NewStatesman

Spotlight

CYBER SECURITY: DEFENDING MODERN LIFE

James Brokenshire MP / Ian Levy / Jaya Baloo

BAE SYSTEMS

A cyber imperative

Towards the end of November, Manchester United made headlines not because of their prowess on the pitch, but because the club had become the latest target for hackers. A full week after the 20 November cyber attack on the Premier League club, staff still could not access their emails. Manchester United said it was not "aware of any breach of personal data associated with our fans and customers", and had not confirmed – at the time of writing – whether the hackers had demanded a ransom.

Meanwhile, in London a "serious cyber attack" on Hackney Council in October was still causing "significant disruption" to services a month later.

These are only two out of millions of such attacks over the past year, as Ed Targett points out (see page 27). One of the themes of the coronavirus pandemic has been a spike in cybercrime. In August the UN reported a 350 per cent jump in phishing websites in the first quarter of 2020. Many of them targeted hospitals and healthcare systems.

The arc of progress was bending towards the digital before the pandemic, but, as has been repeated ad infinitum, the shift has proceeded at warp speed since Covid-19 upended the world. As is being borne out by the data, this fast pace has come with serious risks to the cyber security of nations, citizens and businesses.

As has also been repeated ad infinitum, the rise of remote and hybrid working has increased system vulnerabilities. The move of many businesses to e-commerce in a bid to survive the effects of Covid-19 restrictions has brought economic benefits, but has been accompanied by risk, too.

Tools for detecting and responding to attacks have grown more advanced as attackers become more sophisticated, as Laurie Clarke reports (see page 16). Artificial intelligence is a double-edged sword. But the key remains, perhaps, in the mundane: raising general awareness of "cyber hygiene". As our lives become increasingly connected with the online world – from work, to accessing government services, to making toast – awareness of cyber risk is not something any organisation can afford to leave just to the experts.

NewStatesman

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

Commercial Director
Dominic Rae

Account Managers
Harry Browning
Arthur Jones
Jugal Lalsodagar

Special Projects Editor
Alona Ferber

Special Projects Writers
Jonny Ball
Rohan Banerjee
Samir Jeraj

Design and Production
Emily Black

Cover Illustration
Sam Falconer

BRITISH SOCIETY OF MAGAZINE EDITORS AWARDS 2017 WINNER

First published as a supplement to the *New Statesman* of 4 December 2020. 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

Government launches cyber taskforce

Rohan Banerjee

The UK government has publicly confirmed the launch of a new defence body, the National Cyber Force (NCF), which brings together personnel from GCHQ, the Ministry of Defence, the Defence Science and Technology Laboratory, and MI6 under one command.

Although it has been in operation since April, the government only acknowledged the NCF's existence last month, alongside an announcement of £16.5bn in new defence spending. Alongside monitoring the UK's security, the NCF will be charged with carrying out offensive missions against terrorists and other organised crime networks. It will also assist with support for government bodies and the military, and help police monitor harmful internet use.

Jeremy Flemming, the director of GCHQ, said: "For over a century, GCHQ has worked to keep the UK safe. Cyber security has become an integral part of this mission as we strive to make the UK the safest place to live and do business online. Working in partnership with law enforcement and international partners, the NCF operates in a legal, ethical and proportionate way to help defend the nation."

New telecoms standards proposed

Rohan Banerjee

The UK government has called on telecoms companies to play a bigger role in safeguarding the country's future national 5G and full-fibre infrastructure, as it tabled a new cyber security bill last month. Following its Telecoms Supply Chain Review, the government has called for Ofcom, its communications regulator, to set and impose new security standards on telecoms firms, rather than allowing the companies to set their own, as is the case currently.

The new bill will give Ofcom "unprecedented" powers, including the ability to fine offending firms up to 10 per cent of their turnover, or £100,000 a day for every day an issue is not resolved. If passed, the government bill will comprise strict standards for building and maintaining digital architecture, tighter controls on the management of customer data, regular audits of third-party tech providers, and more.

Ticketmaster receives £1.25m fine from ICO

Rohan Banerjee

The UK arm of the online ticket sales platform Ticketmaster has been issued a fine of £1.25m after failing to protect its customers' personal data. After investigating a cyber breach on the company's website in 2018, the Information Commissioner's Office (ICO), this country's information regulator, has reported that more than 9 million customers across Europe, using a range of different bank cards, may have had their information stolen.

(CYBER TASKFORCE): GETTY IMAGES/WPA POOL, (COVID): GETTY IMAGES/LEON NEAL, (INDIA APP): SHUTTERSTOCK/RATHONG MANUSTRONG

Ticketmaster has since announced it will appeal against the ICO's ruling.

The ICO discovered a vulnerability in a third-party chatbot tool developed by Inbenta Technologies that was being used on Ticketmaster's payments page. The ICO said that several banks, including Monzo and Barclays, had tried to warn Ticketmaster about suspected fraud, but the company had not taken action quickly enough.

Law firm Keller Lenker has confirmed that it has started proceedings against Ticketmaster on behalf of thousands of victims of fraud.

Covid-19 intensifies cyber issues, says report

Jonny Ball

The National Cyber Security Centre (NCSC) has published its latest report on the progress of the government's National Cyber Security Strategy, which runs from 2016 to 2021. The strategy sets out "the government's plan to make Britain safe and secure in cyberspace", and this latest report is the first to be published since the beginning of the pandemic.

The report emphasises the increased reliance of many UK citizens on digital technologies during the coronavirus pandemic, particularly for individuals and companies that have moved to a remote working model. It also highlights the vulnerability of the UK's critical national infrastructure (CNI) to cyber attack by malicious actors, and says ensuring CNI cyber-resilience will be a priority over the coming year.

The NCSC responded to 600 cyber incidents in 2019 and over 700 in 2020, according to the report. A Suspicious Emails Reporting Service received more than 2 million reports from members of the public in just six months.

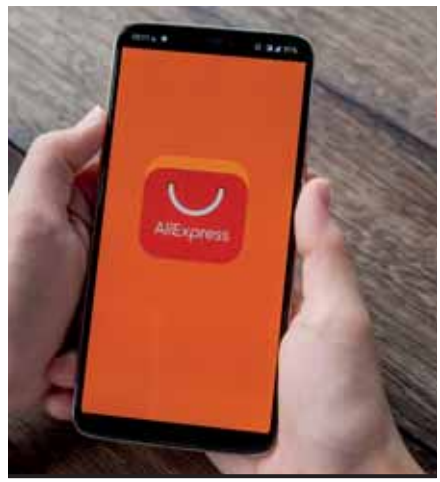
The NCSC's new CEO, Lindy Cameron, formally replaced predecessor Ciaran Martin in October. Martin has joined Paladin Capital Group, a cyber investor, as managing director, alongside his professorship at the Blavatnik School of Government at Oxford University.

Hackney Council breach could last "months"

Jonny Ball

In October, Hackney Council suffered what it described as an "advanced" cyber breach that left many of its online services paralysed. The council has been working with the NCSC on an investigation into the attack, which is still affecting service delivery. In November, the local authority's ability to make and receive payments was severely hampered, as was its online licensing, housing and council tax services. "Some of our services may be unavailable or disrupted for months," the council has warned, but hey pointed out that many had now been either fully or partially restored. Benefit payments and council tax services are said to still be affected.

The council has given little detail on the nature of the attack and has been unable to confirm whether it has been a victim of ransomware. Redcar and Cleveland Borough Council was hit by a ransomware attack in February, costing the authority an estimated £10m.



India continues to ban China apps amid stand-off

Jonny Ball

The Indian government has banned the sale of a further 43 Chinese apps, bringing the total number to 220. Tensions between the two countries have been rising since border skirmishes near the disputed Pangong Lake and China's Tibet Autonomous Region. India has stepped up its rhetoric against China and taken several diplomatic measures, as well as banning Chinese mobile apps over what it cites as "data security issues".

One of the latest victims of India's app bans was AliExpress, the e-commerce platform founded by the billionaire Jack Ma. In November a multibillion-dollar Initial Public Offering for Ma's Ant Group, an affiliate of AliExpress and his Alibaba conglomerate, was cancelled at the behest of Chinese regulators. There is speculation that the decision was linked to his criticisms of China's state-owned banks. While Indian and Chinese diplomatic and military officials remain locked in talks over their border issues, popular video sharing service TikTok, as well as WeChat, Baidu and AliExpress, among others, will be removed from India's app download platforms.

The National Cyber Security Centre offices in Victoria, London

How to live and work safely online

James Brokenshire, Minister of State for Security, outlines the government's cyber security strategy against the backdrop of Covid-19

It goes without saying that the coronavirus pandemic has fundamentally changed how we go about our daily lives. We are spending more time at home and are more reliant on the internet for work and services such as food shopping and banking.

Today's technology has helped keep us connected and maintain contact with friends and family. However, it is a sad reality that scammers, fraudsters and hackers will seek to exploit any opportunity to steal money or data from businesses and individuals. The pandemic has been no exception, with cyber criminals attempting to capitalise on people's anxieties.

But those behind this despicable opportunism are firmly in our sights. Across government and law enforcement, we are determined to ensure they have no safe spaces to operate in. It is critical that our citizens and businesses can operate safely and securely online. Central to that effort is the world-leading National Cyber Security Centre (NCSC), which is working around the clock to help keep our country safe.

Figures released recently underline the shift in the threat. Between September 2019 and August 2020, the NCSC dealt with a total of 723 cyber incidents. Almost 200 of these – more than a quarter – were Covid-19 related. With the rapid increase in home-working, the NCSC has published guidance to help people and organisations large and small stay secure online. While the pandemic has undoubtedly brought fresh scrutiny of these threats, tackling cybercrime has been a priority for the government for a number of years.

Alongside the NCSC, the National Crime Agency has been making an important contribution in the fight against cybercrime. For example, in December last year, a multi-year investigation from the National Crime Agency and US partners in the FBI led to the indictment of the suspected leaders of a Moscow-based cybercrime group known as "Evil Corp", who had allegedly stolen at least £75m through

SHUTTERSTOCK/SIMONA FLAMIGNI

Covid-themed email scams are on the rise

malware attacks. We have been working closely with law enforcement partners to develop an effective, coordinated response at both a local and national level.

Our five-year National Cyber Security Strategy, backed by £1.9bn of investment, was launched in 2016. It brings together the best from government and industry to strengthen our defences and fight criminals. At a local level, we have funded dedicated crime units in each of the UK's 43 police forces, to ensure that all local businesses can access advice and support on how to guard themselves online.

As well as ruthlessly pursuing the criminals behind cyber attacks, we have created dedicated Regional Cyber Resilience Centres. These bring together police, academia and local businesses to provide help to small and medium enterprises that fall victim to attacks and guide them through recovery. We know that businesses need the right support to protect themselves. The NCSC provides high-quality security advice to ensure all UK businesses, from sole trades to large, global organisations and critical national infrastructure, are fully equipped and secure. All advice is informed by the latest information on the current cyber threat.

There is no doubt, however, that the pandemic has brought the threat of cybercrime into sharp focus. For example, there has been an increase in coronavirus themes in "phishing emails", emails that lure users into disclosing sensitive information or downloading malware.

So we have provided funding for the NCSC Suspicious Email Reporting Service, which allows people to forward any emails that cause concern to report@phishing.gov.uk so they can be properly investigated, and malicious content can be taken down. The latest statistics show that this service has led to the removal of 18,071 scams and the taking down of 39,313 URLs.

It is also important to emphasise there are some simple but effective steps that everyone can take to help protect themselves. They include: creating a strong password to your email that is different to all your others, as personal email accounts often contain useful information to hackers; making sure you create a strong password using three random words; using the same passwords for all your accounts makes you vulnerable; saving these in your browser saves you having to remember them all; and turning on two-factor authentication, a free security feature that gives you extra online protection and stops cyber criminals getting into your accounts, even if they have your password.

While we are taking concerted action to tackle the threat of cybercrime, we are not complacent. We are working on the next National Cyber Security Strategy and hope to set out more detail on this next year. We remain committed to making the UK the safest place to live and work online. But that collective mission extends beyond government and law enforcement – and everyone can play a role by remaining alert and ensuring they protect themselves during this unprecedented time.

The future of threat intelligence

Predictive analytics must be an essential component of companies' cyber resilience strategies, says **Kevin Brown**, managing director at BT Security

The pervasiveness of technology – more and more products and services are becoming digital, with that transition sped up by lockdown measures against the coronavirus pandemic – has led to a massive expansion in the quantity of data we create and transmit. In both our personal and professional lives, we are accessing and creating more data than ever before. As the Internet of Things (IoT) becomes more inclusive, it is important to note that with convenience come new risks to mitigate.

New technologies present a challenge for cyber security organisations that rely on having oversight of as much data as possible, and the ability to analyse, contextualise and act upon it quickly. While older technologies placed a limit on the quantity and pace of data they had to deal with, in 2020 those limits are now being stretched. Consider, for example, that BT's Assure Cyber Security Platform was receiving around 100,000 events per second in mid-2017. That has now increased to around two million events per second.

As so-called attack surfaces expand, particularly within the context of the home-working revolution catalysed by Covid-19, companies must become more cyber resilient. Organisations need full sight of the scope of threats they may be facing. At BT Security, we are constantly investing to evolve and improve the platforms that we use to assimilate and analyse data, so that we can spot these threats. We are utilising advancements in artificial intelligence (AI) and automation tools to enable faster proactive detection and analysis of anomalies, and the immediate implementation of proven techniques to prevent and disrupt attacks.

These have been supported by our R&D team, which has spent many years developing innovations which allow us to rapidly analyse real-time data and to build predictive models that forecast and anticipate threats. All of this allows us to automatically put defences in place before cyber attacks happen, and is a strategy that we are employing to protect customers.

We are also constantly learning from the insights that we gain from protecting our network and our customers across 180 countries. For example, the past few months have seen a surge in extortion-focused distributed denial of services (DDoS) and ransomware attacks as

criminals look to capitalise on the changes 2020 has brought. The graph (Figure 1) gives an example of how cyber criminals adapt to and exploit changing conditions, with the quantity of DDoS attacks rapidly increasing as much of the world moved to remote working.

Our insight also allows us to see how cyber trends don't proceed in a linear fashion. For example, the "Emotet" malware first surfaced in 2014, and has continually evolved and adapted. Emotet initially was spread via spam emails, before developing to propagate "intelligently" to other devices on the same network – creating a huge risk for businesses. Despite the many protections that have been put in place against this malware, it is still devising variations that create new issues.

In the modern world, it is vital that organisations are able to forecast the cyber challenges they will face and able to prepare in advance for an attack. Cyber security must transition into cyber resilience – which is proactive, rather than reactive. Companies' cyber strategies are no longer the preserve of IT departments. Cyber resilience must start in the boardroom and trickle down to the individual, particularly as working from home continues.

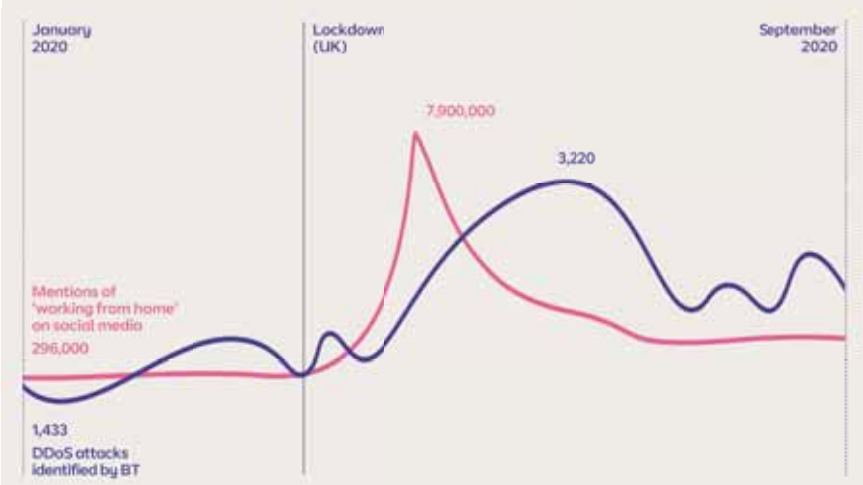


Figure 1

Technological convenience also creates new risks

Organisations need to maintain and update their defences, leveraging AI and automation where possible, but all the while briefing employees on those changes. Cyber resilience is not an option for businesses going forward; it is a necessity. ●

For more information, please visit: www.bt.com/security/we-see-further

SHUTTERSTOCK/IMYANIS

The technical director of the National Cyber Security Centre, Ian Levy, on rising cybercrime and protecting vaccinologists. By Oscar Williams

An unusual year

As the government's most senior cyber security expert, Ian Levy always has a heavy workload. But 2020 has been unusually busy, even by his standards.

As the technical director of the National Cyber Security Centre (NCSC), the daunting list of tasks to have faced Levy over the course of the year includes overseeing the security appraisal that led No 10 to ban Huawei, protecting the NHS, vaccinologists and government networks from hackers, and devising systems to help businesses and consumers safely and securely navigate a period of unprecedented digital upheaval.

Following the publication of the NCSC's annual review last month, we spoke to Levy about his work and how the pandemic has shifted the security landscape. The interview has been edited for clarity and length.

Spotlight: Your report noted a sharp increase in ransomware attacks this year. Why has that form of malware taken off in such a big way in 2020?
Ian Levy: I wouldn't necessarily look at ransomware as a type of malware. It's a business people are in, and a piece of malware is a part of that. It's certainly evolved over the last couple of years. It used to be that people would throw out malware and if people looked like they could pay for it, they'd go and ransom them.

That seems to have changed quite considerably, and it seems to have become much more targeted. People are going after particular organisations – spending lots of effort to get in there, understand what the crown jewels are, deploy stuff in a very stealthy way, make sure they can exfiltrate – so they breach data as well as ransom it, and so on.

The short answer is because that's where there's money. It's developed into a proper business now and that's the way we're going to have to go after it.
S: Has the pandemic and the rise of remote working also made people more susceptible to ransomware?
IL: I don't think we've got the data to show that to be a causal thing, but certainly we see lots of different threat actors using the pandemic as a lure for their attacks, whether that's someone sending out hundreds of millions of emails to citizens saying, "pay here for your test", or it's a very direct hit against specific people in specific organisations to achieve something. It could be intelligence, it could be ransomware, it could be anything.
S: What work have you done to assist government departments and major businesses in transitioning to remote working?
IL: We've published a whole bunch of guidance on the website which helps individuals and organisations of all sizes to understand the different sorts of threats and risks they can be exposed to through this. There's design guidance, there's understanding about threats, and we're sharing lots of threat information directly with organisations so that people can defend themselves better.

For the public sector and the health service, our protective DNS service filters [out attacks]. We put all the information we know about that DNS server on to it so that they can be protected. A couple of weeks ago, we completed the entirety of the health and social care network onto that service.

NCSC

Boris Johnson during a visit to the Jenner Institute in Oxford in September, where he met scientists who are leading the Covid-19 vaccine research.

"Covid-19 has become a lure for cyber attackers"

They are now all under its protection.

S: Tangentially related to that is the work you've been doing to protect British vaccine research. Are you able to talk about how you've sought to protect vaccinologists at Oxford University, Imperial College London, and some of the other places where this research has taken place?

IL: The type of service we provide to a public sector organisation is different to somewhere like a university. A university has its own infrastructure and they can manage that perfectly well themselves. It's about us giving them better advice, better guidance, better data. But also making sure they are on our list of organisations to care about. So if we watch a particular threat actor, and we see [researchers] being targeted, we can use them to go and talk to them and say: "We need you to do these things because we can see an attacker preparing to do something or another." That obviously doesn't scale very well. It's very, very resource intensive.

The vaccine taskforce directs our work on this. They tell us who they want us to put that resource against. But what we're doing is trying our best

GETTY IMAGES/ KIRSTY WIGGLESWORTH/POOL/AFP VIA

to make sure that the vaccine research remains integral and confidential and all the other things it needs to be, but more importantly that the testing is integral. So the test results are absolutely authentic and haven't been messed about with.

S: What are you actually looking for?

IL: It's a bit of a cartoon. If you're looking at communications and how people attack systems, they have to send some packets to those systems. Those packets have to go over networks and they have particular characteristics. If we happen to see one of those, that will alert us that something might be going on.

Similarly, if you know that particular infrastructure is used, some of those indicators of compromise might be, "oh they're using this particular IP address". If you then see a connection from that IP address you know it's likely to be related to an attack. So it's those sorts of things, it's using the knowledge and intelligence they have and turning them into actionable things that either organisations can do themselves or we can do on behalf of those organisations.

S: There have been reports of GCHQ (NCSC's parent agency) targeting cyber attacks at state-sponsored anti-vaccine campaigns, and of a new cyber force. Would NCSC or GCHQ take offensive action against one of the groups seeking to target the researchers?

IL: Any sort of response, whatever that response is, needs to be part of a campaign and needs to be a government response. NCSC wouldn't do something unilaterally. It would need to be part of a government response. Obviously, any use of any offensive cyber capability has to go through very strict oversight and authorisation regimes. And that's a government-wide thing. The offensive cyber capability that has been talked about is a tool and toolbox to be used as the government sees fit, under the appropriate authorisation and oversight regimes.

S: I guess you can't tell me then whether offensive action has been taken then…

IL: Correct. Sorry!

S: Have you seen attacks on researchers take place in recent weeks? Has the pattern of these attacks changed over the course of the year?

IL: We've talked about some of the nation state-sponsored attacks that we've seen against vaccine research. It's reasonable to say that vaccine research is among the most valuable intellectual property in the world. So you would imagine a bunch of people being interested in it. Our job is to make sure their job is as hard as it can be while still allowing those organisations [to do what] they have

"Our job is to make hackers' lives harder"

to do… You could put security in place that is not quite impenetrable – because nothing is ever impenetrable – but it would mean those organisations could not do their work. So there's always a balance to be had here.

S: Are you confident that no British IP has been breached?

IL: I'm not going to answer that one I'm afraid… You can't prove a negative.

S: The Trump administration imposed tough restrictions earlier this year on Huawei's use of American chip technology. The NCSC said this would make it significantly harder to reliably test Huawei's telecoms kit and you advised the government you could no longer manage the associated security risks, triggering a seven-year phase-out.

With Joe Biden having won the presidential election, there has been speculation that the US restrictions might be eased, although this is still uncertain. If Huawei's old supply chain was restored under a Biden presidency, would you change your guidance?

IL: No, and we've said so publicly. The Chinese state as a sovereign country is never going to be dependent on one of its main strategic allies ever again. Regardless of what the US does over the next couple of years, the Chinese are now on a course of building sovereign capability. Whether it's this year, next year, five years time, it doesn't matter, the same risk accrues.

Remember when you're talking about critical infrastructure, you're often talking about 15-year life. If you're talking about when the risk actually starts and when it accrues, it doesn't really matter. Certainly in all of the different situations we've gamed out, we can't see us changing our advice.

CISOs should prioritise the "human firewall" during Covid-19

The pandemic has introduced many significant cyber security challenges, none more so than the hybrid home worker, says **Richard Beck**, director of cyber at QA

IN ASSOCIATION WITH

The pandemic has driven a huge increase in the adoption of "collaboration tech". According to McKinsey's most recent global survey of executives, remote working and/or collaboration increased more than 40 times more quickly than executives thought possible before the crisis. Chief information security officers (CISOs) have had to race to empower remote workers by providing access to collaboration tools such as Zoom or Microsoft Teams and secure access via virtual private networks (VPN), balancing the need to enable productivity with the responsibility to minimise organisational risk.

Adapting to this new way of working has not been without issue. Remember the early days where uninvited guests barged into meetings and high-profile individuals shared sensitive conference meeting details on screen?

We have now become accustomed to family members making an appearance in our team meetings and our colleagues have become a little more conscious of secure ways of working. For example, when taking part in video meetings, we are more sensitive to what appears behind us when on camera. However, full-time remote working on such a large scale, with cloud-based scanners and printers, and unsecured home routers sharing interconnected home devices, including Alexa or smart TVs, has increased the digital attack surface a CISO has to protect.

At the same time, our heightened curiosity for Covid-related information has elevated the risk of email-borne threats. Eager to read the latest data about the pandemic, or distracted with events happening at home, our guard is lowered, making us all easier targets. Researchers at security firm Barracuda reported a 600+ per cent increase in worldwide email phishing threats with a coronavirus theme during March 2020 alone.

Covid-19-related fraud is a genuine challenge for the CISO because the behaviour and actions of our staff are now less predictable. Worryingly, in a recent survey by cyber security firm Tessian, 48 per cent of respondents said they were less likely to follow safe data practices when working from home. Extending the corporate security reach into the home to discover if this working environment is safe or has already been compromised will be a persistent challenge post-Covid.

So how should the CISO respond? New working environments – and the associated changes in risk profiles – demand new responses. Working hours have changed, with colleagues now establishing really quite diverse working patterns to provide a work-life balance. This changes the traditional threat profile that the security team has worked hard to understand. Security teams must carry out new modelling scenarios that work through what could go wrong in the new

work-from-anywhere environment – for example, security threats caused by home tech – and revise incident response procedures accordingly.

Previously, scenario "playbooks" were likely to have had guidance on how the security team should deal with an affected laptop or device they could physically access. If the workforce is dispersed across a wide geography, then third-party incident response services could be critical to recovering an incident. Dusting off and, if the opportunity allows, renegotiating and reviewing both parties' obligations should be a high priority. Alternatively, building the capability internally may provide more control and more flexibility to deal with the unexpected. Building capability internally is a great opportunity to invest in an organisation's most valuable asset – its staff. It is also a clear signal to the rest of the business that cyber security is being taken seriously.

The "office" landscape has changed forever

SHUTTERSTOCK/FIZKES

UK households have, on average, 10-15 internet-connected devices, which with the continued explosion of the Internet of Things (IoT), is set to rise to 50 by 2023. This presents increased complexity as data moves in-transit across global networks, cloud platforms and apps, sometimes out of sight of the organisation's security controls. It is imperative that the training cyber security professionals receive is frequent and reflects the latest threats an organisation is likely to encounter. For example, using a simulated environment to better prepare for the changing threat advisory builds internal competence – and confidence – in a safe-to-use gamified cyber practice range.

With state-of-the-art virtual learning labs and gamified learning provided by organisations like QA, there is no reason for Covid-19 to be a barrier to regular and engaging cyber security training. Instead, learning should be a key driver for organisational culture, which is likely to need constant reinforcement in times of change, especially when many are physically disconnected from the office and co-workers.

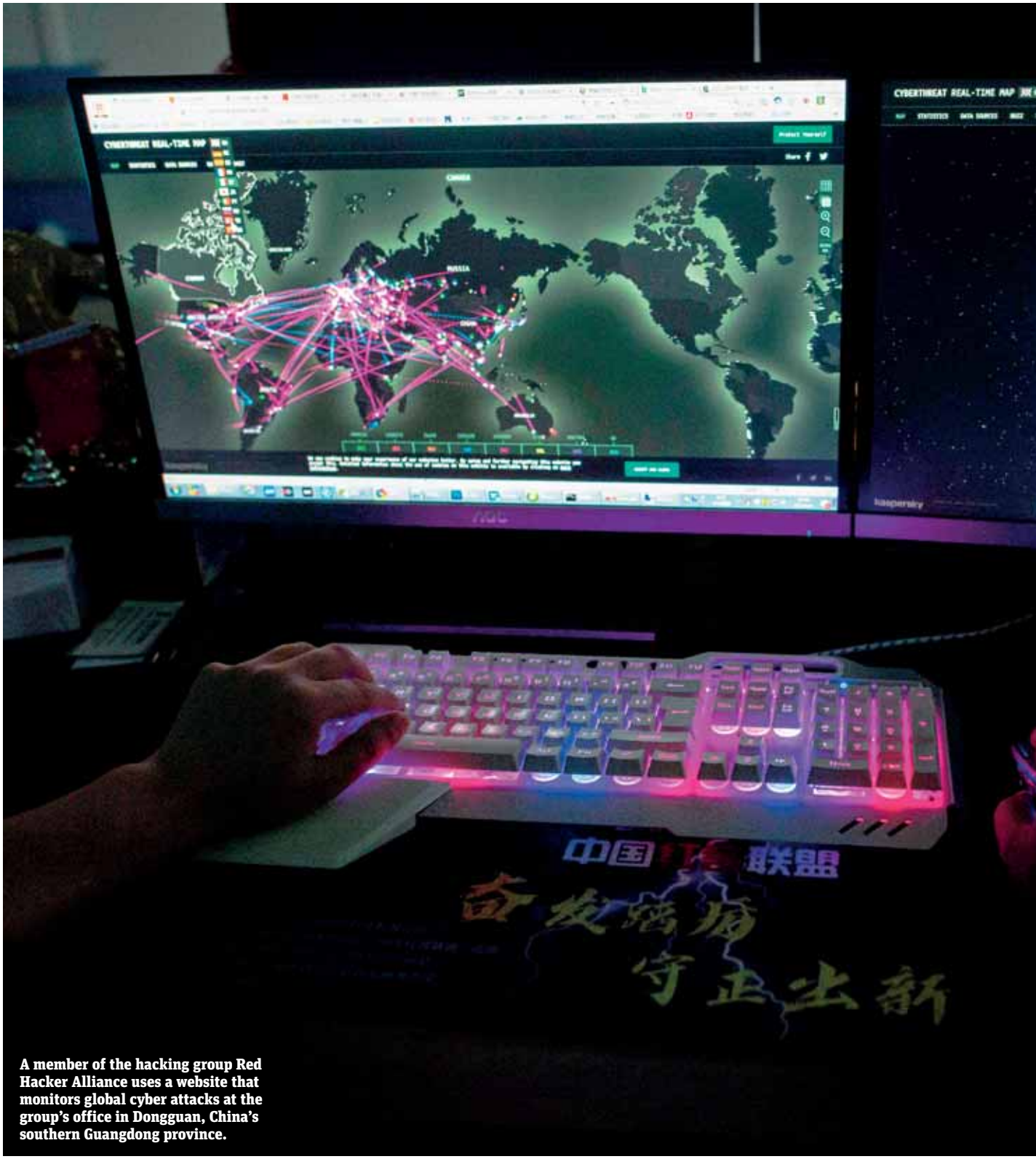
Why education and training are key to cyber resilience

As employees look to balance convenience and productivity at home, work data is now regularly traversing both corporate and personal devices. Borderless challenges require security training for every user in the organisation. Transferring security culture and hygiene into the home-working environment is paramount.

The emergence of technology like Amazon AWS or Microsoft Azure hubs that can protect all of our integrated devices will help secure, regulate and protect interconnected remote worker devices. Using this type of solution, CISOs can not only secure the corporate perimeter but help staff protect their increasingly connected homes, their digital personal lives and their loved ones from cyber threats. At this point, we will begin to strike the right balance and empower employees to become more cyber-resilient without compromising productivity. But we have to continue to educate our best line of defence – the "human firewall" – to be vigilant and security-conscious at home.

During a time of change, we have the opportunity to enhance security culture and improve behaviours, with role-specific security training and staff hygiene adopted by every member of staff for the new normal. This should also include targeted messaging for executives working from home. It is worth noting that many new homeworkers may lack the digital skills – or inclination – to safeguard their smart tech in the home. CISOs need to prioritise and educate to protect their organisation and staff whenever and wherever they work. ●

QA has armed more than 17,000 individuals with cyber security skills over the past five years. QA's cyber portfolio is aligned to the NCSC Cyber Body of Knowledge (CyBOK) and delivered through instructor-led training and hands-on learning environments including cyber labs and cyber challenge events.



A member of the hacking group Red Hacker Alliance uses a website that monitors global cyber attacks at the group's office in Dongguan, China's southern Guangdong province.

GETTY IMAGES / NICOLAS ASFOURI

How AI changed online security

Laurie Clarke

Cyber attacks are predicted to cost the world $10.5trn each year by 2025. It's a trend that has accelerated during the Covid-19 pandemic. At the height of the crisis, Kaspersky reported soaring remote desktop protocol attacks on home workers, while IT security company Barracuda Networks found that Covid-related email scams leapt by as much as 667 per cent.

"Artificial Intelligence is playing an increasingly significant role in cyber security," says Kevin Curran, a researcher at Ulster University. According to a study last year by Capgemini, a consulting and services group, 61 per cent of firms say they cannot detect breach attempts without using AI tools.

AI has a range of applications in cyber security, including network security, fraud detection, malware detection, and user or machine behavioural analysis. Its most popular application is in network security, where "the huge dimensionality and heterogeneous nature of network data" as well as the "dynamic nature of threats", make it extremely useful, Curran says. "AI can use statistics, artificial intelligence, and pattern recognition to discover previously unknown, valid patterns and relationships in large data sets, which are useful for finding attacks."

AI and machine learning systems can scan an organisation's information systems to preemptively discover vulnerabilities. These AI network-monitoring tools can detect and fix more irregularities than humanly possible by processing all of an organisation's relevant data to create a picture of the "baseline" threat level. Any significant deviation from this baseline will result in the model flagging the activity as suspicious.

As such, AI can be important for reducing "zero-day" attacks – where hackers take advantage of vulnerabilities in the software before developers can fix it. Curran says this market is "flourishing".

But AI can also be wielded by malicious actors for large-scale attacks. Malware is increasingly automated by cyber criminals. Conventional cyber security systems flag malware attacks by identifying malicious code, but because attackers often tweak the code, it is difficult for traditional security software to spot it. AI systems can check the code against a vast database, and so they are much more adept at designating it as potentially malicious, even when the malware is incorporated into benign code.

"Building static defense systems for discovered attacks is not enough to protect users," says Curran. "More sophisticated AI techniques are now needed to discover the embedded and lurking cyber intrusions and cyber intrusion techniques". But security professionals are quick to caution against AI evangelism. Humans will still be integral to security for the foreseeable future – necessary to fine tune AI models and see if they are working correctly. If not, organisations can be lulled into a false sense of security. And this could lead to far more devastating attacks.

Laurie Clarke is a senior reporter at Tech Monitor

The cyber skills gap

Earlier this year, the Department for Culture, Media and Sport and Ipsos Mori surveyed businesses on cyber security skills shortages. They found:

Source: DCMS and Ipsos Mori 2020

27% have a skills gap in incident response

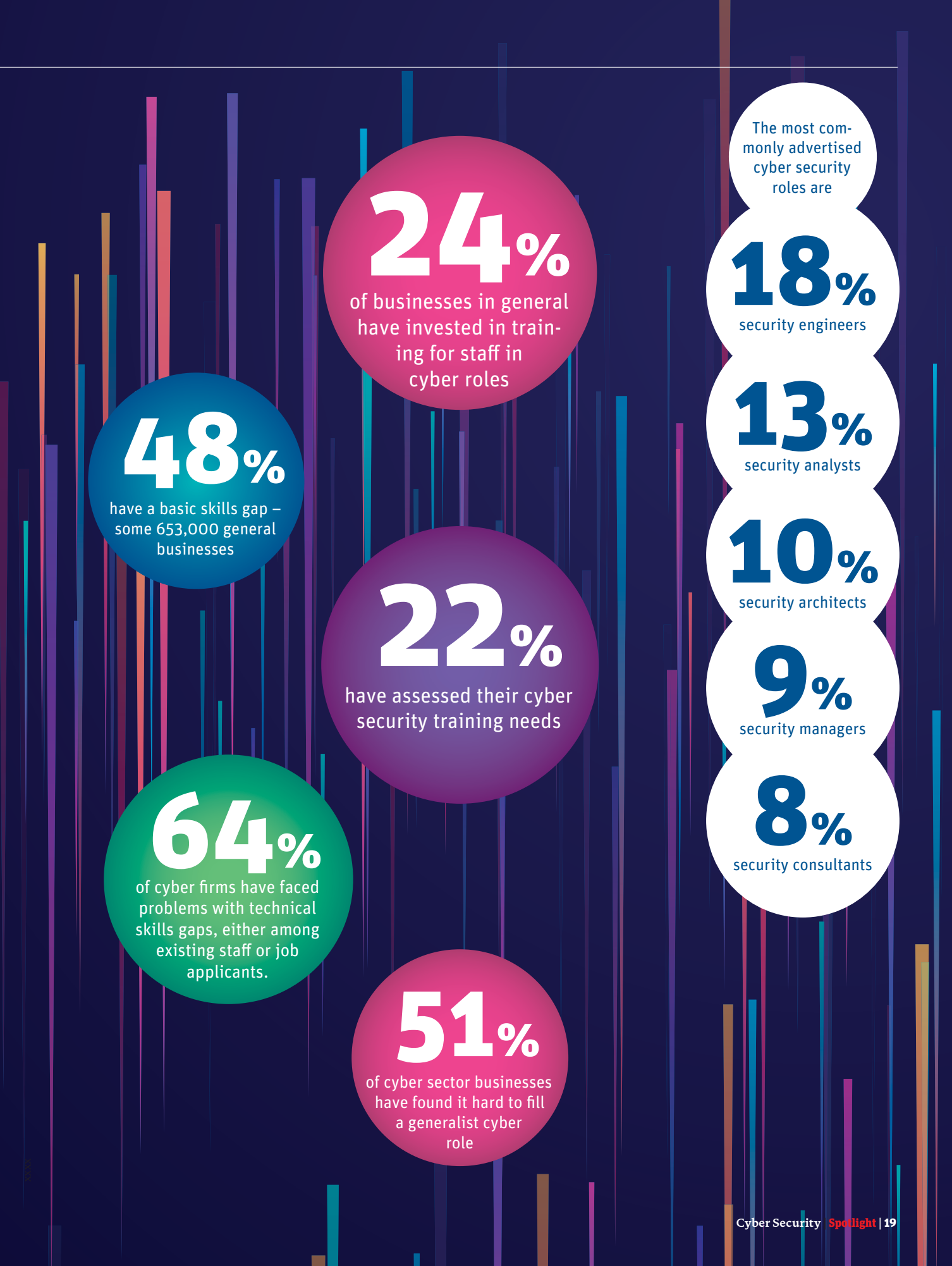
30% have advanced skills gaps, particularly in penetration testing, forensic analysis and security architecture

THE CYBER SECURITY WORKFORCE

15% are female

16% come from ethnic minority back-grounds

9% are neurodivergent


24%
of businesses in general have invested in training for staff in cyber roles
48%
have a basic skills gap – some 653,000 general businesses
22%
have assessed their cyber security training needs
64%
of cyber firms have faced problems with technical skills gaps, either among existing staff or job applicants.
51%
of cyber sector businesses have found it hard to fill a generalist cyber role
The most commonly advertised cyber security roles are
18%
security engineers
13%
security analysts
10%
security architects
9%
security managers
8%
security consultants

A personalised approach to cyber security

Understanding hackers' motives and tactics is key to better defensive strategies, says **James Muir**, threat intelligence research lead at BAE Systems Applied Intelligence

At the end of October, dozens of US hospitals were compromised in a series of apparently co-ordinated ransomware attacks. The disruption these caused to healthcare organisations currently battling Covid-19 was morally reprehensible, but sadly not an uncommon sight. The truth is that certain ransomware groups today are operating with a sophistication that a few years ago would have been the preserve of only state actors and a select few organised cybercrime gangs.

Improving our threat intelligence capabilities is the best chance we have of understanding, disrupting and mitigating the business risks that the cyber threat landscape poses. This will not only require buy-in from chief information security officers (CISOs) and boards, but changes to the threat intelligence industry itself.

What have we learned?

By volume, the majority of the threats seen on a daily basis are automated, commodity attacks— "spray-and-pray" efforts designed to catch out organisations and individuals who have obvious gaps in their defences. The real threat to businesses, however, comes from more targeted approaches, such as the "human-operated" or "hands-on-keyboard" activities seen in the evolution of ransomware attacks in recent years, and the motivated and persistent targeting of state-backed threat groups.

Ransomware operators have found a number of ways to get scale and speed in their attacks. Scanning for exposed Remote Desktop Protocol (RDP) logins, and exploitation of vulnerabilities in networking services are two popular techniques for gaining access; tried-and-tested approaches using phishing emails also remain prevalent. Off-the-shelf pen-testing tools such as Cobalt Strike and "living off the land" techniques are used to blend in and move laterally. This allows the operators to stay undetected, providing the time needed to exfiltrate large amounts of data for "double extortion" attacks, and deploying ransomware across the victim estate. Recent cases have shown that these attacks can move from "end to end" in a matter of hours.

While the limelight of the threat landscape has been dominated by ransomware in 2020, a number of other developments have been taking place. State actors have diversified their interests, and while sectors such

SHUTTERSTOCK/JELENA ZELEN

as government and defence remain key interests, healthcare and Covid-19 responses have occupied a greater portion of their tasking.

Furthermore, "hacker-for-hire" groups such as Dark Basin have come to the fore in 2020. Such activity is increasingly commonplace, with groups such as these tasked to obtain login credentials and network access to targets in a range of sectors.

What can be done?

Security experts often talk about the need for IT hygiene: best practices like prompt patching, endpoint security and multi-factor authentication. These certainly play an important role, and the steps outlined by the National Cyber Security Centre (NCSC) and the government's Cyber Essentials scheme are a great place to start. Yet best practice security will only get you so far, and time has also shown us how difficult it can be to "do the basics right" without leaving gaps.

To proactively enhance threat defence, you need to understand the tactics, techniques and procedures (TTPs) of those seeking to harm your organisation. Threat intelligence is therefore a strategic necessity for a growing number and range of organisations – including those who may not traditionally have thought of themselves as targets of motivated attackers. When done effectively, threat intelligence allows CISOs to be more proactive about security, stopping attacks before they've had a chance to cause serious reputational or financial damage. Threat intelligence can also help to improve resilience, for example by enabling security teams to prioritise patches based on which vulnerabilities are being currently exploited.

Intelligence sharing can help deliver a safer society

An industry-wide challenge

However, there are some industry challenges which threaten to undermine the organisational ability to reap these kinds of strategic benefits. On the supply side, the glut of threat intelligence offerings on the market – few of which offer a comprehensive range of capabilities – means those that can afford to buy multiple overlapping solutions, while smaller peers aren't able to get complete coverage.

On the consumption side, many users of threat intelligence find it challenging to optimise their solutions. The result can be response teams chasing the wrong leads, or being flooded with alerts which they can't prioritise. In some cases, the data itself is too old to be useful.

Many in the industry are calling for more intelligence sharing. If systems were free and open to all comers, they could be infiltrated by nation states and cyber criminals. On the other side, if barriers are put up around intelligence sharing organisations, those without economic clout may be left at a disadvantage. There are also persistent concerns that too much sharing could damage brand reputation.

These are difficult problems to solve, but one initiative offers some prospect for positive change. The Intelligence Network is a BAE Systems-backed body focused on safeguarding society in the digital world by changing the way we think about cyber security. Its 2,000+ global members include cyber and financial crime professionals and industry influencers committed to creating a safer society. We have already ear-marked seven crucial areas for change by 2025, and Understanding Adversaries is right at the top of the list.

By working together, we are confident we can drive change within the threat intelligence industry to improve our ability to understand adversaries, and make further progress in stopping them. ●

The role of the CISO in the age of coronavirus

Cyber security specialists discuss how the pandemic has affected their sector

GETTY IMAGES/ANDREAS SOLARO

Becky Pinkard
Chief information security officer
Aldermore

Financial service concerns as they related to our Covid-19 response were very similar to those experienced by all tech-driven companies around the world – how to relocate entire teams of people to working from home conditions that were functional, secure and worthy of an "office-like" replacement, yet for an unknown quantity of time. Our response was driven in multiple ways – in some circumstances it meant sourcing kit for entire teams to be able to work remotely and in conjunction, teaching them how to work remotely, efficiently and securely.

Our challenges meant we leant heavily on our communications IT, data protection and security teams to work hand-in-hand across these various departments. There were additional regulatory oversight considerations that factored into every move and process change, mandating detailed tracking and reporting of the risk landscape as it evolved through our response. Lastly, an increase in attacker-led targeting of individuals across each facet of possible Covid-related fraud you could imagine meant that we were kept constantly on our toes, again tracking and informing our users of the latest possible way we could be attacked as a company or even themselves in their personal lives.

Graham Ingram
Chief information security officer
University of Oxford

A university is a collection of great minds; the progress of knowledge is partly enabled through a non-conformist culture. This culture can also extend to the past development of bespoke information communications technology. Now mixed with recent commercial systems, this sets the conditions for the cyber challenge. Add Covid-19 and the challenge just became more significant. It is a remarkable feat that universities switched to remote working so quickly; IT staff moved mountains to mitigate disruption in the delivery of teaching and learning.

This complex ICT landscape is a considerable threat surface. The older the services, the less cost effective the security. In a largely Bring Your Own Device (BYOD) organisation achieving zero-trust networking is challenging. However, ambitious targets are needed and strong security principles applied. Research of global interest needs to be secured and shadow IT usage reduced. Academia must prepare for a near future of higher security and privacy expectations from donors, research sponsors and collaborators.

The near-term security challenges of our new normal are yesterday's worry. An opportunity now presents itself, with a new appetite for transformation, to develop conformity to emerging IT standards and security expectations. This reduces the risk of a breach causing reputational damage, generates trust in the protection of research, and preserves academic freedom.

Jaya Baloo
Chief information security officer
Avast

The antivirus (AV) industry had to adapt quickly to a significant increase in the volume of attacks, from phishing to ransomware to stalkerware. For instance, in the UK our detection of stalkerware rose 83 per cent between March and June this year. But the industry also had to adapt to the changes that attackers were making as a result of Covid-19. We have seen financially motivated attacks from state actors, not just opportunistic cybercriminals, which is interesting because state actors are not usually in it for the money, they tend to focus on attacking one another. So, as volume increases and attack types and motivations evolve, the security industry must understand and act on this if it is to get better at detection.

A challenge that we are concentrating on right now is business transformation. Specifically, how we transform digitally, how we transform organisationally with new working arrangements and how we transform technologically with our infrastructure setup, our approach to innovation and visibility over the large quantities of log information and threat intelligence data we have. There are cyber security challenges that come with each, but this is where Covid-19 has had a major impact. It has been a catalyst for organisational change.

Councillor Peter Fleming
Chair of the Improvement and Innovation Board
Local Government Association

The work of councils has never been so vital to the most vulnerable in our society, and the digital communications and services that they use have never been so critical to our efforts. From video conferencing and new data sharing, to the digitisation of public meetings, local government's response to Covid-19 demands continuous and accelerated digital innovation.

But despite the crisis, cyber threats have not gone away, and many criminals are using the current situation as an opportunity to extort ransoms. When combined with the increase in vulnerabilities brought by distance working, new partnerships, and our increased reliance on digital services, this means that the risk associated with a cyber incident is greater than ever.

Ten years ago, cyber security was a niche technical topic; something only the IT crowd had heard of. Today it is something that every senior manager and leader in local government needs to understand. The reason for that is that the last decade was the first since the Second World War that civil institutions in the UK came under regular attack from foreign actors. That's a remarkable change in the context within which our 1.4-million-person workforce is operating. To mitigate the cyber security risks that come from this brave new world, local government must – like everyone else in the public sector – invest in the upskilling and awareness of our people. The LGA remains committed to being part of that effort.

Hacking democracy

Trust in elections is under attack and cyber security is on the front line. By Samir Jeraj

In the month leading up to the 2016 US presidential elections, Wikileaks published 58,000 emails and messages hacked from John Podesta, the chairman of Hillary Clinton's campaign. It was the most high-profile in a series of cyber attacks that cast a shadow over the entire election.

Four years later, the next US election took place in the middle of a global pandemic – and attitudes to cyber risk, and indeed the nature of the risk to the democratic process, have changed.

There are few examples of the disaster scenario of an attempt to "steal" an election. More often, attacks are now about undermining public trust in the system, rather than trying to change election results. But it is difficult to measure the impact of disinformation, for example, on votes.

Maggie MacAlpine is a US expert in testing and auditing election systems. In 2016, she says, out of concern for the security of elections, some hackers in the US were testing electoral systems and trying to alert authorities about potential weaknesses. They found it difficult to be heard, however. "If you rolled up somewhere and said 'your cyber security needs shoring up because it's a potential vector of attack' you would get a lot more pushback, or even confusion," MacAlpine told *Spotlight*.

This attitude has largely shifted over the past four years, she says, but it still lingers in places where officials insist they do not need outside help to identify vulnerabilities. One of those places, the state of Georgia, is now at the centre of disputes about the conduct of the 2020 elections. President Donald Trump's campaign requested a recount of the vote in the state after Joe Biden was declared the winner. When we spoke, before the election on 3 November, Georgia had just appealed a ruling by a judge that would have required election officials to have a paper back-up in case there were issues with technology used to "check in" voters, including cyber attacks.

Outside the US, some countries have stepped up their efforts to protect elections and democratic institutions from cyber interference. Sam van der Staak has been working on this for

Supporters of US president-elect Joe Biden at the Michigan State Capitol, November 2020

JEFF KOWALSKY/AFP VIA GETTY IMAGES

five years at International IDEA, an intergovernmental organisation based in Sweden, which has run workshops in Europe to get a sense of cyber security challenges to electoral processes in different countries.

There was an initial "cyber scare" following the US election in 2016, the hacking of the German Bundestag in 2015, and the French presidential elections, when President Macron's campaign was targeted by hackers in 2017, he says. The issue has gone quiet in the past two years, however. "The old ways have continued, but in addition to that it's broadened, it's diversified and the aims have shifted," he added.

Cyber attacks undermine trust in voting

People assume when they see a headline that says "election hacked" that it is about changing the results, MacAlpine explains. But if your goal is about undermining the credibility and trust in elections, attacks can take many forms. That includes direct attacks on campaign security, such as hacking and releasing emails, or election infrastructure, such as the websites used to register to vote. They can be launched independently by hackers or be sponsored by a state, with Russia frequently accused of being behind such disruption campaigns.

However, simple attacks on vulnerable targets can be carried out by anyone with basic technical knowledge, and disinformation can be created and spread by anyone with a social media account. In the US, MacAlpine notes, it would not necessarily be against the law if a citizen spread false information, given free speech protections. "It's not illegal to be an idiot," she says.

MacAlpine's biggest concern in the run-up to this set of US elections was that Trump would amplify disinformation about the integrity of the vote. Her concerns were indeed borne out during and since polling day. Trump recently fired the head of the US cyber security agency for refuting the president's claims of electoral fraud.

Worldwide, electoral commissions have invested in different systems and turned to the security services for support in response to the threat of cyber attacks, according to van der Staak. "Every electoral commission is vulnerable," he explains. Those who use electronic voting and counting are at greatest risk, but even countries with little use of electronic systems are at risk. They will likely still use email to communicate and have a website to announce results, even if their votes are cast and counted by hand.

Some countries have made efforts to educate citizens about these dangers. In 2018 in Sweden, for instance, information packs were posted to each household about the risks of election hacking. A high school programme was launched to teach young people about propaganda.

The coronavirus pandemic also means some electoral commissions have had to shift more of their services, like candidate registration, from in person to online. But this has happened rapidly, without the preparation and time to secure those systems. Staff are working at a distance and dealing with more postal votes, so capacity to do cyber security is lower. In the US, says MacAlpine, the money for states to adapt their elections to Covid-19 came too late to make a big difference in moving services online for the presidential election.

Political parties and civil society organisations are among the most vulnerable parts of an electoral system. There are hundreds, potentially thousands of political parties and organisations in each country, often lacking the money to invest in cyber security and reliant on volunteers.

"The risk is potentially enormous," explains van der Staak. In some cases, electoral commissions have asked the security services to train political parties in how to help protect themselves online. In countries with a recent history of totalitarianism and dictatorship, where these types of organisations may have rigged elections in the past, this has been controversial.

Cyber attacks and disruption more broadly give people who are already sceptical about democracy, elections, or "the quality of their politicians," another argument to say, "this system isn't working for us," explains van der Staak. This is much easier to achieve and only takes small attacks that anyone could do, for example a distributed denial of service (DDoS) attack on a political party's website. This is what happened to the UK Labour Party during the 2019 election.

In Latvia's 2018 elections a popular social network, Draugiem.lv, was targeted and its homepage filled with pro-Russia content. All of this contributes to a general environment of suspicion and doubt. "It's all about trust," said van der Staak.

Why get a state-of-the-art laptop, if you can't keep it secure?

Only BT broadband gives you expert security to help protect you from cyber attack with tools worth over £100.

Why choose anyone else?

BT BEYOND LIMITS

Terms apply. Verify at bt.com/verifysecurity

As cyber attacks proliferate, the answer lies in dull detail

Companies need to get the basics right and build a security culture, says Ed Targett, editor at Tech Monitor

In March staff at Finastra were forced to switch off servers – temporarily freezing millions in financial transactions – after a ransomware attack on one of the world's largest financial technology services firms. In June, Honda factory floors fell silent after network infrastructure was shut down following an attack. In August, New Zealand's stock exchange faced four days of interruptions to trading after a sustained Distributed Denial of Service (DDoS) attack.

These are just three high-profile examples of cyber incidents in 2020. There were millions of others, from cities forced to halt vital services to casinos knocked offline.

Yet organisations remain complacent. Perhaps many see the big names targeted and think "that's not me"; the smaller names quietly fix the problem and nobody – sometimes not even regulators, GDPR or otherwise – is any the wiser.

The truth is, however, that you don't have to be a target to be attacked. Cyber security researchers who set up "honeypots" to track attacks say automated vulnerability probing is immediate and sustained. One security researcher, Jason Schorr, told me that a honeypot he set up for 48 hours saw 24,992 offensive probes per hour from all over the world.

In newsrooms, editors are beginning to be inundated with predictions pieces for 2021. On the cyber security-front, many feature the alarming viability of the deep fake: synthetic media used to underpin sophisticated social engineering scams. Picture a Zoom call with a spitting image of your CEO, now AI-powered, asking for an urgent transaction to be made to a company account.

The technology is 95 per cent there and likely to become common place within the decade, if not sooner. Yet most organisations would find fretting over the less dystopian and much more mundane a better use of their time. They should be taking steps like fixing the software that has been unpatched since 2012 or killing off the credentials of that employee who left last year, but whose email still gives them access to company databases.

In a list of the top 10 most exploited software bugs, the FBI and US security agency CISA lamented in a joint post this year that one stemmed back to 2012. It has been known about, and a patch has been available, for eight years.

"Foreign cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organisations," they noted, adding "the public and private sectors could degrade some foreign cyber threats… through an increased effort to patch their systems and implement programs to keep system patching up to date".

Getting the basics right is hard. End-users hate multi-factor authentication and prompt patching can knock applications offline. Deep fakes sound like a big threat, but security hygiene is 99 per cent small detail.

For that, IT teams need to be resourced and security taken seriously from top to bottom of a company. It might be painful building a security culture, but not as painful as being targeted by hackers who 21st century law enforcement remains deeply ill-equipped to catch or hold to account.

Delivering the next generation of connectivity

5G can be an engine of economic growth with security at its heart, says **Victor Zhang**, vice-president of Huawei

The fifth generation of wireless technology, 5G, will spark economic growth around the world by enabling new capabilities in industries such as manufacturing, construction and information communications technology (ICT). By 2035, according to IHS Markit, 5G will produce around $13trn in global economic output.

In the near term, schools, households, hospitals and businesses can all benefit from much faster internet connections. A bit further down the line, the Internet of Things (IoT), particularly its industrial applications, will usher in an era of advanced factory automation, driverless cars, and significant improvements in efficiency powered by big data analytics.

Critics point out that by letting consumer goods such as refrigerators and cars connect to the internet, the IoT greatly expands the "attack surface" available to malicious actors who would seek to compromise our communications networks. But 5G makes use of 4G's best defensive technology, while adding new innovations that could make it even more secure.

In previous generations of mobile technology, the burden of authentication tended to rest with telecom operators. They authenticated users by means of a SIM card, a small chip placed inside users' smartphones. The SIM card identified users and managed cryptographic keys that verified their identities.

Then the IoT came along. It involves a host of devices and systems connected to the internet, from smart washing machines in homes to the networks operated by governments and corporations. These connections differ in size and power consumption, and in the type and quantity of data they can send and receive. A simple SIM card, issued by a telecom operator, can barely cope with such a diverse range of requirements.

5G solves that problem by assigning unique identities to each individual device. This eliminates the need for a SIM card, shifting responsibility for authentication from telecom operators to individual service providers. That is good news, because it enables a more flexible approach to security. For example, a hospital will be able to impose strict authentication requirements on a critical piece of equipment, such as a pacemaker in a patient's body, while a provider that supplied a less critical application could use a less stringent security policy.

Then there is encryption, an area where 5G also appears to outshine its predecessors. First, 5G data is encrypted

SHUTTERSTOCK/ EUGENIO MARONGIU

using 256-bit encryption, rather than the 128-bit standard used by 4G. Cracking a message protected by 256-bit encryption could take a quantum computer millions of years.

Second, 5G encryption shields a user's identity when their smartphone first connects with a base station. When a 4G phone makes this connection, it authenticates the user's identity, but does not encrypt the information. 4G encrypts calls and texts, but not the user ID. In contrast, 5G encryption makes it impossible to identify or locate the user, from the moment they get on the network.

Another 5G security enhancement concerns roaming. Previous generations of wireless leave connections exposed when a device roams outside of the network run by a user's main provider – for example, when the user travels abroad. Left unencrypted, these roaming devices are vulnerable to attack, requiring operators to set up firewalls to keep out intruders.

5G strengthens these connections by using a security protection proxy, or SEPP. Unlike a simple firewall, a SEPP will encrypt all messages sent while a user is roaming or using multiple networks. It will also impose a filter that validates the source of all messages and discard anything suspicious; limit the information about network topology that is visible to outside parties; and hide any confidential information from intermediary networks as it passes between the two core networks.

5G also reduces the risk of data being modified in transit. In 5G, the "user plane," the layer on which data is transmitted, "knows" if the data has been altered. If alteration is detected, 5G's security systems will discard the data and ask the host to resend the message.

Schools and hospitals can be empowered by 5G

How a 5G-enabled society could thrive post-pandemic

Faced with the disruption of the Covid-19 pandemic, society is experiencing profound and rapid change. But the necessity of recovering from the Covid-induced recession could give rise to a whole series of innovations – many of them enabled by 5G.

Countries around the world are focused on containing Covid-19. Yet many organisations have already begun looking to the post-pandemic future and thinking about how their operations, products and services will have to change. Technology plays a central role in their planning efforts, especially emerging platforms such as blockchain, facial recognition and virtual and augmented reality.

For example, the UK's National Health Service (NHS) has long aimed to broaden its services to include telemedicine as part of the Digital First programme. But the use of video consultation in the UK has grown significantly during the pandemic. Hospitals and other traditional healthcare providers have entered the space with offerings of their own – for example, Raffles Connect, which lets patients consult remotely in-house doctors and specialists.

In addition to healthcare, education will be transformed by the rapid uptake of digital technology brought about by the pandemic. In France, the Centre National d'Enseignement à Distance created a digital platform called Ma Classe à la Maison (My Classroom at Home) to offer classes to students. The platform provides distance learning modules to students and teachers and can be accessed from a phone, tablet or computer.

The security enhancements made to 5G reflect a collective effort by the ICT industry to create a more secure communications environment. Building on experience gained from previous generations of mobile technology, it will be possible to engineer a seamless transition from the security of 4G to the newly enhanced levels of security available in 5G, the next generation of wireless communication.

The latest contracts, jobs and training

THE LARGEST PUBLIC SECTOR CONTRACTS AWARDED RECENTLY

Cyber security perimeter service, NHS Digital
CONTRACT VALUE: £48m
DATE AWARDED: 5 November
NHS Digital has agreed a security package over the next five years with Accenture, incorporating cloud-based data protection, firewalls and technical support for staff.

Provision of a Foundry Data Connector, Cabinet Office
CONTRACT VALUE: £20m
DATE AWARDED: 22 October
The Cabinet Office has agreed a data security software package with Palantir, lasting 12 months.

THE LARGEST PUBLIC SECTOR CONTRACTS NOW OPEN FOR TENDERS

Security software development services, London Grid for Learning
CONTRACT VALUE: £4.5m
DEADLINE: Ongoing
The LGfL, which provides a filtered broadband connection across 33 local education authorities in the UK capital, is looking for a cyber security partner to manage and protect its network over the next five years.

Security software package, V&A Museum
CONTACT VALUE: £0.5m
DEADLINE: December 2020
The V&A's Kensington base is looking for a cyber security partner to help with its digital transformation, moving more customer and staff data online, and integrating services between different V&A sites.

Public security, law and order services, Home Office
CONTRACT VALUE: £177.5m
DEADLINE: December 2020
The Home Office is seeking a technology partner to assist with the digital development of its civil defence, police provision, border control systems and more.

JOBS NOW OPEN FOR APPLICATIONS

Cyber Security Risk and Vulnerability Manager, Department for Transport
SALARY: £34,708
LOCATION: London
CLOSING DATE: 6 December
The DfT wants to recruit a new member to its cyber policy team, who will assist with the maintenance of the organisation's digital architecture, and also work on new projects relating to intelligence sharing and counter-terrorism.

IT and Cyber Security Manager, Care Quality Commission
SALARY: £50,466-£65,348
LOCATION: Birmingham, Leeds, London, Manchester, Newcastle
CLOSING DATE: 8 December
The CQC, the government's regulator for the National Health Service, is looking to recruit an experienced cyber security professional to manage and protect the organisation's data, relating to various trusts' finances,

patient and staff information, and more.

Chief Digital Information Officer, Crown Commercial Service
SALARY: £149,500
LOCATION: Birmingham, Liverpool, London
CLOSING DATE: 15 December
The CCS, the executive agency and trading fund responsible for investment in goods and services used by the public sector, wants to hire a CDIO to oversee the continued digitisation of the organisation and assess the cyber security of its partners.

NHS Test and Trace – Grade 6 – Head of Security Architecture, Department of Health and Social Care
SALARY: £62,404-£75,410
LOCATION: Remote (nationwide)
CLOSING DATE: 18 December
The DHSC is looking to hire a cyber security specialist to build and improve new and existing hardware and software architecture of the NHS Test and Trace app used to track the spread of Covid-19.

Lead Developer, Department for Business, Energy and Industrial Strategy
SALARY: £53,375-£59,650
CLOSING DATE: 6 January 2021
The successful candidate, who will have experience in coding, will line-manage a growing IT team at BEIS, while overseeing the organisation's digitisation and transition to cloud-based office systems and regularly reviewing its security hardware and software.

Chief Data Officer, The Money and Pensions Service
SALARY: £100,000
LOCATION: London
CLOSING DATE: 13 December
The Department for Work and Pensions' arms-length financial advisory body is looking to recruit an experienced manager to oversee the governance and storage of consumer data.

EDUCATION/TRAINING OPPORTUNITIES

Certified cyber security training, National Cyber Security Centre
The NCSC runs a range of short awareness and application courses, in conjunction with its industry partners, for both businesses and individuals. These courses help people to stay abreast of the latest cyber threats, including ransomware, malware and phishing emails.

MSc cyber security, Glasgow Caledonian University
GCU's one-year full-time postgraduate course blends practical assessments with coursework – mainly online, with written examinations kept to a minimum. It covers network and hardware design, and teaches students to evaluate current and emergent technologies, within their legal, social and commercial contexts.

PhD studentship, Royal Holloway, University of London
Royal Holloway's Centre for Doctoral Training in Cyber Security for the Everyday is offering ten four-year doctoral courses, fully funded by the Engineering and Physical Sciences Research Council (EPSRC). The project-centred courses will explore the technical resilience of everyday digital infrastructure, and its place within wider society.

MSc/PgCert Cyber defence and assurance, Cranfield University
Cranfield is offering full and part-time iterations of a taught postgraduate course with some industrial placements. The focus of both is on data curation and management, including human risk factors. This training is aimed at aspiring chief information security officers.

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, phishing awareness and reputation management. Courses can be paid for in monthly instalments.

★ ONLINE SAFETY TRAINING ★

Introductory phishing course, Cybrary
Training platform Cybrary is offering a two-hour introductory course, administered online, teaching people how to spot common phishing tactics in their emails. The course is targeted at more junior employees at large organisations, and also covers how to set up automated emails safely. Certificates can be awarded on the same day as enrolment.

Tender and framework data supplied by Global Data

GlobalData.

SHUTTERSTOCK/VISUAL GENERATION

HOW TO WIN THE WAR FOR TECH TALENT.

(Without hiring a single hotshot.)

A slow down is not the time to slow down.

Digital transformation has always been a priority for businesses. What's been missing is urgency. The lockdown has created that urgency, making digital transformation existential for a lot of firms. Now, the backburner isn't sensible.

Most companies can buy the tech solutions they need to spur that transformation. But building the tech talent to support those solutions? Not so easy. Most businesses are way short of the talent they need in the key transformative tech areas. Areas like cloud, security, DevOps.

At QA, we address these in-house gaps fast. We call it TechTalent Acceleration. Rather than force you to rely on expensive consultants or tech rock stars, we provide a way to train and reskill people who already work for you, or to find, train and deploy affordable new digital talent to solve your hardest problems.

We train almost 300,000 people in key tech talent disciplines each year. We turbo-charge your in-house tech teams. And – because 100,000 new people apply to us annually – we sift for attitude and aptitude and then recruit and train the right candidates from outside your organisation and plug your most critical gaps fast.

Helping to power transformation. Helping our customers Emerge Stronger from this horrible crisis. We're here to turn the war for talent into a big victory for you and your transformation journey.

To find out more visit www.qa.com/emergestronger

We're here to accelerate your transformation.

QA

Classroom & Virtual Training | Apprenticeships
Cloud Academy | Tech Bootcamps | Cyber