SMART CITIES AREN'T SMART WITHOUT TRUST

Innovation can bring astounding benefits but anything digital can be hacked, and anything connected to it then becomes vulnerable

BY **TONY GAUNT**

PHOTO: ISTOCK.COM/SINOLOGY

SINGAPORE'S Smart Nation initiative is on its way towards transforming how its inhabitants live, work and play as business and government organisations launch initiatives in preparation for Internet of Things (IoT) and the newly-connected world.

So far, we have seen Singapore initiate SingPass Mobile, which enables people to log in to government services using fingerprint authentication instead of passwords.

Smart Nation is also facilitating a safer living environment for Singaporeans. A new Personal Alert Button is also in the trial phase for older citizens to call for help, and other smart sensors are being developed to facilitate an improvement in their standard of living.

As this initiative develops to make more of these advancements possible, S Iswaran, Minister for Communications and Information, has expressed how critical the adoption of 5G technology and networks will be to Singapore's digital economy.

BEYOND NEW FANCY INNOVATIONS

As the above examples show, the smart city environments being developed can improve our safety, but the necessary increases in connectivity and reliance on new technology such as 5G and edge computing could also threaten it. 5G is critical to managing the sheer quantity of sensors and their data volumes.

Aggregating hundreds or thousands of sensors at the hub, which in turn has to access multiple external sources such as weather, events, planned roadwork and accidents makes 5G a critical component for the future of smart cities.

Before long, we will be leaning on digital health, autonomous cars, robots and more. This is innovation that could bring astounding benefits to our lives, but if there is one thing we have learnt, it is that anything digital can be hacked – including network edge data centres or other critical infrastructures – and anything connected to it then becomes vulnerable.

2019 has provided no respite from cybercrimes in Singapore as attacks seem to grow more and more sophisticated every year. We have seen the personal records and medical statuses of patients compromised, raising concerns about the security and safety of the nation's citizen data.

Vertiv's research shows that around one in five outages can be traced back to security failures such as denial of service (DoS) attacks. As it stands, these are inconveniences at best, financially destructive at worst.

They affect people because their data is compromised, or a digital service that they rely on does not work. For businesses, they carry a sizeable cost – not just financially, but through customer, stakeholder and reputational damage.

It is bad news all around, and the risk gets worse the more we rely on IoT-enabled devices in our daily lives and the more businesses and government invest in technology. This begs the question: what happens if a robot surgeon gets hacked? Or an autonomous car? Or the smart traffic system connected to the autonomous vehicle?

With so many things connected in our smart cities, cyber criminals will have new access points to infiltrate. To avoid such life-threatening disasters, we need to get smart in securing the critical infrastructure that is supporting smart city applications.

This will include modular data centres and other smaller "network edge" infrastructure – which are vital to security, maximising speed and minimising latency in these services – as well as traditional core data centres and cloud environments running services and transmitting data between devices.

If these systems are vulnerable, our smart cities – and potentially our lives – will be too.

SMART CITIES RAISE PRIVACY CONCERNS

While our personal safety must come first, businesses and government organisations developing smart city applications must also be conscious of keeping our data safe.

Whether through breaches or uninvited data sharing, there is a growing sense that people have lost control over their data, and many are questioning why our human right to privacy does not get the respect it deserves.

If data is used in the right way, society can reap the rewards – safety, retail, transport, energy and more can be optimised, and smarter applications within these industries can reduce costs.

CHANGING OUR ATTITUDE TO DATA

But constant breaches and misuse of our data are keeping trust levels low. The mentality of how we approach data is off – for example, we are forced to "opt out" to keep our data from being used, rather than opting in to enable it.

Taking the European Union's General Data Protection Regulation (GDPR) regulation as an example, it may be time for businesses and government organisations to reverse this and create a more open dialogue about what data they own, what they plan to use it for and why customers should let them.

This, coupled with better security measures to protect our data, will go a long way to regaining people's trust and changing our attitudes to our data being used.

There are other concerns about smart cities that a more open dialogue could help solve – what impact will an increasingly automated society have on jobs? A number of significant job cut announcements have already been made this year, and people have legitimate concerns for their livelihood. The government, communities and individuals need to understand how these concerns will be addressed.

Smart cities have the potential to deliver huge benefits to all of us and enable us to leverage technology in a way that we have not seen before. On the surface, it is about machines connecting with machines; but businesses and government organisations need to remember that the true purpose is to benefit people.

Those people need to feel safe and trust that their data is secure and being used for their benefit – otherwise smart cities will fail, or, at best, be a shadow of what we have dreamt them to be. ■

The writer is senior director of co-location, cloud, and banking, financial services and insurance, Asia, Vertiv