THE SMART APPROACH

Nick Smith *reports on what it takes to make 'smart enough' cities a reality*

In 2020, the research firm IDC forecast global spending on smart city initiatives would total nearly $124 billion. Yet it also predicted that 10 to 30 percent of smart city IoT projects would fail as a result of poorly organised frameworks.

From a security perspective, more and more cities are trying to leverage data and data sources in the hopes of becoming 'smart'. So, what separates those that succeed from those that fail? Here we outline some of the starting principles that we believe help municipalities to succeed against clear objectives.

Firstly, many organisations actually fall at the first hurdle, as their strategy is wrong from the outset. It goes without saying that technological advancement is pivotal to the realisation of a smart city. Yet, projects should start with a clear definition of the issues that need solving. Each city is idiosyncratic in its own ways and has its own unique challenges. Any stakeholder that takes a top-down approach that fails to consider these issues is almost doomed to fail.

The projects that tend to be most transformative instead tend to begin through community consultation that prioritises the issues that need to be tackled, defines clear actionable goals and outlines specific measurable ways in which members of the community can benefit. Technology can then be considered not as an end in itself, but as a means of achieving the desired innovation. It helps to crystallise which technologies are crucial to the outcome and which may be being deployed just for the sake of it.

SHARING AND SCALING

The key to building solutions from the ground-up in this manner is for it to be underpinned by an open-architecture, unified platform that allows for the requisite data sharing and scalability. It allows maximum scope to evolve and grow in line with community needs and for stakeholders to continue to respond to emerging challenges and adapt accordingly.

Cities are made up of a diverse and complex mix of independent institutions, ecosystems and infrastructure, but getting these disparate components to work cooperatively can be a huge obstacle. Breaking down siloes is perhaps the most fundamental aspect of a successful smart city initiative. Data is the lifeblood of the modern world, and smart city technologies fundamentally rely on the free movement of data between their many assets and sensors to function. Initiatives can therefore only succeed when data is openly shared across jurisdictions – public and private – in ways that better serve the needs of the community as a whole.

To put this in context, in 2016, the city of Detroit managed to curb its violent crime rate by 50 percent with 'Project Greenlight'. An analysis of crime patterns in the city revealed nearly a quarter of violent crimes were happening within 500 feet of a petrol station after 10pm. It therefore launched an opt-in initiative that enabled registered local businesses to share real-time footage from their security cameras with the Detroit Police Department. The result was a true win-win. The police department gained an enhanced level of camera coverage for these crime hotspots and businesses gained the peace of mind that police could quickly respond should an incident occur.

ANPR AND CCTV FEEDING INTO VMS SYSTEMS ARE KEY TO FLAGGING ALERTS IN REAL-TIME

This unprecedented collaboration improved crime rates by shortening response times, expediting the evidence gathering process and acting as a deterrent to any would-be criminals. Security aside, it also improved the bottom-line of participating local businesses as customers recognised they were a safe place to shop. At its inception, the project was only active in a few locations that were identified as crime hotspots, most of which were petrol stations. However, there are now hundreds of different Greenlight locations across central Detroit. The project illustrates that seemingly simple changes can have a powerful and tangible effect on crime when implemented on a large scale. This initiative also shows that a top-down approach would have been very different proposition, as it would have been much more expensive, much less effective and its unlikely there would be the same level of collaboration between public and private organisations.

Movement is another key piece in the smart city jigsaw, and you only have to look at how people travel has changed over the past five years, with mobility as a service (MaaS) taking off and moving us towards a more digital approach. With the ever-increasing number of vehicles on the road, it's important for those trying to enforce the rules – transport authorities and law enforcement in the most serious cases – to work together to spot incidents worthy of response. Automatic number plate recognition (ANPR) and safety cameras feeding into VMS systems will be key to this, helping to flag alerts in real-time. For instance, if a traffic accident occurs, a resilient smart city uses technology to minimise the impact by detecting the incident in real-time, dispatching emergency services and rerouting traffic automatically – to create a much more comprehensive, automated response.

Smart cities rely on the free movement of data between their many assets and sensors to function properly

Smart cities promise so much, yet if implemented incorrectly can leave entire swathes of cities vulnerable. Over the last few years, we've seen the rapid proliferation of cyber-attacks, which likely won't abate anytime soon. But perhaps most concerning of all is that many of the most high-profile incidents have been state-sponsored events, which blur the lines between run-of-the-mill criminals and international espionage. A 2020 report from Microsoft found that activity from state-sponsored groups in Russia, China, Iran and North Korea is on the rise. These well-funded organisations are becoming more sophisticated and therefore able to target organisations of any size. In fact, it was only in December 2020 when Russian hackers were able to compromise software used by The Pentagon, intelligence agencies, nuclear labs and Fortune 500 companies across the US, and the true scale of the damage is still being assessed.

In the context of smart cities, these kinds of attacks could target a city's key infrastructure, such as the traffic management system, causing major disruption and potential for loss of life. New technologies, such as the long-awaited arrival of 5G, will no doubt bring increased levels of connectivity,

Picture credit: iStock

but each new connection brings another possible avenue of attack. When cybersecurity is prioritised and maintained from the outset it is very possible to benefit from IoT technologies with strong protections against cyber-attack.

An often-overlooked cybersecurity risk is that of deploying IoT technologies from high-risk vendors, especially in the public sector. The security camera and IoT device manufacturers Hikvision and Dahua are both subject to US federal bans, yet are widely deployed within Europe.

MANY ORGANISATIONS FALL AT THE FIRST HURDLE, AS THEIR STRATEGY IS WRONG FROM THE OUTSET

In fact, the US blacklisting has resulted in these companies redirecting their resources towards the European market, offering state-of-the-art equipment at incredibly low prices. As a result, it was recently revealed that over half of London's councils use security cameras from companies subject to US federal government bans despite these devices having been widely shown to present considerable risks.

This pricing strategy can be too tempting for cash-strapped procurement teams to ignore, but it prompts the question – if profit isn't the motive, what is? There are also the additional financial risks to consider. For instance, if the UK and Europe were to follow suit and impose bans on certain suppliers, as we've already seen with Huawei 5G infrastructure, it could leave organisations with no option but to rip out and replace deployed cameras well before they reach end-of-life. Instantly eliminating any cost savings and requiring them to pay twice.

Although COVID-19 has put many initiatives into stasis over the last year, hopefully 2021 will allow for projects to pick up where they left off. And of the many lessons learnt over the course of the pandemic, none have been as stark as technology's ability to tackle increasingly complex issues. South Korea has been hailed for its response to the virus, with many attributing the country's success down to its use of advanced technology to contain the spread. So perhaps incidents like this, and the clear value these technologies provide, will prove the catalyst for a greater push towards making smart cities a reality in the coming year.

Smart cities are within touching distance, the technology is out there and ready to use, but it's about bringing it all together, deploying it intelligently and adapting it to the local needs of a city. Crucially, all of this must be underpinned by a comprehensive cybersecurity strategy to protect cities from the myriad of evolving threats. Similarly, organisations must begin to operate with a new level of scrutiny with the suppliers they choose to do business with and the technologies that they deploy ●

Nick Smith is UK Regional Manager at Genetec

Smart cities promise so much, but if implemented incorrectly can leave entire swathes of infrastructure vulnerable