STOCK CONNECTION/REX/SHUTTERSTOCK

ARE YOU BEING HACKED BY YOUR KETTLE?

From smart kettles to cars, the new devices helping hackers get their hands on your data may not be the ones you expect. So how can firms protect themselves against a tide of new threats? Catherine Kennedy finds out more

It's not what you'd expect from a kettle. But as we navigate the ever-expanding "internet of things", there are now a multitude of unexpected sources and entry points that can be used to exchange and ultimately hack data. From cars to electrical appliances, attacks via something as seemingly innocuous as a smart kettle are fast becoming the next big threat to cybersecurity.

Worldwide cybersecurity spending increased by 8% in 2018, according to research firm Gartner, reaching a value of $96bn (£74.7bn). The firm predicts that up to 60% of businesses will be using multiple security tools such as data loss prevention, encryption and data-centric audit and protection tools in 2019, compared with just 35% in 2018.

A growing problem

Why then, despite more money being spent on cybersecurity and protection, are attacks on the rise? In April last year, a government-commissioned report revealed that nearly all British firms have been affected by cybercrime, with a jump up in figures year-on-year.

The report revealed that for the 12 months to April 2018, 87% of small firms experienced a breach, up 10% from the previous year, while 93% of large organisations were targeted. The average number of breaches experienced by large organisations increased from 71 to 113, and by small companies from 11 to 17 – a rise of more than 50% compared with the previous year.

At the RICS Commercial Property Conference last November, the director of a UK-based cybersecurity company attributed at least some of this increase to the growing means of accessing company data. There is no doubt that attacks are on the up, and according to Chris Woods, director of CyberQ Group, "that doesn't look likely to change over the next five years".

He added that the problem was simply spiralling faster than companies could keep up: "If you look back to 10 years ago, you had a mobile phone and that was it," he said. "But now you have cars, kettles, TVs – all smart devices which make it easier to gain a foothold inside an organisation."

Add to this the fact that, on average, it takes more than 200 days for companies to realise they've been hacked, as these breaches go unnoticed, and the real estate sector has a serious problem on its hands.

So what can be done?

Woods and Vishvas Nayi, CyberQ Group's cybersecurity consultant, said that awareness was as good a place as any to start, adding that "proper cyber hygiene" would make a big difference. Consistently monitoring for suspicious activity or connections is also key: "On occasion, we've seen connections to, say, North Korea or Russia," said Woods. "That would be something that [the organisation] needs to investigate further."

Supply chain risks

Supply chains can also present unexpected problems, depending on the security of each organisation in the chain. "You're only as strong as your weakest link," said Woods. "You may think that you're secure, but your supply chain may not be as secure as you. It has connections into your organisation."

With threats coming from various angles, cybersecurity measures shouldn't be limited to the workplace. It is becoming increasingly important for people to understand the steps which can be taken towards security at home as well. "People often have the same password for their personal e-mail account and their work e-mail account," Nayi said. "You don't want to be doing that."

Inevitably, cybersecurity has become a constantly changing environment, with the emergence of new security tools being quickly followed by new ways to bypass them. "You're always going to have that cat-and-mouse situation," said Woods. "You don't stop. There's no such thing as 100% security. You have to keep monitoring, improving and looking at how the landscape is going."

It was a fitting end to a conference that kept coming back to the evolution of technology.

Investing in security

Alison Nimmo, chief executive of the Crown Estate, took to the stage earlier in the day to talk of the need to keep up with the pace of change. "It was the dawning realisation that 'we're never going to be experts in this stuff' that has made us start to look for new collaborators and partners on the tech side," she said.

On an innovation breakout panel debate, Simon Prichard, senior partner at Gerald Eve, said that companies need to put their money where their mouth is when it comes to engaging with tech. "We have moved from technology being support to being central," he said. "You've got to substantially up your annual spend on tech to stay in the game. We've done that, and we won't be alone in doing that."

Ultimately, though, many would argue that it comes back to the balance between human and machine. In his keynote address, tech influencer Antony Slumbers said that "in the world of exponential technology, we need to be exponentially human, because human plus machine wins". This is a pertinent comment in relation to cybersecurity, where the need for human monitoring and awareness sits alongside the use of security tools.

As technology transforms, security must evolve with it. Companies must just be mindful that, as this game of cat and mouse continues, they are the ones doing the chasing.

SEE OVERLEAF FOR PRACTICAL ADVICE ON AVOIDING BEING HACKED