Insurance Times

12 February 2021

Amazon's Ring incidences expose cyber insurance inconsistencies and new IoT risks

Insurance Times explores the emerging risks from Internet of Things' devices, as well as how it could be opportunity for brokers and insurers

Inconsistencies in cyber insurance cover have been exposed after a series of alleged security flaws were identified in Amazon's smart home doorbell product – Ring.

This was the view of chief executive, Daniel Lloyd-John at Broadway Insurance Brokers, who told *Insurance Times*: "It is an emerging threat and one which the industry certainly needs to come to terms with.

"An increasing number of households in the UK are connected to the so-called Internet of Things (IoT). That degree of connectivity presents a potential risk of hacking and yet there are few policies available which include provisions to deal with such a problem."

Lloyd-John pointed out that in the US faster adoption of IoT technology has meant that these risks have been addressed in standard cover. But the UK is still behind.

As more people are using smart devices during lockdown and technology is ever evolving, cyber insurers must keep abreast of emerging risks. *Insurance Times* explores how understanding these incidents might help the industry be more prepared to underwrite risk for IoT products, as well as it being a new opportunity for brokers and insurers.

In January, the US Neighbours app for Amazon's Ring allegedly exposed users' personal details, according to the *Daily Mail.* A bug in the smart video doorbell's app led to locations and addresses being leaked, however no "bad acts" have been tied to this.

And in 2019, two incidents occurred, Ring user log-in credentials of more than 3,600 users which included emails, passwords and phone numbers were leaked onto the dark web.

That same year, Amazon's Ring was hit with class action after hackers allegedly infiltrated the cameras' microphones with some users claiming they received death threats and racial slurs.

Security by design

Oliver Brew, CyberCube's head of client success, said the incidents highlighted the need for IoT manufacturers to implement "security by design" processes which is integral to the device.

Speaking about Amazon's Ring, he said: "Additionally, the nature of the invasions of privacy that have been alleged could be taken into account, and if these are deemed to be sufficiently egregious, the terms of service may be overruled.

"Overall, the case reflects some of the challenges in the rapidly growing market for smart IoT devices where privacy and security concerns may be in tension with the potential convenience and attractiveness of connected homes."

Brew explained that the alleged Ring case illustrates some of the challenges for smart home devices without the necessary security.

He warned: "The size of the class could grow, given it appears to include anyone who purchased a Ring device between 2015 and 2019."

Several factors could influence potential liability against Ring, Brew said this could include any existing contractual protections that exist in the terms of use, and whether these are enforceable."

Although he highlighted that the Ring terms of service dated 8 December 2020 included a full waiver of class action rights. This, Brew said: "States that the user may not proceed in a class, consolidated, or representative capacity. This also includes strict limitations of liability amounting to a one-year subscription."

Insurance Times contacted Amazon for comment, the e-commerce giant pointed to its terms and conditions, which states: "You should protect against any risk of loss with the appropriate insurance coverage, and you are responsible for obtaining all insurance coverage you believe is necessary."

Speaking about the security breach for the Neighbours app, a spokesperson for Amazon said: “At Ring, we take customer privacy and security extremely seriously.

“We fixed this issue soon after we became aware of it. We have not identified any evidence of this information being accessed or used maliciously.”

Great challenges

Paul Mang, Guidewire’s chief innovation officer, said: “Innovating our insurance products in light of these new 21st century threats are one of the great challenges for our sector today — and one of the major focus areas for us at Guidewire.”

He highlighted that for consumers, smart camera breaches might be addressed by some personal lines policies under cyber bullying, but previously when breaches of business databases allowed thieves to target out-of-town families, home-owners policies might cover the losses.

Mang warned: “The current risk-transfer situation is not completely satisfactory, however.

“The convenience of modern IoT devices does come with alarming potential risks. The IoT phenomenon represents the convergence of activity sensing, large scale connectivity, and actuation which exposes us to new privacy and physical risks.”

This he said is because potential weaponised devices go beyond simple household gadgets with autonomous vehicles, telemedicine, wellness monitors and work-from-home collaboration tools all unfortunately being concerns.

He added: “As a society, we rely on new technologies to respond to evolving customer needs; the insurance sector will need to develop the risk management solutions, so we can all manage the new exposures that will be associated with these new technologies.”

What is the Internet of Things?

The Internet of Things (IoT) is a network of physical objects “things” that are interrelated and connected by the internet, they can transfer and collect data via this connection without human intervention.

Why should smart home devices with IoT be insured?

Some smart home products that use IoT can also transfer huge volumes of data to providers and third parties in real-time or as a triggered response, this information is often sensitive containing names, addresses and locations. Many smart home devices are controlled using a central app which means they can be targeted by hackers.

So far insurers have used IoT to communicate with customers as well as accelerate underwriting and claims, but management consulting firm, McKinsey highlights that insurers could potentially partner with companies to provide a cross-industry product or service, or by offering a discount with a device.

What kind of smart devices could be insured?

According to Ecclesiastical’s research in collaboration with the Blackstone Consultancy, two thirds of Brits are worried about cyber risks associated with smart home devices. The broker said that this could be an opportunity for brokers, the top devices found in people’s homes were:

- Smart TVs (56%)
- Smart speakers (41%)
- Smart heating systems (20%)
- Smart lighting (17%)
- Smart security camera (12%)

Who is liable?

But the question for IoT device security remains – who is liable?

BLM partner and cyber expert Nick Gibbons pointed out that it is not clear cut. He said: “Claimants will try to claim that a hacking incident is the result of a defect in the product, whereas manufacturers and software providers may argue that the incident occurred because of the manner in which the consumer used and maintained the product.”

Although he stressed that legislation and case law, as with all things cyber, are still playing catch-up with IoT-related issues.

“Ironically, perhaps, the very fact that legal liability is unclear arguably presents an opportunity to insurers, he added.

“Consumers studies and press reports evidence that there is significant concern amongst the general public about the possibility that their smart devices and the data that they collect could be hacked and used by cyber criminals.”

Therefore, Gibbons said if such events do happen, many homeowners do not know who to turn to in a crisis they grapple to comprehend. This is because as the insurance solution for business has involved working with the government and industry to create usable benchmarks.

Meanwhile, Lloyd-John questioned whether a mobile phone or home insurance policy would be triggered if a hacker gained access to a device outside the home.

“Our experience is that an instant, sympathetic and knowledgeable helping hand is what many businesses appreciate most about their cyber insurance when they’ve just been hacked, Gibbons said.

“And just as replacement and repair insurance often comes with a new fridge or cooker, Amazon might think about offering cyber cover like that to the customers of Amazon Ring smart doorbells – can’t go wrong with that, can you?”