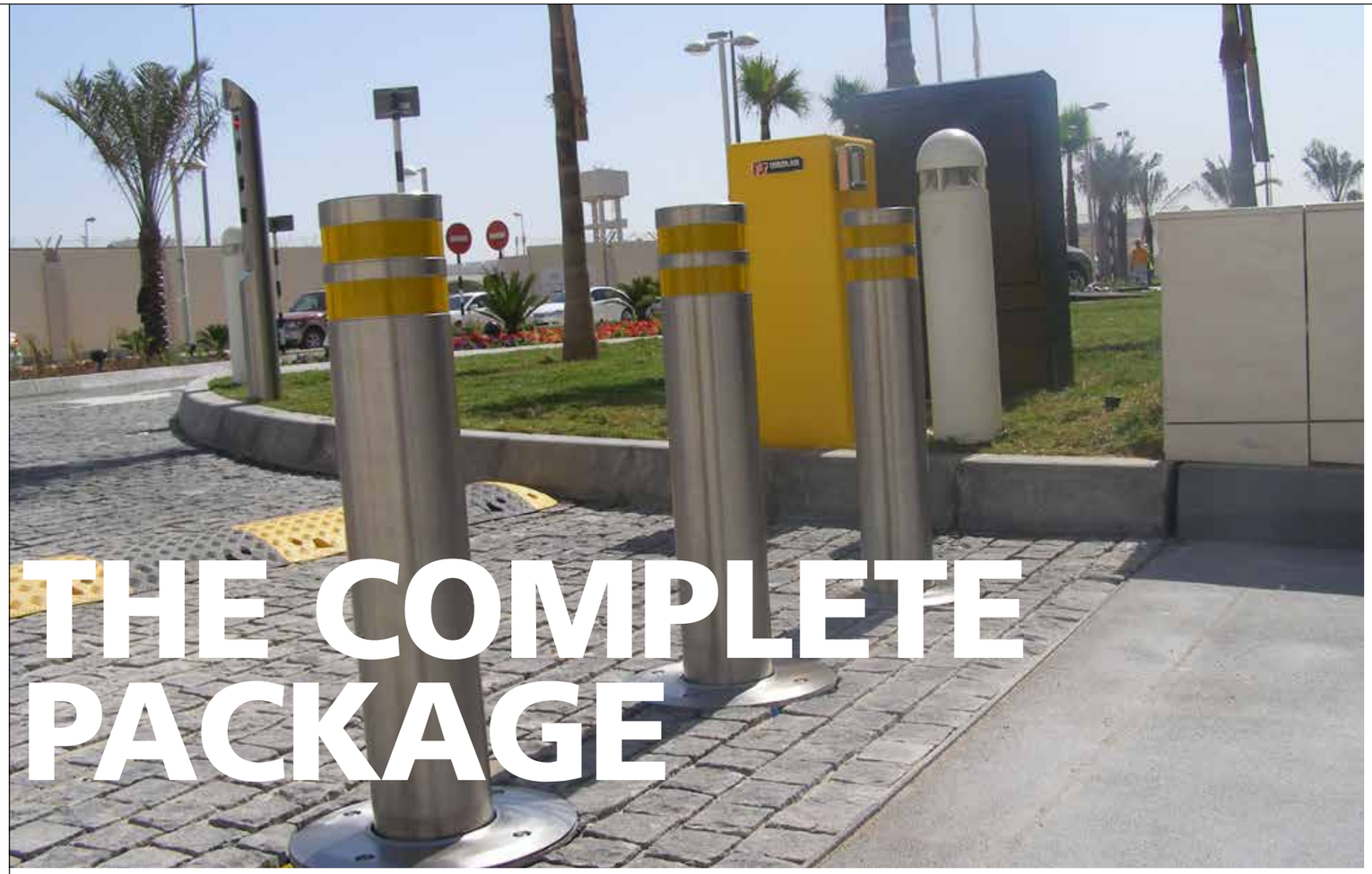

THE COMPLETE PACKAGE

Lucy Ketley *delves into the fundamentals of physical and cyber security convergence*

The exploitation of the internet for radicalisation and research means that many abhorrent hostile vehicle terror attacks now originate in the digital realm. This has likely been the case for several years. And although hostile vehicle threat levels are generally low, the digital component is on a worryingly upward trajectory. Understanding the interplay between physical and digital infrastructures is vital to keep people and assets safe from vehicular attacks. But how can physical security consultants – working in a critical specialism that demands full attention – own yet another niche? Are they accountable for a job they can't possibly do alone?

DO SECURITY CONSULTANTS NEED A DIGITAL STRING TO THEIR BOW?

The short (but somewhat reductive) answer is no. Although the duty of care now considers the role of digital in HVM, physical security professionals are not expected to become anti-terror cyber security experts. Not now, and not ever.

But – and there is a but – they need to understand the fundamentals of how physical security and cyber security converge. Both the basic interdependencies and the most effective ways to coordinate the two for better threat mitigation.

After all, we know that digital tools are abused for radicalisation and reconnaissance. We also know that digital communications are the fastest way to coordinate emergency help. Therefore, to successfully mitigate, manage and monitor vehicular threats, security projects and professionals need a preliminary understanding of how digital and physical vectors interact.

Before discussing this further, we will note that we use an extended definition of cyber security. In the context of HVM, 'security' refers to physical safety, which digital components can reinforce. Therefore, we interpret cyber security not just as defending technology integrity, but as ways digital solutions can protect people and assets from harm.

With that said, let us explore the core strategic objectives of security convergence, its most valuable applications in HVM and how you can start coordinating physical and digital channels more effectively.

Picture credit: ATG Access

To successfully mitigate, manage and monitor vehicular threats, security projects and professionals need a preliminary understanding of how digital and physical vectors interact

Lucy Ketley is Sales and Marketing Director at ATG Access. With over three decades of experience within the physical security industry, ATG Access specialises in Hostile Vehicle Mitigation (HVM) and Perimeter Protection, within national and international markets, including the UK, Europe, Australia, Americas and the Middle East.

Security convergence can be briefly summarised as: "the integration of physical and cyber security measures and strategies to address threats in both the physical and digital domains". With much planning and coordination of hostile vehicle attacks happening in the digital world, security convergence enables us to better adapt to the nature of terror threats.

THE FUNDAMENTAL OBJECTIVES OF SECURITY CONVERGENCE

The strategic objectives of security convergence are twofold and in the interests of any security consultant or safety project stakeholder. These objectives are to: prevent hostile vehicle attacks more effectively. More data – through enhanced monitoring, integration and data sharing – means stronger situational awareness about how and when threats are changing and the solutions that deliver proportionate and appropriate HVM; and to respond to hostile vehicle attacks more effectively. When digital infrastructure and communications are leveraged, emergency response can happen faster to complete the job performed by physical security measures.

Although security convergence is unlikely to result in the mass digitalisation of physical security infrastructure (especially HVM hardware), its insights can be game-changing. Experts note that data consolidated and generated by advanced, integrated digital security tools may influence vital factors like product specifications and threat-level evaluation. As a result, physical security professionals are teaming up with specialist partners to help make sense of the challenge and set priorities.

THE MOST VALUABLE APPLICATIONS OF SECURITY CONVERGENCE

When done correctly, security convergence can and will aid the continued effectiveness of HVM measures. This is especially true at the risk and threat assessment stages (and subsequent VDAs and product specifications) and post-attack.

Therefore, security convergence is of growing interest among security consultants, project managers and public realm managers alike. Its value is immeasurable, but we are noticing an uptick in security projects uniting the physical and digital in the following ways:

Securing space surveillance: Spaces protected by HVM are often accompanied by video surveillance and access control systems. Should these digital assets be hacked or compromised, they may be leveraged for hostile reconnaissance. Working with a specialist cyber security provider can reduce the risk significantly.

Monitoring space data points: Those video and access systems are rich with data – pedestrian volume and movement patterns, vehicle near misses and irregular behaviour. Specific cyber security monitoring, detection and response solutions can automatically consolidate vast amounts of data and flag developing risks or potential changes in HVM requirements.

Sharing threat intelligence: Although the latest threat intelligence is always available, it can be challenging to localise and apply in context. Enhanced security convergence can expedite threat intelligence data sharing and enable more timely evaluations of vulnerability and, therefore, HVM measures.

Automating communications/responses: If the unthinkable were to happen, good security convergence could help reduce casualties. From rapidly coordinating emergency services to warning the nearby public, convergence is powerful for those actively managing the security of HVM-defended spaces.

As discussed, those responsible for physical security are not to become cyber security experts or know all the details. But taking decisive action to establish security convergence is now part of the duty of care – and will undoubtedly improve HVM measures in more ways than one.

One security convergence expert put it as: "needing to become a conductor of an orchestra, not a master of every instrument". The most sensible next step is to have a conversation with an accredited cyber security consultant who specialises in your sector or space and bring your physical security consultant into the discussion too. From here, you can work collaboratively to shore up your security convergence fundamentals and develop a HVM strategy fit for the digital age.

SECURITY CONVERGENCE CAN AID THE CONTINUED EFFECTIVENESS OF HVM MEASURES

In general terms, the coming together of the physical and cyber realms must surely be considered a good thing. But when there is a new approach, we cannot assume all will be plain sailing. In terms of physical and cyber convergence that is especially true.

One of the key risks the industry faces is trust, which extends to both the what and the who. There exists a relatively small pool of established market players in the world of physical HVM security and the products available are tightly scrutinised. Taking a product through an IWA, ASTM or PAS testing procedure is expensive and time consuming – and rightly so. The output of such tests gives confidence that a product is fit for purpose.

With cyber technology however, the risk landscape changes almost daily and solutions to combat the risks must keep pace. That means rapidly changing technology and a near constant stream of new market entrants. Undoubtedly some of these will be outstanding, but just what solutions can be trusted. And as the cyber industry is largely unregulated, a supplier's capability must be assessed some other way, but how?

Which leads on to the who. For a purely physical scheme, risk identification and appropriate measures are identified by a security consultant. But with cyber, such a vast array of threats and potential solutions exist that security consultants will be hard pressed to stay abreast of the best approach. Those that can, will be in high demand, potentially creating a skills vacuum.

All of which means a rethink. New processes are required and established industry practices and skills need to change. That could and arguably should include regulation, which all takes time. In the meantime, convergence is a hot topic and that creates a pressure cooker where mistakes can be made. We must proceed, but caution is the watchword ●