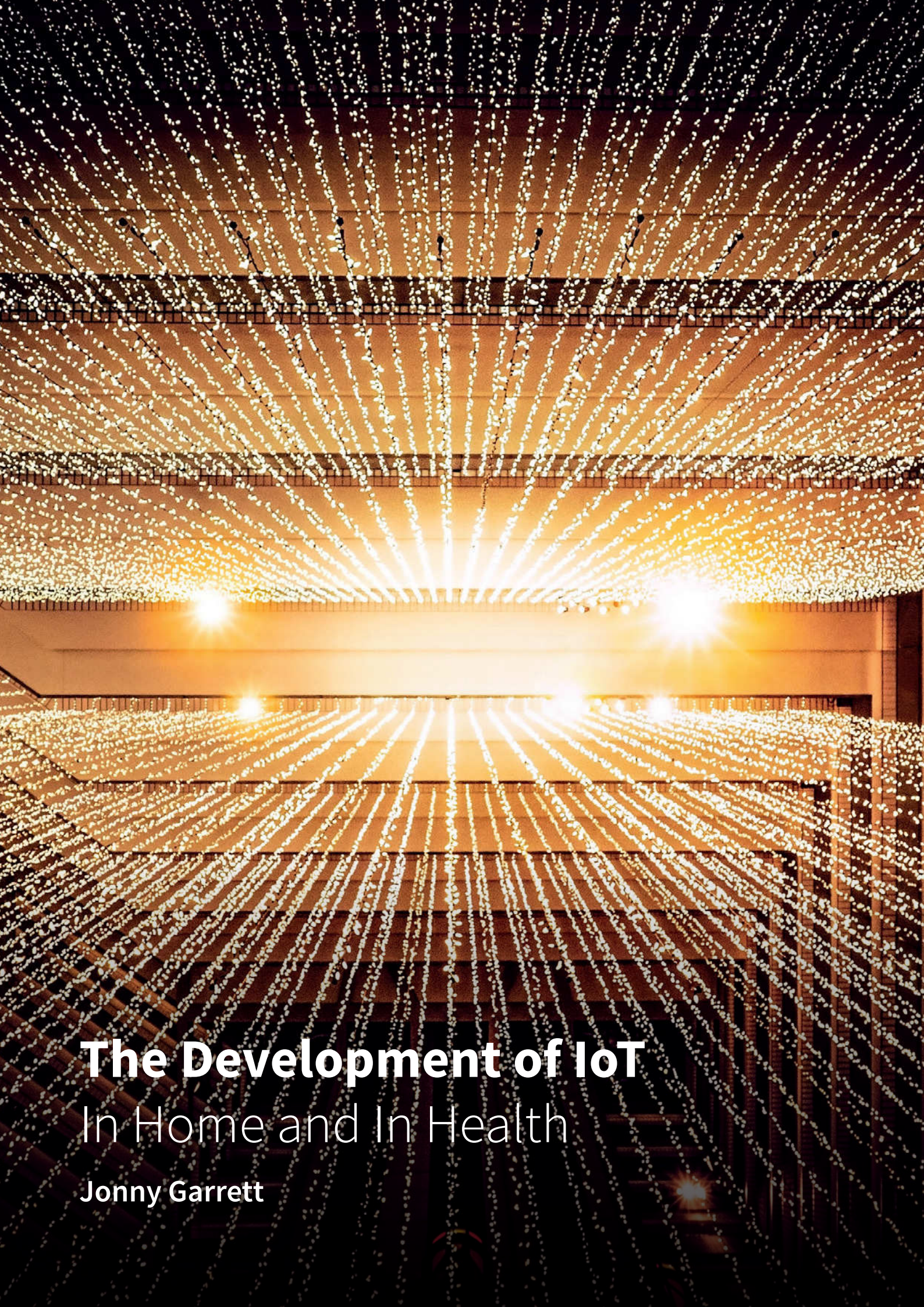


# The Development of IoT

## In Home and In Health

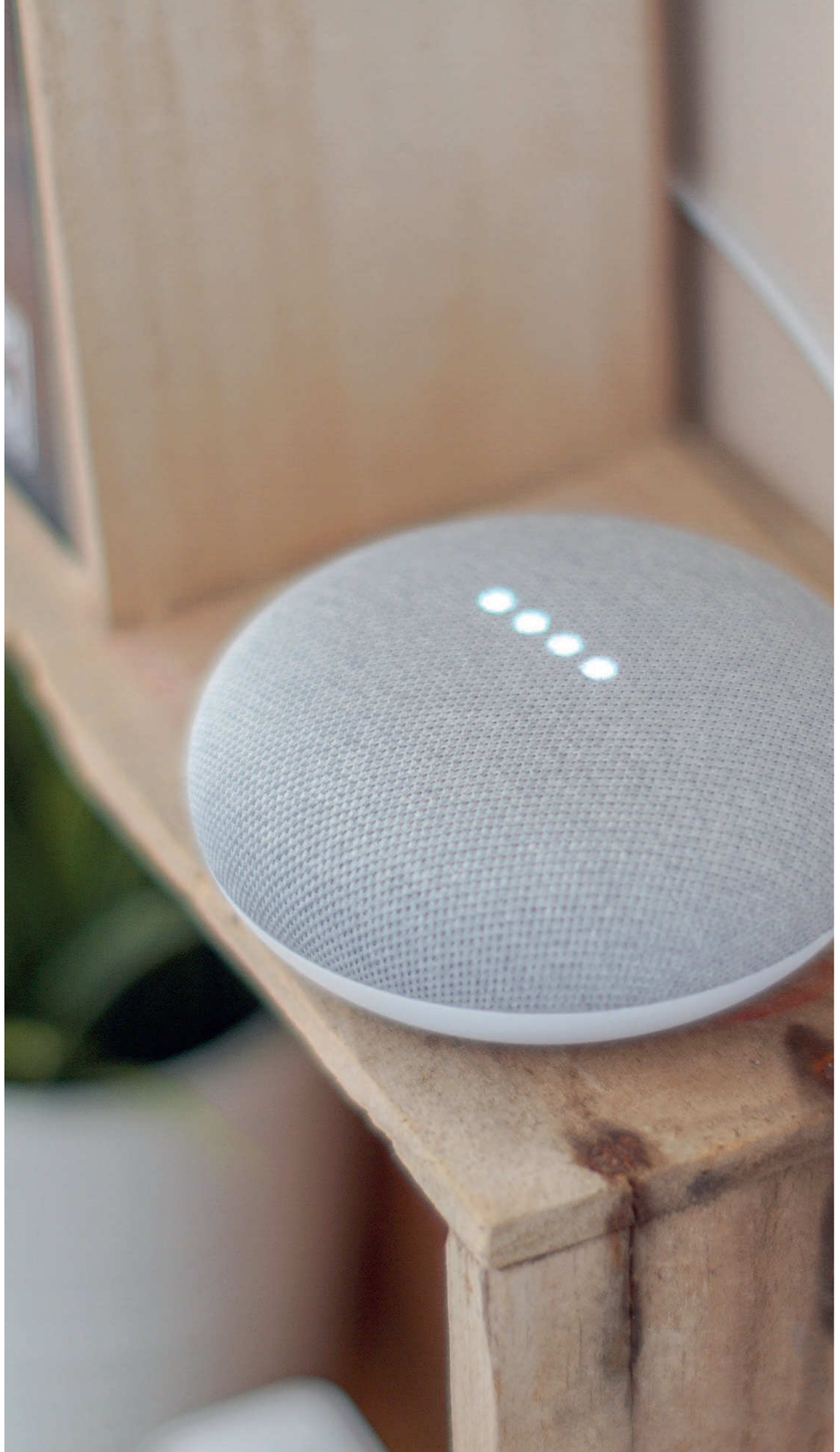
**Jonny Garrett**

# Contents

The use of internet-connected devices in our daily lives has exploded in recent years and shows no signs of slowing down. From smart phones measuring the number of calories burnt in a day, to smart homes reacting to the environment, to Wi-Fi coffee machines automatically ordering coffee when required, Internet of Things (IoT) technology is providing new and innovative ways of making our lives more interactive.

Along with the everyday devices mentioned above, there has been a drive to use IoT to assist with the health and safety of the general population. “Internet of Medical Things” is now its own category within IoT. It promises to change how and where medical care is delivered, and how patient health is monitored.

But as technology plays a growing role in our personal lives and medical care, how will technology companies use and protect our data? How can we all manage these risks and others?



# Smart Home Technology

The amount of smart home technology available and integrated in houses has been on the increase over the last five years. A recent PWC survey estimates £10.8 billion was spent on smart home devices last year in the UK.

The availability of internet-connected plug-in devices has made smart home technology commonplace in homes throughout the UK. A June 2019 report from TechUK found that 31 percent of consumers aged 35-44 own three or more smart home devices.

To date, residential use of IoT technology has commonly included lighting, heating, entertainment and security systems. For the most part, the installation of this technology has required the help of a custom installer, though that is evolving: The rapid development of personalised technology has made it possible for consumers to spend less than £50 on smart light bulbs they can install themselves and control from their smart phone. Although plug-and-play technology is reducing the requirement for custom installers to integrate IoT into people’s homes, it is also normalising the use of residential smart tech, so there is still a need for professional custom installers within this growing market.

New and established brands are increasing the availability of smart home technology. Hive and Nest, which provide heating controls, as well as Ring doorbells, which allow residents to use smartphone technology to see who is at the door, are now well known brands. Huge companies like Amazon and Apple have developed smart home technology such as the Echo and HomePod. As these global companies enter the space and use their resources to compete, smart home technology will continue to develop to meet the demands and expectations of the public.

# Medical care

IoT is taking an increasingly important role in medical care. Most of us have already had some exposure to the Internet of Medical Things (IoMT), whether through automated appointment scheduling or the use of smart watches which collect data on lifestyle characteristics.

However, IoMT has the potential for greater applications. Goldman Sachs reported that IoT, used correctly, could save the United States over $300 billion in annual healthcare expenditures.

Alder Hey Children's Hospital in Liverpool is one example of how the latest IoMT can benefit staff and patients. The hospital holds a vast amount of patient information and traditionally the way patients gain access to the information they need is via a medical professional, according to Iain Hennessey, Clinical Director at Alder Hay. However, he said when a doctor or nurse has to access the information and then relay it to the person who needs it, this creates more work for staff. Patients have to wait until someone is available to help, which causes a delay in receiving the information. At Alder Hey, however, patients are able to use interactive systems to get this information directly, quickly and without staff involvement.

# Medical Care In the Home

An ageing population, combined with developments in smart home and medical care technology, is creating potential for IoT to assist healthcare at home. There are a number of benefits: Receiving medical support at home rather than spending time in a medical facility is not only better for the patient's wellbeing but is also more cost effective. Further, the ability to continually monitor an individual will allow potentially life-threatening issues to be discovered earlier and result in a much better chance of successful treatment.

Medical treatment in the home also allows for treatment over a longer period of time. Considering the finite amount of space in hospitals, coupled with government-driven targets surrounding waiting times, the amount of time a patient spends with a medical professional is often extremely limited. If the diagnosis, monitoring and ongoing support of a patient can be provided as much as possible from home, this should benefit patient waiting times and make space more available for individuals who need to see doctors.

So what kinds of IoT technology can help in the challenge to provide medical care at home?

For individuals who require domiciliary care, sensor technology can be used to provide alerts about abnormal activities, such as when an Alzheimer's disease patient misses meals, for example. IoT sensors can connect to a number of different home appliances and then measure everything from a person's sleep activity to body waste to infections. This data can be used to identify the early signs of illnesses such as cancer.

Remote patient monitoring for patients with heart problems and diabetes can be particularly important. By reducing the requirement for people to have to physically visit a hospital for monitoring, hospitals decrease expense and patient waiting times.

Behaviour modification technology addresses certain health characteristics with individuals, such as high cholesterol. The technology provides advice on diet and daily routines in order to prevent health problems in the future.

If someone has a medical issue, telemedicine makes it possible to address the problem remotely from the person's home. Time is saved for the patient who does not need to book an appointment and travel to see a doctor and then visit a pharmacy to deliver a prescription.  All in all, IoT technology can help patient information to be collected and evaluated more quickly and efficiently along with their medicine.

# Challenges with IoT

TAt a time when there are so many benefits to using IoT technology, the security of IoT data is under increasing scrutiny. High-profile data breaches at such companies as British Airways and TalkTalk, along with the controversy about data use by Cambridge Analytica, has led to increased scepticism and concern about how personal information is being used.

Medical data is particularly sensitive given the language used in the General Data Protection Regulation (GDPR):

1. “Data concerning health” is defined by the GDPR as “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.”
2. “Genetic data” is defined by the GDPR as “personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.”
3. “Biometric data” is “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.”

The broad range of medical data being collected, along with healthcare organisations’ need to maintain patient records over a long period of time, can make medical information vulnerable to security breaches.

Internet connectivity breaches of general IoT devices have demonstrated the risk that often accompanies the benefit of the technology. Ethical hackers have shown how easy it is to gain access to all the data going through a household connection to the internet by breaching a seemingly novelty device such as a Wi-Fi kettle that can be controlled remotely. Devices like this, when developed with more of a focus on the product than on its connectivity, may offer poor security protection.

As medical technology enters the home, care must be taken to protect the data being shared between devices. Recent cyber attacks have shown that the stakes are high: The 2017 WannaCry ransomware attack, for example, cost the National Health Service an estimated £92m. Measures to prevent these types of attacks and the impact they can have must be actioned and developed as the technology evolves.

# How to mitigate issues

The first line of defence is the IoT products themselves. They need to be designed and manufactured with cyber security in mind. This may require updates to be made to the security on products just as computer systems require updates to improve security as techniques used by hackers evolve.

It can also help to consult an experienced professional custom installer who can provide expert advice on products. The Custom Electronic Design and Installation Association (CEDIA), for whom Flint is an affiliate insurance broker, have many custom installers listed on their website. CEDIA requires members to carry professional indemnity insurance prior to achieving membership, which can demonstrate that the installer has been educated about how to minimise the likelihood of risks (cyber and otherwise) that may arise from IoT technology.

After a breach, the correct measures must be performed to reduce the impact of the incident. If it is a company which has been breached, there are legal obligations to fulfil that require time and resources, as well as the involvement of public regulations works to protect the entity's brand. Having the correct cyber insurance cover will assist with these requirements by providing the resources and, possibly more importantly, the expertise to manage and recover from a cyber breach.

Like all insurance, cover should form part of the overall risk management strategy. As technology develops, so will the techniques for breaching these systems. Both the risk management strategy and the insurance must continually react to these changes.

Although there are some challenges with IoT, it can benefit society, particularly in protecting the health and safety of the population. As new products enter the market and make IoT technology more accessible to consumers, the security measures needed to keep data safe must continue to develop. The insurance industry must evolve as well; whilst there have been recent developments in commercial packages, particularly in cyber insurance, to deal with the increase in security concerns and new GDPR protocols, the option to have these protections on household personal policies is still limited.

This paper was written as part of the Travelers Techsure Academy 2019. Techsure Academy provides a unique training experience for insurance brokers wishing to develop and refine their tech knowledge and who are looking to increasingly specialise in this exciting and evolving sector. For more information, visit travelers.co.uk/techsureacademy