THE NEW STATESMAN

Spotlight

Thought leadership and policy

Cybersecurity: New risks and old enemies

Mike Fell | Patricia Lewis
Lindy Cameron

A new frontier

Liz Truss had barely left office last month when she attracted yet more negative press. This time it wasn't a story of economic vandalism, but the report that her personal phone had been hacked by a foreign entity while she was foreign secretary, a position she held from September 2021 to September 2022.

More than a year's worth of conversations, including sensitive exchanges with international foreign ministers about the war in Ukraine, were believed to have been accessed by the hackers. The former prime minister's device was reportedly so heavily compromised that it had been locked away in "a secure government location".

Truss wasn't the only senior member of her own government to have been at the centre of a security breach. Suella Braverman resigned as home secretary on 19 October after sending confidential policy documents from her personal email address to a back-bench Tory MP and a staff member of another. She was reinstated to her ministerial position by the new PM, Rishi Sunak, within a week.

That organisations – and certainly governments – need to vigilantly guard their systems and data in the face of malign hackers and rising cybercrime is old news. Throughout the pandemic, as more people went online to work, shop and socialise, the National Cyber Security Centre (NCSC) warned businesses and individuals that scammers were increasingly targeting the vulnerable to extort money.

Now, however, it seems that the threat has shifted. As the NCSC CEO, Lindy Cameron, writes, this year cybersecurity's most significant challenges came from Russia's invasion of Ukraine (see pages 8-9). And in fact, the NCSC's latest annual review states that the UK is the third most targeted country for cyberattacks, behind the US and Ukraine.

Which brings us back to Truss's phone and Braverman's emails. Organisations large and small are still failing on the cyber-risk basics. They would do well to listen to Mike Fell, the NHS's cybersecurity lead. As he tells *Spotlight* (see pages 10-12), the key to averting threats is to focus on the "hard-to-do foundations more than the shiny new technology". ●

Contents

Spotlight

40-42 Hatton Garden
London
EC1N 8EB

THE NEW STATESMAN
Subscription inquiries:
digital.subscriptions@newstatesman.co.uk

Director of Client Solutions
Dominic Rae

Account Managers
Jugal Lalsodagar

Special Projects Editor
Alona Ferber

Design and Production
Rebecca Cunningham

Special Projects Writers
Jonny Ball
Harry Clarke-Ezzidio
Sarah Dawood
Samir Jeraj
Oscar Williams

Cover Illustration
Klawe Rzeczy

BRITISH SOCIETY OF MAGAZINE EDITORS AWARDS 2017 WINNER

First published as a supplement to the New Statesman of 18 November 2022.

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/spotlight/reports

UK provides £6m of cybersecurity support to Ukraine

The UK has provided £6.35m of cybersecurity support to Ukraine, to protect the country's critical national infrastructure from Russia during the war.

The support was mobilised in response to a spate of Russian cyberactivity following the invasion of Ukraine in February 2022.

The UK's Ukraine Cyber Programme is "drawing on Britain's world-leading expertise to support Ukraine's cyber defences" in the fight against the Kremlin, James Cleverly, the Foreign Secretary, said.

Details of the programme were not revealed until November, in order to protect its operational security. The programme has provided both software and hardware to Ukrainian authorities to help fight Russia's cyber-threat. It has also involved the development of firewalls and Distributed Denial of Service protections, as well as access to enhanced forensics.

The UK government said its support had helped to prevent a potential Russian cyberattack using Industroyer2 malware – an evolution of the original software that shut down Ukraine's energy grid in 2015.

Lindy Cameron, the chief executive officer of the National Cyber Security Centre, said Ukraine's cybersecurity experts "have mounted an impressive defence against Russian aggression in cyberspace, just as they have done on the physical battlefield".

Medibank CEO "can't trust" hackers to return stolen data

Cybercriminals have seized data belonging to 9.7 million current and former customers of Medibank, one of Australia's largest private health insurers. But the firm is refusing to pay a ransom offered by its attackers because it "can't trust" that the criminals will return the stolen data, its CEO has said.

A hacker, using compromised high-level credentials, was able to access the personal information of Medibank's customer base, the company revealed last month. Following advice from cybercrime experts and the Australian government, David Koczkar, the CEO of Medibank, told the Australian Stock Exchange that the ransom offer put forward by hackers would not be paid.

"Our advice is that not paying the ransom will provide the best security for our customers and also other Australians," Koczkar told the *Guardian*. "The weaponisation of their private information in an effort to extort payment is malicious."

Koczkar refused to disclose the amount hackers asked for as ransom, but admitted that it did play a factor in the decision not to pay.

After initially underestimating the scale of the breach, Medibank has determined that 9.7 million customers – including 1.8 million of the company's international users – have had their names, dates of birth, phone numbers and email addresses accessed by hackers.

The Australian federal police are investigating the attack. Companies such as Medibank are legally required to keep the data of customers for up to seven years after they part with a provider. Koczkar said that reviewing these laws would be "an important question for the community" to answer. "I think there needs to be consultation [and] discussion," he added.

ED RAM / GETTY IMAGES

SHUTTERSTOCK / BILANOL

Construction giant Interserve fined £4.4m for ransomware attack

The Information Commissioner's Office (ICO) has fined the British construction company Interserve £4.4m after hackers stole the data of up to 113,000 former and current employees.

According to the ICO, Interserve broke data protection laws by failing to ensure the "appropriate security" of personal data between March 2019 and December 2020.

The ransomware attack stemmed from a phishing email masked as an important document, which was forwarded from one colleague to another. A malicious zipped file was opened, and the attacker installed malware. The virus spread to multiple servers, including four HR databases, and locked Interserve out of its systems in demand of payment. Compromised data included financial information, such as bank account details and salaries, and personal data such as mobile numbers, birthdays, gender, ethnicity, religion, disabilities, sexual orientation and health information. The ICO said that Interserve did not sufficiently prepare for a cyberattack.

Interserve entered administration in 2019 and was officially wound up in March 2022.

"The real agent Q" leaves NCSC after two decades' service

The National Cyber Security Centre's (NCSC) long-standing technical director Ian Levy is stepping down after a 22-year career in the civil service.

The computer scientist joined GCHQ's ranks in May 2000 after completing a PhD and working as a research fellow at Warwick University.

As the NCSC emerged out of the shadows of GCHQ in 2016, Levy became one of the most high-profile figures in the UK's cybersecurity industry. His work over the past six years has ranged from overseeing the technical review of Huawei's role in UK telecoms, to defending Covid-19 vaccinologists during the pandemic. He has also played a key role in forecasting future tech trends, an increasingly significant function of the NCSC.

Unlike many career civil servants, Levy is known for his candour. In an interview with *Spotlight* in 2019 he described Huawei's kit as a "bag of spanners". He would relish in telling audiences his job was "not to beat cybercrime", but to "send it to France".

Ciaran Martin, the former chief executive of the NCSC, said that he had been "struggling to think of any other civil servant" that had "as much positive impact... in their specialist field". Levy is yet to announce his next move.

SOURCES: STATISTA / ONS / THE CYBER SECURITY BREACHES SURVEY

236m

Global ransomware attacks in the first half of 2022

25%

Increase in fraud offences in the year to March 2022 vs the year to March 2020

3%

Decrease in UK businesses acting to identify cyber-risks in 2022 vs 2017

Advertorial

A new day, a new threat vector

Chris Parker, director of government strategy at Fortinet, on the contemporary cyber-threat landscape

In association with FORTINET

Every day, new cybersecurity threats emerge that pose significant risks to public sector and government organisations. The use of ransomware is no longer the preserve of sophisticated, tech-savvy cybercriminals or hackers, but is openly touted and sold, available to download on the dark web for as little as the price of a pint.

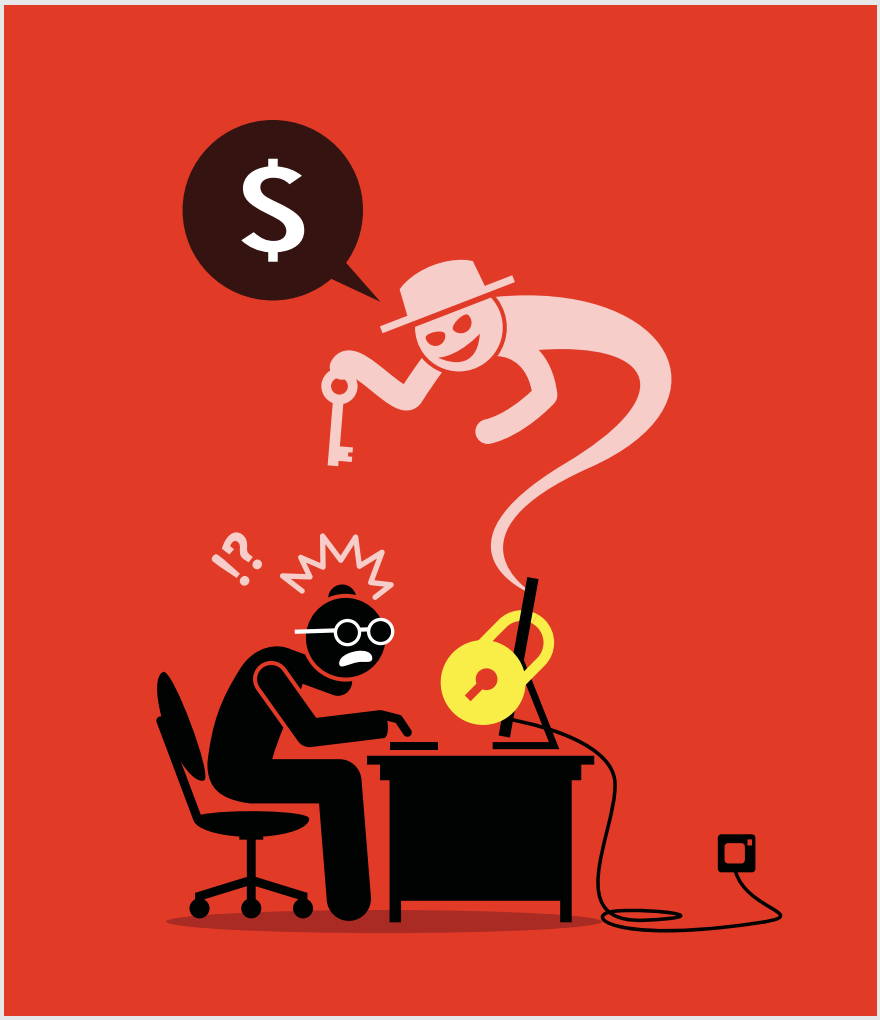
State actors and authoritarian geopolitical competitors emerge and re-emerge on the threat landscape, creating challenges for organisations and governments when it comes to protecting citizens' privacy, public service delivery and critical national infrastructure.

The coronavirus pandemic precipitated the beginning of a work-from-anywhere culture that massively exacerbates cybersecurity issues, and places increasing demands on teams working to maintain cyber-safety and resilience. Meanwhile, the digital skills gap places huge strain on institutions looking to secure their networks and data.

To discuss the huge range of contemporary cybersecurity challenges facing large organisations in an era of digital transformation, Chris Parker, director for government strategy at Fortinet, talks about what is at stake today, and how much has changed.

How did you develop your expertise in cybersecurity?

I've been lucky enough to have had a really varied professional life. There's my military background, involving big operations, then I went into construction as a chief operating officer, then I went into oil and gas exploration. But the common thread running all the way through my career has been the mitigation of that risk. I'm a risk mitigation expert. I've also led a number of businesses, with one of them in cyber, so I've been in that space for about seven years and have since joined Fortinet. This isn't the usual route for a cybersecurity professional – which would probably involve doing computer programming at university and doing a master's afterwards – but it means I can see things from a slightly different perspective and, crucially, from a customers' perspective, because I've worked in so many roles across a range of sectors.



The use of 'ransomware as a service' is increasingly commmon online

SHUTTERSTOCK / LEREMY

What are the biggest cyber-threats to public sector and government institutions in the UK at the moment?

Firstly, the ransomware threat is getting worse because of automation. It's getting much easier for both experienced and beginner threat actors to use and engage in cybercrime. If the cybercriminals are using automated technology, then we – the good guys – have got to step up with automated technology to keep them at bay.

There's "push and shove". It's almost like a seesaw between what we've got coming at us on the one hand – complex cyber-threats – and on the other hand, your resources, your kit, your money, your risk appetite, and crucially your people all helping counterbalance that seesaw.

If you're a well-known bank or financial institution you're probably putting significant resources into mitigating risk. But the public sector usually has fewer resources, money is obviously more scrutinised and there's slightly less agility. So, there's a compelling need to keep that seesaw balanced in their favour, and the way to do that is to make sure you're using the very latest technology to add extra weight to the seesaw. Where you can't employ 50 expensive analysts and get a load of new hardware all the time, you've got to use the very best automated technology to keep that balance tipped in your favour.

What kinds of technology can be used to mitigate these threats?

Because Fortinet is the number one cybersecurity company in the world, we have the largest collective memory in the industry which enables the best data for threat analysis in the world.

We look at dangers in real time, collecting huge amounts of data on the ever-evolving cyber landscape and cyber-threat actors. Unfortunately, we're seeing a significant increase in automated ransomware and the rise of so-called ransomware-as-a-service, in which people are hiring tools and people on the dark web to help them to easily launch attacks.

The challenge is to offer solutions that can counter these threats. In an age of digital transformation and the rise of a work-from-anywhere culture the challenge is greater than it's ever been.

How has digital acceleration affected cybersecurity?

An unexpected phenomenon that the pandemic triggered was the acceleration of digital initiatives. With a largely 100 per cent virtual workforce, organisations across the board embraced digital technologies as the way to combat the disruption caused. Unfortunately, the bad guys really upped their game in response to that and subsequently we saw a marked increase in cyberattacks. Regrettably, it is another new day, another threat vector in this world.

However, there's a lot that we can do and a lot that we've already done. Much is about upskilling the workforce because it's not just IT teams that need to be plugged into these threats but the whole organisation from top to bottom. Cybersecurity awareness training is an absolute must, along with implementing tools like two-factor authentication and "zero trust" policies.

More broadly, on a less granular level, we're lucky enough that the government is very much aware of the challenges facing organisations and the role that cybersecurity must play. Fortinet is fully on board with the UK government's Cybersecurity Strategy, and we share our data with the Cyber Threat Alliance and our threat research ecosystem. It's all part of a one-nation approach to threat mitigation. We're not hoarding our knowledge and resources for ourselves – it really is extremely collaborative.

Fortinet's primary objective is to make possible a digital world that we can always trust through its mission to protect people, devices and data everywhere. That's our purpose and we're working in partnership with government and with others in the industry to counter the ongoing cyber-threat. ●

The view from government

Lindy Cameron
CEO of the National Cyber Security Centre

"Russia's invasion of Ukraine is one of the biggest cybersecurity challenges this year"

It has never been more important to defend our digital lives and secure our most critical systems and services. The UK faces a range of evolving and diversifying threats, from the ever-present ransomware threat and the scourge of online scams to the cybersecurity risks that came with the return of war to Europe.

The cybersecurity landscape has experienced profound change over the past 12 months and the threats, risks and vulnerabilities we collectively face require a whole-of-society response to keep the UK safe online.

At the National Cyber Security Centre (NCSC), we have been part of a huge effort to bolster our national resilience at every level, working with allies and partners in government and the private sector. We have reflected on some of the recent successes and challenges in our latest *Annual Review*. It is worth considering what we can learn from the past year so we can effectively tackle the emerging and persistent threats that lie ahead.

One of cybersecurity's most significant challenges came from the invasion of Ukraine. While Russia's brutal and destructive war has sought to redraw the physical map, its consequences have been felt globally, including in cyberspace.

As a part of GCHQ, the NCSC has unique capabilities to monitor cybersecurity threats, and from the very start of 2022 we warned of heightened cyber-risks as a result of Russian hostility. We responded by publishing expert guidance to help organisations bolster their defences, and have worked closely with partners to ensure that critical infrastructure, businesses and the whole of society are as resilient as possible.

Building resilience is vital for preventing attacks during periods of heightened threat and for raising the bar for other threats. This is a key lesson we can take away from the conflict in Ukraine: that with strong cyber-defences in place, the defender has significant agency. Ukraine's defences have been exemplary and I'm proud the NCSC has supported them, in conjunction with the Foreign, Commonwealth and Development Office.

While the threat from Russia has been particularly blatant this year, it's important not to forget the other threats we face, some of which are, unfortunately, all too familiar.

Ransomware remains one of the most acute hazards for UK businesses and organisations and we have seen the real-world consequences that attacks can have: hitting businesses' operations, finances and reputations, and leading to widespread disruption for customers. The NCSC has published guidance to help organisations take the necessary measures to protect themselves and we continue to urge CEOs to take the issue seriously and not delegate it to technical experts.

We have also seen low-sophistication cybercrime continue to hit the public, with commodity attacks such as phishing and malware – in the 12 months to March, 2.7 million cyber-enabled frauds were recorded. The NCSC, working with law enforcement, is more resolute than ever in thwarting cybercriminals. And it is heartening to see a growing awareness of how we can all play a part in this.

In the 12 months to September there were 6.5 million reports of suspicious emails made to the NCSC by the British public – a 20 per cent increase on the year before, and this is a trend we are keen to see continue. It has made a demonstrable contribution to improving our collective resilience.

Over the past year I'm pleased to say the NCSC has helped to stop hundreds of thousands of attacks upstream while bolstering preparedness and helping institutions and organisations better

MARTA SIGNORI

understand the nature of threats, risks and vulnerabilities downstream.

We have seen more organisations sign up to our pioneering Active Cyber Defence services, such as Early Warning, which had a 90 per cent increase in uptake in the 12 months up to September, and Exercise in a Box, where there was a 42 per cent increase. Meanwhile, our Cyber Aware campaign is a great place for individuals and smaller firms to learn practical steps to improve their cyber-hygiene.

By following our advice in using three random words to create a strong password and turning on two-step verification to secure online accounts, people can protect themselves from the most common attacks. As people's thoughts turn to online shopping ahead of Christmas, now is a good time to be considering this.

However, with an evolving threat landscape, there is always more we can be doing to stay ahead of future threats. In our *Annual Review*, we consider the challenges on the horizon – in particular, the growing commercial availability of malicious cyber-tools and the risk of them falling into the wrong hands, being used with greater frequency and with less predictability.

As a responsible and democratic cyber-power, the UK is at the forefront of understanding and responding to this increasing threat and calling it out where we see it. There is growing competition for technological advantage between states, which is creating an increasingly fragmented ecosystem that brings risks for interoperability, and could undermine the free and open values that underpin our technologies.

This contrasts with the positive insight that NCSC experts provide in support of the UK's values-driven approach to developing capabilities and innovations. And finally, while Russia remains a persistent cybersecurity threat to the UK, the scale and pace of China's technical development is still likely to be the single biggest factor affecting our cybersecurity in the years to come.

At the NCSC, we are addressing these challenges now to ensure the UK can continue as a global cyber-power in the future. Our blueprint for doing so is set out in the National Cyber Strategy, which recognises that a thriving cyber-skills and growth ecosystem is vital for maintaining this advantage, and we champion the diversity of talent at its heart.

Initiatives such as CyberFirst have engaged thousands of young people from all across the country in the past year, while our NCSC for Startups programme has supported businesses that generate hundreds of millions of pounds in investment.

This is a source of great optimism for me and my team as we look ahead to 2023. But cybersecurity is a team sport and it is only through mobilising the whole of society that we can achieve our goal of making the UK a safe place to live and work online.

“Cyberattacks can cause patient harm”

The NHS cyber chief, Mike Fell, on protecting Europe’s largest health service

By Sarah Dawood

Pandemics come in many forms. Prior to the Covid-19 outbreak there was another virus that overwhelmed the NHS and brought many of its essential services to a standstill.

The WannaCry cyberattack on 12 May 2017 – a global ransomware virus, which locked people out their devices in demand for payment and infected 200,000 computers in more than 100 countries – affected more than a third of NHS trusts in England and 595 GP practices. Staff were shut out of their computers and emails, thousands of appointments and operations were cancelled, and patients requiring urgent treatment had to travel to further away accident and emergency departments. Later in the day a security researcher managed to activate a “kill switch” and stop the virus.

The attack caused financial and

KLAWE RZECZY

logistical chaos. The Department for Health and Social Care estimated the cost at £92m, more than three quarters of which was designated to IT restoration and improvement. The other effects were harder to quantify. Writing in the scientific journal *Nature* researchers at Imperial College London concluded that while WannaCry "may not have led to a direct impact on mortality, we are unable to ascertain the true impact on complications, patient morbidity, or changes in care processes that resulted from the attack".

Mike Fell, the executive director of national cybersecurity operations at NHS Digital, which oversees the health service's federated IT operations, tells *Spotlight* that the repairs undertaken after the attack were essential. "As well as rebuilding it as it was, one also needs to harden it, to make sure that the same thing doesn't happen tomorrow," he says. "So that's where there are significant costs involved."

NHS Digital runs national services such as the NHS app and the 111 service. The role of Fell's team is to ensure NHS Digital's own systems are secure, and to support other organisations across the health and social care sector in England in preventing cyberattacks. Before joining the NHS this year, Fell was in charge of cybersecurity at HM Revenue and Customs for five years. "The two things you probably don't want your neighbour to know are how much money you earned last year and the last thing you spoke to a healthcare professional about," he says.

Indeed, healthcare is one of 13 sectors recognised as critical national infrastructure by the government's National Cyber Security Centre, alongside others such as food, finance, energy and transport. A large cyberattack on one of these sectors can cause severe societal disruption, loss of essential services, and in some cases loss of life.

Cybersecurity is particularly complex for the healthcare sector. The NHS has 1.5 million electronic devices and thousands of disparate organisations of varying size and digital competency. There are 7,454 GP practices. In short, Fell's team does not have an easy job.

"You're talking about everything from some of the most technologically advanced research organisations in the country through to individual GP surgeries," says Fell. "As a result of that, we can't make any assumptions. We have to look at each case and maintain proportionate security."

Despite the investment that has been made since 2017, cyberattacks have still slipped through the cracks. While not of the same scale, on 4 August this year an NHS external software provider called Advanced was hit by another ransomware virus, which affected NHS 111 urgent care and disrupted appointments, note-taking systems and patient check-in processes. NHS Digital and NHS England have declined to comment on the recent attack but Simon Short, the chief operating officer at Advanced, told *Spotlight* that the software company had worked "tirelessly to accelerate the restoration of our systems".

Fell says his team is constantly devising new ways to secure the health and social care sector's systems. "Getting cybersecurity wrong has the potential to cause patient harm and to undermine public trust," he says. "Both these things are critical for me because data saves lives, and data makes it easier for the public to access health services, such as booking a Covid vaccine. We've learnt a lot of lessons from WannaCry and other incidents, and we continue to learn."

NHS Digital has increased its preventative work since WannaCry to help organisations meet basic security standards. This includes guidelines and educational resources, such as the data security and protection toolkit, a mandatory online tool used to teach and test NHS employees on data security skills, and a cybersecurity ▸

◂ guide for senior leaders and board members. Given the WannaCry attack exploited a vulnerability in outdated software (a common cause of cyber-breaches), NHS Digital has also done a lot of work to get organisations off unsupported software and hardware that can no longer receive security updates.

Fell believes that those working in cybersecurity need to demystify the terminology that surrounds it and emphasise how individual complacency has real-life consequences. NHS Digital runs a communications campaign for NHS staff called Keep IT Confidential to teach NHS workers in an accessible way about risks and the simple ways they can mitigate them, such as keeping files organised and ensuring their screens are locked when they leave their desks.

"Talk of cyber-risk is often quite techie or bizarre," says Fell. "We talk about phishing, whaling and denial of service. Ultimately, what we're talking about isn't a cyber-risk – it's a risk that a cyber-event prevents successful patient outcomes."

NHS Digital has also employed new technology such as a centralised firewall system called Secure Boundary, which detects and blocks most attacks, and centralised surveillance called the high severity alert system. This entails the NHS Digital team monitoring and assessing thousands of known vulnerabilities in hardware and software used in the NHS. They identify the ones that could cause the most damage, based on the potential scale of the impact and whether they could be exploited remotely, and notify all NHS organisations to prioritise fixing them. All organisations are obliged to report back to NHS Digital to show how they have done this.

The establishment of new cybersecurity groups has also made it easier to share intelligence across the sector. The Cyber Associates Network brings together people working in cybersecurity in health and social care to share best practice, while the Central Data Security Centre, within NHS Digital, offers advice and support for any organisations that need it.

Despite this centralised support, Fell is adamant that individual organisations, whether a major hospital or a small GP surgery, need to take responsibility for their own security. "We provide a level of protection at the centre through monitoring and building public trust," he says. "But we also support individual organisations to own and manage their own risk. Individual organisations that contribute to the NHS, whether private or public, have an obligation to keep themselves secure and resilient from cyberattacks."

Mike Fell: "Data saves lives and makes it easier to access health services"

For less technically savvy organisations especially, small changes can make a big difference in reducing online threats. Using multi-factor authentication to access systems, for instance, is "key to upping the barrier", says Fell, as is using strong passwords. The focus should be on the "hard-to-do foundations more than the shiny new technology", he says. So, rather than investing all energy and money in state-of-the-art laptops or the most expensive electronic patient records system, NHS organisations should instead stop using unsupported IT, integrate cybersecurity into the design of any new digital services, monitor and audit systems regularly, and limit access to software and patient data to those who need it.

> "Focus on the foundations, rather than the shiny new tech"

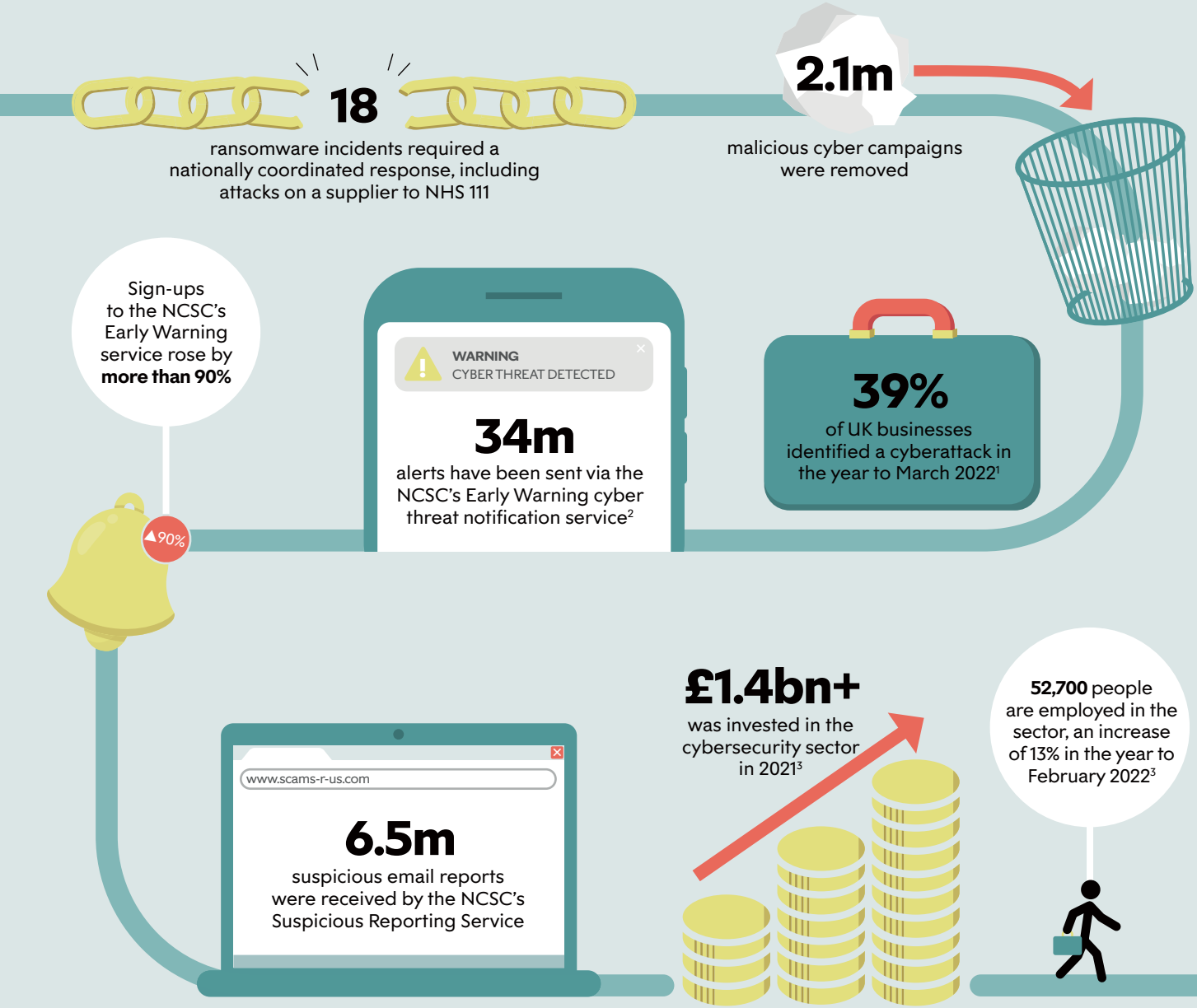
A sector as vast and varied as health and social care will always struggle to be infallible when it comes to cybersecurity. The breadth of its digital platforms, from appointment booking and blood taking services to electronic prescriptions and cancer screening, makes it difficult to mitigate against all possible breaches. But all organisations can make a difference by following NHS Digital's advice and making small adjustments to everyday practice, says Fell. He believes that persuading individuals to adopt better practices is integral to increasing the security of the NHS. "I think I've got one of the best jobs in the public sector," he says. "It's different every day. And ultimately, it's a people game." ●

This is the first article in a new series, Critical Condition, exploring the cybersecurity challenges faced by providers of the UK's critical national infrastructure. Read the series online at newstatesman.com/spotlight/cybersecurity

NHS DIGITAL

Security in numbers

Tracking the UK's threat landscape



UNLESS OTHERWISE STATED, ALL STATS FROM THE NCSC'S ANNUAL REVIEW AND FOR THE TIME PERIOD SEPTEMBER 2021 TO AUGUST 2022.
[1]ACCORDING TO THE CYBER SECURITY BREACHES SURVEY 2022, GOV.UK. [2]SINCE ITS INCEPTION IN MAY 2021. [3]ACCORDING TO CYBER SECURITY SECTORAL ANALYSIS 2022, GOV.UK

Advertorial

Cybersecurity in the quantum age

A new era of computing requires a new kind of cryptography

By Professor Liqun Chen

In association with

Cybersecurity has become one of the hottest topics in the modern digital world. How to make cybersecurity solutions trustworthy is a highly relevant question. Cybersecurity solutions make use of cryptographic mechanisms, so trusting in these solutions means trusting in cryptography. Cryptography helps the world build trust. Without cryptography, trusting any information that is processed, distributed and stored is impossible. From this point of view, cryptography plays the role of a "root of trust".

However, cryptography itself relies on trust. Cryptographic mechanisms need to be trusted, but there are many barriers. In recent years, a substantial amount of research on quantum computers has been reported and this has drawn enormous attention from the cryptographic community, governments and the cybersecurity industry. Quantum computers can solve mathematical problems that are difficult or intractable for conventional computers, such as the factorisation problem and the discrete logarithm problem. For the factorisation problem, you are given the product of two large prime numbers and asked to find these numbers. The discrete logarithm problem involves modular arithmetic (numbers wrap around, as in a clock, where hours run from 0 to 11 and back to 0 again – this is written as "mod 12"). Given three very large integers (g, y, p) where y is equal to (g x g x ... x g) mod p, find how many gs are involved (this is the discrete logarithm). Current public-key cryptographic solutions rely on these computationally hard problems to make them secure. If large-scale quantum computers become reality, they will be able to break most of the cryptographic public-key algorithms currently in use. Therefore, these public-key cryptographic algorithms need to be replaced to protect against a potential future quantum computer.

Currently available quantum-resistant algorithms are based on five different computationally hard problems, which have been used to build algorithms for a range of cryptographic applications, including public-key encryption and digital signatures. These algorithms are all difficult to implement efficiently, and avoiding side-channel attacks in their

implementation is more demanding. The security analysis of many algorithms is still not rigorous. This is an active research area that is full of challenges.

In 2016, the US National Institute of Standards and Technology (NIST) asked for submissions for post-quantum algorithms in asymmetric encryption and digital signatures for standardisation. On 5 July 2022, after three rounds of testing and review, the NIST announced the first group of four post-quantum algorithms selected for standardisation. The NIST's choices of two lattice-based signature schemes and one lattice-based key encapsulation mechanism (KEM) scheme, along with a symmetric setting signature scheme, give the cryptographic community sound choices with which to begin the transition from today's cryptography to that suitable for the quantum age, although more algorithms are still being evaluated by the NIST. Many international standard bodies are also involved in the development of post-quantum cryptography standardisation activities.

Cryptography is useable in a broad range of applications. It can be used to help build trust in applications; this is achieved by using trusted computing technologies, including authentication and attestation. However, adding trusted computing technologies to any application is challenging, without then requiring quantum-resistant solutions. These are extremely interesting problems and along with many academic and industrial partners, the University of Surrey is working in this area:

Quantum-resistant algorithms

Surrey served as a technical leader of the EU Horizon 2020 project, FutureTPM. A Trusted Platform Module (TPM) is a tamper-resistant component that is embedded in a host computer platform and acts as a root of trust. It also provides many cryptographic-related services, including authentication, attestation, and secure storage. TPMs have been embedded in billions of computer platforms. Since 2016 it has been a requirement that systems running Windows 10 should have a TPM 2.0 present and enabled. In the FutureTPM project, we have developed and identified a list of quantum-resistant cryptographic algorithms, which are suitable for inclusion in a future TPM. Some of these algorithms are taken from the NIST's post-quantum cryptographic standardisation activities, and others are developed by our project consortium. We have also implemented these algorithms to test their performance. We have presented our project results to the Trusted Computing Group (TCG), which is an international industrial standard body and develops TPM specifications.

EU Horizon

Surrey has been involved in several other EU Horizon projects as a technical partner. These projects are using cryptography and trusted computing technologies for a number of different applications:

- ASSURED – building trust in information and communications technology.
- SECANT – providing security and privacy protection in healthcare ecosystems.
- CONNECT – securing digital connectivity between vehicles and between vehicles and transport infrastructure.
- REWIRE – providing new trust management mechanisms for the auditability and certification of software and hardware.
- ENTRUST – making medical devices, for example glucose sensors, secure.

(These projects are funded by the UK government Horizon Europe guarantee and administered by UKRI.)

Anonymous digital signatures

We need post-quantum anonymous digital signatures to protect users' privacy. For example, the current TPM has a Direct Anonymous Attestation (DAA) signature scheme, which is used for authentication and attestation of a user's computer platform without identifying them. This type of digital signature provides a good balance between security and privacy. However, the existing DAA schemes supported by TPMs are not quantum-resistant. Surrey has been working on such signatures for some time and we do have several post-quantum DAA designs, but further work is needed to make them practical.

At Surrey we are proud of the work we have undertaken to accelerate the transition to post-quantum cryptography. We look forward to continuing our research in the field, to ensure that the benefits of a new era of computing can be felt by all. ●

Professor Liqun Chen is head of the applied security group at the Surrey Centre for Cyber Security, University of Surrey

SHUTTERSTOCK / BARTLOMIEJ K WROBLEWSKI

Quantum computers can solve problems that are otherwise intractable

Is the Online Safety Bill fit for purpose?

Arguments persist over whether this new legislation will protect people or cause harm

Kieren McCarthy | Monica Horten

FOR

Kieren McCarthy
Executive director, International Foundation for Online Responsibility

It's been five years since an initial attempt to tackle "online harms" in the UK was launched through the Internet Safety Strategy green paper. But despite determined and focused efforts, practical solutions continue to elude lawmakers.

Nowhere has this been clearer than in the effort to tackle "legal but harmful" content on the internet – everything from hate speech to sexual content to posts promoting suicide and self-harm.

The phrase has been subject to growing criticism, even mockery, as attempts to define it have floundered. But the truth is that "legal but harmful" remains a concise and candid statement of the problem. It is reminiscent of the famous former US Supreme Court judge Potter Stewart's description of hardcore pornography: "I know it when I see it."

The problem lies in understanding where people "see it", and how frequently. A video talking about how to take your own life or blaming societal ills on a specific group of people can be offensive or in poor taste, but on its own, its impact may be limited and quickly forgotten.

When aligned with dozens of other videos saying the same thing and viewed by the same individuals in short order, however, the impact is very different, as the recent case of the teenager Molly Russell, who died in 2017, made clear.

As reportedly confirmed by YouTube's chief product officer Neal Mohan in 2018, roughly 70 per cent of people's time on YouTube is spent watching videos automatically queued up by an algorithm, rather than something they have searched for.

Tech companies that serve as the gateways to online content have optimised systems to fit their business models: more users spending more time with them equals more market share and more money. Those companies don't

create the content they share, and their algorithms are designed to give users more of what they want. They aren't going to change that approach until they are under a legal obligation to do so.

This is where the Online Safety Bill has, belatedly but effectively, got it right. It will impose a new "duty of care" on tech giants and require them to make promises to users that are more than just words on a webpage. The version that will be reintroduced to parliament this month will dump unworkable efforts to control "legal but harmful" content, but give regulators the ability to keep tabs on promises and make changes where necessary.

What has been called a watered-down approach is perhaps better described as having been smartened up. We don't know what will work to limit online harm, nor do the tech companies that are indirectly causing it. It's going to take experimentation, adjustment, measurement and flexibility to get to a better place.

The main recipient of the new law's powers – the regulator Ofcom – is under no illusion that it has the answers. The man in charge of the effort, online safety policy director Jon Higham, said this month that the regulator will make small changes, wait to see their impact, and adjust accordingly.

But internet-style regulation will only be possible with clear legal authority, and that is what the Online Safety Bill will provide. It's far from perfect, and we will need the House of Lords to clean it up, but it will at least allow us to start solving these problems. It's time to make this bill law and get on with the job of making online life safer. ●

AGAINST

Monica Horten
Policy manager for freedom of expression, Open Rights Group

In seeking to address harms to children, the Online Safety Bill proposes remedies that will create new harms. Internet services used every day by British consumers would be obligated to scan all public posts and private chats against government-specified criteria. It's a serious interference with free speech and privacy rights.

If these services don't want to do it, they could pack up and leave the UK. If they do comply, it would open the floodgates to scanning requests from governments seeking to undermine democratic debate around the world. Who then would be the loser?

Internet companies will be required by the government to police social media posts for criminal offences across 11 areas of law. These offences include assisting illegal immigration and public order offences, as well as terrorism and child sexual abuse material. It is not clear why public order and immigration offences are in a bill to protect children.

Untrained civilians working for private companies will determine illegality and criminality based on what they "reasonably consider" without gathering evidence. They will be aided by context-blind algorithmically driven systems that will look for matches in images and video. The potentially high number of false flags (posts wrongly categorised as illegal) makes this a risky approach. The danger is that innocent posts could be swept away – potentially before they are even published – and legitimate public debate suppressed.

Private chat platforms, such as WhatsApp, Signal, Facebook Messenger and Telegram, will also fall under the bill's mandate. Under a recent amendment to the bill, they will have to scan for government-specified forms of illegal content using Home Office-approved systems. It is a deeply intrusive form of surveillance that will compromise the end-to-end encryption that currently keeps our chats confidential and secure. The template is one that governments in non-democratic countries could copy for political surveillance.

Monitoring of all public posts on social media sites, 24 hours a day, with the aim of removing those that meet prohibited criteria – this is an interference with free speech rights. Moreover, pervasive surveillance of private chats conducted without warrants is a violation of privacy rights. The likely chilling effect will be to make it more difficult for victims of crime and vulnerable people to seek help.

None of this cancels out the objectives of the bill to address online content that is harmful. Indeed, there are very serious concerns that the bill seeks to address. For example, the coroner's conclusions in the Molly Russell inquest raise grave concerns around self-harm content.

The government is right to want to address these issues, but under law, it must state clearly and precisely what content it wants to tackle and it must put in place procedures to rectify any errors if they occur. The bill should ensure that online platforms must justify their actions when they remove content and offer an effective appeals process.

The idea that technology can provide a silver bullet to solve complex societal issues does not stand up to examination. The back-of-a-fag-packet nature of this bill reflects an inept failure of due diligence in policymaking. Ideally, the government should go back to the drawing board; in its present form, large swathes of the bill will be unworkable, and we will be struggling with the consequences for years to come. ●

DON PABLO / SHUTTERSTOCK

Data is the crux of your organisation's security

Search-based solutions are crucial in spotting potential threats

By Peter Dutton

In association with elastic

Cyberattacks are a growing threat for organisations. Cisco estimates that distributed denial-of-service (DDoS) attacks – where victims' servers are flooded with disruptive traffic – will grow to 15.4 million by 2023 globally, while ransomware attacks more than doubled between 2020 and 2021 to 623 million. The UK government's *Cyber Security Breaches Survey 2022* also found that nearly two-fifths of UK businesses had identified a cyberattack in the year up to July 2022.

Public sector organisations, particularly those that manage critical national infrastructure, are particularly susceptible. Healthcare continues to be a major target: 20 per cent of the 777 cyber-incidents that the UK's National Cyber Security Centre (NCSC) dealt with in the year to September 2021 were linked to the health sector and vaccines. The non-profit Jisc, which provides IT support to the education sector, also found that 57 per cent of UK higher education institutions surveyed had reported a cybersecurity incident in the past 12 months.

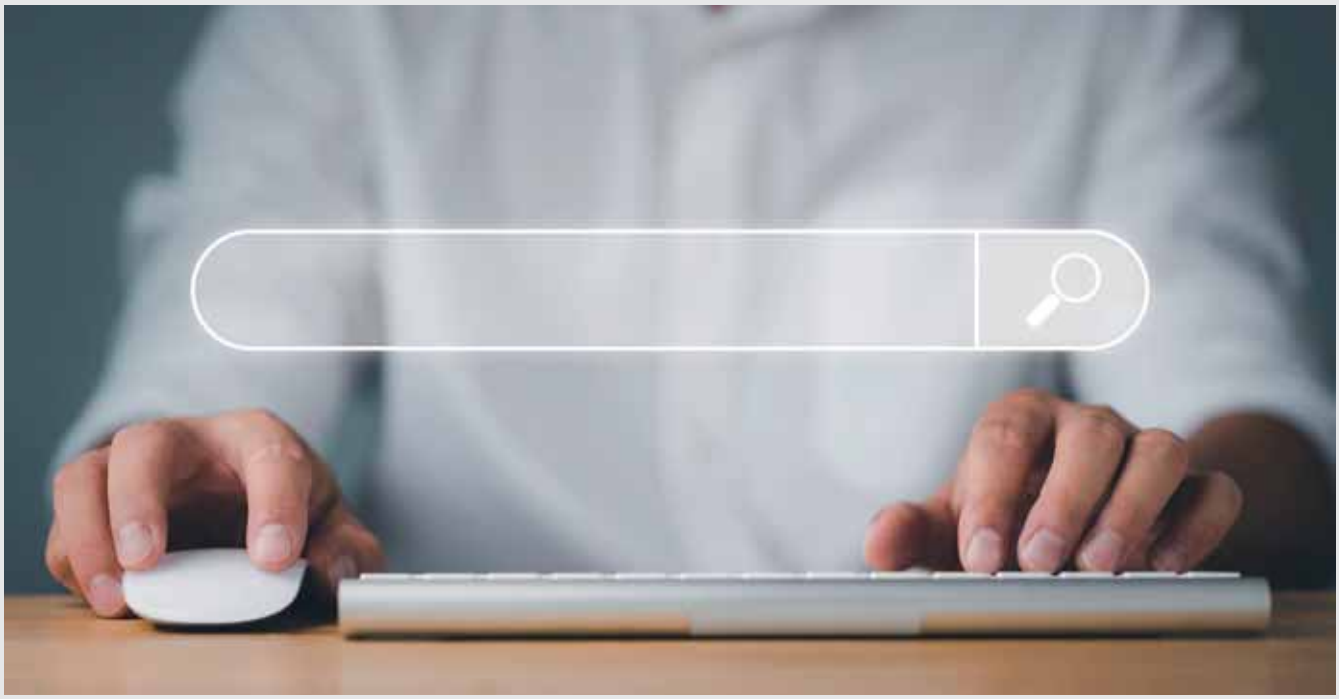
A big challenge for the public sector is the sheer scale and complexity of the cybersecurity threat and the sophistication of cybercriminals, which can include entire nation states (such as Russia) alongside individuals or criminal groups. As a result, public and private sector organisations need help identifying the most serious threats and acting on them quickly.

To achieve this, they need to put data at the centre of their organisations. Cybersecurity is fundamentally a data and search problem. According to Elastic's *Global Threat Report* for 2022, cyberattacks are becoming more diverse, enabling hackers to bypass an organisation's security defences and stay undetected for longer. Organisations need to be able to search through huge tracts of data to find vulnerabilities and mitigate them quickly. The other crucial element is creating a holistic, cohesive environment where everyone in the organisation is engaged in the process.

The task of improving business operations and keeping IT networks secure starts with the data organisations collect. The same data and systems used to improve user experience can also keep an organisation safe from cyberattacks and ransomware. However, if organisations cannot quickly surface key insights, they will be at a disadvantage.

At Elastic, our search solutions are designed around a single data analytics platform that enables organisations to search, observe and protect their business. To stay ahead of cyber-threats, Elastic's threat team continuously research security topics to improve our products, then share their learnings with the wider security community, helping to increase collaboration and foster workplace environments that are better at mitigating attacks.

As the company's vice-president for public sector across the UK and Ireland (UK&I), I lead a team who work with government departments and other agencies and public bodies, and empower them to make better use of their data, both to improve their own security and to benefit the country.



Organisations need to be able to surface key information from their data at pace

We help organisations unify their data on one centralised platform. This enables separate teams or departments to significantly reduce technical debt – when speed of software development is prioritised over well-designed code – by eliminating the need for multiple tools across the organisation. This allows organisations to address multiple challenges at once, break down silos separating teams, reduce duplication of effort, and ultimately improve efficiency and save money. By working through one system, organisations can harness and pool the skill sets of different individuals, helping them to develop a cohesive, collaborative approach to cybersecurity.

A great example of how we help organisations take a data-centric approach is our work with the NCSC, the government's cybersecurity arm. Using Elastic's search platform, the NCSC built a free, open-source tool called Logging Made Easy (LME), which is available on its website for any organisation to download and use. This software is a simple solution to help organisations get started with logging: recording all events in an organisation's IT network, from emails to logins to firewall updates – a crucial first step in strengthening cybersecurity. While not a full solution to an organisation's needs, LME means it has a starting point from which it can build with more sophisticated software in future.

Alongside focusing on centralising their data, organisations also need a platform that enables them to search through their data easily and at speed. We've helped organisations adopt a platform-based approach that means they can sift through huge amounts of data very quickly. For example, global technology company Cisco's cybersecurity team monitors billions of emails daily, of which a significant proportion are spam. Using Elastic's unified data analytics platform, Cisco can successfully search these emails and find crucial information relating to cyberattacks at pace.

But strengthening an organisation's security posture is more effective when you can also observe its IT infrastructure thoroughly. As an enterprise conducts business, its infrastructure systems, application logs and customer interactions generate information. Searching through this operational data and finding valuable insights will make organisations more self-aware and proactive.

Observability solutions allow teams to identify issues at their source and quickly improve the performance of their systems. HMRC's multi-channel digital tax platform (MDTP) is a digital platform that brings together hundreds of public services in one place, including tax services and Covid-19 schemes, such as the Coronavirus Job Retention Scheme and the "Eat Out to Help Out" scheme. Many people use the MDTP for different services at any given time, so HMRC must be confident that the platform can stay up and running for all those users. Using Elastic's observability solution, the department can ensure that it can search this complex landscape at speed to find critical information, preventing the site from going down.

Ultimately, improving an organisation's security posture comes down to successful data handling and collaboration – by investing in tools that can aggregate, centralise and make better sense of data, organisations can empower all employees to work together to tackle cybersecurity threats. Reducing silos is key to establishing good cybersecurity practice at any organisation, and we are keen to play our part in this. Elastic holds regular meetings with public sector organisations where we discuss how to tackle the evolving threat landscape. Get in touch to find out more by emailing ukgov@elastic.co.

Peter Dutton is vice-president, public sector, UK and Ireland, at Elastic

LOOKERSTUDIO / SHUTTERSTOCK

Comment

Josephine Wolff
Associate professor of cyber-security policy at Tufts University

"The private sector can't handle civilian cyber-risks without the state"

For the past decade, policymakers in both the US and UK have eagerly championed insurance as a way to manage private sector cyber-risks. The rationale for these efforts to promote cybersecurity insurance is typically something along these lines: where the government is slow and unwieldy and lacks technical expertise and good data on cyberattacks, the private sector can move quickly, and can continuously collect data to help it adapt to a changing threat landscape, all the while harnessing considerable tech talent to inform its risk modelling and mitigation efforts.

So it's striking that, even as the cybersecurity insurance market has continued to grow, insurers have repeatedly sought assistance from governments to help them both pay for and promote their cyber-related coverage. Far from taking over from governments in handling civilian cybersecurity issues, insurers have instead created a new set of policy challenges for regulators trying to understand how far they can and should go to assist the growth of a still relatively young sector of the insurance industry. Those challenges have taken on renewed urgency in the past two years, as cybersecurity insurance premiums have soared and insurers have signalled that they may cover fewer state-sponsored cyberattacks in the future, essentially offering their policyholders less coverage for more money.

No picture of the cybersecurity insurance industry is complete without an understanding of the role that regulators have played in pushing for it as a market-driven solution to cyber-risk, or the role that insurance carriers hope governments will play in the future by providing a backstop for their coverage for catastrophic cybersecurity incidents.

In 2012, in the United States, the Department of Homeland Security began hosting a series of roundtables and workshops on cybersecurity insurance intended to address concerns that such coverage was "expensive, rare, and largely unattractive" to buyers. At the first workshop, in October 2012, participants from the insurance industry asked the government for two things: better actuarial data about cybersecurity incidents and a federal backstop for large-scale catastrophic incidents that might otherwise bankrupt the insurers. By 2015, the US government had formed a dedicated Cyber Incident Data and Analysis Working Group (CIDAWG) to look at whether it might make sense to create a centralised repository for incident data that insurers could collectively contribute to and draw on for building their risk models – but that effort later fizzled due to administration turnover and lack of participation from insurers.

By 2015, cyberinsurance was also gaining traction in the UK as an important component of addressing cyber-risk. In March of that year, the UK Cabinet Office issued a joint report with insurance broker Marsh aimed at "helping the insurance industry to establish cyberinsurance as part of firms' cyber tool-kits". To help promote the importance of cybersecurity insurance, the report said, the UK government, together with Lloyd's and the Association of British Insurers, would develop a guide and host that guide on their websites. The government would also work with insurers to create a forum for exchanging data and insights about cyber-risks. And the report also announced that Marsh would offer cybersecurity insurance coverage for small- and medium-sized enterprises that would pay for those companies to go through the Cyber Essentials certification process the UK government had just launched. In other words: the UK government would promote cybersecurity insurance, and the cybersecurity insurance industry would, in turn, promote the cybersecurity certification scheme endorsed by the government.

MARTA SIGNORI

But even as they helped drive adoption of cybersecurity insurance, all these government efforts in both the US and the UK fell short in one of the key areas insurers were most worried about: would the government help them pay for really big, really expensive cyberattacks? The 2015 UK report touched on the topic briefly, saying, "While some market participants have suggested that a possible government backstop may be necessary, there is no conclusive evidence of the need for such a solution at present." In 2016, the US Treasury Department also signalled that, in the event of a sufficiently devastating cyberattack, existing government backstop provisions for terrorism risk insurance would apply, but offered little clarity about what kinds of cyberattacks, specifically, would trigger those provisions. The UK also extended its government-backed terrorism reinsurance fund to include cyber coverage in 2017, but has offered similarly little guidance on what kinds of cyberattacks would be eligible for such coverage.

In the absence of any clear policy from governments about when they will step in to help insurers pay for cyberattacks, and faced with growing fears about cyber intrusions from Russia and China, as well as Iran and North Korea, carriers are increasingly looking to exclude large-scale cyber-risks from their coverage. Earlier this year, for instance, Lloyd's issued guidance to its underwriters that they should exclude catastrophic state-backed cyberattacks from future policies if those attacks "significantly impair the ability of a state to function".

Such exclusions are a good indicator of just how ill-equipped insurers currently feel they are to model and cover serious cyber-risks without some greater financial support from governments. And the changes proposed by Lloyd's and other insurers are not small tweaks that will expose businesses to only a small number of infrequent risks – in fact, a cybersecurity insurance market that does not cover attacks from Russia, China, Iran or North Korea is a largely useless one.

Fortunately, governments are beginning to pay heed to the fact that they have been pushing a cybersecurity service that is not, in fact, able to provide protection from the full range of threats that businesses are worried about. To that end, the US Treasury Department announced this autumn that it was seeking comments on the creation of a federal backstop for catastrophic cyber incidents. That's only a first step towards actually clarifying what cyberattacks governments will pay for and whether insurers will decide to cover everything that falls below that threshold, but it's at least a step in the right direction in terms of recognising that the private sector was never going to be able to handle civilian cyber-risks on its own.

Josephine Wolff is the author of Cyberinsurance Policy

Patricia Lewis: "Weapons treaties have been destroyed through political posturing"

The director of the international security programme at Chatham House on prohibiting nuclear weapons, preparing for cyberattacks and the character of Nelson Mandela

How do you start your working day?
Black coffee, the papers, social media and emails. And, depending on the day, either a commute to Chatham House via the Piccadilly Line or to my desk at home in London or Ireland.

What has been your career high?
It is an impossible question to answer. I was an academic physicist in my early career and there is nothing like teaching quantum physics to young people, or seeing nuclear experiments reveal nature's wonders. I loved working in arms control at the Verification Research, Training and Information Centre (Vertic) and heading up the United Nations Institute for Disarmament Research (Unidir) in Geneva. But probably Chatham House is the absolute highlight. It is the most iconic of research institutes and my lovely dad, Peter Lewis, was an active corporate member who worked with the energy and environment team, so it has an emotional connection for me.

What has been the most challenging moment of your career?
I have had the privilege of being part of teams who have helped create some of the world's most important treaties on nuclear and conventional weapons. The most challenging thing has been seeing these being destroyed through non-compliance and political posturing. I am grateful for the UN's new Treaty on the Prohibition of Nuclear Weapons (TPNW) as it signifies hope even when the threat of nuclear weapons is again looming.

If you could give your younger self career advice, what would it be?
Don't be afraid to tell the truth. Say when you don't understand or if you think something is wrong. Speak out about sexual harassment and racial bullying and don't be afraid to upset people even when you fear the consequences.

Which political figure inspires you?
Nelson Mandela – he stuck to his truth but was able to change his tactics and adapt to new realities, whether that be on Robben Island or as president of South Africa. He used his extraordinary gifts and intelligence to make the world better for millions of people.

What UK policy or fund is the government getting right?
The UK is getting cybersecurity roughly right. It is a fast-moving field with many threats and opportunities. In the UK, the private sector works collaboratively with government. The way the internet is run – open and free, vs closed and controlled – really matters for the future, and the UK is an international leader.

What policy should the UK government scrap?
I would like to see the UK participate in international conferences on the humanitarian impact of nuclear weapons and the TPNW as an observer, like other Nato countries. The UK has decided not to participate in either. I'm not saying that the UK should unilaterally give up nuclear weapons, but I would like to see an uptick in multilateral efforts.

What piece of international government policy could the UK learn from?
I like the requirement that several countries have put into legislation that every citizen has to vote in elections. I don't think that there should be severe sanctions for not voting and everyone would be entitled to leave their voting card blank or deface it, but I think it would help to create a sense of civic duty and being "all in it together" that democracy needs.

If you could pass one law this year, what would it be?
I would pass a law that required the government to provide detailed annual reports to parliament on national preparations for a range of crises such as pandemics, large cyberattacks and extreme weather events. The legislation would ring-fence budgets specifically for resilience measures and introduce drills into schools and workplaces – like fire drills but for a wider set of crises. I can highly recommend the National Preparedness Commission, chaired by Toby Harris, for practical ideas. ●

MARTA SIGNORI

PressGazette British Journalism Awards 2022

Now in its eleventh year, this event celebrates the best public interest journalism produced for a UK audience. It is open to all publishers and journalists whatever the medium: print, broadcast and online.

As ever, the awards aim to recognise great journalism which is revelatory and which has an impact. The judges are looking for work which displays journalistic skill and rigour and which serves the public interest.

15 December 2022
London Hilton Park Lane

Sponsorship opportunities now open
To support this annual event please contact
kalpesh.vadher@pressgazette.co.uk

Scan the QR code for details:

Headline sponsor:

Starling Bank

Sponsors:

amazon
CAMELOT
Google News Initiative
Newsworks
octopus energy
wiggin