Cyber: An Evolving Threat

Chris Rankin

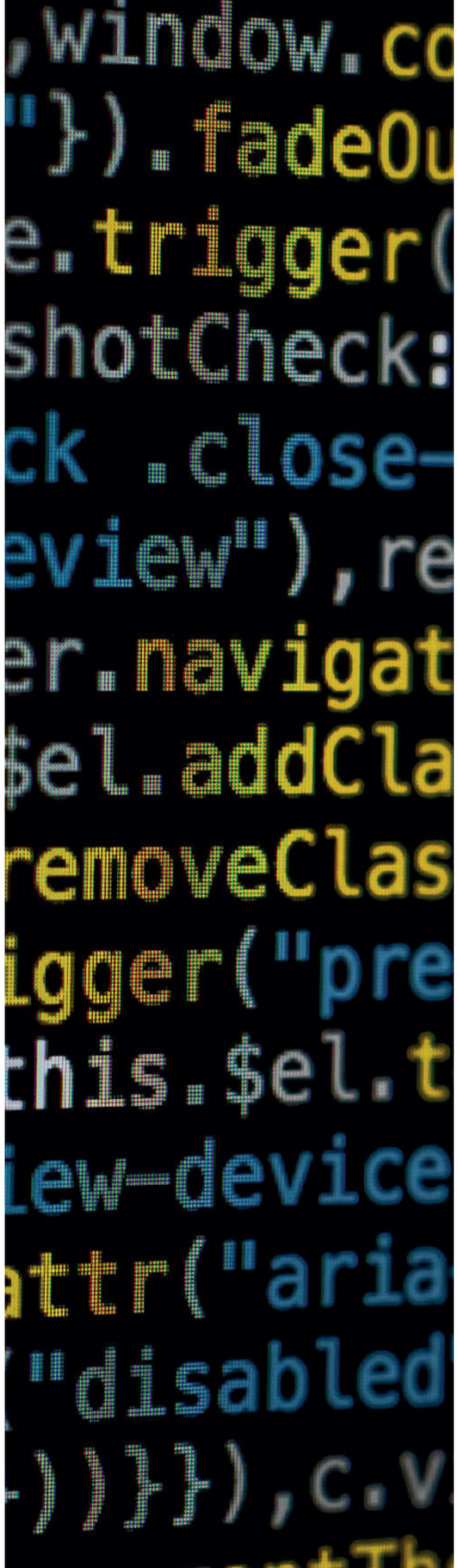
Contents

Abstract

Every day, businesses across the UK and the globe depend on computer technology to run their business – to connect with colleagues and customers around the world and to store data, management information, intellectual property, banking records and the like.

The information we hold on computers is invaluable to the businesses we operate. Cyber criminals want to get their hands on it for their own financial, social or political gain.

Here we have a look at the types of cyber attacks, what they mean for your business and what we can do to mitigate the risks.



Introduction

In 2016, the UK's National Crime Unit found that cybercrime had overtaken all other forms of crime for the first time ever, with over two million incidents recorded in that year. Cyber attacks are becoming an everyday event whilst also becoming more sophisticated as more of our devices are connected to the internet.

However, despite advances in technology, human and system error are ever-present threats, while everything from a lost laptop to a disgruntled employee can now pose a major risk.

In today's data-driven world, keeping information, data and finance safe and secure online is essential.

The introduction of the General Data Protection Regulation (GDPR), which came into effect on 25th May 2018 and is applicable to all businesses and organisations, created the biggest change to data protection rules in over 20 years. It states:

"Businesses that fail to adequately protect an individual's personal data risk losing consumer trust, which is essential to encouraging people to use new products and services."

In other words, consumers value their data and place importance on how their data is being kept and for the purpose of which it is being used. Companies who fail to adequately protect consumer data face the consequences of irreparable reputational damage.

This brings more onerous requirements for a company to protect the personal information of individuals. Companies may need to appoint an in-house data protection officer to oversee the company's data protection strategy and ensure compliance with the new regulation.

"Businesses that fail to adequately protect an individual's personal data risk losing consumer trust, which is essential to encouraging people to use new products and services."

In the event of a data breach under these new guidelines, there are strict timeframes in which to notify the Information Commissioner's Office (ICO), on top of having to manage the adverse publicity of a data breach and the heavy fines imposed: €20 million or four per cent of a firm's global turnover (whichever is greater).

In July 2019 we saw the ICO impose record fines of £282m for data breaches relating to British Airways (£183.4m) and the international hotel group Marriott (£99.2m). Whether GDPR fines are insurable remains to be seen and tested by the courts.

In today's connected world virtually all UK businesses rely on computers and online services in some shape or form through email, websites and social media, which increases the everyday threat of a cyber attack.

Cyber attacks may include the following dangers:

- Data breach, identity theft, fraud and extortion
- Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Denial-of-service and distributed denial-of-service attacks
- System infiltration
- Intellectual property theft or unauthorised access

All of these cyber incidents can lead to the theft of money, data or goods, network interruption to critical business systems, and reputational damage to your company or brand.

The scale of the threat is ever increasing.

Types of Cyber Attack

"It's official: Cyber attacks cost UK businesses £34 billion."

The numbers are eye-watering. According to a just-published report from the Centre for Economics and Business Research (CEBR), cyber attacks are costing UK firms £34 billion – split roughly 50-50 between revenue and intellectual property losses (£18bn) and subsequent increased IT spending (£16bn).

This makes cyber attacks the No. 1 risk facing business today. It could be argued that a large-scale cyber attack that causes both monetary and reputational damage for organisations could open the door for personal litigation – from employees, customers and shareholders alike – against directors who are failing to prioritise this risk. Cyber attacks should be on every boardroom agenda to assess and mitigate risk.

Let's have a look at some cyber events that can impact your business:

Phishing

It is a common cyber event where fraudsters attempt to gain confidential information, generally by sending genuine-looking emails from well-known organisations such as banks; and ask the recipient to confirm bank details and credit card information.

Users need to be on guard; banks will not email asking for account details, and these emails may contain spelling or grammar mistakes in the body of the email or the email address, which can alert a user. We have to be vigilant.

Distributed denial of service

Potentially seen more in the retail and e-commerce sector, this form of cyber attack involves deploying malware to random computers. The hacker gains control over hundreds of computers without the owners noticing, then causes interruption to a website or network by flooding it with data requests to the extent that it slows the site down or brings it to a standstill.

This situation can inconvenience customers and cause them to abandon affected websites, resulting in a significant loss of sales for retailers, especially over holiday sales seasons.

"It's official: cyber-attacks cost UK businesses £34 billion"

Social Engineering

This common cyber event occurs when attackers clone the email addresses of an organisation's senior management, such as the CEO or managing director, and send an email to the accounts department asking for urgent payment of an invoice. Who is to question the CEO or managing director? The payment is made and once discovered that it was fraudulent, it is too late.

A phone call to the CEO or managing director to verify if payment should be made will take a minute and could save thousands.

Malware

A malicious type of software; malware is designed to damage, disable or infiltrate a computer system.

Inside attack

A person with authorised access to a computer system can carry out an attack – for example, a disgruntled employee leaking information to a competitor or accessing an organisation's data with criminal intent.

Ransomware

In May 2017 ransomware hit the headlines when the WannaCry attack affected hundreds of thousands of computers across the globe with ransom demands. The most notable victim here in the UK was the National Health Service. The attack led to more than 19,000 appointments being cancelled and ambulances being diverted to other hospitals. Costs, between lost output and subsequent clean-up expenses, totalled £92m.

Ransomware is a type of malware infection that encrypts information on a computer or network and locks it down. The attackers will then demand a ransom in order to release the decryption key. It impacts organisations both large and small.

Two months after the WannaCry attack, the NotPetya attack crippled global business.

As the National Cyber Security Centre reported in February 2018:

"An assessment by the National Cyber Security Centre has found that the Russian military was almost certainly responsible for the 'NotPetya' cyber attack of June 2017.

The UK government has made the judgement that the Russian government was responsible for the attack, which particularly affected Ukraine's financial, energy and government institutions but its indiscriminate design caused it to spread further, affecting other European and Russian business.

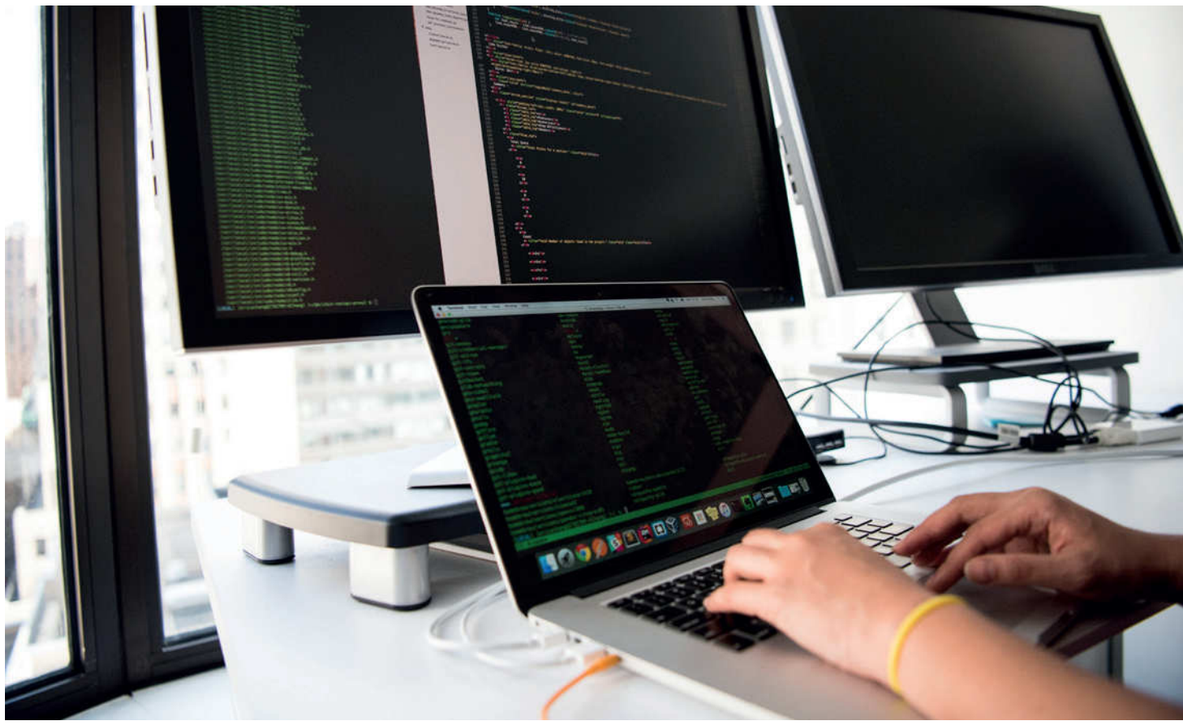
The destructive attack masqueraded as ransomware, but its purpose was principally to disrupt. Several indicators seen by the NCSC demonstrated a high level of planning, research and technical capability.

The decision to publicly attribute this incident reiterates the position of the UK and its allies that malicious cyber activity will not be tolerated."

Estimated costs associated with these two attacks are USD 5.2bn.

A Microsoft Windows security vulnerability made these attacks possible. Microsoft released patches for the vulnerability but a cyberattack strategy developed by the US National Security Agency was leaked soon afterwards. Computer systems that didn't yet have the security patches were exposed. Had these security vulnerability patches been installed, the WannaCry and NotPetya attacks would not have infected the systems of these organisations.

It's important to plan a strategy around these updates and schedule regular downtime to ensure the fixes are installed as advised. Preventative measures are more cost-effective than those required to recover after the event.



Cyber Catastrophe Event

"Category-one national cyber emergency: A cyber attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life."

In a 2018 Hiscox London Market feature article, Robert Hannigan, former Director of Government Communications Headquarters, explained why escalating international tensions could have catastrophic consequences in cyberspace.

"Given the way that some nation states are behaving quite recklessly, then it [a category-one attack] has become more likely – either because they plan to do it or because they miscalculate. It's very hard in cyberspace to understand the consequences of your attack – they go way beyond what you think they will be," he said.

Escalating tensions between the West and Russia, China and Iran are leading to an increased cyber threat. Hannigan said geopolitics are reflected in cyberspace, so if the nuclear deal with Iran falls apart, we should expect to see an increase in Iranian cyber attacks. He believes the same is true with Russia.

"We've seen a big increase in their cyber activity in recent years, matching their aggression in the real world," he said.

Businesses at risk

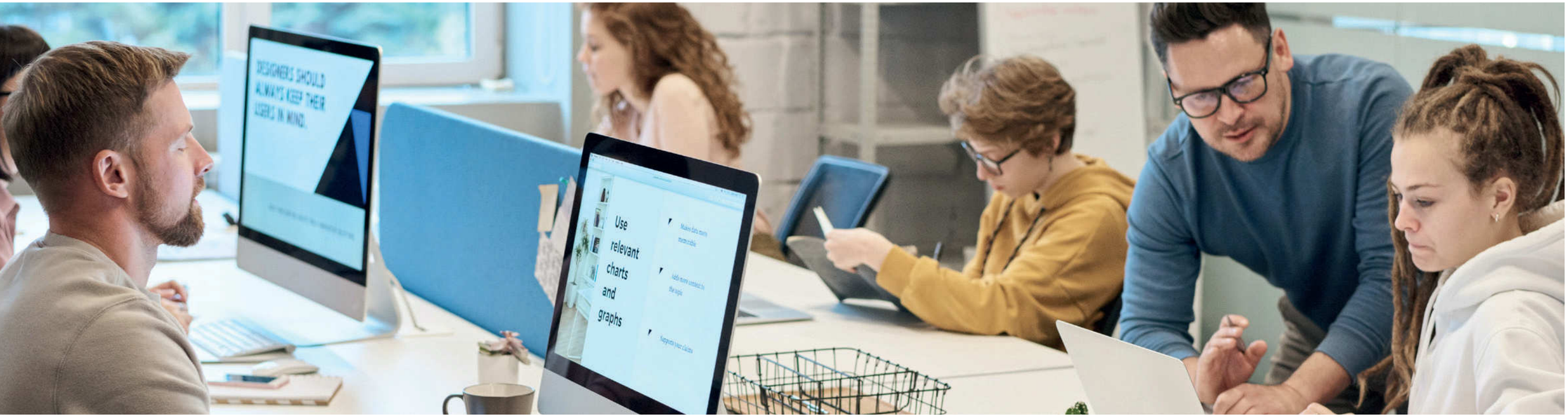
Companies now face a direct threat from cyber attacks by foreign powers. Hannigan said that just five years ago, it wouldn't have been necessary to worry about nation-state attacks because governments would have handled them, but that is no longer true. "WannaCry and NotPetya were [deployed by] North Korea and Russia," he said. "States are leaking tools and techniques to criminal groups. It's a strange mixture now of high-end sophistication, nation-state and criminal. [It is] hard to protect against, but can be done."

Neither WannaCry nor NotPetya were declared category-one events, even though they were among the biggest cyber attacks of 2017.

Hannigan set up the National Cyber Security Centre in 2017 to help the UK prepare and defend against a major cyber attack. Information sharing about potential threats between the public and private sectors "is pretty good," he says, explaining that the government shares over 90% of the software vulnerabilities it knows about. Full disclosure isn't desirable, he argues: "Government's first responsibility is cyber defence. If they don't hold back anything at all then effectively they can't do their job."

This puts the risk from a cyber security attack from hostile nations and large criminal groups in the same category as an international military crisis, international terrorism and a major accident or natural disaster.

Such an attack from foreign powers could bring down critical national infrastructure such as national power grids, airlines, railways, power plants and weapons systems. Resulting prolonged power outages and travel disruption could easily bring chaos to parts of the UK.



Emerging Threats

Emerging technologies bring threats and vulnerabilities that will challenge business in new ways.

Cyber criminals are becoming more sophisticated and creating more innovative ways to carry out an attack. New threats to business include:

Artificial Intelligence

Artificial intelligence (AI) is being used as a defence against cyber attacks, though criminals are turning the tables.

AI-generated phishing emails are designed with current security in mind and are capable of bypassing spam filters, directing emails to the recipient's inbox.

Cryptojacking

A malicious software attack, cryptojacking accesses a victim's computer to mine for cryptocurrency.

The software infects a computer or a website when a computer user clicks on a link that downloads a cryptomining code.

Mobile Malware

As people increasingly treat their smartphones like computers, using them to store banking details, credit card information and other personal data, these devices have become a target for cyber criminals. Research from Kaspersky Lab found that between 2017 and 2018, attacks doubled from 66.4m to 116.5m.

Cyber Security

Cyber security is the first line of defence against a hacker. We wouldn't leave the house without locking the front door, so why do we make it easy to be hacked? Here are security precautions we can all implement to help stay secure.

1. Make sure your computers are running the latest versions of software. A lot of software updates are made due to system vulnerabilities. Hackers are aware of that and will use it to their advantage. Ensure security patches are installed on your chosen software applications and your anti-virus software. Remember WannaCry!

2. Educate employees and ensure strong passwords in the workplace. Don't use the same password for all of your applications and change passwords regularly. If your password is compromised for one system then you have comfort knowing your other applications are safe.

3. Two-factor authentication uses your password and adds a second layer of security, such as sending a code to your smartphone. You can also set up a biometric finger print on your phone to provide a second layer of security.

4. Back up your data regularly as no matter how secure your systems are, there is still a chance you will be hacked. Use external drives or back up your data to the cloud and double check that you can restore your data from them.

5. Restrict access to confidential files to those who need to access the information.

6. Be certain of attachments before downloading. Just because an email is from a friend or colleague doesn't mean you shouldn't be cautious. If you're not expecting an attachment, verify it with the sender.

7. Encrypt highly confidential and sensitive personal information before you send it over the internet and share the password over the phone, not by email.

8. Employees leave businesses all the time. Ensure you restrict their access or close down their accounts once they leave.

Cyber Insurance

Cybercrime is constantly evolving as new technologies emerge. Once you have your in-house security up to date, you can mitigate the risks to your business with a cyber liability insurance policy.

A comprehensive cyber liability policy should cover the following eventualities:

First Response

When a cybersecurity breach is suspected, most businesses do not have the capability to diagnose the issue and respond swiftly. First response cover provides emergency access to a legal response advisor and an IT specialist who can deliver critical support and a coordinated response.

Event Management

After a cyber attack, organisations require a range of services to get their business back on track. Event management pays for legal, IT and PR services, credit and ID monitoring, and data restoration and breach notification costs.

Data protection and cyber liability

Data protection and cyber liability responds to third-party liability claims arising from a failure in network security. This includes cover for defence costs and liability claims resulting from the breach of confidential information, along with cover for defence costs and insurable fines incurred during a regulatory or PCI investigation.

Network Interruption

Almost all consumer-facing businesses now rely heavily on the web for direct sales or customer relationship management, and even traditional industries like manufacturing and transportation require network connectivity to operate efficiently. Network interruption covers loss of income and mitigation expenses when business operations are interrupted or suspended due to a cybersecurity incident.

Cyber Extortion

Businesses may find themselves the target of cyber criminals who use ransomware to encrypt their data until they purchase a key to unlock it. The extortion section of a policy covers losses resulting from an extortion threat. This includes ransoms to end extortion as well as fees incurred from specialist cyber extortion advisors.

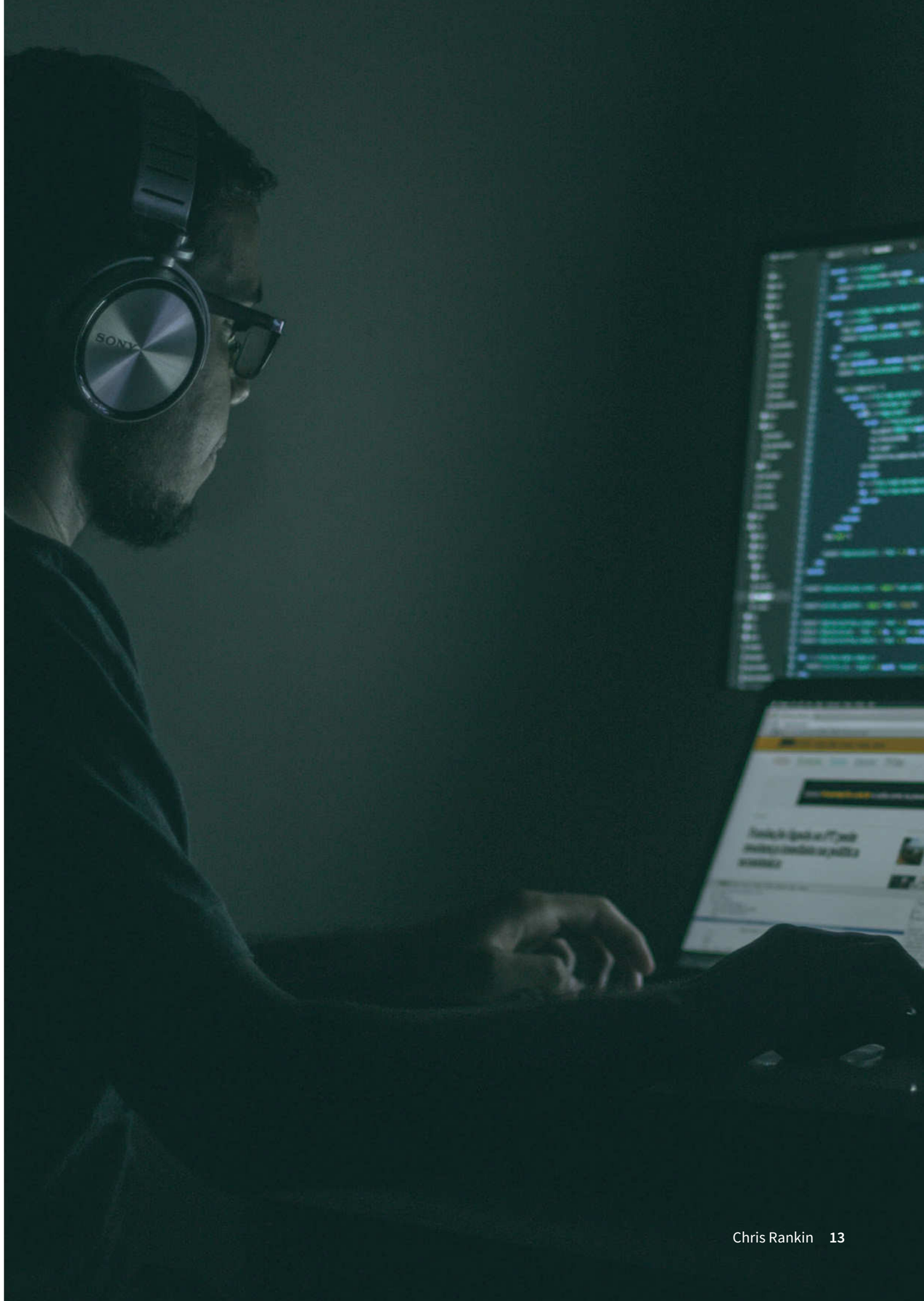
This protection provides peace of mind: The Association of British Insurers (ABI) has revealed that 99% of cyber claims have been met by a cyber policy. But despite this statistic, there is only an 11% take-up in cyber insurance in the UK.

According to a recent report from the ABI:

"The Association of British Insurers has, for the first time, revealed that 99% of claims made on ABI-member cyber insurance policies in 2018 were paid. This is one of the highest claims acceptance rates across all insurance products.*

Despite this, the take-up rate of cyber insurance by businesses in the UK is still worryingly low, with the overall market size estimated at less than one-tenth of the size of the UK's pet insurance market. Just 11% of businesses are thought to have a specific cyber insurance policy in place, meaning millions of small businesses could be at risk."

*Based on the 207 cyber claims that were made and settled in 2018, of which 205 were paid.



References

https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf

https://relianceacsn.co.uk/its-official-cyber-attacks-cost-uk-businesses-34-billion/

https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

https://en.wikipedia.org/wiki/EternalBlue

https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

https://www.hiscoxlondonmarket.com/cyber-catastrophe-horizon

https://www.abi.org.uk/news/news-articles/2019/08/cyber-insurance-payout-rates-at-99-but-uptake-still-far-too-low/

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