THE NEW STATESMAN
Spotlight
Thought leadership and policy

Cyber Security: Protecting the digital world

Damian Hinds MP
Lindy Cameron
Julia Lopez MP

Sophos stops ransomware.

SOPHOS
Cybersecurity evolved.

Who really pays for cybercrime?

In May this year, the Darkside cybercrime group paralysed a crucial part of the United States' energy infrastructure. The Colonial Pipeline is responsible for nearly half of the East Coast's fuel supply. It was brought down, however, not by a sophisticated breach of the technology that manages the flow of fuel, but a vulnerability in its billing software.

The incident served as a powerful reminder of the real-world consequences of cybercrime. The Colonial Pipeline Company took the decision to temporarily stop operating, resulting in fuel shortages in several states.

In the following weeks, Darkside claimed it was shutting down. Security experts believe Russian authorities, facing pressure from the US, may have taken steps to restrict the group's activities. However, few saw the move as the beginning of a more significant retreat from ransomware. As the Security Minister Damian Hinds writes on page six, it remains the most serious cyber risk facing the UK.

In the aftermath of the attack Colonial revealed it had paid a £3.1m ransom. "It was the right thing to do for the country," its chief executive said.

Some security experts question that sentiment. While the FBI recovered around half of the payment, it is feared that by paying the ransom Colonial will have increased the risk of further similar attacks. The incident triggered a surge in cyber insurance applications from the energy industry.

It is likely that Colonial's insurer covered the cost of the ransom, a practice now attracting scrutiny, not least because the sector also stands accused of failing to incentivise prevention.

The former National Cyber Security Centre chief executive Ciaran Martin has accused insurers of funding organised crime. Think tanks have mooted a ban on the practice and, in France, where rates of ransomware attacks are second only to the US, the insurance giant Axa has vowed to stop paying out.

The government must take a formal position on the practice. Until it does, insurers will continue to take the easiest route and cyber extortionists will become greedier still. ●

Contents

Spotlight

Standard House
12-13 Essex Street
London,
WC2R 3AA

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

Director of Client Solutions
Dominic Rae

Account Manager
Jugal Lalsodagar

Special Projects Editor
Oscar Williams

Special Projects Writers
Jonny Ball
Sarah Dawood
Samir Jeraj

Deputy Head of Production
Tony Rock

Design and Production
Rebecca Cunningham

Cover Illustration
Klawe Rzeczy

BRITISH SOCIETY OF MAGAZINE EDITORS AWARDS 2017
WINNER

First published as a supplement to the New Statesman of 19 November 2021.

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

US issues charges against Ukrainian and Russian "hackers"

The US Department of Justice (DoJ) has charged two alleged cybercriminals with perpetrating severe ransomware attacks on major American businesses.

Yaroslav Vasinskyi, a Ukrainian national, is accused of having hacked into software provider Kaseya and then launching an attack on 1,500 of its customers around the world, affecting everything from schools in New Zealand to shops in Sweden. Separately, Yevgeniy Polyanin, a Russian national, is accused of carrying out ransomware attacks on multiple government organisations and businesses in Texas in 2019.

The alleged perpetrators are both accused of using software developed by the core REvil group to encrypt the data of affected organisations and hold them to ransom. The department has since seized $6.1m in funds it said were "traceable to alleged ransom payments received by [Polyanin]".

Vasinskyi was arrested in Poland and is awaiting extradition while Polyanin remains at large. The action was taken as part of an operation against ransomware gangs by the FBI and Europol, with security agencies from across Europe being involved. Twelve people were arrested in raids in Ukraine and Switzerland, according to Europol.

The US has suffered several devastating cyber attacks this year, including an attack by the DarkSide gang that closed down the largest fuel pipeline in the country.

Tech chiefs could face prison over harmful content

Bosses of social media platforms could face far more than fines if they do not tackle harmful algorithms, Digital Secretary Nadine Dorries has announced.

The draft Online Safety Bill was drawn up to tackle the proliferation of harmful and illegal material online, including child abuse, terrorist propaganda, hate crimes, cyberbullying and misinformation. It places a duty of care on websites – especially "big tech" players such as Facebook, Twitter, Instagram and YouTube – to protect their users, imposing fines if they do not.

It is currently undergoing pre-legislative scrutiny by a joint committee, which is due to report its recommendations to government by 10 December.

Speaking to the committee, Dorries said that bosses could face jail if they fail to tackle the algorithms that prioritise harmful content appearing in people's news feeds. This activity was exposed by Facebook whistleblower Frances Haugen, who accused the tech giant of prioritising profits over people's safety.

Bosses could also now face criminal sanctions if they do not respond to information requests from the regulator Ofcom within three to six months after the bill becomes law, rather than two years as originally planned.

"[Platforms] know what they are doing wrong," said Dorries. "They have a chance to put that absolutely right – now. Why would we give them two years... to change what they can change today."

This comes after the Law Commission made recommendations to strengthen the bill. Dorries has said she is minded to accept some of these, including criminal prosecution for individual users who send the most serious threats.

CHIP SOMODEVILLA / GETTY IMAGES

50,000

Phone numbers targeted by Pegasus spyware, created by the NSO Group

31%

Increase in cyber scams targeted at UK businesses in 2020

723

Number of cyber attacks defended against by the NCSC last year

19%

Percentage of 10–15-year-olds who experienced cyber bullying in 2019 and 2020

AMIR LEVY / GETTY IMAGES

Spending review reveals new local authority funding to boost cyber security

Local governments across England are to be given £85.8m towards improving their cyber security. The funds were announced as part of the autumn spending review. The pledge comes after councils such as Hackney and Cleveland and Redcar suffered breaches resulting in millions of pounds of damage.

Hackney's local authority fell victim to ransomware targeted at the London borough by cybercriminals in 2020. The attack resulted in the personal information of thousands of employees and residents being published on the dark web.

Theo Blackwell, London's chief digital officer, told *Tech Monitor* the funding showed government is "waking up" after a number of "very serious cyber attacks".

Iran blames major cyber attack on "state actor"

The Iranian government has said that an unnamed "foreign country" was responsible for a cyber attack on its petroleum infrastructure last month.

The attack affected a smart card system that allows Iranians access to subsidised fuel. Without it, only expensive, unsubsidised fuel was available, leading to severe queues at petrol stations in the capital Tehran and beyond. Attackers also targeted digital billboards on Iran's main highways, displaying a message addressed to the Islamic Republic's Supreme Leader: "Khamenei, where is our fuel?"

A group calling itself Predatory Sparrow claimed the attack, but the country's main internet policy organisation pointed the finger at an unnamed foreign power. Separately, although both countries have denied involvement, it is widely believed that the US and Israel were behind the 2010 Stuxnet cyber attacks against Iran's nuclear enrichment facilities.

Many Iranians rely on subsidised fuel. In 2019, price rises led to widespread protests. Hundreds were killed following a government crackdown.

WhatsApp can sue NSO Group, says court

A US appeals court has ruled that the NSO Group, the Israeli company responsible for Pegasus spyware, will not be able to use its government clients as a shield from litigation. WhatsApp, the messaging giant, had accused the company of illegally providing snooping software.

Earlier this year it was revealed that Pegasus – which is capable of reading text messages, tracking locations, and accessing targeted devices' microphones and cameras – had been used against 50,000 people, including human rights activists and journalists.

Ransomware attacks can wreak havoc

There are steps you can take to protect yourself and your business from the UK's number one cyber security threat

By Damian Hinds MP

Cybercrime has been on the rise both in scale and complexity. Working remotely during the pandemic has given cybercriminals more opportunities to prey on our vulnerabilities. Every case is unique; some have a horrendous impact on lives. Just imagine an elderly person stripped of their lifetime savings by a fraudster, or employees made redundant when company operations are shut down by a cyber extortionist.

From my conversations with cyber experts and companies, I am struck by how sophisticated criminals have become. Two in five businesses and a quarter of charities reported having cyber security breaches or attacks in the past 12 months, according to the government's *Cyber Security Breaches Survey* published in March 2021.

Out of all the cyber security threats we face in the UK, the number one threat is ransomware. This refers to malware attacks used to extort money from victims by rendering their networks unavailable, and which often steal and hold precious data to ransom. More recently, we have seen criminals threaten to leak stolen data in a bid to maximise the pressure on victims to pay.

Ransomware attacks can wreak havoc. We witnessed the damage the WannaCry ransomware attack did to the NHS in 2017. Some services had to turn away non-critical emergencies because much of their hospital equipment was affected. More recently, we saw how a ruthless cybercriminal gang targeted the Colonial Pipeline, a major US oil provider, resulting in fuel shortages and a state of national emergency.

The UK's National Cyber Security Centre (NCSC) reported in its 2020 annual review that it had handled more than three times as many ransomware incidents in comparison with the previous year. It is very difficult to assess the financial damage due to under-reporting. However, ransomware attacks cost the UK economy at least £600m in 2020, according to Emsisoft Malware Lab.

Cybercriminals see ransomware as a low-risk and lucrative endeavour, and it has become more feasible than ever. The advent of ransomware as a service (RaaS) allows many more criminal affiliates to execute attacks without having advanced IT or coding skills. It is not an exaggeration to say your business could be paralysed by an amateur.

These criminals are occasionally backed by hostile states, such as North Korea, as in the case of the WannaCry attack. Most of the groups are motivated by profit, but they can also seek to damage a reputation or sabotage an operation.

Ransomware and cyber challenges don't stop at borders. Our government has been working tirelessly with international partners, especially the US, to fight ransomware criminals. At this year's G7 summit we called on all states to identify and hold to account cybercriminal gangs that operate in their territories. In October, the UK hosted a session on countering illicit finance as part of a multilateral ransomware event to find new global ways of disrupting ransomware attacks.

Last month marked the fifth anniversary of the launch of the NCSC, our nationwide major authority on cyber security. Between September 2019 and August 2020, the NCSC supported nearly 1,200 victims of 723 attacks.

The UK government is also working hard to improve the UK's cyber resilience, investing £195m over the past five years to establish a specialist cyber law enforcement network to disrupt cybercriminals and support victims. Tackling the threat from ransomware crime is a key priority of the Home Office and we are working closely with industry leaders on further steps we can take to clamp down on this pernicious crime. Soon we will publish a new national cyber strategy that will provide significant improvements in the UK's response to cybercrime by strengthening law enforcement, and driving greater collaboration with the NCSC and the National Cyber Force, which tackles issues such as terrorism and child sexual abuse and exploitation.

Cyber security need not be a daunting challenge for organisations of any size and, while larger organisations tend to invest more into their resilience, sound protection and recovery plans can be implemented without needing to pay an arm and a leg. All business owners should follow basic best practices.

Keep offline backups of files, test that they work and ensure that any of your contracted service providers also conform to good cyber practice. If you would like more tailored assistance, contact your regional cyber resilience centre.

SHUTTERSTOCK / RAWF8

Ransomware attacks cost the UK economy at least £600m in 2020

It is essential that your employees receive adequate training about cyber security; for instance, they should know how to recognise phishing emails. The NCSC has published a free e-learning package to help staff stay secure online.

If you or your organisation is attacked, the strong advice is against paying any ransoms to cybercriminals. The payment of a ransom is likely to encourage further criminal activity – it does not prevent the possibility of future data leaks and doesn't guarantee you will regain access to your IT systems.

Some may be hesitant about reporting a ransomware incident. However, it can help crack down on cybercrime by providing our law enforcement partners with precious intelligence. Above all, you will get professional advice on how to recover and how to avoid paying ransoms. Cybercrimes should be reported to Action Fraud, the Information Commissioner's Office (for data breaches under the General Data Protection Regulation, or GDPR), or for major cyber incidents, to the NCSC.

I would recommend that we all take action to protect our data online. The government's Cyber Aware campaign contains six actionable steps that will make individuals much less likely to fall victim to a cyber attack.

The NCSC's Small Business Guide contains affordable, practical advice for smaller businesses, and the centre also has guidance for large organisations. There is information on how to prevent ransomware infections specifically.

Follow these actionable steps and take immediate action to protect yourself and your organisation from ransomware and other cyber attacks. Speak to your colleagues and together we can all be better protected against this threat. ●

Damian Hinds is Minister of State for Security at the UK Home Office

Advertorial

Cyber security is a constant battle

New threats to businesses must be met by innovation

By Christopher Hurst

In association with kaspersky

Every day, millions of us start up our laptops, desktops and devices, and connect to networks at home and at work. Yet, each day hackers and cybercriminals are working away too, finding the vulnerabilities in software, systems, and even specific companies and organisations. The ranks of the hackers include mercenaries, organised criminal gangs and state-sponsored groups, all of whom have the skills and resources to devastate their chosen targets. No company or organisation is immune to every sophisticated attack.

At Kaspersky we looked at these threats as part of our *IT Security Economics 2021* report. What we found was attacks have become more challenging, as companies and organisations have moved to hybrid working, using complex systems to support a workforce more likely to be working from home. Without these systems and risks being fully visible, cyber defenders can find themselves on the back foot, responding late or inappropriately to an attack they struggled to find.

Cyber security is not just about one organisation either. Every external supplier or customer is a potential route into systems, particular where there is shared data. Incidents involving shared data with suppliers were the costliest at an average of $1.4m in 2021, while attacks on supply chains cost an average of $2m.

The best way to protect against and respond to this new wave of cyber threats is through a well-coordinated and professional team of people. At Kaspersky, we work with organisations, big and small, to help them develop the cyber security and infosec systems that work for them, performing managed detection and response and incident response. Part of this process is "hunting" down threats before they strike, using our knowledge and expertise to develop the tools to do this automatically while retaining the skilled personnel to deploy where needed.

Hackers can also take advantage of systems that see "too many" risks and bombard cyber defenders with unnecessary incident alerts that they then have to investigate, increasing the chance that a serious attack slips through. Fortunately, Kaspersky has developed a comprehensive cyber security framework that helps to prioritise truly critical incidents and

Companies and organisations are using complex systems to support hybrid working

focus resources on tackling them.

Unfortunately, many organisations struggle to recruit qualified cyber security personnel, which is part of a wider shortage in the labour market for people with these valuable skills. Globally, it is estimated that there are 3.5 million unfilled cyber security jobs and it is very likely that that number will grow.

Other organisations are too small to be able to invest in an in-house team to safeguard their IT systems against general risks, let alone a targeted attack. Our research shows that the most common reason for small and medium businesses not to invest in cyber security is that management do not see a reason to do it, followed by the belief that their systems or recent investments have secured them against threats. The dilemma facing many businesses is the choice between constant investment in cyber security without any visible benefit or constant risk of getting substantial losses after the incident.

However, not being prepared can be dangerous and costly. According to our research, in 2021 the average cost of a data breach for a small business was $105,000 and closer to $1m for larger enterprises. That cost includes having to bring in external help after the incident, lost business, fines, compensation and damage to credit ratings. Investing in new staff, systems and training in cyber security after the breach may help mitigate the brand damage and reassure investors, but it is a poor substitute for having been prepared in the first place. Yet, the average budget for cyber security fell during this time and professionals are concerned about how to secure the more complex systems they are now working with.

Small and large businesses, and the public sector, face ever-changing cyber security threats from a range of sources, costing data, time and money to repair.

Hackers and cybercriminals work together across the dark web, trading and sharing in new tools, exploits, tactics and methods. That is why we need to be constantly innovating, investing in and developing cyber security to meet those challenges and create a safe environment for businesses and organisations to thrive. ●

Christopher Hurst is general manager, UK & Ireland at Kaspersky

The stats

Key findings from Kaspersky's *IT Security Economics 2021* report:

$1m

is the average cost of a data breach for larger enterprises

of an SME's IT budget was spent on cyber security in 2021

cyber security jobs are unfilled, a number that is expected to grow

SHUTTERSTOCK / BBERNARD

Forecasting tech's future at GCHQ

Lindy Cameron discusses her first year as chief executive of the National Cyber Security Centre

By Oscar Williams

On 13 December 2020, the Biden administration confirmed reports that the US treasury and commerce departments had fallen victim to a major cyber espionage campaign. Orchestrated by hackers thought to be working on behalf of Russia, the campaign stunned the US intelligence community. But for Lindy Cameron, the new chief executive of National Cyber Security Centre (NCSC), the incident was just the latest in a series of geopolitical crises she had witnessed as a senior civil servant.

"I had quite an amusing conversation with Jeremy [Fleming]," says Cameron, referring to the GCHQ intelligence chief she reports to. "I had to remind him that the bread and butter of what I've done for 20 years has been managing crises and conflicts. So, in some ways, a rapid-onset, complex, international crisis allowed me to work out how to apply my skill set to the new organisation."

Having worked on conflicts in the Balkans, Iraq and Afghanistan, Cameron applied to become NCSC's second chief executive last summer. "I've known Jeremy for a while and he called me up to ask me if I was interested," Cameron tells *Spotlight* during a recent interview at NCSC's headquarters in central London. "We had a really great conversation about how the skill set that I had – which was effectively about convening across Whitehall and being able to communicate a set of tricky issues really effectively – would work in this space."

While Cameron notes that she is still working with many of the same people in the national security community she has "grown up with", she likes "doing new and different things. I get bored easily and I like to stretch myself." That she was succeeding Ciaran Martin, the first CEO of NCSC, also appealed: "I like taking over from people who have done a brilliant job."

Cameron's first year as Britain's most senior cyber official has coincided with an extraordinary era in national security. Less than a month after the Russian attack on the US government came to light, it emerged that China was exploiting vulnerabilities in Microsoft Exchange email servers in what became an even larger crisis. Five months later, cyber extortionists believed to be operating out of Russia triggered the shutdown of one of the most vital parts of US energy infrastructure: the Colonial

Pipeline, which is responsible for transporting millions of barrels of fuel between Texas and New York each day.

The pipeline attack "parachuted" cyber security onto the agenda of the G7 meeting in Cornwall in June, says Cameron. "Of all the many things Ciaran left me, what he didn't leave me was the expectation that we would be right at that level on the agenda of a very high-level political meeting less than a year later." The real question now, she says, is how to take advantage of that moment of opportunity. "World leaders understand that cyber security is a really big issue for the future, both in technological terms but also in operational risk terms," she explains.

During the G7 meeting, leaders issued a communique calling on Russia to "hold to account those within its borders who conduct ransomware attacks" and "abuse virtual currency to launder ransoms, and other cybercrimes". Cameron says the meeting has led to closer international cooperation on how best to tackle the "complex system that is the ransomware criminal network".

In February, Cameron's predecessor, the aforementioned Ciaran Martin, called on governments to consider banning insurers from subsidising their clients' ransom payments. "I see this as so avoidable," Martin said. "At the moment, companies have incentives to pay ransoms, to make sure this all goes away. You have to look seriously about changing the law on insurance and banning these payments, or at the very least having a major consultation with the industry."

Does Cameron agree? "The government's got a really strong position on this that people shouldn't be paying," she says. "I can understand that there are specific contexts in which, more actually from a law enforcement perspective, sometimes you don't want it to be absolutely binary. I just think we need to make it much easier for people to feel like that's not the choice."

Cameron believes that because the cyber insurance market is still relatively new, providers are not yet at a point where they incentivise prevention rather than payment. "I think about it a bit like the car insurance market," she explains. "When I was 17, it was quite cheap to insure myself with a learner driving permit. It's definitely not that cheap for my godchildren to do it these days." Cameron would really like insurers to be "incentivising businesses to be demonstrating that they're not a risky proposition". This is because, in her opinion, businesses have done a "fantastic job with their own cyber resilience", and therefore, she adds, "they're a very good insurable risk".

NCSC

I'm not on a mission to be expansionist, says Cameron

Over the coming weeks, the government is expected to publish an updated national cyber strategy. Cameron is keen that the remit of NCSC, which is now five years old, is clearly articulated. "It does require us to slightly more carefully redefine what's the thing that we need to do and only we do or that we always do," she says. "I'm definitely not on a mission to be expansionist. If I was, this organisation would be ten times the size."

As the government seeks to transform the UK into a "science and technology superpower", one role NCSC will increasingly play is as an advisor – drawing on GCHQ intelligence – on the threats posed by emerging fields of technology.

The government needs to be "driven by a real understanding of what that 20-year vision looks like, not just a single political cycle", says Cameron. "We have a real responsibility to be doing the stuff that is the very long-term understanding of trends and technology, both in terms of intent and in terms of capability, in a way that means that we are helping to proof the UK against future cyber security threats."

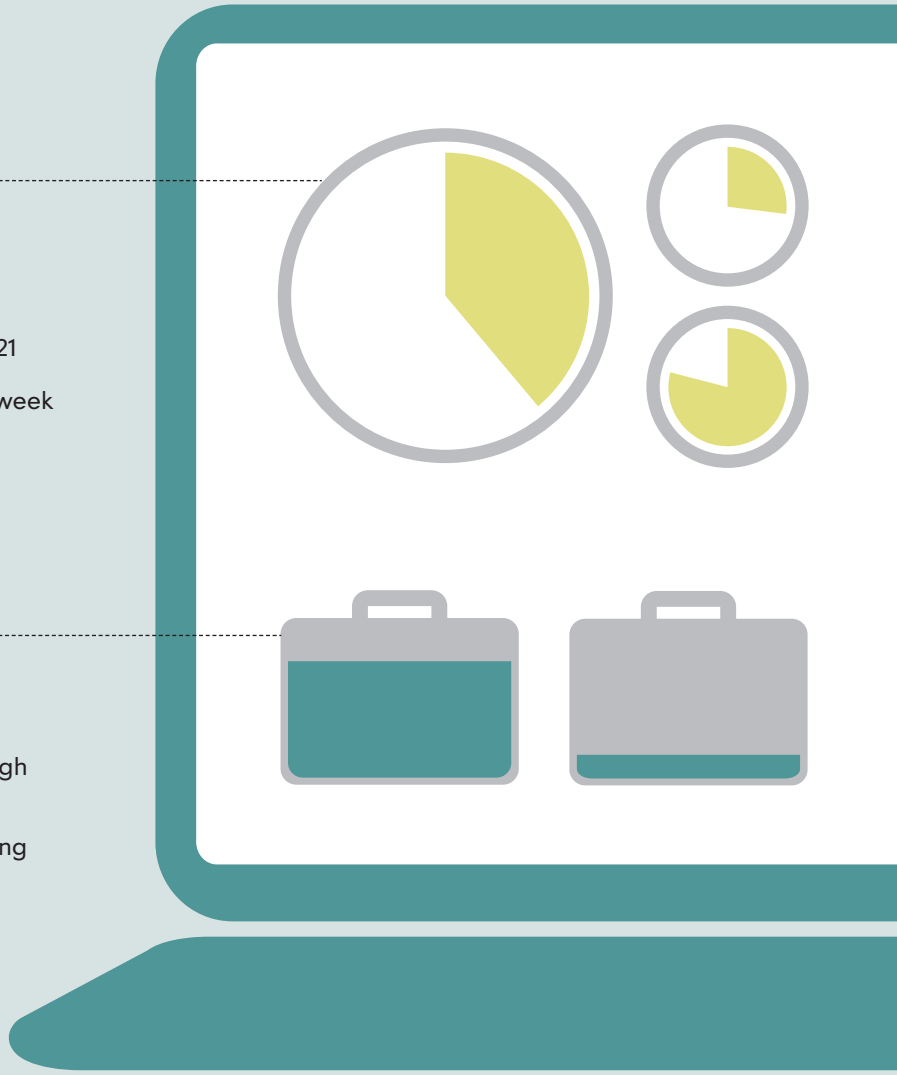
How cyber attacks impact businesses

Remote working, outdated software and a lack of security tools make organisations more vulnerable to breaches

39%
of businesses reported having cyber security breaches between March 2020 and March 2021

27% of these have breaches at least once a week

83% experience phishing attacks



77%
of all businesses say that cyber security is a high priority for their senior management

14% say it has become a higher priority during the pandemic

SOURCE: GOVERNMENT CYBER BREACHES 2021 SURVEY
BASED ON A SURVEY OF 1,419 UK BUSINESSES

Following a cyber security incident:

- [ ] **44%** attempt to identify the source
- [ ] **36%** formally log the incident
- [ ] **34%** have guidance on who to notify
- [x] **32%** take no action

£8,460

is the average cost to businesses of cyber breaches that resulted in loss of money, assets or data

£8,170 is the cost to micro and small businesses

£13,400 is the cost to medium and large businesses

83%

of businesses have up-to-date anti-virus software

78% use a network firewall

35% use security monitoring tools

34% use a virtual private network (VPN)

Advertorial

Community safety includes cyber security

Local government needs to take urgent action to tackle its cyber security weaknesses

In association with SOPHOS

Local government is the heart of communities in the UK and around the world. From public parks and bin collections to schools and social services, it provides the day-to-day services we need in our lives. But a combination of cuts to funding and new cyber threats are leaving these vital services and the personal data they collect open to attack.

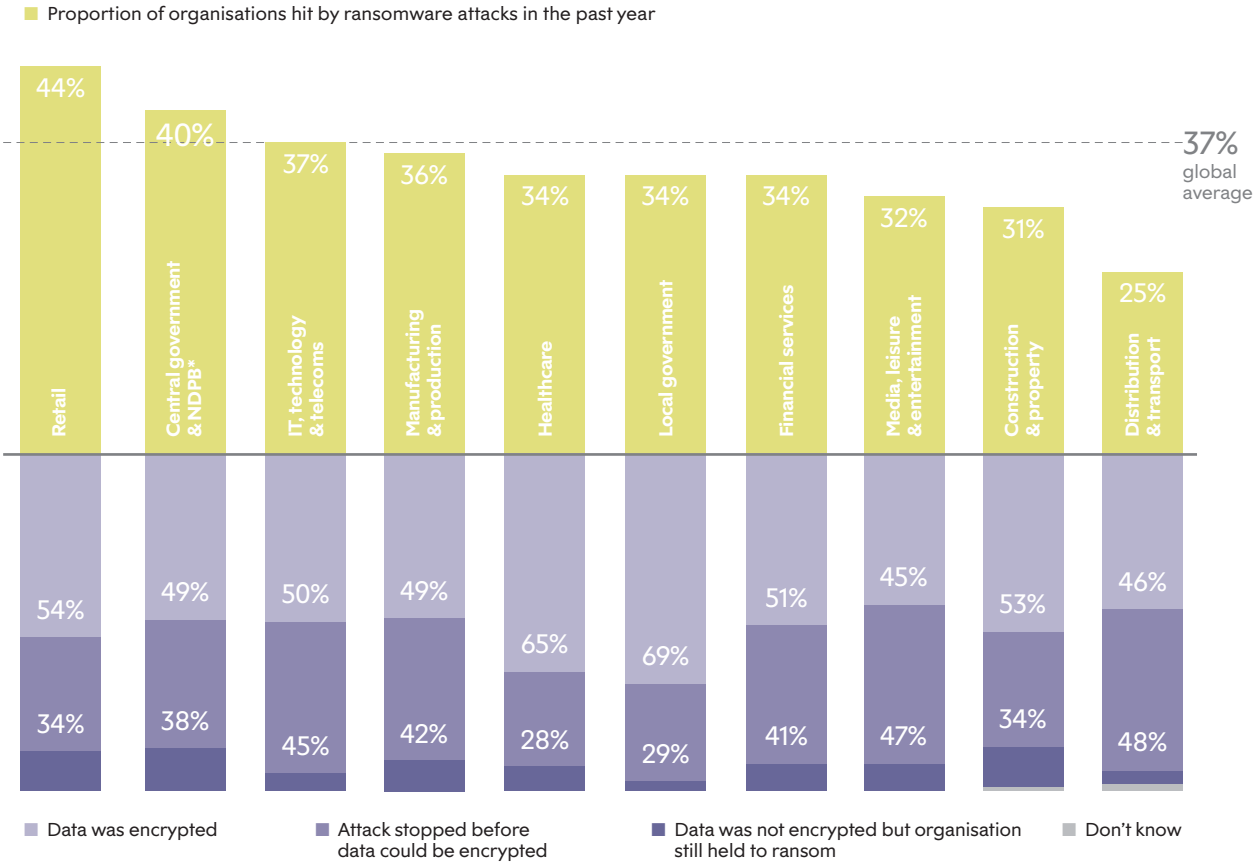
Councils, including Copeland in 2018, as well as Redcar and Cleveland and also Hackney, both in 2020, have become one of the most tempting targets for cybercriminals using ransomware to extort public money. The two most recent of those attacks are estimated to have cost more than £20m on top of the serious disruption that went with them.

The research in Sophos's *The State of Ransomware 2021* report shows that a third of local governments were hit by a cyber attack in the past year. In more than two-thirds of those cases attackers managed to encrypt their data, and where that happened around four in ten victims paid out a ransom. This relatively high proportion of local governments paying out to cybercriminals is perhaps because only four in ten of those whose data was encrypted were able to restore their data from backup. The average cost of an attack to local government around the world was $1.64m (£1.2m).

Ransomware and the infrastructure around it are constantly evolving and adapting in technology and tactics to new defences and vulnerabilities. Attackers now not only encrypt files but steal and threaten to release them publicly if a ransom is not paid. This "double extortion" technique has become almost universal. Once that data is stolen, even if it can be recovered from backups or the ransom paid, it is out there and cannot be "un-stolen". Nor can the trust between local government and citizens easily be repaired.

For the ransomware attackers, local government offers several attractions, including legacy systems and a relatively low level of IT resources to defend it. Attackers also know that local government is under pressure to maintain public services, something which multiplies the effect of any disruption. Despite these risks, according to *The State of Ransomware*

Local government is still a vulnerable sector



SOURCE: THE STATE OF RANSOMWARE 2021. *NDPB = NON-DEPARTMENTAL PUBLIC BODY

2021, more than a quarter of local government respondents globally admitted they had no malware recovery plan, the lowest of any sector surveyed.

Local authority IT professionals are under no illusions about the threat posed by ransomware. When Sophos polled 200 IT staff in this sector in March 2021, ransomware was rated the top concern by 63 per cent of respondents. As with any sector, local authorities depend on a variety of systems old and new, with some old enough to be classed as legacy – for example, applications that require server operating systems that are end-of-life or beyond. In many cases, migrating from these takes time both for budgetary and organisational reasons. Likewise, physical hardware such as PCs, mobile devices and network infrastructure is also used beyond its intended life for reasons of financial necessity. However, cyber attacks now efficiently target an ever-wider range of flaws, which means that legacy systems have turned from abstract risks into concrete liabilities.

The move to fully working from home during the Covid-19 pandemic took these risks and multiplied them even further. Again, as with other sectors, the logistical challenges of this rapid transition were massive and mean a much greater ongoing workload to keep those systems safe and secure. Even when enough devices and connectivity are available it places huge pressure on endpoint security, network segmentation, data access policies, remote access and cloud security, and authentication, and raises the risks of shadow IT.

The biggest target for any attacker is, however, the employees or end users, hence the ubiquity of targeted email phishing attacks, designed to steal credential or money. This emerged from the realisation that it doesn't matter how much technology organisations deploy to defend themselves if this can be bypassed by a simple play on human psychology. User education is the obvious answer, changing the assumptions of trust that users make when using systems such as email. However, it's not a magic fix. Staff and end user awareness needs to be about constant reminders as well as hands-on training and adapting to new tactics.

If local government is going to continue to be a trusted part of our community, it needs to take its security seriously because it is the security of the community it serves. We entrust it with information about our lives, the education and safety of our families, and the taxes we pay to make it happen. It is one thing to see and understand the problem, which many local governments and the people who work for them do, but it is another to take the necessary action to safeguard critical services and protect the data of residents. ●

Red Guards in cyberspace?

How hacking became the new frontier of tensions between China and the West

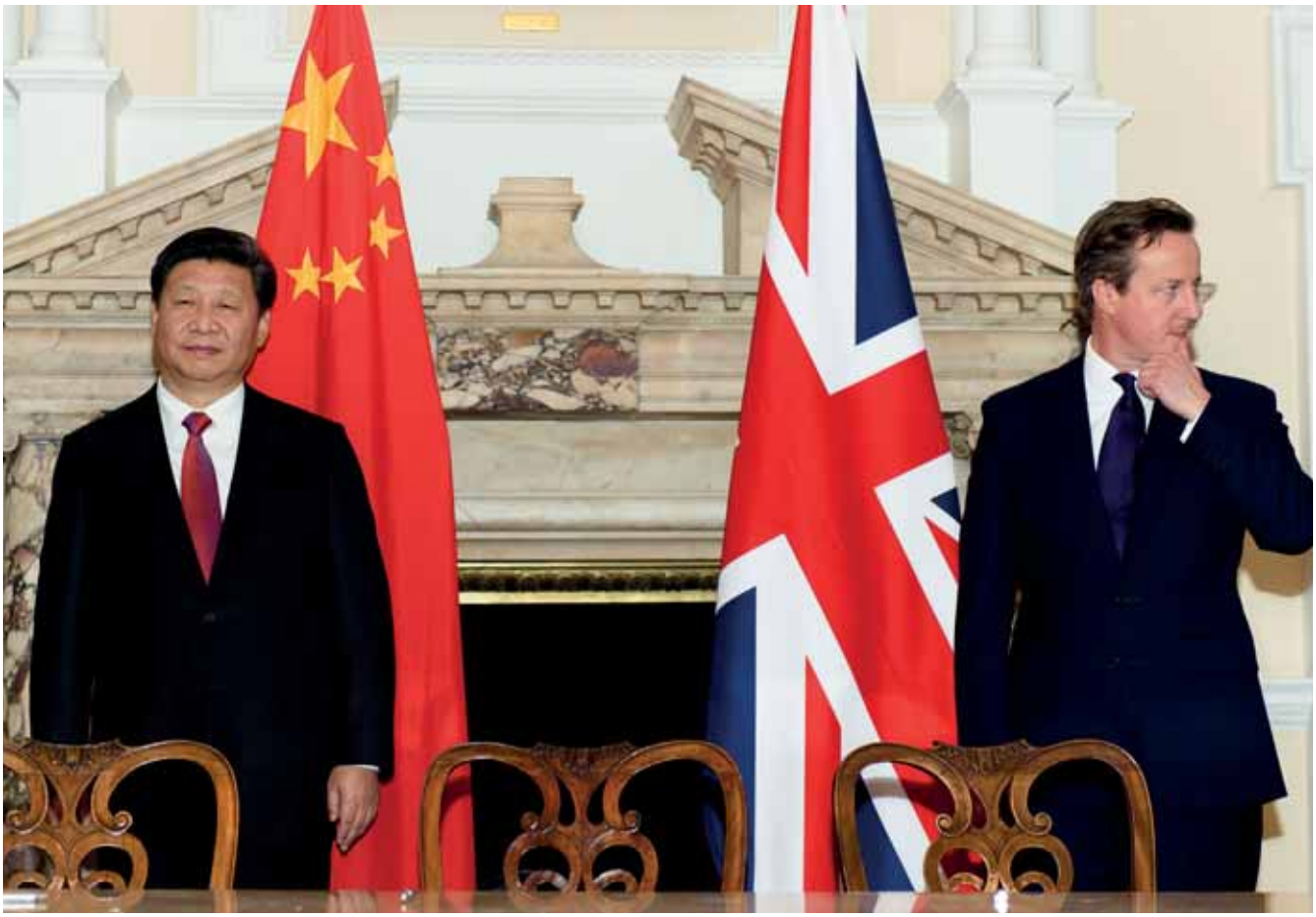
By Jonny Ball

When Xi Jinping became Chinese premier in 2012, some Western observers heralded his takeover as a welcome sign of political and economic liberalisation. Eleven years had passed since China had joined the World Trade Organisation (WTO), an event itself hailed as a victory for Western-style multilateralism. And although the WTO still categorised China as a "Non-Market Economy", it was felt that the communist state, as a rising economic powerhouse, was a clubbable partner for the capitalist West.

Xi's takeover presented commentators with the opportunity to continue in the rich vein of Western triumphalism that characterised Nineties and Noughties Sinology. Cheng Li, a senior fellow of the Brookings Institution, a US think tank, predicted that Xi would pursue "policies to promote the development of the private sector". David Lampton, director of the China programme at the John Hopkins School of Advanced International Studies, claimed his conversations "with people in the United States" led him to believe that the "reigning understanding" of Xi was that he was "'a guy we can work with'".

Much was made of the new premier's backstory. A red princeling scion of a senior party official, his father had been purged and imprisoned during the Cultural Revolution, and the young Xi had spent seven years in internal exile living in cave houses deep in the Chinese countryside. It was thought that this first-hand experience of Maoist overreach would have placed him firmly in the camp of the Chinese Communist Party's reformist wing, pursuing rapprochement with the West, democratising the opaque structures of the state, and embracing free-market economics. But this was not the case.

In July this year, the UK, EU and US accused China of carrying out a cyber attack against Microsoft Exchange servers. Around 30,000 organisations globally were said to have been affected by the hack, reportedly carried out by Hafnium, a group Microsoft described as "state-sponsored and operating out of China". From January onwards, IT systems in businesses, local government and state institutions were said to have been compromised. Defence contractors, legal firms and medical researchers were among those that had



Xi Jinping meets David Cameron at a joint press conference as part of a state visit to the UK in 2015

LEON NEAL / WPA POOL / GETTY IMAGES

been spied on. To make matters worse, once the software vulnerabilities had been exposed, other hacker groups also started exploiting them.

The EU said the attack had "resulted in security risks and significant economic loss for our government institutions and private companies". Dominic Raab, the UK's foreign secretary, described it as part of "a reckless but familiar pattern of behaviour" from the Chinese state. A consensus has emerged among Western governments that the Hafnium group and its counterparts have affiliations with the Chinese Ministry of State Security, which they say uses arms-length hacker organisations as proxy forces. China denies any involvement.

The immediate, unified response of Western allies to the Microsoft Exchange breach gave a signal as to the breadth and depth of the attack, which intelligence officials said was more serious than anything they had witnessed before.

Its scale was said to outstrip the recent SolarWinds campaign, suspected of being undertaken by the Russian authorities against US federal government targets last year. That had led to ramped-up sanctions on Vladimir Putin and the Russian Federation, but so far there has been little practical response to this latest incursion, save for a large amount of sabre-rattling: Nato's General Secretary Jens Stoltenberg even warned that cyber attacks against member states could lead to land, sea or air responses from the military alliance and a triggering of the Article 5 common security pact (only ever invoked once – by the US after September 11).

"People often try and segment this as a separate cyber security issue," says Chris Painter, an associate fellow at Chatham House and former senior cyber official working at the FBI, US Department of Justice, White House National Security Council and State Department. "The way I look at it is not that we have a cyber problem with China, we have a larger geopolitical issue with China... [and] cyber is part of that larger geopolitical fabric."

When Donald Trump became president in 2016, US attitudes towards China's seemingly inexorable rise hardened aggressively. Trade barriers were erected between the great power rivals after Trump's Republicans made an appeal to working-class voters in deindustrialised Rust Belt states a key part of their election platforms. China's unfair, mercantilist trade practices, including industrial subsidies, domestic preference, and maintenance of an artificially cheap currency were cited as primary factors behind the decline of US manufacturing. "China's entrance into the World Trade Organisation," ▸

◂ said Trump, "has enabled the greatest job theft in the history of our country."

Open rivalry with the People's Republic has continued into the Biden era, with anti-China tariffs maintained, and a multi-trillion-dollar spending package brought to Congress aimed partly at restoring US competitiveness in industry and infrastructure, countering China's economic might. The last two administrations have done away with a bipartisan policy of "strategic engagement" that had held since President Nixon's 1972 meeting with Mao. Biden's Democrats are pursuing a policy of government intervention and protectionism that edges the US's liberalised Anglo-Saxon economy just a little closer to something resembling China's own statist system, but nevertheless aimed at decoupling itself from the rising power by reshoring industry and bolstering domestic supply chains.

The recent deal between the two countries at the Cop26 summit provided a rare glimmer of bilateral cooperation. As the two biggest emitters of greenhouse gases, both agreed to ramp up efforts to reduce coal consumption, introduce methane targets and protect forests. Prior to that, observers had cast doubt on the ability of the two superpowers to set aside their differences at the conference.

Despite this unexpected success story, cyber is just one field of many where the two global hegemons now stand in a tense face-off.

"Given the tensions with the US," says Painter, it's "not surprising" that China is engaging in malicious cyber activity. Relations have deteriorated so far, he says, that they now have "no incentive to rein themselves in".

Xi's People's Republic, against the predictions of many, has abandoned his reforming predecessor Deng Xiaoping's foreign policy doctrine, which favoured "keeping a low profile and biding your time". Instead, a stance of aggressive "wolf warrior diplomacy" has been adopted, pursuing open competition, including propaganda and information warfare with the West. But is China the only aggressor in cyberspace?

"I work on the principle that both sides do it," Martin Jacques, author of the acclaimed book *When China Rules the World*, tells *Spotlight*. "The Western media is ridiculous. It presents these things as totally one-sided – as if China is at it and the West isn't, which is complete nonsense. The United States has an extremely bad record of such spying and espionage. Look at the [Edward] Snowden revelations – they were listening in on everyone, including Western leaders."

Indeed Snowden, the National Security Agency (NSA) contractor turned whistleblower, who leaked large amounts of classified material on the espionage activities of the NSA in 2013, found the US had spied on 35 world leaders, many of them Nato allies, including the German Chancellor Angela Merkel. His disclosures also revealed specific instances of cyber espionage targeting China, with servers at telecoms equipment giant Huawei hacked along with two of the country's largest mobile networks.

But for Painter, the Chinese approach stands out as "particularly egregious". "There are rules a country should play by... To talk about Hafnium's Microsoft Exchange hack, many people say it's just espionage," he says, "but... it was carried out in a very haphazard and grossly negligent manner that left a lot of victims exposed to other criminal activities like ransomware... This wasn't just the theft of trade secrets, the stealing of information (which is bad enough), it actually opened people up to further abuse by non-state actors."

Lack of regard for intellectual property is another area where Chinese cyber activity stands out as exceptional, Painter claims. He had a hand in negotiating a 2015 agreement between the US and China, which the then president Barack Obama declared would mean an immediate end to "cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage".

Clearly, the Microsoft Exchange hack breaks that agreement. "It's not that we haven't seen malicious Chinese activity in the past," Painter tells *Spotlight*. "For many years [before the 2015 deal] we had theft of intellectual property on a grand scale."

"This is all about the rise of China and the growing influence of the US in the region," says Jacques. "The real problem for the United States isn't [the threat of Chinese hackers], it's that it has been losing economic influence and presence in the most rapidly growing and largest economic region in the world." As late as 1986, the US was the largest trading partner of all ten member states of the Association of Southeast Asian Nations (Asean), the regional economic bloc, as well as of South Korea and Japan. In that same year, the US's GDP was 15 times larger than that of China's. Today, Japan, South Korea and all ten Asean nations count China as their largest trading partner, and, measured by purchasing power parity, China's economy is now larger than the US's.

It is that rate of growth, says Jacques, and the relative decline of Western influence, which has prompted the formation of new military alliances like Aukus – between the US, UK and Australia – along with Britain's defence tilt towards the Indo-Pacific.

Britain's latest integrated review of defence and foreign policy promised a modernisation of its military and an "embrace of the newer domains of cyber and space". It warned of a new era of "China's increasing international assertiveness" and "systemic competition" between "democratic and authoritarian values and systems of government". We've moved a long way from the days when David Cameron and George Osborne posed for photos with Xi Jinping and Manchester City's star footballers, sipping pints of real ale in country pubs and declaring a "golden era" of relations, with the UK "cemented" as "China's best partner in the West".

Cyber incursions, along with disputes over Hong Kong, the South China Sea, and treatment of the Uighur minority in Xinjiang, can now be added to the long list of Western grievances against a rising China that refuses to act how the UK had once hoped. ●

All ten Asean nations count China as their largest trading partner

SHUTTERSTOCK / STUDIO.51

The big online safety debate

Can a new bill protect people from harm while defending free speech?

By Sarah Dawood

Take a short scroll through Twitter or Facebook and you're bombarded with information. In just five minutes you can view, comment on and share the latest headlines, political opinions, cultural trends and celebrity mishaps. Social media has democratised information dissemination to such an extent that half of UK adults now get their news from these networks.

Cyber utopians would argue that the internet's unbridled freedom has helped us build a more equal society. But in giving everyone a voice, social media has also increased the spread of vitriol, misinformation and illegal material. A third of people are thought to have been exposed to online abuse, while false information about the Covid-19 vaccine has become a major public health issue.

What is the Online Safety Bill?

There is an obvious need to rethink the regulation of online communication. The government published the Draft Online Safety Bill in May this year, which aims to safeguard young people and ▸

◂ clamp down on online abuse while protecting freedom of speech. It is currently undergoing pre-legislative scrutiny by a joint committee, which will report its recommendations by 10 December.

It places a "duty of care" on social media websites, search engines and other websites where users interact to protect people from dangerous content. If they fail to do so, companies face fines of up to £18m or 10 per cent of their annual turnover, plus access to their sites being blocked.

Companies will be grouped into either Category One or Category Two, with the first including social media giants and being subject to harsher rules – they will be expected to tackle both illegal content, such as terrorist propaganda and child abuse, and "legal but harmful" content, such as misinformation and cyberbullying. Adherence will be overseen by the regulator, Ofcom.

A Department for Digital, Culture, Media and Sport spokesperson said it is "committed to introducing the bill as soon as possible" following the joint committee's report. Minister for Tech and Digital Economy, Chris Philp, told *Spotlight* the proposed online safety laws are "the most ambitious in the internet age... No other country has published a bill that will go so far to make 'big tech' accountable for the content on their platforms, and for the way they promote it."

Does the bill go far enough?

The bill is controversial with both safety advocates and freedom of speech campaigners, with the former saying the legislation does not do enough and the latter saying it goes too far.

Many worry that the "duty of care" approach coupled with the "legality" of some online harms mean that individuals face little retribution. The Law Commission recently made recommendations around reforming criminal law in this area, asking for offences to be based on "likely psychological harm", with perpetrators facing up to two years in prison. Digital Secretary Nadine Dorries has said that she intends to accept some of the suggestions, such as an offence for the most serious threats.

Lindsay McGlone, a 23-year-old body positivity campaigner, regularly faces online abuse. These tend to be derogatory comments about her appearance but also include pornographic images and a running commentary about her on gossip forum Tattle Life. She says the comments have affected her mental health and that abusers should be punished. "I've always faced discrimination but online abuse can be the worst because there are so few repercussions. People forget or don't seem to care that there's an actual person behind the screen."

Some campaigners believe that board directors and company owners whose platforms fall foul of the new laws should face more than fines. Richard Pursey, CEO of the safety tech company SafeToNet, notes that "the idea that board directors should be disqualified or even imprisoned if they do not follow their duty of care has been mooted. One of the biggest motivators of humankind is self-interest – policymakers should bear that in mind."

Over a third of 8-11-year-olds own a smartphone and nearly a fifth have a social

95%

of 16-24-year-olds have a social media profile

1 in 5

10-15-year-olds in England and Wales experienced online bullying in 2019 and 2020

Legal but harmful

Safety campaigners such as Pursey argue that the "wishy-washy" definition of "legal but harmful" will make it easier for the robust big tech legal teams to avoid fines. Roughly one in five 10–15-year-olds in England and Wales experienced online bullying in 2019 and 2020.

"It's an absolute tragedy that the bill doesn't mention bullying," says Pursey. "It needs a much clearer definition of what is and isn't acceptable – such as, if you wouldn't say it to someone's face, you shouldn't say it via a screen."

Helen Margetts, a professor at the Oxford Internet Institute and director of the public policy programme at The Alan Turing Institute, agrees that some "legal" abuse is indeed very harmful, such as misogyny. "If it's harmful, we need to think about why it isn't illegal," she says. "I'm a believer in the internet but I'm also a believer in democracy – and I

SHUTTERSTOCK / ZAITSAVA OLGA

media profile

think the kind of unbridled free speech that we have seen online is a threat to democracy."

She adds that the bill should be more nuanced in how it assesses online safety. Researchers at Cambridge University found that people with lower levels of numerical literacy are more likely to believe Covid-19 misinformation – but the same will not necessarily apply to those who commit hate crimes. "We tend to treat these things like a lump," she says. "They all have different targets, actors and remedies."

Free speech as fundamental freedom

Opposing critics argue that the "legal but harmful" concept will lead to censorship, causing platforms to over-delete as a precaution.

Ruth Smeeth, a former Labour MP and now CEO of free speech organisation Index on Censorship, is a victim of regular misogynistic and racist abuse, and has received death threats. She worries that the bill gives too much power to tech companies, will make it harder to scrutinise those in power and will stop researchers from assessing cultural change – for example, analysing extremist language to prevent future terrorist acts.

"There is a difference between feeling offended and feeling threatened and vulnerable," she says. "In this country, British parliament determines our laws – it should decide whether speech is illegal. It shouldn't be outsourced to anybody else."

Deleting abuse impacts victims, she adds, as individuals will be unaware they are in danger and it can make it harder for police to prosecute. She also worries that vulnerable people, such as rape victims and political dissidents, will not be able to speak openly because it could be flagged as inappropriate content – evidence of war crimes in Syria, for example, has reportedly been removed from YouTube due to it violating the platform's policies.

Her proposed solution is a "digital evidence locker" – an archive that could be accessed by the police, civil society and journalists, alongside designated online safe spaces for people to talk about their experiences. She also thinks greater transparency over social media's algorithms and content moderation would help identify discrimination, such as when TikTok, for instance, was accused of censoring disabled people's content last year to appear more "aspirational".

Confusion over categories

Tech advocacy groups are concerned that the bill's categorisation is vague and some smaller businesses could face the harshest restrictions. Camilla de Coverly Veale, head of regulation at the Coalition for a Digital Economy (Coadec), a trade body for start-ups, says that tech companies seek clarity and are worried about being pushed into Category One by lobbying campaigns, where they would not be able to cope with rigorous reporting requirements and possible huge fines. This could hamper innovation and competition because they will avoid user-to-user functionality, add age gates to their products or pivot to less risky areas such as financial tech.

"It feels like the government is regulating as if the internet is five companies," she says. "We worry that the perception of harm will become very politicised."

But Pursey of SafeToNet says that children's safety must come before business interests. "Paedophiles often build trust with children, encourage them to leave Instagram and move onto lesser-known platforms to isolate them," he says. "I don't see the logic in only going after the big guys – the law should also apply to small businesses."

The wonderful thing about the internet is its ability to give everyone a voice. But this brave new world of unrestrained viewing, sharing and commenting is inevitably causing trauma, be it psychological or physical. While freedom of speech is a cornerstone of any democracy, the online world should be treated the same way as the real one, with an ongoing conversation around culturally appropriate language – or we risk prioritising libertarianism over people's health. ●

"If you wouldn't say it to someone's face, you shouldn't say it via a screen"

View from the opposition

Why we need to improve our national cyber security strategy

Many areas of the government's policy have been found wanting

By Conor McGinn MP

Cyberspace has been a key frontier of Britain's national security challenge for some years now. Costly and debilitating attacks from hostile state and non-state actors are at their highest-ever levels, and continue to grow in scope and sophistication.

In March 2021, four in ten businesses, plus a quarter of charities, reported having cyber security breaches or attacks in the previous 12 months, with many causing lasting damage. This malign activity brings a financial cost to the UK of some £27bn every year. And by jeopardising the increasingly digital means by which people go about their lives, it carries a heavy social price too.

As our personal and social dependence on online systems and smart technology deepens within our homes, cities, businesses and lifestyles, the imperative for a robust cyber policy becomes ever more urgent.

But despite the efforts of UK law enforcement, our intelligence and security services, plus those working in cyber resilience, ministers have left us exposed. Their failures have seen Britain fall behind the curve compared to our international partners – and, crucially, those who wish us harm.

Not enough is being done to target the organised criminals and cyber terrorists who often work transnationally to maximise their devastation. In many cases, they function like large corporations, backed by sophisticated teams of developers, coders and hackers with the latest tech. In their pursuit of maximum gain and disruption, these criminals rarely discriminate between public and private sectors – all of society stands at risk.

Nowhere is this felt more acutely than in the rising threat posed by ransomware, of which there were some 305 million incidences globally in 2020. Lindy Cameron – head of the UK's National Cyber Security Centre (and interviewed on page 10 of this issue) – has said that this digital blackmail poses the "most immediate danger" to our country, with GCHQ disclosing that the number of these attacks on British institutions has doubled in the past year.

The government is yet to get serious about this. There was no specific strategy on tackling ransomware in the Beating Crime Plan, nor anything of substance on shutting down those who cynically employ these tactics at home and abroad.

Government has left us exposed to cyber attacks, says the shadow security minister

SHUTTERSTOCK / MAKSIM SHMELJOV

These threats don't just emanate from organised crime. Hostile states increasingly see cyber as a front line, a grey zone, in conflict. More than half of all cyber attacks are reported to now come from Russia. Iran and North Korea are emboldening their capabilities. Chinese state-sponsored agents attacked Microsoft earlier this year, affecting 30,000 organisations globally. And the Russian-backed SolarWinds compromise in 2020 was estimated to be the worst-ever cyber espionage attack on the US government with several departments hit.

For our foes, cyber has become a means by which to target critical infrastructure, peddle falsehoods in our democracy, and wreak havoc in our communities. This activity is becoming more overt and reckless. Yet, instead of instigating tougher responses, ministers are reticent to bolster our systems.

It beggars belief, for example, that over a year since the damning report on Russia by the Intelligence and Security Committee (ISC), ministers are yet to implement any of its recommendations. It contradicts the Integrated Review's aim to make the UK a world-leading cyber power.

The long-delayed Online Safety Bill (explored on page 19) is also ineffective. It could see cybercriminals let off the hook. The government must swiftly address its flaws to better protect the public – for example, by introducing criminal sanctions for bosses of the "big tech" companies that do nothing to stop scammers and fraudsters freely operating on their platforms.

Together, these failings reveal this administration's inability to take strategising, planning and the meeting of targets seriously. A 2019 report from the National Audit Office on the latest cyber security strategy – now five years old – confirmed this. It concluded that the strategy had "inadequate baselines for allocating resources, deciding on priorities or measuring progress effectively".

The government also shows scant regard for cyber security in practice. Whether ministers are conducting official business via WhatsApp, or using personal email accounts, leaving sensitive data exposed, their failure to attend to the most basic rules of online security is telling.

Reports that ministers are set to outsource the storage and protection of classified data held by the security and intelligence agencies to Amazon raises further serious questions. For a deal with this scale of impact on national security and cost to the taxpayer, it is vital that there be proper scrutiny. We cannot trust ministers' private assurances given their record on wasteful projects.

Keeping the country and the public safe is Labour's top priority. This means working to strengthen our resilience in cyberspace, together with those across society who use and rely upon it.

With local authorities, the NHS, engineering firms, tech companies and schools all in the line of fire, the need for a more joined-up, whole-of-systems cyber resilience strategy is clear.

This requires input from the private sector, institutions, researchers and academia. It means improving the recruitment and retention of the UK's best cyber specialists – a task the government is failing on.

It also means improving cultural awareness of cybercrime and the processes by which hostile cyber activity is reported, monitored and understood. This crime is prevalent, but it is seriously under-reported, with a lack of clarity on who to turn to for UK organisations. The Conservatives have let cybercrime become a cost of doing business – Labour will not.

Finally, we need to ensure our laws are fit for the challenges of today and the future. The Computer Misuse Act, which remains in use, is 30 years old. It was created before most of us could even get online. Reviewing our legislative tools against cybercriminals must be given greater priority.

As we await the next national cyber security strategy, Labour is clear that we need to get ahead of the dangers of cyber threats. If ministers cannot, they will be putting the public, and the country, further at risk. ●

Conor McGinn is the shadow security minister

Cyber security is a team game

Collaboration is the key to innovation, but too often geopolitics gets in the way

By Jeremy Thompson

In association with HUAWEI

The growing sophistication of the cybercriminals who prey on digital vulnerability presents a real threat to all of us. Only by working together can we stop them.

You only need to be aware of what's happening on the dark web to see that cybercriminals are getting better and better at what they do and that they're starting to collaborate. That's why the cyber security industry needs collaboration too. From users, operators, builders, designers and vendors to installers and everyone else, input across all these links in the chain is critical. Security by design has to be a team game.

There is a role for everyone in cyber security, from the initial design of new software through to each end user at home. The pandemic has highlighted just how important the end user is in ensuring strong cyber security in their homes and businesses; attacks take place on multiple levels and are no longer purely technical. However, they're not the only players. There's a role for every participant in the supply chain, and different parts of the chain see different risks and can make different contributions. We are all responsible for getting technology safely and securely into everyone's hands.

Security is all about collaboration

If we go back to basics, the phrase "security by design" is often used in the industry when we talk about product creation. In order to fulfil this principle, software designers need to have full visibility on what threats are out there and understand how they work. The only way to achieve this is through collaboration across the supply chain. Working in isolation will only result in incorrect or missing information.

Our products are the perfect example of the benefits that working across all these links can bring. We're just one part of the chain. Huawei doesn't run networks – we provide technology in the networks. It's a small part that's integrated with many other parts.

We make the biggest strides forward when all the industry's stakeholders work together collaboratively to come up with a set of standards that helps the whole industry. Common standards create economies of scale that everyone benefits from. It means the industry can constantly pool innovation. If cyber

innovation is left to one organisation we'll all be weaker as a result.

Take the unit price of a 4G handset as an example. In many cases you can buy one for less than $50. That low cost would be inconceivable if you had five or six different sets of standards across the world because you wouldn't get the benefits from those economies of scale. It took several generations of having separate wireless standards in different regions before we arrived at a global, universal standard with 3G wireless. The improvements in the telecommunications industry are vast. The security for 4G is better than 3G, and 5G is substantially better than 4G. That's a result of working together and identifying where the weaknesses are, fixing those, then trying to anticipate new threats.

But geopolitics can too often get in the way of collaboration. Putting politics over technology results in the fragmentation of standards – and that's a huge step backwards. If we all end up having different technology for different places, that would take us back 20 to 30 years.

Innovation should not be political

We need to maintain trust, and this means we need to have a voice and a conversation based on innovation and on investment in research and development (R&D) – without letting politics get in the way.

5G technology involves having billions of devices connected to masts. It's the key facilitator for the Internet of Things, which will boom in the coming years. The connected devices will be varied, from monitors that keep a track of what's in your fridge, what the temperature is outside, and what your heart rate is, right through to electric and autonomous vehicles, and wide applications in industry and high-value manufacturing.

It's not as simple as just smartphones any more – it's multiple devices. Securing those devices in a consistent way is vital. Government is an extremely important stakeholder in all of this, and you can give the UK government credit for pre-empting threats by setting standards for security for the Internet of Things. These standards mean that if someone in Asia is creating a device for the UK market then they know how they should build those devices. That's

SHUTTERSTOCK / RAWPIXEL.COM

Working on problems and solutions together makes the most of our strengths

hugely helpful, not least for the manufacturers, but also for end users, who have an assured level of security.

In 5G that's even more relevant for business-to-business applications, so the private sector can start relying more on sensors and data from connected devices when it comes to things like just-in-time logistics and production, smart manufacturing, and anything reliant on big data. Different sectors can have high levels of confidence because of a guarantee of this base level of security. In turn that will result in greater adoption, and scope for further investment and innovation. It creates a virtuous circle of improvement rather than having seeds of mistrust in the industry. It isn't good for the economy at large if we're blocked from getting the benefits of new technology.

Huawei is an equipment manufacturer. We make hardware. What we're great at is innovation – which is why we invest so heavily in R&D. Last year, our R&D spend was $22bn, comparable to the entire UK government's target of £22bn per year. It's a huge amount that's going towards developing products that are secure by design. We work with others in the industry to create a high set of security standards and a security ecosystem, so our key contribution is some of the basic innovation and R&D that will create patents and technologies to support customers. Our contribution to common standards is that basic R&D, which is then enhanced with specific initiatives for customers.

Our key message is that this is a team game. It's end users, operators, governments, vendors, standards bodies and more, and it's the relationship between them that makes a secure environment. We're at risk of losing all the benefits of innovation if we start fragmenting based on country of origin and on political machinations. Technology and innovation should be above that. ●

Jeremy Thompson is executive vice president at Huawei UK

People are the first line of defence

Vigilance is a necessity in today's digital climate

By Julia Lopez MP

The past 18 months have sped up the adoption of new technology to a pace we've never seen before. Video calls have replaced phone calls, we're using new apps and software to help us work, learn and socialise, and shopping online has become a regular habit for many.

Technology has also transformed the way we do business. I've seen first-hand how cutting-edge firms are using technology to improve the way they do things, not just in allowing staff to work from home but also to serve their customers more efficiently and in a smarter way – whether it's a popular restaurant using a food delivery app or a local butchers processing orders online.

Although technology brings great benefits, we must pay even more attention to the cyber security that protects the data flowing around our digital infrastructure. Data released in March this year highlighted that two in five businesses and a quarter of charities reported cyber security breaches over the previous 12 months. Where a breach has resulted in a loss of data or assets, the average cost of a cyber attack on a business is £8,460 – rising to £13,400 for medium and large businesses.

Criminals have always attempted to con people by capitalising on what's in the news or on people's minds. Recently, we've seen scams related to the Euros football tournament, cryptocurrencies and even summer holidays.

Individuals and businesses need to make sure they have the digital skills to operate in this rapidly changing world. As well as being able to use technology, it's crucial we know how to do so securely, to protect our money and data.

As a parent I know the importance of helping young people get the digital skills they need to be safe online. It's why the government has made sure the school curriculum provides important basic knowledge in areas such as digital literacy and online safety, which help children avoid harmful content, protect their privacy and recognise misinformation and disinformation.

Likewise, the government's popular CyberFirst programme aims to help 11 to 17-year-olds develop online safety skills and encourages them to pursue a career in cyber security. Improving the digital skills of young people not only provides the building blocks for good, secure digital citizenship, but also sets out a pathway for future careers in exciting, well-paid areas such as artificial intelligence and software engineering.

Digital business is booming; according to Growth Intelligence, 85,000 businesses launched online stores or joined online marketplaces in the four months from April 2020 alone. The government's Cyber Aware campaign encourages people and small businesses to improve their cyber security by taking a few important actions, such as setting stronger passwords and switching on two-factor authentication. We're also working with

The government's CyberFirst programme teaches 11 to 17-year-olds how to be safe online

the banking and finance sector on a national campaign to tackle fraud called Take Five, which offers people advice to prevent online and phone scams.

Improving the nation's digital know-how is important but can only take us so far; we are working hard to stop online fraudsters. Last year, the government's National Cyber Security Centre (NCSC) launched a Suspicious Email Reporting Service (Sers) allowing the public to flag suspected scams. Anyone can play their part by simply forwarding suspicious emails to report@phishing.gov.uk, and the experts will step into action. Sers has now received more than 7.7 million reports, helping the NCSC remove more than 64,000 scams and 119,000 malicious websites up to the end of September 2021.

There has also been a surge in ransomware over the past year. These lock an organisation's IT systems, putting them out of use until a ransom payment is made. But there is help at hand and the government has produced advice for firms – an excellent first step is to follow this guidance and back up critical business data. Businesses with no defences make easy targets, so I urge bosses and security teams to act.

For company owners and managers, knowing how to protect your business is crucial. The government's Cyber Essentials scheme offers small and medium-sized businesses (SMEs) a cost-effective way to get basic measures in place to prevent most cyber attacks.

Employees can help too. The government's free, easy-to-use online training package for staff explains the importance of cyber security, how to defend against email phishing attacks and how to secure devices at work. There's even a Board Toolkit to help management ensure they protect their most valuable digital assets.

It's crucial that we know how to use tech securely

Securing prosperity and competitiveness in the digital age is at the heart of the Integrated Review of Security, Defence, Development and Foreign Policy, and we want to secure our status as a science and tech superpower by 2030.

The UK's cyber industry is one of this country's success stories and is helping us achieve that goal, with investors looking to capitalise on our skills, ingenuity and business environment. Despite the pandemic, it attracted record investment last year and is now worth an estimated £8.9bn. UK businesses such as Darktrace, Clearswift and Sophos are helping protect companies at home and abroad.

While our entrepreneurs in this space surge ahead, everyone needs to have essential cyber skills. Let's all take steps to protect ourselves online so we can seize the opportunities technology brings and boost the UK's prosperity. ●

Julia Lopez is Minister for Media, Data and Digital Infrastructure at the Department for Digital, Culture, Media and Sport

SHUTTERSTOCK / INSTAPHOTOS

Advertorial

A brave new world of cybercrime

Fake vaccine passports are one of the latest traps being used by email scammers

By Paul Anderson

In association with FORTINET

Offers of fake vaccine passports are being used

As the world navigates post-pandemic life, cybercriminals are continuing to evolve and shift their priorities and targets. At the start of the pandemic, it was remote work, then as the world has reopened, attacks against the supply chain and operations environments became more disruptive, plus ransomware evolved as the most prolific threat. In fact, according to *The 2021 Ransomware Survey Report* by Fortinet, more than two-thirds of organisations have been the target of at least one ransomware attack this year. So, the question is: what's next?

Targeting vaccine passports

The next phase of the battle against Covid-19 includes proof of vaccination. Because of this, opportunistic cybercriminals have begun selling

to entice people into opening malicious email attachments

SHUTTERSTOCK / WHYFRAME

counterfeit vaccine passports on the black market. While this is not necessarily new, unlike other criminal activities, this strategy is going mainstream. FortiGuard Labs, Fortinet's threat intelligence platform and research organisation, has begun to encounter offers of fake vaccine passports as lures in email scams. Successfully enticing the general population to open a malicious email attachment with the promise of receiving an illegal product may be a first. It reflects how polarising the issue of proof of vaccination is and why cybercriminals think that they can successfully exploit it.

FortiGuard Labs has also found various markets on the dark web offering fake vaccine passports. As expected, a wide range of products and services are available, from blank vaccine cards to verifiable passports that can be checked against legitimate vaccine databases worldwide.

It's a prime example of criminals who are taking advantage of the current opportunities through these broad spam and phishing campaigns to not only target the general public but professionals as well. Cybercriminals are not only requesting bitcoin payments and personally identifiable information (PII) but are also using official-looking email communications from government organisations to trick people into believing their legitimacy. Demand for fake vaccine passports is growing due to the large population of unvaccinated people who want to avoid restrictions. Without missing a beat, email scammers and black-market criminals have acted on this demand.

The importance of training

Because these criminals are using phishing techniques to socially engineer and lure victims into a trap, it's vital to address these challenges. These attackers have shown immense agility to pivot to the latest vulnerability, therefore training employees must also be as agile and proactive.

Organisations need to conduct ongoing training designed to educate and inform personnel about the latest phishing and spear phishing – phishing that is targeted at specific individuals or groups within an organisation – techniques and how to spot and respond to them. This should include encouraging employees to never open attachments from someone they don't know and always treat emails from unrecognised/untrusted senders with caution. Fortinet has recently pledged to train one million people and offers free cyber security training and certification to customers, partners and employees.

Since many phishing and spear phishing attacks are being delivered as part of social engineering distribution mechanisms, end users within an organisation must also be made aware of the various types of attacks currently in use. This can be accomplished through regular training sessions and impromptu tests using predetermined templates originating from an organisation's internal security department. Simple user awareness training on how to spot emails with malicious attachments or links can also help prevent initial access into the network.

Businesses must also look to a secure email gateway with advanced detection and response technologies as an effective way to fight against these attacks.

The threat landscape is constantly evolving and the rate of change has only accelerated now that the world is reopening. Attackers are looking towards the path of least resistance and capitalising on divisiveness to exploit money from individuals and potentially larger businesses. With the right training and education platforms alongside effective solutions, businesses can be confident that their workers don't fall prey to the latest threats and scams. ●

Paul Anderson is director, UK and Ireland at Fortinet

When the internet goes dark

How states are weaponising digital shutdowns to stifle dissent

By Samir Jeraj

Kashmir during a recent internet shutdown

The shutdown began for journalist Shams Irfan on 16 October 2019. Irfan lives in Pampore, a town known for growing saffron and being near to Srinagar, the traditional summer capital of the Indian-administered territory of Jammu and Kashmir, which is part of the wider Kashmir region. A few days before, there had been a gun battle between Kashmiri rebels and Indian security forces in which two rebels died, he says. "As it is a norm now, if there is a gunfight in any area, the first thing that is shut is the internet." Usually, service is fully restored in around three days, but this time that did not happen.

"I started noticing a pattern; it was not shut randomly," Irfan continues. The internet was down from 7.30am to 11am and then from 2.30pm to 10.30pm. He believes it is a "proper curtailment plan". During earlier internet shutdowns there was usually a reason given by the authorities, he says, but this current pattern has left even journalists like him "clueless". "What I came to know is that the same pattern is followed in many other areas across Kashmir," he says.

YAWAR NAZIR / STRINGER / GETTY IMAGES

As of October this year, there have been 317 internet shutdowns in Kashmir since 2012, part of 548 across India in the same period, contributing to a collapse in media freedoms. Governments are increasingly turning to internet shutdowns to control the spread of information often connected to political instability. The estimated cost to the global economy was $8bn in 2019.

Shutdowns are also becoming more sophisticated and targeted. "No longer does a regime have to plunge a whole nation into darkness – it can lock onto a certain group of people it determines as a threat and disconnect them from each other and the rest of the world," says Felicia Anthonio, a campaigner at Access Now, a digital rights NGO.

Access Now is also tracking a rise in the length of internet shutdowns. In the Tigray region of Ethiopia, where there is a separatist conflict, there has been an internet shutdown since 4 November 2020. This has made it more difficult for journalists and human rights activists to document war crimes or for ordinary people to carry on their lives.

"You see this increasing confidence [of] countries with recurring internet shutdowns and it seems to reflect the complex geopolitical situation," says Iginio Gagliardone, associate professor in Media and Communication at the University of the Witwatersrand, South Africa. In the 1990s and early 2000s, he explains, there was more of a sense that infringing on internet freedom would risk some form of sanction from the international community. However, by 2005 Ethiopia could claim its two-year shutdown of SMS texting services was due to "technical problems".

There are several ways that governments can block internet use, explains Hanna Kreitem, technical expert, Middle East at the Internet Society, a global non-profit organisation working to promote an open, globally connected and secure internet. From limiting access speed, particular services and websites in places as small as a few streets or an organisation, through to a full blackout across a country, as happened in Egypt in 2011, these techniques have been in use for "many, many years", according to Kreitem, and are a continuation of pre-internet restrictions to information.

"Nowadays we are seeing more targeted shutdowns," he continues, limiting services in specific regions – for example, preventing protesters in an area live-streaming on Facebook. This is enabled, he says, both by the willingness and acceptability of using blackouts and by advancements in technology, such as deep packet inspection (DPI), that allow specific websites to be blocked.

"Internet service providers have no choice," Gagliardone explains. Some of them are only notified of a shutdown by a call direct to the CEO, and while most do push back by asking for an official order, governments can mobilise national security laws in particular to make it happen or else the providers will lose their licence to operate. "There is very little room for negotiation," he adds.

But there are ways to counter internet shutdowns. Access Now believes that awareness-raising is important along with monitoring and understanding the impact on human rights. The group has also used strategic litigation to challenge government decisions to impose shutdowns in Zambia, Togo, Indonesia and Sudan.

"Circumvention tools are catching up with many of the techniques that are used to limit access," says Kreitem, but there is still no tool that can protect against a full blackout. VSAT (very small aperture terminal) data transmission technologies might be able to do this, but are quite expensive and still quite limited, so are only going to be used by the general public. Kreitem hopes that, at some point, decision-makers will realise that cutting off the internet is an ineffective tool and focus on better ways to solve their problems.

Back in Kashmir, Irfan has adjusted to the new normal. The regular shutdowns have disrupted his work routine and access to information, so he changed his sleep pattern and regularly takes shuttles to areas such as Srinagar city, where there is a better chance of internet access, to read emails, send a single WhatsApp message or just to find out what is happening elsewhere.

"We now live in a world where the internet has ceased to be a luxury but a necessity for everyone, be it a journalist or a small trader or a shop owner or a student," Irfan says. "But such shutdowns during peak working hours are pushing us back to the dark ages."


Kaspersky
Total Security
hackers HATE:
when we join forces
against them
We're a community of 400 million people looking out for each other, backed by 4,000 professionals, making life hard for hackers and shifting the balance to the good guys. It's no surprise hackers hate Kaspersky Total Security.
Learn more at: kas.pr/hackers-hate
kaspersky
BRING ON
THE FUTURE