

# NEW TECHNOLOGY AND THE RISKS OF CONVENIENCE

Do we fully understand the increased risk profile that comes with new technology?



BY KIERAN DOYLE  
Partner, Wotton + Kearney

EDEN WINOKUR  
Special Counsel, Wotton + Kearney

**T**he 21st century has seen rapid technological advancements across many facets of life. From smart phones and drones to early artificial intelligence and the Internet of Things, technology has the potential to enhance our quality of life in so many different ways. While these technological advancements can provide considerable convenience, are we being sold convenience and innovation over security?

## New technologies

One relatively new form of technology that perhaps demonstrates the concept of convenience over security is smart homes. Like many others, some of the leading technology companies such as Apple, Google, Amazon and Samsung are delving into smart home technologies, which integrate various home devices such as appliances, cameras and alarm sensors to create a tech-savvy futuristic home.

Imagine the trip home in the middle of winter after a long day at work. The house is cold and it takes time for the oven to heat enough to cook dinner. Using a smart home a user could use their mobile phone to turn on the heating and oven while on their way home from work ensuring they walk into a warm house with an oven just the right temperature to start cooking the minute they walk through their front door

opened using facial recognition. Even more advanced smart homes can include fridges which know when the milk is running low triggering an alert to order more milk to be home delivered. The inconvenience of running out of milk is a thing of the past.

Futuristic homes offer some of life's conveniences at your fingertips. However, what is often overlooked is that these same technologies are the ones that can be most vulnerable to attack by cyber criminals. Cybersecurity firm TrendMicro points out that as systems become more complex and have more devices and actions added to its network, the more prone it becomes to cyber-attacks and failures. Too often with new technologies there is a rush to market for first mover advantage in innovation but often what is forgotten is assurance that the smart product also provides sufficient security.

## Cyber attacks

It is now trite to say that companies and individuals need to take cyber risk seriously. The statistics are staggering. According to the Australian Criminal Intelligence Commission, by 2019, cybercrime is already costing the Australian economy \$1 billion a year. According to cybersecurity firm Carbon Black, 89 per cent of Australian businesses report that they have experienced some form of cyber-attack in the past 12 months. The most troubling

part about these statistics is that the cost of cybercrime is more than likely going to significantly increase in the coming years.

With smart homes creating a ripe environment for cyber-attacks and cybercrime drastically on the rise, it is important for the insurance industry to consider the types of legal and claim risks that are associated with new technology.

## Legal and claim risks

There are myriad legal and claims risks associated with smart homes. Our voice-controlled command centre creates various data protection and privacy risks. The online smart fridge sending home delivery orders might not contain sufficient software security making it vulnerable to attack by cyber criminals seeking to get into your home network, which could lead to personal data theft and risks such as identity fraud. If a cybercriminal managed to take control of your smart home, could it use a surge of electricity to destroy an appliance and create a general liability or product risk? Or is control of your home Wi-Fi network the gateway to ransomware or data theft on the office network as more businesses shift towards agile working?

The term *silent cyber*, the exposure to cyber incidents contained in traditional policies, is getting a lot of attention in the property and liability insurance markets. However, as technology moves closer to total domination of our everyday lives, new cyber risks and issues for the insurance industry emerge creating silent cyber issues for the industry to consider across all insurance policy types. So the question begs – should silent cyber be excluded in traditional policies or is it the case that traditional risks to perils are becoming redundant? Only time will tell. ■

ARE WE BEING SOLD  
CONVENIENCE AND  
INNOVATION OVER  
SECURITY?