SMART CITY TECHNOLOGY A RISK TO AUSTRALIAN BUSINESSES

The rise of user-friendly 'smart' cities, where many services are automated, networked and online, has put Australian businesses at greater risk of cyber-attack, according to security firm Sapien Cyber.

Chief executive officer Glenn Murray said most businesses recognised the importance of cyber security, with breaches estimated to cost $29 billion each year in Australia and up to US$6 trillion globally. But many overlooked an alarming vulnerability.

"Cyber criminals around the world are exploiting unprotected building management systems to disrupt major businesses and have caused billions of dollars of damage, not to mention the reputational costs of a cyber breach," Mr Murray said.

"We see businesses doing the right thing and investing heavily in IT security to protect their sensitive data and prevent unauthorised access.

"But what they overlook is the risk posed by the systems that control their operational services like lighting, air conditioning, lifts, alarms and building access. Building management systems are the weak link in cyber security."

Mr Murray said criminals with access to a building management system could cause significant physical disruption to a workplace, launch a Distributed Denial of Service (DDoS) attack or extort a business under threat of a DDoS attack.

The building management system could also provide a jump point into more sensitive business IT systems that were otherwise protected from unauthorised access.

"With the development of 'smart' cities, we are seeing the introduction of new technologies for operational services, more networking between them and business IT systems, and greater exposure to the internet," Mr Murray said.

"The increasing convergence of operational technology and IT systems is drawing criminal attention to building management systems as a point of access. Unfortunately, many businesses have little understanding of the scope and complexity of their operational systems and how vulnerable they are to cyber-attack.

"It's crucial businesses are not complacent about their building management systems and that they review them regularly for cyber risks in the same way they analyse their IT systems."

Key examples of cyber breaches through building management systems:

- Hackers used an Internet-connected thermometer in a fish tank in the lobby of a Las Vegas casino to access the casino's database and personal information about its high-roller clients (2017).
- In one of the biggest cyber-attacks reported to date, the credit card details of up to 40 million Target customers in the United States were stolen by criminals who accessed its payments system via a third-party supplier of air conditioning services (2013).
- Security researchers hacked the building management system at Google Australia's Sydney headquarters to draw attention to its vulnerability. They said it was one of thousands of vulnerable building management systems listed on the hacker search engine, Shodan (2013).

Media contact: Carina Tan-Van Baren – ctanvanbaren@canningspurple.com.au, 0414 236 791