ALL CHANGE

Georges Tannous *reports on the changing face of physical security*

Pandemic-related economic factors are likely to continue to present challenges across many industries in 2021. While the global pandemic has certainly taken the world by surprise, the security industry excels at planning for the unexpected and is resourceful in times of crisis.

However, at a time when budgets are tight, many businesses, cities, critical infrastructure and transportation agencies need to be creative about how they use, update and redeploy their security systems across their organisations. And they need to work hard to ensure that their investments not only solve today's problems, but also continue to play a strategic role even once the pandemic is finally in the rear-view mirror.

Based on the key findings of a recent Genetec report – the State of Physical Security in EMEA 2021 – this article takes a closer look at how physical security teams across Europe, the Middle East and Africa (EMEA) are leveraging technology to manage both short-term needs with long-term priorities.

The substantial increase in cyber-attacks as a result of the pandemic is well documented. In 2021, it is predicted that a cyber-attack will be reported every 11 seconds.

Video analytics has evolved considerably to extract very reliable and powerful data from video streams

Against this backdrop, 67 percent of survey respondents are planning to prioritise the improvement of their cybersecurity strategy this year. While it is encouraging to see physical security professionals paying more attention to cyber threats, it is clear there needs to be a lot of catching up to do.

It might seem ironic that a physical security solution designed to protect people and property can be the subject of a cyber-attack, but devices such as video surveillance cameras, access control readers and alarms panels are IoT devices. These devices are small computers that run software and that may contain cybersecurity vulnerabilities that can be exploited by cyber criminals as a beachhead for all kinds of malicious actions. And that is a big problem for the physical security industry.

The attacks against IoT devices are increasingly affecting enterprises. A new report from IDC highlighted that 46 percent of organisations have experienced a breach or security incident associated with IoT security – and 70 percent of those companies reported that the IoT security incident was costlier than a traditional breach. In this era, you simply cannot afford to take any risks when it comes to protecting your physical security system against cyber-threats.

Unfortunately, people are the weakest link when it comes to cybersecurity breaches. Employees not changing default passwords on IoT devices is an easy way for opportunistic cyber-criminals to gain access to your system. Brute force attacks consist of criminals guessing passwords, packet sniffing captures network traffic and man-in-the-middle attacks eavesdrop on communications between two systems, using the gained information to their advantage. Most physical security solutions are a work in progress with new devices being added to expand the system or to replace outdated or broken products. The process of adding new equipment – perhaps from a different manufacturer with less secure standards – is another opportunity for a vulnerability.

One of the most important ways to combat these types of threats is with a strategic plan. Companies must develop training and educate their workforce as to the importance of cyber hygiene and the diligence in adhering to company policy. Choosing a systems integrator that recommends only the most trusted manufacturers and emphasises the importance of cybersecurity is a good start. Once you have strategised and invested in a good cybersecurity strategy to protect your physical security investment, it is important to always remain vigilant.

The report found that 42 percent of respondents identified access control as a strategic technology in 2021 and 37 percent said the same about video analytics.

In the new digital age, organisations of every type and size are looking to deploy intelligence-based tools to give their security teams a clearer picture of what is happening in their environment. In order to improve and plan for a changing world, they want to have access to as much intelligence as possible. Rather than implementing a new information gathering system, many are looking to utilise the data already being collected by their physical security systems.

It is vital to interpret this data and identify trends, and that's where video analytics comes in. In general, analytics tools take large amounts of unstructured data and structure it to allow you to unlock its value and make more informed business decisions. When you are able to correlate and extract information, you can gain a wide range of insight into your business and environment.

Video analytics, powered by the advances in computing power, has evolved considerably to extract very reliable and powerful data from video streams. This is already having a huge impact in several major vertical sectors, including airports. For instance, video analytics is a great tool for understanding how long people stand in security lines, where roadblocks occur and where people gather. With this information, airports can optimise their staffing, reduce known congestion sites and inform passengers where they should go and how long they can expect to wait in security lines. This will allow people to move through lines and checkpoints as quickly as possible, which will not only enhance public safety but result in a direct increase in the revenue generated by duty-free shopping.

46% OF ORGANISATIONS HAVE EXPERIENCED A SECURITY INCIDENT ASSOCIATED WITH IOT

Upgrading modern access control solutions will further strengthen site security and help physical security teams reach new goals in the new normal. As workplaces reopen there will be an increased need to restrict and regulate who can gain entry to different locations or assets and control the movement of people. A modern access control solution can effectively manage every individual within a facility, granting them access to or egress from a building, as well as managing their movements within the building itself.

Moreover, access control has rapidly evolved into more than just keeping the wrong people out of buildings. That is why more businesses are starting to manage identities instead of just keyholders. Identities are digital profiles for every person that comes into contact with your organisation's ecosystem. These profiles can include many attributes such as company role, pay grade, seniority, qualifications, accreditations and more.

By using an identity and access management system, an organisation can automatically assign employee rights to buildings. This eliminates the resource-draining tasks of requesting and granting permissions while ensuring compliance standards are being met.

While physical security departments have traditionally been slower to adopt the cloud, the situation is now rapidly changing. As online usage and remote work have spiked, there has been an increased shift to accelerate digital transformation. Pre-pandemic, just 37 percent of respondents identified as well underway in their adoption of cloud or hybrid cloud infrastructure for physical security. However, almost two thirds (64 percent) reported the pandemic as having somewhat (51 percent) or greatly (12.5 percent) accelerated their cloud strategy in relation to physical security.

This is encouraging as including cloud in all or part of a physical security deployment can positively contribute to an organisation's cybersecurity stance. Cloud services typically have cyber security features, monitoring and updates built-in, ensuring implementations have

policies, controls, procedures and technologies that work together to protect the system and, by extension, the entire network.

Moreover, there are many other reasons why more businesses are turning to the cloud. By incorporating a cloud-based model, businesses of any size can reduce investment in new hardware and easily scale computing and storage resources to facilitate physical security at locations across the globe.

IN 2021 IT IS PREDICTED THAT A CYBER-ATTACK WILL BE REPORTED EVERY 11 SECONDS

Organisations can easily stay connected and share data across departments and locations, which can aid investigations by allowing different organisations to securely collect, manage and share video evidence and other relevant case information from one simple cloud-based application. Moreover, it can improve business marketing and sales functions with powerful business intelligence and can improve the bottom line for system integrators looking to add recurring revenue streams.

In the midst of the short-term chaos, it could have been tempting to shelve longer term decisions related to the evolution of an organisation's security infrastructure. With remote work here to stay, the financial and resilience benefits of cloud versus on-premises deployments are being closely evaluated. Looking ahead businesses should continue to expand their cloud adoption and it is imperative physical security capabilities evolve at the same pace.

The security industry has been challenged in unprecedented ways during the pandemic and security professionals were pulled into the forefront, showing extraordinary resilience and resourcefulness. This crisis, however, has given the industry an opportunity to redefine its role and value proposition. By tapping into highly intelligent security features such as video analytics and working closely with IT counterparts to mitigate against cyber-attacks, security leaders are showing that physical security investments are not just a cost of doing business, but a true strategic value-add to the organisations ●

Georges Tannous is the current Director of Global Partnerships & EMEA Marketing at Genetec. He is an experienced Leader in Global Strategy with a proven track record in Partnership Management and Strategic Sourcing within the technology industry.

People are the weakest link when it comes to cybersecurity breaches