionally, aesthetics have dominated the overall building design with architects' concern for the working environment being compromised by security provision and the security expert worrying about the lack of security provision at the concept phase.

A simple solution we implement is to have a security expert engaged during the concept phase and working closely with the design team to ensure security is woven into the fabric of the building. This ensures all teams involved will achieve the common goal of keeping tenants, workers and visitors safe.

Sadly, we are too often involved in projects where security (let alone integrated security) is thought about too late in the process to be most effective. It's usually planned into the process, but at a point where it is much more complex to implement security changes and so is much more expensive.

If not picked up at the design stage, the built environment affects the patterns and behaviour of the building's occupants and this could have a negative impact on security. Conversely, good design can encourage good security behaviour and discourage detrimental tendencies in the occupants of a building.

FORWARD PLANNING

As threats change, so must we and there is always room for improvement. But there are also many security measures I have seen retrofitted in buildings that would have been much cheaper, more effective and less headache inducing had they been planned in at the design stage.

Lighting and CCTV is a good example. CCTV needs a constant light level to operate effectively, but so often LED lighting is either not positioned correctly or too little or too many LEDs are used, affecting the camera's ability to record a clear image. The post-installation cost to bring the lighting up to standards is considerable.

Blast and ballistic resistance is also a regular, and very costly, afterthought. For example, if the building structure itself is not designed to accept the extreme loads a blast impact would impose, then post-strengthening is required. But post-strengthening is expensive, less effective in many cases, will cause major disruption to the staff and can destroy the aesthetics too. Likewise, installing resilient back-up power sources and redundant systems is never cheap, but it's much less expensive, and less inconvenient, to include back-up systems at the design stage. Post-strengthening is always expensive and occasionally unattainable.

In conclusion, safety should be considered in every decision – especially the architectural materials chosen, as this will underpin all subsequent safety and security systems. Designing for security also has additional benefits, such as mitigating risks of damage to servers and other data centres, helping to prevent the potential loss of critical functions. Clearly, integrated security solutions are the new standard to reach for and it's imperative we do so.

WE SHOULD BE ASKING HARDER QUESTIONS OF OUR SECURITY PROCESSES AND OF OURSELVES

The technology and materials to make this a reality already exist and the expertise to design, manage and implement these security solutions is also available. The challenge is to act on the messages we keep hearing at security events and ensure an integrated approach to security takes place on an every-day basis ●

Ian Robinson, director of business development at RWS Ltd, has managed and installed key security projects for the national infrastructure and government agencies worldwide.

The WannaCry attacks showed the world how vulnerable a country's infrastructure can be

Picture credit: Getty