Picture credit: AXIS Communications

MINIMISING RISK

Andrea Sorri *reports on the importance of tackling cybersecurity risks in smart cities*

Many organisations around the globe have security cameras installed to increase safety, security and often also efficiency of processes. From schools to hospitals to businesses and more, surveillance cameras are monitoring people, buildings, and public spaces. Unfortunately, network-connected surveillance cameras have become the focus for attack by extremely organised, technically proficient and well-resourced cyber criminals. The consequences of an attack are potentially devastating.

If cyber criminals gained access to the live video footage of hundreds of thousands of security cameras, it would effectively allow the attackers to spy on the affected organisations and the people within them. It would leave people at the establishments feeling worried about their safety and the privacy of their data, and the organisations themselves concerned about potential corporate espionage. These kinds of cyberattacks aren't created in the imagination of a Hollywood movie or novelist, they're happening today and aren't isolated cases.

Whether looking to cause disruption or extract a ransom, cyberattacks are growing in numbers and in sophistication and smart city infrastructure has become a popular target. A key reason is that the unique set-up of a smart city provides numerous potential entry points – the success of these types of cities relies on an increasingly interconnected network of Internet of Things (IoT) devices such as connected sensors, lights, surveillance cameras and meters to collect, share and analyse data.

The data from these is being used to optimise and streamline services, infrastructure, public utilities and other operations. While the common rule is, the more connected IoT devices providing their data, the better the outcome, it also means more network entry points that need securing. And with the growth in smart cities comes an associated growth in risk.

Different stakeholders in a smart city should ideally join forces so that the security chain is as strong as possible

It is reported that governments have been investing £124-billion over the past year in smart city initiatives globally and according to the GSMA, an industry organisation that represents the interests of mobile network operators across the world, the number of IoT devices is expected to grow to £18.1-billion by 2025. Ensuring that all these touchpoints of the network in a smart city are cybersecure is a challenge and requires an advanced cybersecurity strategy – on both a physical and electronic level.

THE RIGHT MIX

The reason why the 'attack surface' of a smart city's infrastructure is increasing almost exponentially, as more IoT devices are being added to the network and more separate systems become integrated, doesn't lie in the transformation per se. It comes through a mixture of outdated technologies, poor control and maintenance of connected devices and a lack of a digital transformation and security strategies.

It's crucial for municipal authorities and operators to adjust to the new networked urban landscape and set the right priorities. The scenario described earlier, and which reflects aspects of real cases, gives an insight into the risks that a successful cybersecurity breach can pose to a smart city, particularly when targeting critical infrastructure. While the implications clearly depend on the size and circumstances of the attack, the consequences in a smart city would be chaos in the 'best' case scenario and disruption or even loss of life in the worst.

An example for one of these large-scale impacts (aka worst-case scenarios) that posed a genuine security risk for the city and its residents, was a ransomware attack on the majority of police surveillance cameras in Washington DC. The devices had to be rebooted to function again, leaving the system offline for four days. The police had been using the surveillance system to ensure public safety and security, for example in rapid response to incidents and by investigating criminal cases with material evidence from the video footage. The implications of these systems being rendered inoperable was potentially disastrous.

There is also the aspect of reputational damage and fines. If a city's surveillance system was attacked, the chances that people trust these solutions again are decreased. Plus, regulations like the General Data Protection Regulation (GDPR) make the protection of data a legal requirement, which can result in fines if the terms aren't met and unauthorised third-parties are allowed access to personally identifiable information (PII).

The key principles that smart city authorities need to apply to avoid situations like the above and to achieve a successful security approach are consistent for both physical security systems and cybersecurity: the identification and classification of a smart city's assets and resources and understanding what needs protection; the identification of plausible threats and vulnerabilities that these threats may exploit; and an analysis of the consequences/risks of such an attack.

Protecting cities from cyberattacks has two levels: on the one side it's essential to ensure as many IoT devices and potential entry points that are connected in a smart city's network are as secure as possible. This aspect of is a shared responsibility between all stakeholders: users, organisations, manufacturers and integrators.

But we shouldn't just think about cybercriminals as acting remotely - often they are aided by those with physical access. Physical security systems therefore play an important role. Video surveillance and access control solutions help to keep crucial physical assets, facilities and control rooms secure from intruders (and even disgruntled employees) who could use physical access as a route to infiltrate the network.

As sophisticated as cyber criminals are nowadays, the IT experts responsible for cybersecurity haven't been sitting around twiddling their thumbs. The cybersecurity measures are being improved on a constant basis. It is often still necessary or advantageous for the attackers to find a physical touchpoint to the network. Data centres and important control rooms are attractive targets as once infiltrated, criminals can potentially move through the network to disrupt critical infrastructure and processes within a smart city. Thus, deploying a layered protection at these locations is key.

CYBERATTACKS ARE GROWING, AND SMART CITY INFRASTRUCTURE IS A POPULAR TARGET

Hence, physical security – eg in the shape of video surveillance – can be the solution to protect these assets and shield the network from a cyberattack by preventing unauthorised people from accessing the facilities.

This starts with perimeter protection, for example, with the help of radar and audio speakers. Once an alert is triggered, they can play live or pre-recorded messages to deter an intruder. Access control solutions that combine video verification with access credentials through mobile phones or cards can be set up to only grant selected and authorised individuals access to the respective buildings.

Within the critical rooms – for instance the server room in a control centre – installing high-resolution cameras programmed to automatically pan and zoom when specific server cabinet doors are unlocked or opened can help to prevent the implanting of malware or spyware, which would effectively give cybercriminals access and control over the system.

While physical security of key data management points plays an important role, it's even more essential to ensure that these physical devices and touchpoints themselves are as cybersecure as possible across the whole supply chain, particularly as many IoT devices often have no built-in security. That requires understanding the vulnerabilities of a network; if operators aren't aware of potential cyber vulnerabilities, threats and issues, the prevention of these threats becomes challenging (if not impossible).

In previous cases, the attackers have gained access to the system after finding the password for one of the administrator's system accounts, which was, for instance, accessible on an internal service that had become exposed to the internet. It's an example of the human error creating a cybersecurity risk and it's only one of several aspects that can create a vulnerability for an interconnected system. Often the vulnerable links

▶

are created through poor 'cyber hygiene' of the network, which can roughly be separated in three main factors:

A lack of alignment between security and IT: if the teams have different understandings of the security protocols or processes, the risk of breaches increases.

> IT IS STILL NECESSARY FOR CYBER ATTACKERS TO FIND A PHYSICAL TOUCHPOINT TO THE NETWORK

Failing to put in place and follow IT security policies: many cybersecurity issues have their origin in lapses in security protocols or human errors. These can arise if operators in smart cities haven't clearly defined the requirements to secure the IoT devices and the network or if network users aren't following the procedures that are in place.

Having no device lifecycle management and proactive maintenance in place: systems that are not well maintained, updated and cared for provide a higher risk of becoming the target of a cyberattack. Thus, installing updates when they're released and staying informed about security controls for services and devices is key. In a city with thousands of connected devices, such as air sensors, street lights or cameras, it's critical that these upgrades can be performed in bulk, rather than manually.

The solution is to find the optimal way of merging the best practices of both the physical security world with the best practices of a traditional IT domain without introducing new cybersecurity vulnerabilities for other components in the converged system. A converged security approach breaks down silos and empowers different teams to collaborate towards a common goal. Cybersecurity is a shared responsibility, meaning the different stakeholders in a smart city should ideally join forces so that the security chain is as strong as possible.

Integrators, installers and distributors need to be transparent about the origin of the equipment and make sure the installed devices are patched with the most recent updates. Device manufacturers are responsible for hard coded passwords and that the devices don't have a backdoor, which allows hackers to enter the system easily. Plus, they should be informing partners and channels if a vulnerability is detected. This information usually comes from the researchers, who typically inform the manufacturer and give them a chance to fix the issue before making it public (unless it's a critical vulnerability).

It's not only the number of smart cities and cyberattacks that's growing, it's also the level of sophistication on both sides. Smart cities will incorporate increasingly advanced technologies and criminals will upgrade their approaches accordingly.

Therefore, it's cities and operators that have to think about appropriate steps now, ensuring that a foundation for cybersecurity is created that can keep IoT devices and network end points secure and withstand the future.

The task is never completed, and it is crucial to understand that cybersecurity is all about hard work and diligence every day. Comprehending and detecting potential threats is the basis and working with an ecosystem of partners that work closely together (and towards the same goal) is critical ●

Andrea Sorri, Segment Development Manager Smart Cities EMEA at Axis Communications, is a 20-year veteran in the company and has created and implemented the Smart Cites strategy for Axis. He has held various positions such as Global Business Development Director, Regional Training and Engineering Manager and Country Manager.

Video surveillance solutions help to keep crucial physical assets secure from intruders looking to infiltrate the network

Picture credit: AXIS Communications