NewStatesman

Spotlight

CYBER SECURITY: NEW THREATS, NEW SOLUTIONS

Ciaran Martin / Simon Fell MP / Mark Galeotti

Sophos stops ransomware.

SOPHOS
Cybersecurity evolved.

Defending the digital economy

One defining feature of the past year has been the key role played by remote work and cloud computing – not only enabling far-flung research teams to join in the global relay race for a vaccine, but allowing entire sectors of the economy to stay afloat, while adapting to the stringent demands of lockdowns and social distancing.

But the more digitally dependent economies become, the more exposed they are to mishaps and maleficence: the sudden surge in the sea of online data provides ample fishing (and phishing) grounds for hackers, blackmailers and spies. Data breaches rose by a third in 2021, according to the Verizon Business *Data Breach Investigations Report*, and instances of online misrepresentation rose by 15 times. Closer to home, almost half the businesses in the UK and over a quarter of charities reported experiencing cyber security attacks in the 12 months before 2021, according to the government's *Cyber Security Breaches Survey*.

Vigilance, conversely, has been slipping. Fewer businesses were deploying any form of security or user monitoring than in the preceding year – alarming news, considering that already in 2020, 48 per cent of businesses surveyed for the government report on cyber security skills in the UK labour market said their employees lacked the confidence and the skills to set up even rudimentary cyber security measures.

In this issue, Simon Fell MP (pages 26-27) lists the crucial steps the government needs to undertake to fix these yawning gaps in the UK's cyber skills set, from addressing digital poverty to actively encouraging women to enter the cyber security field.

We also look at the delicate choices facing the UK and the US when trying to contend with the threat of commercial cyber espionage emanating from rivals like Russia and China; we learn of thriving new marketplaces where established companies vie for the services of friendly hackers willing to put their defence systems to the ultimate test; and we consider the risks online bullying and stalking pose to mental health, asking whether these can really be contained through tech solutions alone.

NewStatesman

Standard House
12-13 Essex Street
London, WC2R 3AA
Subscription inquiries:
digital.subscriptions@
newstatesman.co.uk

Commercial Director
Dominic Rae

Account Managers
Jugal Lalsodagar
Cyrus Ramezani

Special Projects Editor
Dimi Reider

Special Projects Writers
Jonny Ball
Rohan Banerjee
Samir Jeraj

Senior Sub-Editor
Tony Rock

Design and Production
Henrik Williams

Cover Illustration
Sam Falconer

BRITISH SOCIETY OF MAGAZINE EDITORS AWARDS 2017 WINNER

First published as a supplement to the *New Statesman* of 21st May 2021.

Registered as a newspaper in the UK and US. The paper in this magazine is sourced from sustainable forests, responsibly managed to strict environmental, social and economic standards. The manufacturing mills have both FSC and PEFC certification and also ISO9001 and ISO14001 accreditation.
This supplement can be downloaded from: newstatesman.com/page/supplements

News

Raab issues Russia warning

Rohan Banerjee

The Foreign Secretary, Dominic Raab, has said that Russia has a "responsibility to prosecute" individuals and organisations behind malicious cyber activity. Speaking at the National Cyber Security Centre's Cyber UK conference this month, he underlined the importance, in an increasingly digitised world, of more action on the part of governments.

A rise in the use of ransomware – a type of malicious software designed to block access to a system or data until money is paid – has coincided with more businesses and services moving online. The US company Colonial Pipeline is currently dealing with the fallout of a major ransomware attack, which shut down almost half of the fuel supply to the country's east coast. The attack has been linked to a criminal gang called DarkSide, which is thought to be based in Russia (see story, above right).

According to a BBC report, former US intelligence officials have suggested that while the Russian government is not directly involved, it is possible that Russian political leaders were aware of the attack. Raab warned that without more vigilance from governments, hackers could become "industrial-scale vandals of the 21st century".

Major US oil pipeline hit by cyberattack

Jonny Ball

The Colonial Pipeline, which travels through 14 US states and carries 45 per cent of the east coast's fuel supplies, was shut down for several days following a cyber attack at the beginning of May. The shutdown led to fuel shortages, panic buying, and a sharp rise in prices across the US. The FBI quickly laid the blame at DarkSide, a shadowy cybercriminal organisation likely based in Russia, but not believed to be directed by Russian agencies.

Despite statements from the pipeline operator that the company would not be paying the ransom demanded by the group, Bloomberg has reported that $5m in cryptocurrency was transferred to the hackers in exchange for a decrypting tool.

In response to the pipeline shutdown, as well as the recent SolarWinds debacle (see full report, pages 18-20) and a Microsoft Exchange Server attack, President Biden has signed an executive order to bolster the US's cyber defences.

Cybercrime thriving on human error, report finds

Rohan Banerjee

A record number of cybercrime incidents have been recorded and analysed in Verizon's 2021 *Data Breach Investigations Report*. The study, which was published this month, considered 29,207 security incidents from 83 different contributors from around the world, of which 5,258 were confirmed breaches. This rose significantly from the previous year's report, in which 3,950 breaches were identified.

RAAB: GETTY IMAGES/PETER SUMMERS; SCHOOLS: GETTY IMAGES/MARTIN CARDY; WMTRAINS: SHUTTERSTOCK/WOZZIE

With a mass shift to remote working during the coronavirus pandemic, the report suggested cybercriminals had found it easier to exploit human weaknesses within organisations. The research found that rates of cyberattacks involving fraudulent emails and ransomware attacks had risen by 11 per cent and 6 per cent respectively.

Over half (61 per cent) of the breaches identified by Verizon involved credential data, such as usernames and passwords. The vast majority of cyber breaches (81 per cent), the report said, involved some form of human error.

DfE to launch new security tool for schools

Rohan Banerjee

Working in partnership with the National Cyber Security Centre (NCSC), the Department for Education (DfE) will launch a new cyber security tool for schools and universities to regularly self-assess their networks, cloud storage facilities, and email systems. Speaking at the recent Cyber UK conference, the Schools Minister Nick Gibb confirmed the development of the tool, which should launch at the start of 2022.

The move comes in response, he said, to a spike in cyberattacks targeting the education sector over the course of the coronavirus pandemic. An NCSC report in March revealed that many schools had lost financial records, students' coursework, and Covid-19 testing data due to hacks.

"Not only does this threaten children's education, it can be really frightening for schools and can distract teachers from doing their jobs," Gibb warned. The DfE, he added, is also working with the NCSC on more guidelines and cyber resilience training for school staff.

The DfE has also confirmed the launch of a Risk Protection Arrangement (RPA) Cyber Risk Pilot with over 500 schools. Each school in the scheme will be supported to achieve certification that aims to protect them against 80 per cent of the most common cyberattacks.

Royal Mail users warned over phishing scam

Jonny Ball

The Royal Mail delivery service has warned customers of a "highly convincing" scam, in which users are sent text messages asking them to pay a "£1.99 unpaid shipping fee" for a held package. The texts contain a payment link in which customers are asked to share bank details. Royal Mail has told customers to be especially vigilant about texts, and said it "will only ever request payment for a fee due on a parcel by leaving a grey card at your address, and will only contact you via text or email if you've specifically requested it".

Cybercrime has seen a dramatic rise during the pandemic, with the steep growth of homeworking, e-commerce and online retail presenting more frequent opportunities for scammers. Some 6,000 instances of Covid-related cybercrime and fraud have been reported to the UK police since March 2020. The National Cyber Security Centre told the BBC it is grappling with 30 "significant attacks" every month.

West Midlands Trains tricks staff with training email

Jonny Ball

The Transport Salaried Staffs' Association (TSSA), a trade union representing railway workers, has criticised the West Midlands Trains (WMT) company for testing its members' cyber security awareness with a fake phishing email. The email claimed staff were entitled to a bonus – a "gift [that] will inspire you to keep up the good work" – for their efforts during the coronavirus pandemic.

If a link in the email was clicked, purportedly to give more information on the bonus entitlement, a second email was triggered telling staff "this was a test".

WMT defended its actions, saying its cyber security strategy involved regular tests, with this one intended to mimic the type of email and language used by genuine cybercriminals intent on accessing company data. The transport industry at large lost "billions of pounds every year" to this type of fraud, it said.

Manuel Cortes, general secretary of the TSSA, called on the train operator to honour the bonuses falsely promised in the fake phishing emails, and accused WMT of "reprehensible behaviour".

The price and politics of security

Companies should brace themselves for breaches but not bow down to intimidation tactics, says **Jonathan Lee**, public sector director UKI at Sophos

Ransomware is a widespread threat to organisations across all sectors in 2021. According to *The State of Ransomware 2021* report by Sophos, 37 per cent of organisations around the world were hit by ransomware in 2020 and the average cost of recovery from such an attack has more than doubled, from $0.76m in 2019 to $1.85m in 2020.

The average ransom paid was $170,404 – and almost a third of victims paid up. In addition to the significant financial cost and resource demands of recovering from an attack, ransomware can destroy brands and reputations, especially when personal data and other confidential information is involved. The annual Sophos survey, which polled 5,400 IT decision makers in 30 countries around the world, (mainly from mid-sized organisations) shows how not all industry sectors have been impacted as adversely by ransomware attacks.

Media, leisure and entertainment along with distribution and transport topped the list of sectors able to block an attack before their data was encrypted – with 47 per cent and 48 per cent, respectively, able to do so, compared to a global average of 39 per cent. In local government, which can have limited IT resources, only 28 per cent managed to avoid encryption, while healthcare (28 per cent) and oil and energy (25 per cent) also struggled.

The threat landscape for ransomware is changing. At one end of the spectrum there are unskilled criminals using off-the-peg ransomware-as-a-service (RaaS) software, such as Dharma, in a spray-and-pray approach. At the other end there are advanced, targeted and manually orchestrated attacks that involve innovative tactics, techniques and procedures as well as tools that are often also used by IT administrators and security professionals for everyday tasks. These advanced attacks involve the highest ransom demands, often running into millions of dollars. In addition, such attacks can combine encryption with the theft of data, which the attackers then threaten to make public unless a ransom is paid.

Some adversaries are skipping the data encryption stage altogether and are simply demanding a ransom to delete, or agree not to publish, the stolen data. A small, but significant 7 per cent of respondents to the global

SHUTTERSTOCK/POPTIKA

survey had experienced such attacks – double the 3 per cent affected in 2019. Anecdotal evidence suggests that central government and retail organisations may be particularly vulnerable to this kind of approach.

Does it pay to pay a ransom? The universal answer is no, but not everyone feels they have a choice. If you don't have up-to-date offline backups, a decryption key provided by the attackers may be the only way of getting your data back. But it is rarely that simple. The survey found that of the organisations that pay a ransom, fewer than one in ten (8 per cent) get all their data back, while 29 per cent recovered no more than half.

Chester Wisniewski, principal research scientist at Sophos, says: "This could be in part because using decryption keys to recover information can be complicated. What's more, there's no guarantee of success. For instance, as we saw recently with DearCry and Black Kingdom ransomware, attacks launched with low-quality or hastily compiled code and techniques make data recovery difficult."

Some attackers remain in the victim's network after launching the ransomware, to see if the attack succeeded, but also so that they can threaten a repeat attack if the victim doesn't pay. Identifying and removing any trace of the intruders is vital to prevent this from happening.

Does it pay to pay a ransom? The universal answer is no

What did the survey respondents expect from ransomware in the future? Of the 62 per cent of organisations that had not been hit by ransomware in the past year, nearly three-quarters expect to be targeted at some point. Around half of them (47 per cent) said this was because of the increased sophistication of attacks. The good news is that 6 per cent of those that had escaped attack – and felt they were unlikely to be a target in the future – said this was down to the expertise of their IT teams. ●

Sophos recommends the following best practices to help defend against ransomware and related cyberattacks:

- **Assume you will be hit**. Ransomware remains highly prevalent. It's better to invest in preparation, even without being hit.
- **Make backups and keep copies offline**. Backups are the main method organisations surveyed used to recover their data after an attack.
- **Deploy layered protection**. As more ransomware attacks involve extortion, it is more important than ever to keep adversaries out in the first place. Use layered protection to block attackers at as many points as possible across an estate.
- **Combine human experts and anti-ransomware technology**. The key to stopping ransomware is in-depth defence, combining anti-ransomware technology and human-led threat hunting.
- **Don't pay the ransom**. Easy to say, but far less easy to do when an organisation has ground to a halt due to a ransomware attack.
- **Have a malware recovery plan**. The best way to stop a cyberattack from turning into a full breach is to prepare in advance.

Ciaran Martin warns against retaliatory cyberattacks

The UK's first cyber chief on the defence review, China and Russia. By Oscar Williams

On 24 September 2015, President Barack Obama and his Chinese counterpart Xi Jinping signed a landmark agreement on cyber espionage. While the agreement didn't dwell much on state and military secrets, it explicitly banned the parties from passing on any commercial secrets they uncovered to the private sector.

The deal was heralded as a major victory for US businesses, whose executives had long complained that China was routinely stealing intellectual property (IP) that had cost them billions of dollars to produce. And, for some time, the agreement did have a substantial impact on rates of IP theft, which fell as the number of Chinese patents rose. But a mere two years after Obama left office in 2017, US intelligence officials warned that the accord with China had begun to weaken.

Then, in January of this year, five years after the bilateral agreement was signed, security experts uncovered evidence that hackers working on Beijing's behalf were targeting employees of NGOs and think tanks. The hackers were exploiting vulnerabilities in Microsoft's Exchange email servers to spy on the individuals and extract sensitive data. While Beijing has denied involvement, a former White House chief information officer in March described the attack as a typical example of Chinese "industrial espionage".

The abuse of the vulnerability, which at first was highly targeted but ensnared tens of thousands of organisations, came just weeks after the disclosure of a widespread attack – attributed to Russian state actors – on dozens of US government organisations and businesses using software produced by Texan IT firm SolarWinds.

The two attacks sparked calls for retribution. The *New York Times* reported in March that the White House was planning to hit back at Russia with a series of cyberattacks that would be evident to the Kremlin but not the Russian public. The Biden administration then faced pressure to launch retaliatory attacks on China too.

Ciaran Martin, the founding CEO of the UK's National Cyber Security Centre (NCSC), cautions against such interventions. Martin, who stepped down as the UK's most senior cyber security official last September and now

We militarise the internet at our peril

Martin (centre) speaking at the NCSC's Cyber UK conference in 2019

GETTY IMAGES/JEFF MITCHELL

Offensive cyber is best left for countering terrorism, organised crime and cybercrime, says Martin

runs a venture capital firm for security start-ups alongside his professorship at Oxford, notes that the Moscow-linked attack is little different to the kind of digital espionage carried out by the US National Security Agency, or the NCSC's parent agency GCHQ.

"If SolarWinds is seen as beyond the pale, then there are serious implications for the Five Eyes," Martin tells *Spotlight*, referring to the intelligence sharing alliance between the UK, US, Canada, Australia and New Zealand. "There does not appear to be the appetite for that kind of restraint in the Five Eyes [for good reasons]: spying can reduce the risk of miscalculation and harm."

However, Martin was more concerned about the alleged China attack. According to Brian Krebs, the security journalist who broke the story, hackers working within an "unusually aggressive Chinese cyber espionage unit" compromised at least 30,000 organisations. In order to maintain access to the networks, the hackers deployed back doors that are now vulnerable to further hacking by cybercriminal groups who may wish to hold organisations to ransom. Martin described the campaign as "reckless", but again rejected calls for retaliatory cyber action, preferring to name and shame the perpetrators – a strategy he says has more of an effect on Beijing than Moscow.

His comments came as the UK was preparing to significantly expand its capacity for offensive cyber attacks. As part of the integrated foreign and defence review, the government committed to a new "full spectrum approach to the UK's cyber capability". This includes bolstering the cyber defences of critical infrastructure and also placing a greater emphasis on the capacity to carry out attacks through the National Cyber Force, which was announced last year.

In March, before the review was published, Downing Street said: "In recent years our adversaries have invested in their own capabilities and are constantly finding new ways to exploit our weaknesses and gain advantage in cyberspace. To cement our competitive edge and keep ahead of our enemies a full-spectrum approach is therefore needed." Boris Johnson added: "We need to build up our cyber capability so we can grasp the opportunities it presents while ensuring those who seek to use its powers to attack us and our way of life are thwarted at every turn."

The West is going to have a tough time

Martin is wary of overstating the role that offensive cyber can play in a country's defences. "It's most useful for things like countering terrorism, countering serious organised crime and cybercrime, and supporting military organisations," he says, referring to a 2016-17 attack on Isis. "Recent history shows it's actually much less effective at deterring state-sponsored cyber attacks against us. While it's correct that it's a major part of our national security capabilities, it's not actually a major part of our cyber security capabilities." In a speech at King's College London in November entitled "Cyber weapons are called viruses for a reason", Martin warned that "we militarise the internet at our peril".

The integrated defence review positioned the UK at the centre of efforts to uphold democratic values internationally. And there have been calls from the tech industry to codify the UK and US's approach to cyber security in standards agreed between countries. But Martin is downbeat about the chances of such a system being realised.

"What's our big bugbear with China? It's commercial espionage," he says. "It's not lost on the rest of the world that the UK stopped commercial espionage all the way back in the mid-1990s and made it unlawful all the way back in 2016. For us to suddenly say (and, of course, we're seen as a privileged country economically) that it is an inviolable moral truth that companies should not undertake digital espionage for commercial reasons – most of the world does not find that credible."

Martin warns that "the West is going to have a tough time and needs to undertake some self-examination about its own appetite for aggressive digital activity before a set of globally acceptable norms are possible". ●

SHUTTERSTOCK/ R8 STUDIO

Detecting hate online

Policymakers have a responsibility to monitor and manage digital discourse effectively. By **Nishanth Sastry** (University of Surrey), **Margarita Amaxopoulou** (King's College London), and **Edward Wood** (House of Commons Research Library)

IN ASSOCIATION WITH

Surrey Centre for SCCS Cyber Security

UNIVERSITY OF SURREY

Rarely have the impacts of hateful speech been more tangible and serious than in our contemporary digitalised political discourse. The January attack on the US Capitol building, for example, indicates that hateful language may be more effective than before in triggering violent reactions and threatening social peace and cohesion. In the UK, the government has expressed concerns about the impact of online intimidation and abuse on public life.

With digital interactions booming, especially during the Covid-19 pandemic, courts in Europe and the US seem to be confining themselves to only the most serious instances of hate speech violating human rights and criminal or tort law. Algorithmic content-moderation systems are increasingly used to filter the massive amount of online interactions and assess whether their content is hateful.

Legal and computational understandings of hate speech, however, are by no means easy to harmonise. Legal assessment is very context-specific, taking into account the particular circumstances of each case, the degree of interference with countervailing rights or interests, and the reasonable expectations of the parties.

This makes it a very expensive remedy that will be out of reach for most people. In contrast, computational assessment operates on a high level of abstraction, seeking to operationalise classification criteria into a mathematical language that can generate universally applicable tools and apply them to a huge volume of content. The twin risks with this approach, depending on the sensitivity of the algorithms deployed, are that too much hateful content is permitted or that robust debate on matters of public interest is stifled.

According to our research, current state-of-the art machine learning tools to detect and classify hate speech rely on slightly differing definitions of hateful speech and, crucially, are sensitive to the annotations and labels that are used to train the machine learning models. Abundant caution must be exercised before relying exclusively on automatic tools.

Bringing the legal and computational ways of thinking closer to one another may help us move closer to more effective real-world solutions. Forthcoming legislation on online harms will bring algorithmic models for controlling hate speech within a legal framework for the first time. This will put the onus on those models to provide safeguards that are simultaneously proportionate and effective.

In our research, we seek to contribute to bridging the divide between the two ways of thinking by using as a case study the daily conversations between MPs and their constituents on Twitter. Our project combines data science analysis of tweets addressed to UK MPs with legal analysis of the same content. We aim to develop new computational ways to recognise and classify hate speech by learning from how legal experts recognise and classify hate speech. ●

For more information, please visit: www.surrey.ac.uk

Additional commentary by Pushkal Agarwal (University of Surrey), and Oli Hawkins and Noel Dempsey (House of Commons Research Library).

A question of trust

Cyber security strategies must extend to supply chains, says **Mark Jackson**, national cyber security adviser at Cisco

Cyber security, rightly, has been elevated to a board-level concern in recent years. As businesses and services across all sectors move increasingly online, cyber security is no longer the preserve of IT departments. At the same time, the ability to keep data safe has become an important metric by which to judge any organisation that wants to operate in the modern world. Beyond the considerable operational cost that a cyber security breach may inflict, the potential for reputational damage from failing to prevent one, or at least, handling it effectively, can be costly or even catastrophic.

Against the backdrop of the coronavirus pandemic, national lockdowns, and a seismic shift toward remote working, it is vital that organisations take their cyber security seriously. Protecting your own enterprise seems obvious, but many companies lack the visibility and processes to protect one of the weakest links – their supply chains. If hackers can exploit a vulnerability within an organisation's supply chain, they are effectively able to access that organisation through a "back door". There are many examples of supply chain attacks, including network or computer hardware being compromised before it is installed or malware inserted into software at the development stage.

In 2020, the US technology firm SolarWinds fell victim to a sophisticated supply chain attack, with hackers inserting malicious code into its software development environment. The software, Orion, is widely used by companies across different sectors to manage their IT resources, including 425 of the Fortune 500 and both British and US government departments. The attack, widely attributed to nation-state hackers, was delivered through a routine software update, which customers unwittingly installed, giving attackers direct access to the heart of their networks. Once inside, attackers were able to move around the network unhindered, strengthening their foothold and stealing highly sensitive data.

It is hard to deny the level of skill and audacity required to execute such an attack. The incident is a stark reminder of both the sophistication of hostile actors, as well as the degree of vulnerability that exists in today's complex digital supply chain. But in the face of such sophistication, what steps can be taken to better mitigate the risk, and who has the responsibility for managing those steps?

Supply chain attacks seek to exploit situations of inherent trust. The SolarWinds incident was difficult to detect because the problem was well hidden, in a trusted software upgrade that companies simply accepted and deployed. Mitigating such attacks is challenging, but companies would do well to think about applying a zero-trust principle to their cyber security strategy. This includes incorporating role-based access controls, not just for users on their networks, but also for the applications and servers that they host. Segmenting or splitting company networks into smaller domains of trust will, at the very least, help to slow down any potential breaches.

A strong technology partner can inspire confidence, but, in the context of cyber security, there are no guarantees. Even high-profile technology brands aren't without risk, and when it comes to auditing a supply

chain, a vendor's brand reputation should not serve as an excuse to be less rigorous. Companies need to ask questions — ask questions at every opportunity, about every stage of every process, from the development life cycle to the manufacturing of a product, to the physical delivery of that product. Asking close questions to assess a vendor's supply chain security is a sound strategy to increase trust. The best security assessments have a clear understanding of what "good" looks like, and given the dynamic nature of cyber security, "good" is always a moving target.

For their part, suppliers must recognise they have a significant role to play in managing supply chain risk. It is imperative that vendors take proactive steps to strengthen internal development processes and bake in controls to protect product and service integrity. Technology vendors themselves often rely on an extensive set of external suppliers, and scrutiny must flow through all levels of the supply chain to build end-to-end integrity and trust.

The dialogue between technology companies and policymakers also needs to evolve. Economic prosperity and national resilience have become reliant on digital technology and adversaries have clearly demonstrated their willingness to target the complex supply chains that underpin them. The Department for Digital, Culture, Media and Sport's supply chain review, published in 2019, was a welcome move and has led to the Telecoms Security Bill, which will include new obligations on telecoms operators to scrutinise their supply chains. But this should be viewed as a first step, not a panacea.

The UK government should carefully consider further action to help manage the evolution of risk that comes with an increasingly digitised world. This doesn't necessarily mean further regulation; however, should this be required, policymakers must strike the right balance between encouraging positive action and not creating barriers to market entry or stifling innovation.

Hackers will look to exploit "back doors"

Stronger advice and guidance from government, drawing on the work surrounding the Telecoms Security Bill, would serve other industry sectors well, especially those delivering critical services. Building a consistent set of supply chain security objectives and outcomes would benefit all parties by providing a common language through which to communicate expectations and understand risk.

Accountability and transparency are the keys to building trust in technology. Trust can no longer be implied and must instead be proven. It is pertinent to remind ourselves of the Russian proverb, ironically made famous by numerous US politicians: "Doveryai, no proveryai." Trust, but verify. ●

SHUTTERSTOCK/GAUDILAB

When your abusers are everywhere

Online trauma is affecting more people, but little seems to be happening to tackle effects or causes.

By Samir Jeraj

It should have been a moment of professional joy for Somriddho Dasgupta. The model and actor had appeared in a 2020 video that went viral, clocking over a million views. But the abuse began almost at once, with the sheer volume of hostile comments and messages aimed at Dasgupta making it impossible to ignore. The vitriol quickly escalated to death threats – most of the bullies seemingly incensed by Dasgupta, who identifies as androgynous, looking too "feminine" in the video.

Dasgupta started to avoid YouTube and the torrent of hateful comments underneath his work, but the perpetrators quickly followed him to Instagram, where it started all over again until he turned off the comments altogether. Dasgupta tells *Spotlight* he was traumatised by the events, feeling depressed for months while stopping all work on videos. He felt he was being coerced into presenting in a more "masculine manner" and felt unhappy and "claustrophobic" because he could not express himself as he wanted.

Cybertrauma covers a range of emotional and psychological responses to online experiences: from bullying and threatening messages, through to falling victim to online fraud, to cyberstalking and grooming. This isn't something limited to influencers like Dasgupta. A third of all homeworkers experienced online abuse in the past year, according to research from the

Online trauma is re-lived over and over again

GETTY IMAGES/JEFF J MITCHELL

Suzy Lamplugh Trust, an organisation that aims to reduce the risk of violence and aggression through campaigning, education and support.

Catherine Knibbs is a therapist with a background in computing and has researched and written on cybertrauma. These types of traumas, she says, are different because unlike a traumatic event in physical reality that happens only once, with cybertrauma "you can go back and you can re-read the text, you can revisit the image, you can listen to the sounds again. It can also be downloaded by somebody and then uploaded [somewhere else]."

Nor can the technology "just be turned off" as some professionals suggest. Knibbs says perpetrators will often have enough information and skill to know when their victims come back online or switch to other platforms. She feels neither services nor many therapists are equipped to deal with the intersection of technology and trauma, let alone working with perpetrators to address their behaviour.

Dasgupta stresses how central online existence has become to everyday lives – the notion that it's somehow less important because it's mere lights on a screen doesn't really hold up. "Sure, it's online, but it is about my reality, the stuff that is super important to me and super personal to me," Dasgupta says. At the same time, support networks outside the web can be crucial. Dasgupta had a sister and a close friend living with him; he credits them with helping him persevere. "I'm not sure I would have been able to go through that [without them]," he says.

Abuse can't just be switched off

For Knibbs, there are larger questions at work. She would like to see more work being done by therapists to talk people through their behaviours online and offline, as well as broader education from childhood about "compassionate and empathic relationships", to make people consider the effect their online behaviour has on equally real human beings. She also thinks there is a role for legislation governing the acceptable use of technology, but feels it is wrong to simply blame the social media companies when a wider, societal issue is being played out through technology. "We need to be working on critical thinking skills, relationships, and then, of course, we look into technology and educating the general public," she concludes.

Friendly hackers are reshaping the digital economy

Once a twilight zone, hacking is now a dynamic, lucrative marketplace – and more and more professional players are entering the game. By Amy Borrett

While some people may be eager to return to the office, Aidan Preston, a 22-year-old working at a cyber security consultancy in Edinburgh, is anything but. Since he started working from home because of the pandemic, he has become the UK's top-earning "friendly hacker" – a coder that helps firms identify bugs in their new software, in exchange for money.

"It's bad to say, but Covid helped me," he says. "Working from home definitely kicked everything off for me big time – I can't imagine going back to an office now. It sounds too alien."

Without the need to commute into the office and with constant access to his own personalised set-up, Preston has effectively turned his side hustle into a second full-time job. Hacking into the early hours of the morning after working a standard nine-to-five, Preston admits that he sometimes does 90-hour weeks to hunt down vulnerabilities in companies' software.

In the elusive world of "bug bounty hunting" this practice is not uncommon. The past decade has seen the rise of a booming new market for platforms matching hackers with companies looking to crowdsource vulnerability testing for their software.

Traditionally, companies rely on costly external consultants to run penetration – or "pen" – testing for bugs. But these tests are often run only once or twice a year, and the rapid pace of software development necessitates a more dynamic approach, says Marten Mickos, CEO of leading US bug bounty platform HackerOne. As more and more of the world shifts online, there is a dawning realisation that digital society in its current state is "nowhere near as solid and resilient as it needs to be", he says.

"Today, everything of value is running on software and we must rush to make sure that all that software is being constantly tested, followed up, checked by external, unbiased people," says Mickos. "Covid accelerated the digital transformation for everybody and laid bare the risks and vulnerabilities we inherently have in software."

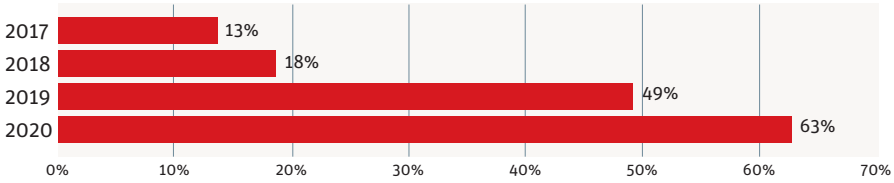
The data reveals snowballing interest in bug bounty: HackerOne reports a 63 per cent year-on-year increase in the number of hackers submitting vulnerabilities in 2020, while Paris-based platform YesWeHack says that the number of active hackers and registered programmes more than doubled over the same period.

The pandemic has also shifted the demographics of the industry. More full-time professional pen testers, like Preston, have joined the community, partly because it is an increasingly lucrative side hustle but also because bug bounty is the "ultimate test of the currency of your skill", says Mickos.

A number of hackers have already earned over $1m through their work on HackerOne – the first to make it past the milestone being 19-year-old Santiago Lopez. Ballooning bounties are the result of increased demand and rising complexity, meaning that the industry will only become more lucrative over time, says Mickos, although he adds that, as with sports leagues and Hollywood, it is only top-tier hackers that earn the big bucks.

THERE HAS BEEN A SURGE IN THE NUMBER OF FRIENDLY HACKERS IN RECENT YEARS

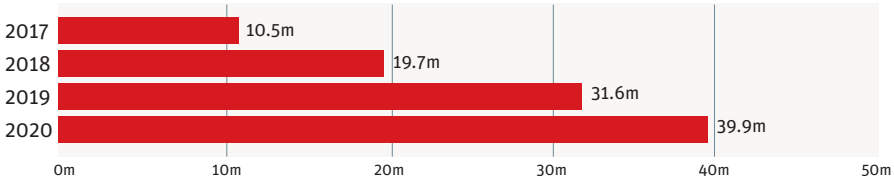
Year-on-year increase in hackers submitting vulnerabilities on HackerOne's platform



SOURCE: HACKERONE

BUG BOUNTY HUNTING IS BECOMING INCREASINGLY LUCRATIVE

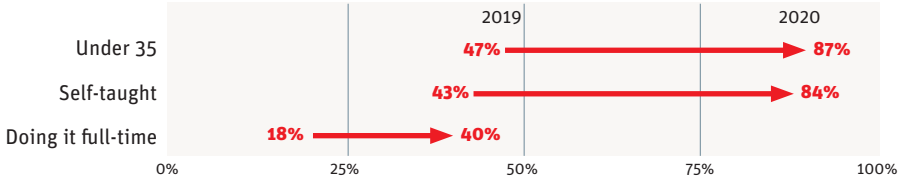
Money made on the HackerOne platform ($)



SOURCE: HACKERONE

THE PANDEMIC HAS CHANGED THE PROFILE OF FRIENDLY HACKERS

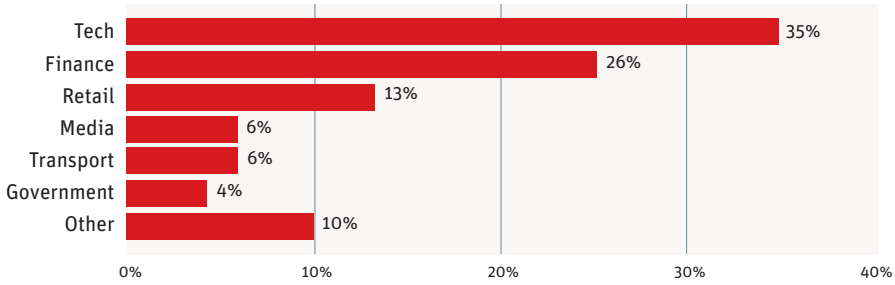
Percentage of hackers on HackersOne platform in 2019 and 2020 that are...



SOURCE: HACKERONE

OVER A THIRD OF PROGRAMMES WERE LAUNCHED BY TECH COMPANIES IN 2020

Percentage of programmes launched on YesWeHack by sector



SOURCE: YESWEHACK

Growing bounties are tempting an increasing number of cyber security professionals to become full-time bug bounty hunters: the number of members on HackerOne using the platform as their main source of income more than doubled in 2020. But, for now, Preston intends to continue as a professional pen tester.

"Most people don't go straight in full-time – it's way too risky; they do it part-time and build up savings and a steady income," he says. "I've thought about it a lot, but I still value professional experience over money, and I think I need to build up my career in an actual consultancy."

The pandemic has also been a watershed for corporate attitudes towards bug bounty hunting. Now, what was only a few years ago seen as "very experimental, if not risky" is on the verge of becoming best practice, says Rodolphe Harand, managing director at YesWeHack.

A driving force for this has been the rapid pace of digital transformation, turbocharged by the pandemic. Industries that have been hard-hit by the economic fallout from Covid-19 – retail, luxury, logistics – are increasingly running programmes on YesWeHack, says Harand.

While tech companies, unsurprisingly, still constitute a large share of the programmes, there is also growing interest from less tech-savvy organisations, such as national governments: the French government used a bug bounty programme to test the resiliency of its contact-tracing apps last year.

As governments ramp up their digital offerings, relying more on these programmes will help them to win the trust of citizens, says Harand: "Bug bounties are a great way for governments to provide some guarantees in terms of transparency – it's a way of saying 'I have nothing to hide'."

YesWeHack has already run public sector bug bounty programmes outside of a Covid-19 context, but Harand predicts that the number of government-run projects will surge in the coming months, expanding to cover all core public services. "It is going to be healthcare, it is going to be tax services, it is going to be social security," he says.

Government buy-in is a clear signal that bug bounties are becoming mainstream, but HackerOne's Mickos hopes it is a harbinger of policymakers starting to take the issue of digital security more seriously. Perhaps surprisingly for someone invested in the swashbuckling world of hacking, Mickos thinks tighter regulation and purpose-made legislation are a key part of making a frantically digitising world more secure. "The physical world is in good shape, but the digital world is not, and we are all moving into the digital world," he says. "Society should know that if our lives are governed by software, we must govern software by law."

GETTY IMAGES/JEFF J MITCHELL

President Biden and the new theatre of war

The SolarWinds hack has exposed the centrality of cyber security in geopolitical strategies.
By Jonny Ball

At the beginning of April, large numbers of Russian troops began to gather along the borders of eastern Ukraine. Stretches of the troubled region have been under the control of pro-Russian separatists since 2014, the year so-called "little green men" – special Russian military operatives working without the insignia of the Russian armed forces – appeared all over Crimea, annexing the Ukrainian peninsula.

While this time, Russia withdrew its troops, just over a week after they arrived, the episode had sparked fears of a full-scale land war, one in which the breakaway republics in eastern Ukraine could be invaded and integrated into a "Novorossiya", or "New Russia".

A physical confrontation between Russia and Ukraine did not come to pass (the troop build-up could have been initiated in response to Nato exercises in the Baltic, or as a ruse to push President Biden into attending a summit with Putin). But in cyberspace, breaches of countries' virtual "borders" by state actors – including Russia – are far more common.

Late last year, the SolarWinds attack was uncovered in the US. Microsoft president Brad Smith described this enormous operation as the "largest and most sophisticated cyberattack the world has ever seen". Although Moscow has denied any involvement, the US and the UK governments have both been emphatic that the attack had all the hallmarks of state-sponsored "Cozy Bear" hackers, believed to work under the auspices of the Russian Foreign Intelligence Service. Democratic Senator Dick Durbin described the hack, named after the Texan network monitoring software company through which the security breaches occurred, as "a virtual invasion" of the US. "We are dealing with new weapons of war," said Durbin, "and the Russians continually test the limits."

In all, 18,000 SolarWinds users are known to have been compromised, including US government agencies like the Commerce and Treasury departments, the Department of Homeland Security, and the National Nuclear Security Administration. The hack went undetected for at least nine

President Joe Biden and Vice President Kamala Harris in the White House Rose Garden

GETTY IMAGES/ALEX WONG

months, leading Biden to accuse the Trump administration of "failing to prioritise cyber security".

The full depth and breadth of this penetration into US government systems is still unknown, as are the purposes for which Russia was possibly using this hack. "We still don't actually know what the intent was," says Juliet Skingsley, a military legal expert, "and that's probably one of the most unnerving aspects of SolarWinds." Was this simple cyber espionage, a case of information harvesting through spyware? Or was this a more malicious cyberattack, designed to create glitches and disable defence systems or critical national infrastructure?

"This could take months, if not years, to completely remove the intruder's back doors into the systems and establish whether any data has been stolen, altered, deleted or damaged in any way," Skingsley tells *Spotlight*. But the combative language employed by some US officials and elected representatives has been unhelpful, she adds. "When you have people referring to this as an act of war," says Skingsley, "or akin to an invasion, it's just not true – it's espionage, and in international law espionage is perfectly accepted by all states as a necessary part of statecraft."

The US and its allies are almost certainly engaging in similar activities. In 2010, a sophisticated piece of malware technology, the so-called "Stuxnet" worm, was discovered in Iran. It had been successfully targeted at the country's nuclear facilities, setting its enrichment capabilities back years. An incident like this qualifies as a cyberattack, as opposed to espionage, and the malware is widely believed to have been developed by US intelligence agencies.

Russia "tests the limits" continually

"The Americans are annoyed [about SolarWinds] precisely because it was such a good job," says Mark Galeotti, a Russia specialist at think tank the Royal United Services Institute. "But, to be blunt, if that's not what the [US] National Security Agency or, indeed, [the UK's] GCHQ are trying to do in Russia, I would be amazed. And frankly, if GCHQ isn't doing it, I want some of my tax money back."

In any case, the newly installed Biden administration has reacted to SolarWinds with fury, expelling ten diplomatic officials and imposing stringent new sanctions. "In some ways, Biden has to," says Galeotti, "because it has been such a hot-button issue for the Democrats since 2016." Trump's surprise victory in the election of that year led to accusations of collusion with Russia. Many Democrats thought that online campaigns by anti-Hillary Clinton Russian "troll farms", based at shadowy state-affiliated organisations, had affected the result in key states. A crackdown, then, in the wake of SolarWinds was politically expedient for the new Democratic regime.

Russian President Vladimir Putin, with WWII veterans at the Victory Day parade in Moscow

As well as impositions on Russian individuals and companies, the sanctions attempt to limit Russian access to international credit markets by banning US companies from trading in roubles or rouble-denominated bonds, and prohibiting them from lending to Russia's state financial institutions. In a break with the Trump era, when cyber security roles were abolished and cyber operations in the State Department were scaled back, Biden has also appointed a string of cyber security experts to senior positions in his administration.

"Biden is not actually working for Russia, unlike Trump," Keir Giles, a Russia expert at Chatham House, tells *Spotlight* somewhat hyperbolically. "Therefore, he will be taking more of an interest in protecting the US against threats that come from Russia in particular." He qualifies his depiction of Trump as a Kremlin stooge by conceding that his pro-Russian biases could have been "consciously remunerated or not", but that in any case he had presided over a White House that had seen to pro-Russian strategic goals being accomplished (he cites the weakening of Transatlantic defence partnerships as an example). In a recent research paper, *Assessing Russian Success and Failure*, Giles referred to Trump's period in the White House as "the greatest prize of all" for a malign state focused on "subversion of democracy".

This view is far from universal. Galeotti is keen to stress that despite the Russians enjoying the fallout of Trumpism as a disruptive force in Western democracy, the chaotic Republican populist was no stooge – by the time Trump left office, the US was taking a harder line against Moscow than at any other period since the fall of the Soviet Union. He believes the origins of Trump's victory lie closer to home: "It's so much nicer to be able to feel that some sort of Machiavellian foreign power has done this, rather than thinking, and accepting, that 'OK, my own fellow citizens have voted this way'", he says.

"Cyber is the big security challenge"

Giles, for his part, is keen to stress that whatever the origins of Trump's victory, information extraction and dissemination are key to Russia's geopolitical thinking. For the Putin regime, he writes that "overt or covert armed force [is] only one of the many tools... for resolving foreign policy challenges" – conventional warfare is combined with cyberattacks, disinformation campaigns, fake news, cyber espionage akin to SolarWinds, and the use of irregular troops and proxies in a strategy that has come to be known as hybrid, or "non-linear", warfare. (The term is "a misnomer" according to Giles, but it was popularised after the annexation of Crimea.)

For Russia, Giles adds, cyber in particular is "bound up in the broader concept of information warfare, which covers not only technical aspects of how you work in cyberspace, like hacking or cracking... but also activities in cognitive space". There is, he contends, "a long-standing Russian tradition of using information far more effectively than Western nations have traditionally done".

As Biden begins his presidency and sharpens the US's focus on cyber security issues, it's clear, says Galeotti, that "cyber is the big, looming security challenge". The SolarWinds hack has demonstrated the strength of rival state actors in the field, and has provoked a strong response. "No one quite knows what to do with [the cyber threat], or quite what it looks like," says Galeotti, "but everyone agrees that it's there." The Biden administration may have to learn fast.

GETTY IMAGES/SERGEY GUNEEV

Why companies must get set for a digital future

As technology evolves, so too do the risks attached to it, says **Steve Knibbs**, head of Vodafone Business Security Enhanced at Vodafone Business UK

As cyber security professionals, we don't want to inhibit innovation, but occasionally the blue-sky thinkers need to be reminded about the risk inherent in anything new. Digital technologies are presenting companies with new ways to interact with their customers, and the opportunity to create products/services that would not have been possible even a few years ago. However, for all the good that digital promises, there are individuals hiding in the corners of the dark web waiting to take advantage of any slight oversight or technical nuance. Cybercrime is big business, estimated by *Cybercrime Magazine* to be worth $6trn for 2021.

The intention of such statements is not to scaremonger. It should be taken as a reality check, an element of the due diligence process needed to ensure organisations are not taking unnecessary risks to place themselves or their customers in difficult positions. At Vodafone Business Security Enhanced, our objective is to work with the public sector and critical national infrastructure – organisations who deal with hyper-sensitive data, both commercial and personal – to ensure they can thrive in the digital economy.

We work in partnership with our customers to constantly evolve security protocols, technologies and processes, to keep data in the hands of those who need it, and away from the hands of those who don't. An evolving cyber security strategy should be viewed as a protection mechanism, but also an empowerment tool to facilitate growth.

You have to consider what a cyber security strategy does. Firstly, it protects your assets, employees and customers. A successful cyber attack can have numerous consequences, any one of which may be disastrous – because a large enough incident can stop your organisation functioning. For some, it impacts on making money (the UK government estimates each cyber security incident costs £8,460 on

How much does cyber security damage cost globally?

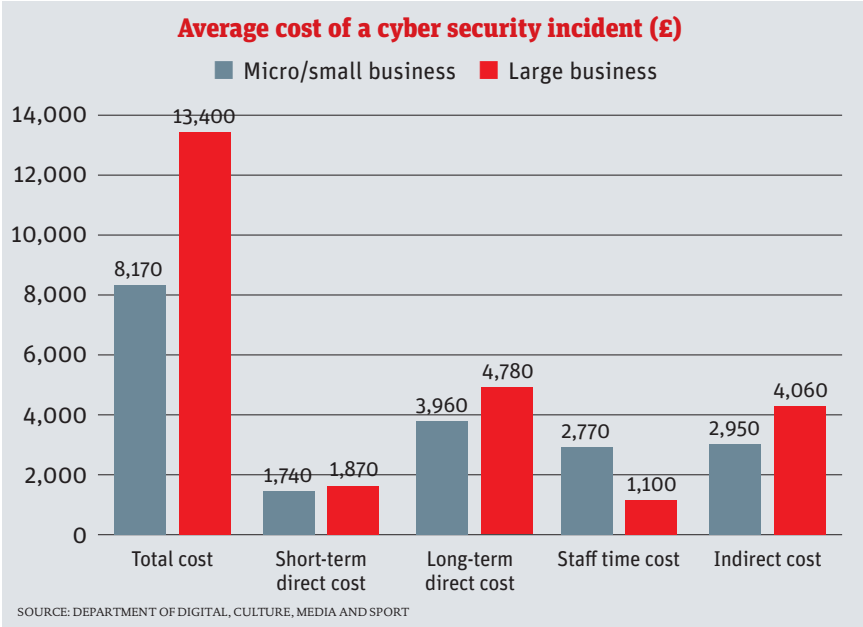
- $6trn a year
- $500bn a month
- $115.4bn a week
- $16.4bn a day
- $684.9m an hour
- $11.4m a minute
- $190,000 a second

SOURCE: CYBERCRIME MAGAZINE, 2020

IN ASSOCIATION WITH

business security enhanced

SHUTTERSTOCK/JKSTOCK



SOURCE: DEPARTMENT OF DIGITAL, CULTURE, MEDIA AND SPORT

average); for others, it affects providing services critical to our daily lives.

Most public sector and critical national infrastructure organisations are responsible for ensuring our lives function the way we expect – read power, water, security, entertainment, transport, emergency services, healthcare and education. Those companies that are not accountable to shareholders must answer to taxpayers, so it is critical they function as seamlessly and efficiently as possible. Either way, there are serious financial and reputational consequences for failing to prepare.

Secondly, a cyber security strategy protects your brand. The impact on a company's brand following a cyber security attack is very difficult to quantify, but you can almost guarantee it will be negative. Today, many of the world's most successful companies are powered by the success of their services or products, as well as the influence of their brands. Companies such as Apple, Google, Microsoft and Amazon have reputations the majority of the world know and respect, and this fuels growth.

By investing in technologies and personnel to reduce the risk of negative sentiment, you are fuelling a potential growth engine for your business. And for those organisations that do not sell their services, such as emergency services, the brand could be replaced by the concept of trust. If the ambulance service is hacked and disrupted, the consequences are frightening.

This is where cyber security investments should be viewed as more than a cost to an organisation. You are demonstrating a proactive and forward-looking position by understanding the risk of digital, perhaps making your products/services more appealing to customers, but you are also protecting your brand from negative sentiment. Commercially, fines could be into the tens (if not hundreds) of millions, while public sector organisations are not fulfilling their promise to the people who depend on them.

Understanding weaknesses is the first step in any effective strategy. This can only be done by identifying the risks and where your organisation might be exposed. We feel this area is underappreciated. According to the Department for Digital, Culture, Media and Sport, only 31 per cent of businesses have a business continuity plan that covers cyber security.

With 20 per cent of the world's internet traffic crossing our networks, Vodafone is in a position to provide insight into developing trends around the globe. Whether it's a new type of threat emerging thanks to internet of things (IoT) devices becoming more common, or a new hacker group gathering momentum in Australia, high-level insight of this nature can be built into an evolving cyber security strategy to ensure protections are as resilient as possible.

Over the past two or three years, it has been plain for everyone to see that cyber attacks and breaches are becoming much more common and significantly more complex and impactful. Research firm Forrester suggest 38 per cent of UK and US companies have lost business because of a cyber incident.

Recognising the risks in digital is a mature way to capture the greatest rewards. That begins with a comprehensive cyber security strategy built into the foundations of the business. By identifying the risk and building it into the overarching model, revenues are protected, customers are protected, and the brand is protected, with the net result empowering the potential of the organisation.

Investing in innovation

Research and development is the key to better connectivity and collaboration within the global technology industry and wider economy, says **Jeremy Thompson**, executive vice-president at Huawei UK

Our growing reliance on technology and connectivity was made clear during the Covid-19 pandemic. These were the tools that enabled us to learn and work from home and access many of the key services we need as businesses shifted online. They helped us stay in touch with our friends and family when our lives were turned upside down.

And there can be no doubt they will be key to the economic recovery we need in a post-pandemic world, fuelling growth and creating the opportunities of the future. For example, 71 per cent of organisations surveyed by Huawei said they would implement a hybrid approach to office and remote working this year. Yet we can only allow technology to play such a significant part in our lives if we feel confident about putting our trust in it.

The next generation of wireless (5G) and fixed-access (full-fibre) technologies can support all sorts of applications, from medicine through to transport or financial services. But as technology evolves, so too do the risks attached to it. And all organisations from governments to small traders have a responsibility to protect their data and their users as best they can.

When we talk about standards, we should not mistake these for regulations for the sake of it. Rigorous cyber security standards are not intended to stifle organisations – quite the opposite. A secure internet, where different providers and users can interact seamlessly, is more likely to encourage innovation, and by extension, a more thriving, globally minded economy.

What is the "splinternet" and why is it best avoided?

The "splinternet" is a term used to describe the co-existence of various internet networks – i.e. those based on different standards and technologies, which results in the fragmentation of the World Wide Web at a conceptual level. This will increase costs for consumers, and limit trade, knowledge exchange or even conversations between people or companies from different parts of the globe.

Technological decoupling – that is, to say, making it so certain technologies cannot work in certain places – would undermine the positive progress that globalisation has made in terms of

SHUTTERSTOCK/ ALPHASPIRIT.IT

business, education and travel. It is in no sector's interest to cut itself off from the rest of the world.

Why is research and development (R&D) so important, and what does this mean for connectivity?

Investment is the key to innovation and Huawei knows that. Our commitment to R&D borders on an obsession. More than half (53.4 per cent) of our workforce, that is 105,000 people, are employed in R&D teams and, as of the end of 2020, we had more than 100,000 patents for products and services. Huawei is equipped to lead on 5G because we have invested in the expertise required to do so.

A shared space with shared rules that benefit and protect everyone should be the aim that companies and governments work towards. Huawei doesn't want to hide away patents. Under a banner of unified standards, and in a cooperative cyberspace, Huawei would relish the opportunity to share innovations with industry partners, and help to establish better connectivity. Everyone wins if we collaborate well.

Huawei's intellectual property needn't be the preserve of Huawei, but rather the catalyst for progress in the connectivity sphere. Huawei wants to follow the FRAND – fair, reasonable and non-discriminatory – principle when engaging with different industry partners on patents licensing. We want our products and services to be available to the masses. This includes companies and consumers in the US, the UK, and everywhere else, for that matter. Huawei wants its intellectual property to create practical value in a globalised marketplace.

Huawei has over 100,000 patents

Again, this is why it is important for the internet to be a shared and collaborative space. Of course, all new products and services need to be secure by design. The best way of ensuring that is to invest in R&D. And on this front, Huawei leads by example, publishing many research papers. Every year, we submit more than 6,000 contributions to international standards organisations, and actively try to advocate for open-source communities.

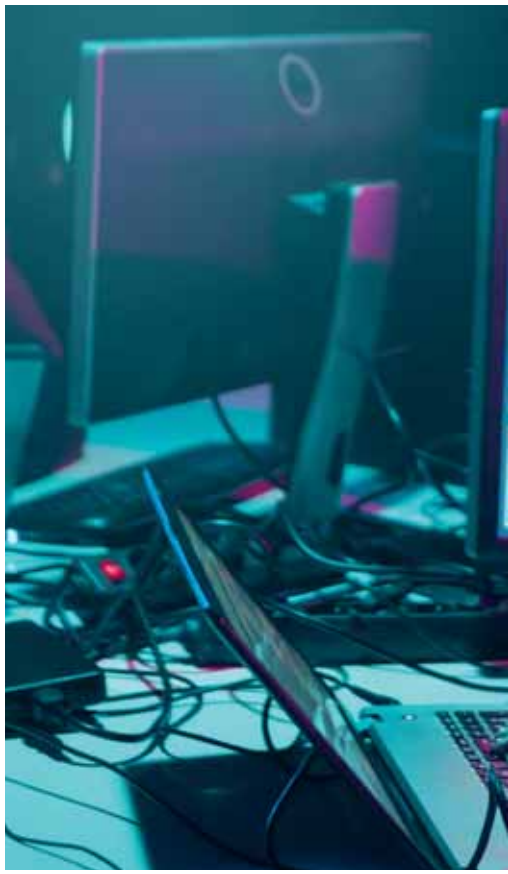
What does the future of internet connectivity look like?

Standards are not meant to spook people. But standards should be strict enough to underscore how important it is to get them right. The onus is on technology firms and governments to work together and make this so.

While Covid-19 may have stunted travel, it did not cause globalisation to abate. The internet kept the world moving. And so, going forward, the internet needs to be reflexive, responsive and able to facilitate and support the many different actors who use it.

Ultimately, at Huawei, we know that people are always more innovative when they can work together. And it is that mentality that underpins our approach to intellectual property. Just as Huawei's patent portfolio includes many of the essential breakthroughs for 3G and 4G previously, we are also well-placed to do the same for 5G. The age of hyper-connectivity is upon us and will transform our lives in ways we can't yet imagine. By sharing our ideas, collaborating on new technology and working in a spirit of transparency, we can build trust in the future so we can all make the most of it. ●

Simon Fell, chair of the APPG on cyber security, on meeting the urgent need for a cyber resilient workforce



How to close the cyber skills gap

Many factors have combined to make cybercrime the scourge of our times. It can be committed from anywhere, repeatedly and anonymously, so the risks to perpetrators are few. Money and information are valuable targets, so the rewards of fraud and hacking can be great. And the disruption to a country or an organisation that a cyber attack can cause can be a potent instrument of power or extortion, or can give a commercial advantage to a competitor. The pandemic has added fuel to the fire, forcing even those with no digital experience to go online to provide or to obtain services as never before. Add to that the number of employees suddenly thrown into the unfamiliar territory of working from home, and you have yet another layer of data security issues for organisations to address, often almost overnight. In today's parlance, it is a perfect storm.

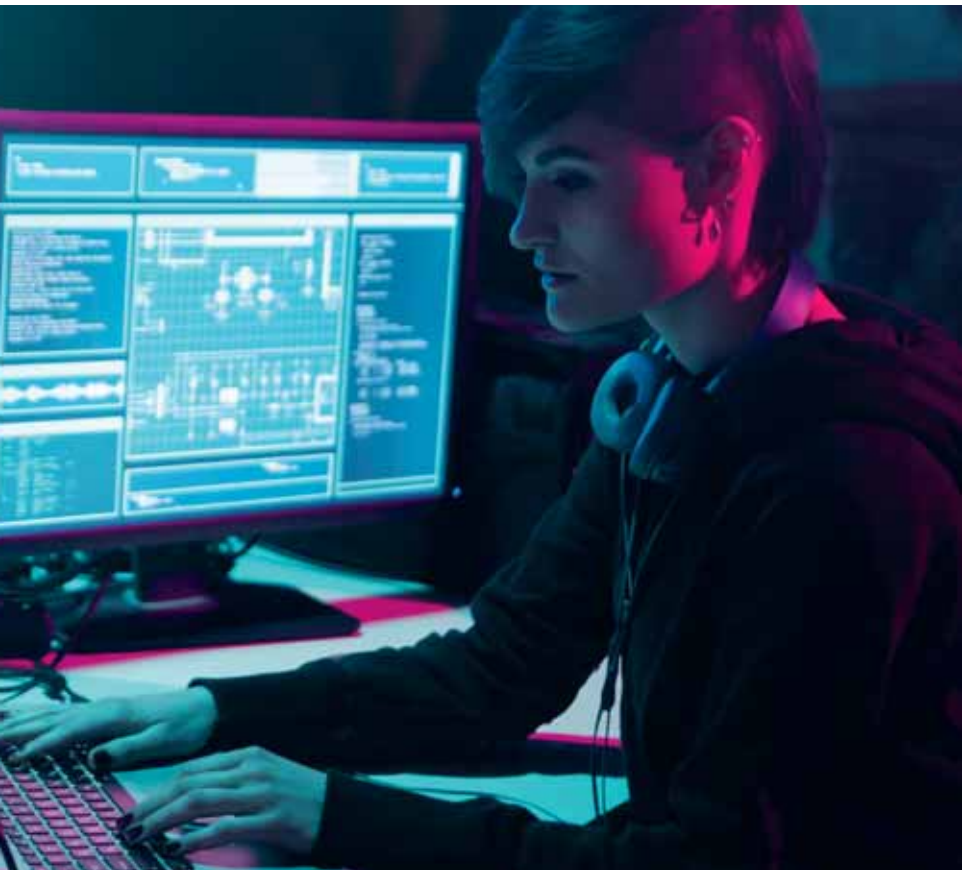
In an economy reeling from the effects of Covid-19, businesses are having to work harder than ever to protect their bottom line. They have also become increasingly aware that cybercrime is indiscriminate and that the likelihood is that, regardless of their sector or size, it could happen to them – so they need to take every possible step to defend their assets. The solution seems straightforward: hire the best, most experienced staff, and take their advice.

Sadly, it's not that simple.

Recruitment specialist Robert Walters and data firm Vacancysoft's 2020 report *Cybersecurity: Building Business Resilience*, found a shortage of 140,000 cyber security professionals across Europe. They also reckoned that 70 per cent of businesses across Europe do not have an adequate cyber security team.

These were findings bolstered by the government's own report *Cyber Security*

The problem is a "ticking time bomb"



GETTY IMAGES/JEFF J MITCHELL

Skills in the UK Labour Market 2020. It found that 48 per cent of the (more than one million) businesses surveyed had a basic skills gap, with their staff having insufficient confidence even to set up configured firewalls, store or transfer personal data, or detect or remove malware. For more complex cyber security skills, including, among others, threat assessments, implementing secure systems, compliance and testing, the gap was even wider, at 64 per cent.

We should be very concerned by these stark figures.

With the threats increasing, and the dearth of skilled staff available to avert them, it is easy to see why cyber security company Kaspersky describe the cyber skills gap situation as "a ticking time bomb".

So what's led to this mismatch of supply and demand? The reports mentioned above identified a number of issues, including:

- Young people discounting, or not even being aware, of such career choices. This is particularly true of young women – something which schools, government, employers and academia must address. Digital poverty in poorer areas compounds this effect.
- The fragmented framework of qualifications and accreditations available in the cyber security area also lead to confusion for students, who can see no clear path ahead, and for employers seeking to find which option best fits their needs. That confusion effectively acts as a deterrent.
- Not all organisations invest in training staff in cyber roles, despite the fact that the rapidly evolving nature of cybercrime makes continuous education imperative.
- Potential candidates sometimes lack the blend of technical and soft skills that employers – especially SMEs – require.

If the skills gap is to be narrowed, then all of the above issues need addressing. In a climate where cybercrime and unemployment are both on the rise, the need to do this becomes ever more compelling. Education and training in all its forms clearly has a central role to play.

Given that educational pathways in cyber security are currently so fragmented, and the differences between the various qualifications and accreditations are not always readily understood, there is work to be done. There is potential for some mapping of all of the qualifications available, so that it is clearer to everyone what is on offer, whether and how they dovetail, and what the pathways are, enabling students and employers alike to choose what best fits their needs. Clearly, it will also be important for government, academia and the business sector to continue to collaborate more closely to ensure that the courses provided are practical and tailored properly to commercial needs. Providers also need to take into account some of the other specific findings of the various reports on skills gaps, and adapt their offers accordingly, ensuring, for example, that they include implementation of skills and soft skills within their courses. Agility will be another vital factor, to allow them to adapt their courses quickly to changing technologies and cybercrime trends.

Another aspect of education is to inspire young people – male and female – to consider cyber security as a rewarding career. Schools and colleges have a role to play in this, communicating the various types of roles on offer, the benefits, the way ahead, and by participating in initiatives like CyberFirst, offered by the government's National Cyber Security Centre.

Employers too have a role to play in prioritising investment in cyber security skills and training for their staff, and ensuring that those skills are regularly updated to meet the sector's ever-changing needs.

This is a complex problem, but one that will not go away. Quite the opposite – there is a growing need for staff with the right skills, and an increasing number of vacancies that go unfilled. It will take a while to solve, but knowing what needs to be done helps to focus attention on, and facilitate, the changes that need to be made. Given the clear risk of not acting, it is imperative that government grasps the mettle on this and ensures that the cyber skills gap narrows.

To pay or not to pay?

How ransomware-as-a-service (RaaS) became the pandemic's most prolific cyber threat. By **Paul Anderson**, director, UK & Ireland at Fortinet

In the past year, the Fortinet FortiGuard Labs team has found a dramatic increase in the cyber threat landscape. Its *Global Threat Landscape Report* determined a sevenfold surge in overall ransomware activity in the second half of 2020. Sectors that have been heavily targeted by these attacks include healthcare, and professional services and consumer services firms, with the public sector being a particularly attractive target. But ransomware has adapted, and the recent spike in its use directly results from the disruption that businesses faced at the start of the Covid-19 pandemic.

In the midst of having to deal with this sudden change in the way organisations run their businesses, the transition to working from home brought critical challenges to IT and security teams. This has been compounded by the fact that IT teams need to ensure that employees are aware of the latest cyber security threats and best practices on how to deal with them.

The growth of ransomware operations

Threat actors generally leverage ransomware to crypto-lock critical systems and business infrastructures, demanding a ransom for the decryption key. Leveraging the threat of releasing the compromised data if demands are not met, it has proven to be a relatively simple and lucrative way to extort money from organisations.

Increasingly, researchers are also seeing encrypted versions of data posted online – not just held for ransom. This is usually along with the threat that if the ransom isn't paid, all data will be released to the public, or sold.

As the volume and frequency of attacks and attackers have drastically increased, a more sinister and targeted form of ransomware scheme has come to the fore.

Traditionally, ransomware attackers have been a few highly skilled coders developing sophisticated malware strains and focusing on making money solely from ransom payments.

That approach has evolved to a service model with its promise of recurring revenue streams from multiple sources. Attackers have realised they stand to make more money by selling or leasing these strains on the dark web to the everyday criminal, and taking a cut from the victim's ransom payments. As a result,

SHUTTERSTOCK/ENZOZO

in the past six months of 2020 there was a steady growth of what is now being classified as ransomware-as-a-service (RaaS), according to the *Global Threat Landscape Report*.

RaaS is proving effective for lower-level cybercriminals who want to jump on the latest boom in ransomware activity, but don't have the technical skills to develop their own malware strains. Demand for RaaS has increased drastically and competition among ransomware developers can lead to special deals being made for aspiring criminals, which could spell disaster for potential victims.

One RaaS threat actor that FortiGuard Labs identified was Smaug, a service that offered ransomware strains that could be deployed across Windows, MacOS and Linux platforms. Most RaaS is restricted to vetted members, but Smaug became a fully public offering in late 2020. Other major players in the RaaS space that organisations need to be aware of are Phobos, Sodinokibi, Conti and Egregor. RaaS makes these types of attacks extremely attractive for cybercriminals, and almost any organisation or business regardless of size or industry can become a potential victim.

Keeping the threat at bay

A compromised digital supply chain and a workforce telecommuting into the network pose a real risk that ransomware attacks can come from anywhere, meaning organisations need to have a strategic, platform approach to cyber security that offers consistent protection and visibility across the entire IT estate and attack surface.

Whether an organisation uses cloud-delivered security solutions, endpoint detection or zero-trust access, a cohesive strategy with the right solutions and an overarching view of the network is the best defence against malware. On top of this, organisations should look at making foundational changes to the frequency, location and security of their data backups as an extra layer of protection.

There is no denying that enterprises and public sector organisations alike face a threat landscape with attacks on all fronts. Threat intelligence remains central to understanding these threats and how to defend against evolving threat vectors. Visibility is also critical, particularly when a significant number of users are outside the typical network scenario. Every device creates a new network edge that must be monitored and secured.

The use of artificial intelligence (AI) and automated threat detection can enable organisations to address attacks immediately, not later, and are necessary to mitigate attacks at speed and scale across all edges. Cyber security user awareness training should also remain a priority; cyber hygiene is not just the domain of IT and security teams.

There has been much debate on the topic of criminalising ransomware payments in an effort to reduce the number of attacks. The official advice from the UK National Cyber Security Centre (NCSC) remains that organisations do not pay ransoms. This debate is likely to continue to divide opinion; however, it can't be ignored that the paying of ransoms can be problematic.

Ransomware and RaaS, in particular, have become more prolific as a result of the ongoing global crisis, with the public sector targeted frequently. It's not going away any time soon and organisations need to know what they're coming up against and how best to mitigate the impact that a ransomware attack has, while understanding that paying the attackers could make their situation worse. But, with a more proactive, platform approach to securing their IT environments and the right cyber security solutions and intelligence, these organisations can be confident that they have the tools to combat these threats. ●

For more information, please visit: www.fortinet.com

The latest contracts, jobs and training

THE LARGEST PUBLIC SECTOR CONTRACTS OPEN FOR TENDERS

Test and Track – Data Platform Services, Department of Health and Social Care
Contract value: £15m
Deadline: 21 May
The DHSC is open to bids from software companies to build and develop new features for the government's Covid-19 tracking app. The contract will last for an initial 12 months.

ICT Infrastructure – Cloud Migration, Shepherd's Bush Housing Association
Contract value: TBC
Deadline: 4 June
The SBHA seeks a technology partner to assist with the development of its digital office capabilities, including cloud-based shared working space, broadband services, and data storage and security. The contract will last for four years.

Network Infrastructure Investment Programme, University of Glasgow
Contract value: TBC
Deadline: 10 June
In light of the shift to mass remote working and learning, the University of Glasgow is seeking a technology partner to modernise its existing network infrastructure, including its on-site internet connections, student and staff intranets, and cloud databases.

IT Software Package – Patient Data, St James's Hospital, Dublin
Contract value: £500,000
Deadline: 31 May
St James's Hospital in Dublin is inviting applications from technology companies to build and maintain its IT infrastructure, specifically relating to storing and protecting patient data. The contract will last for an initial five years.

JOBS NOW OPEN FOR APPLICATIONS

NHS Test and Trace – Senior Service Designers, Department of Health and Social Care
Salary: £49,529-£62,286
Location: Remote
Deadline: 23 May
The DHSC seeks two software developers to work on improving and updating the government's contact tracing app in response to the Covid-19 pandemic over a period of 12 months. They will work on the app's functionality and its ability to keep people's personal data secure.

Cyber Risk Assurer, Home Office
Salary: £57,434-£63,175
Location: London
Deadline: 24 May
The Home Office seeks an experienced cyber security professional to lead on cyber risk management decisions and remedial actions. They will advise and recommend where risks should not be tolerated and escalated in relation to external threats, and conduct regular internal audits of cyber resilience.

Associate Technical Architect, Department for Transport
Salary: £38,654
Location: Birmingham,

Hastings, Leeds, London
Deadline: 26 May
As part of the Digital Services Team, the role-holder will support the roll-out of new technologies and software used across different parts of the DfT. They will conduct regular cyber security audits and offer technical support to non-technical members of DfT staff.

Head of the Incidents and Resilience Unit, Food Standards Agency
Salary: £72,000
Location: Home-based, but with frequent travel to FSA offices in Belfast, Cardiff, London, Birmingham and York
Deadline: 27 May
The successful candidate will be responsible for leading the FSA's efforts to provide effective incident responses to threats to the food system, including supply chain disruptions. They will have oversight of both the physical and digital infrastructure involved in transporting food around the UK.

Senior Data and Technology Insight Adviser, Competition and Markets Authority
Salary: £53,527-£60,599
Location: London
Deadline: 1 June
The Competition and Markets Authority seeks an experienced technologist with a knowledge of finance, economics or law to help shape policy around the regulation of data and the activities of digital companies.

EDUCATION/TRAINING OPPORTUNITIES

MSc Cyber Security, University of Kent
Certified by the National Cyber Security Centre (NCSC), this one-year taught course is aimed at computing graduates with a strong background in programming. It covers encryption, authentication coding, biometrics, network and information security management, and cyber risk within a business context.

MSc Digital Forensics, Cranfield University
The Digital Forensics MSc, available for both part and full-time study, is delivered by Cranfield's renowned Digital Investigations Unit. The course has a practical focus, with scenario-based learning at its core. Students are assessed by a mixture of coursework and independent research projects.

Cyber Security Awareness Training, Bob's Business
Online learning platform Bob's Business offers a range of workplace-based cyber security training courses and vulnerability assessments. From full-scale audits of a company's cyber credentials to individual training programmes around phishing and ransomware, all courses at Bob's Business are certified by the NCSC.

MSc Cyber Security Engineering, University of Warwick
This one-year course is divided into eight taught modules and an independent research project. The course covers network design and security, cyber intelligence in espionage, coding, cybercrime, counterfeiting, and cyber security risk management for companies of all sizes.

Cyber Essentials Programme, CyberSmart
Online training platform CyberSmart is offering a range of short courses in cyber security assurance, with same-day certification available. Courses cover human risk factors, as well as brand management in the event of a breach. Courses can be paid for in monthly instalments.

PhD Studentship, University College London
UCL's department of computer science is accepting applications for PhD programmes designed to equip students with skills and knowledge relating to cybercrime and digital technology policy. Research areas include artificial intelligence, network security, reputation management, cyber security in a military setting, and many others that span the socio-technical divide. The PhD programmes include an independent research project and a work placement.

Tender and framework data supplied by Global Data

GlobalData.

★ SAME-DAY CERTIFICATION ★

Phishing Awareness Training, Cybrary

Training platform Cybrary is offering a range of basic cyber security awareness courses, administered online, and ranging from 45 minutes to two hours, teaching people how to spot common phishing tactics in their emails. Certificates can be awarded on the same day as enrolment.

SHUTTERSTOCK/IGOR POLIVKA

Search Vodafone Business Security Enhanced

business
security
enhanced

Discover Vodafone Business Security Enhanced

Supercharge your cybersecurity against today's everchanging threats

Together we can
vodafone
business