NewStatesman

Spotlight

CYBER SECURITY: THE NEW FRONT LINE

Michael Fallon / Garry Kasparov / Louise Haigh / Ciaran Martin

Special report: Is the NHS prepared for the next WannaCry?

KEEP YOUR ENEMIES CLOSE BUT YOUR FRIENDS EVEN CLOSER

Insider threats are a **challenge for every organisation** but the answer to the problem is in your own hands.

There are simple techniques you can adopt, or you can use something more complex and far-reaching.

We can help you start from scratch - develop your insider threat strategy and introduce you to a variety of innovative technologies to review - or we can help plug a specific gap in your protection plan.

It's up to you...

The insider threat technologies and training recommended by our R&D team include:

- Email protection
- Privilege management
- Digital rights management
- Behavioural analytics and behavioural management
- Advanced malware protection

Give our security team a call today on 01296 621121 to get the conversation rolling.

Avatu – infosecurity advisors to inspiring companies

avatu

www.avatu.co.uk

The emperor's new birthday cards

Two stories from the past month help to illustrate the nature of the internet's disinformation problem. The first was an investigation by the *New York Times* into a Russian company with strong links to the Kremlin that created hundreds of Facebook pages to re-post and promote comments, pictures and videos that supported the Trump campaign in advance of last year's presidential election.

What was significant about this "cultural hacking", as it was described by one expert, was that the content was all generated by real Americans. The Russian pages did not make up their own "fake news", and in most cases barely edited the content they re-posted. They were paying customers of Facebook, playing by Facebook's rules. In fact, noted the *Times*, the divisive memes and the fake stories they promoted were "precisely the kind of engaging content these platforms are hungry for". It is difficult to see how Facebook can really prevent this, because it is for precisely this activity – finding things out about people, and paying to deliver a message to the right ones – that Facebook is built.

For people who find this worrying, the second story should help. The Russian president, Vladimir Putin, received thousands of birthday wishes from an ostensibly adoring public this month, but a BBC investigation revealed that almost all of the accounts retweeting and adding their best wishes were "bots" – fake, automated users. It is rather comforting to consider that in the bizarre attention economy of the internet, even the man thought to be its most powerful malefactor is reduced to doing the same thing those rather desperate people who buy Twitter followers or Facebook likes are doing – paying a machine to pretend to like him.

4 / Michael Fallon
The Defence Secretary on readying for global cyber attacks

6 / Ben Wallace
The Security Minister on cyber cooperation with business

8 / Ciaran Martin & Ian Levy
The NCSC's first year

16 / NHS attack
What's been done to prevent another WannaCry?

24 / Garry Kasparov
The chess grandmaster on AI

30 / National Crime Agency
Convicting cyber criminals

34 / Lord Callanan
Preventing cyber attacks at sea

40 / Louise Haigh MP
Why cyber education is crucial

48 / Prosecuting hackers
Young cybercriminals face very serious punishments

NewStatesman
71-73 Carter Lane
London EC4V 5EQ
Subscription inquiries:
sbrasher@
newstatesman.co.uk
0800 731 8496

Commercial Director
Peter Coombs
+44 (0)20 3096 2268

Special Projects Editor
Will Dunn

Special Projects Writers
Rohan Banerjee
Augusta Riddy

Design and Production
Leon Parks

Cover illustration
Sam Falconer

The paper in this magazine originates from timber that 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.

First published as a supplement to the *New Statesman* of 20 October 2017. Registered as a newspaper in the UK and US.

This supplement and other policy reports can be downloaded from the NS website at: newstatesman.com/page/supplements

The Secretary of State for Defence Michael Fallon explains how the UK is shoring up its defences, and working with other nations to meet the defence challenges of the digital age

The UK is prepared for the international cyber threat

In the past three years as Defence Secretary, I've been confronted by a swathe of complex challenges. Yet whether the danger comes from state aggressors, rogue states or non-state actors, it's striking how often cyber is now their weapon of choice. And there's a very good reason we now regard cyber as a Tier One threat – up there with natural disasters and terror. Virtual attacks have real consequences. We've seen Daesh using online tools to recruit followers and spread murderous propaganda. We've seen Russia using an army of social media bots to steadily drip-feed fake news and disinformation to the West, poisoning public trust. And North Korea's fingerprints appear to be on numerous high-profile cyber strikes.

This year alone Parliament has been hacked and the WannaCry virus has shut down NHS operating theatres, as well as affecting more than 200,000 people worldwide. The consequences for the military are equally significant; it has been claimed Russia used malware to track and target Ukrainian artillery which illustrates how cyber can directly impair military capability. While big set-piece attacks are devastating, lower-level activity is costing business billions, undermining democracy and putting us all at risk.

In recent years we've seen our cyber adversaries multiply, attracted by the anonymous and ambiguous nature of the medium. It's no longer the usual suspects; now any loner with a laptop and a grudge can cause chaos. That's why the UK is taking action. We're investing £1.9bn to strengthen our cyber security capability. This month we marked the first anniversary of the National Cyber Security Centre – bringing together some

SHUTTERSTOCK/FLIK47

of the best cyber security brains from across government and the country. In the past year it has responded to nearly 600 significant incidents requiring a national, coordinated response. Defence is at the forefront of our response which incorporates three key elements.

Firstly, it's about creating better resilience. We're making sure our latest fifth-generation kit, from F35 to future frigates, Ajax Armoured Vehicles to drones, is packed with information sensors that can gather millions of bytes of data per second, to detect cyber intrusions and respond appropriately. We've also set up the Defence Cyber Partnership Programme ensuring companies with whom we've placed defence contracts are properly protected and meeting a host of security standards.

Secondly, we're recruiting the best and brightest cyber talent. We've got cyber reservists from industry and academia putting their high-tech skills at the service of the nation by weeding out network vulnerabilities. We're also building up a new 21st century Cyber Corps. This team of expert volunteers and captains of industry will advise us how to generate the disruptive capability needed, in everything from big data to autonomy, to keep us ahead in the cyber space race. Cyber is now a core part of our military training. In a few months' time we will open a dedicated state-of-the-art Defence Cyber School at Shrivenham, bringing together all of our military joint cyber training into one place.

But, as RAF Second World War hero Air Vice-Marshal 'Johnnie' Johnson once remarked: "The only proper defence is offence." Knowing we have the ability to expose cyber attacks and respond, whether in the air, on land, at sea, or in the cyber sphere, will deter our adversaries. Equally, offensive cyber capability gives us the means to maintain our battlefield advantage, delivering more targeted effects, limiting civilian casualties and protecting our own people.

And thirdly, we're making offensive cyber an essential part of our arsenal, to use it where appropriate and governed by our commitment to international law. Our National Offensive Cyber Programme allows us to integrate cyber into all our military operations, and is being used with great effectiveness to degrade Daesh, not only in Iraq but in Syria too. And we're not just investing in kit capable of soaking up a wealth of data, but running a multimillion-pound competition to develop machine learning algorithms and artificial intelligence too – freeing up our personnel to provide a more co-ordinated and tailored response.

When it comes to cyber deterrence we stand stronger when we stand together, so we're also working with our allies to develop our collective cyber response. At last year's Warsaw summit, NATO recognised cyber as a distinctive domain of operations for the first time. Allied nations signed the cyber pledge, committing to enhance their national defences and strengthen their collective capability to resist attack. Simultaneously we need to continue to develop the ability to provide a proportionate response to cyber attacks against NATO allies. Having honed our own innovative national cyber techniques, we've become one of the first NATO members to publicly offer offensive cyber support to Alliance operations as and when required.

In 1933 Churchill declared: "Air power may either end war or end civilisation", knowing air power could be used for good or ill. He made the right choice and in the dark decade that followed, our planes helped liberate our nation and transform our lives for the better. Now, in this new cyber age, we too are determined to make the right choices – boosting our cyber power to make our nation safer and the world more secure.

Investing in a secure future

Increased training and investment in cyber security infrastructure are essential in the digital age, explains Ben Wallace MP, Minister of State for Security

It is easy to underestimate how crucial the internet is to our everyday lives. It has become an essential tool in the way we communicate with others and conduct business both at home and abroad. More than 1.6m people work in the digital sector or in digital tech roles in the United Kingdom and the internet continues to provide individuals and businesses with huge opportunities.

However, we know that criminals seek to exploit the many benefits of the internet for their own personal gain, often at great expense to others. The WannaCry ransomware attack, which hit the NHS as well as other organisations, highlights the seriousness of the threat and reinforces the need to properly protect ourselves online.

In the recent Cyber Security Breaches Survey 2017, just under half (46 per cent) of all businesses identified at least one breach or attack in the last year. Although it is difficult to put an exact figure on how much this cost the UK economy, it is likely to be in the billions.

We are also all too aware of attacks by hostile state actors who look to exploit the UK through intellectual property theft, in order to further their own interests and prosperity. We take these attempts to disrupt our national security very seriously.

That is why this the government set up the National Cyber Security Centre (NCSC), which provides cyber security at a national level. In its first year of being operational, the NCSC responded to 590 significant cyber incidents, more than 30 of which were sufficiently serious to require a cross-government response.

It is not just large organisations and our national infrastructure that are targeted by online criminals; individuals also face the daily threat of being scammed in their own homes. It is now the case that British citizens are 20 times more likely to be defrauded at their computer than mugged in the street.

It is a threat we all face. I strongly believe that we – individuals, businesses and the government – must play our own part to mitigate the risk and ensure that the internet is a safe and secure space for everyone.

The government has legislated within the Serious Crime Act 2015 to create a new offence that applies where an

The NCSC acts as a bridge between industry and government

SHUTTERSTOCK/PCRUCIATTI

unauthorised act in relation to a computer results in serious damage to the economy, the environment, national security or human welfare, or a risk of such damage occurring.

Legislating against online criminality goes some way to tackling the problem; however, close collaboration between the government, business and international partners is essential in combating the increasingly sophisticated attacks that the UK faces.

We work closely with the NCSC, which acts as a bridge between industry and government, providing a unified source of advice and the management of cyber-related incidents. It is at the heart of the government's 2016 National Cyber Security Strategy, which is supported by £1.9bn of transformational investment to 2021.

Our law enforcement agencies across England and Wales also play a vital role in disrupting the activities of cyber criminals and bringing them to justice. They now operate as a single networked resource with the National Crime Agency (NCA) and Regional Cyber Crime Units using shared intelligence and capabilities. The NCA also has a dedicated Dark Web Intelligence Unit which targets those criminals who exploit hidden areas of the internet.

But we also want people to take their own preventative measures, so that they don't become a target by criminals operating in the cyber space. We are running a series of campaigns and programmes which aim to encourage individuals and businesses to adopt more secure online behaviours.

Cyber Aware works with over 320 public and private sector partner organisations to encourage us all to take simple steps to protect ourselves online including using a strong, separate password for our email accounts and installing the latest software and app updates on our electronic devices.

The NCSC has also recently launched expert guidance on how small businesses can easily avoid common online breaches and attacks. Should organisations seek to improve their cyber security further, they can get certification through the Cyber Essentials Scheme.

To further support the efforts of SMEs in improving their cyber security, regional cyber crime prevention coordinators engage with businesses and members of the public to provide customised cyber security advice based on the latest technical guidance from the NCSC.

We must also look to the future – we now have a whole generation that have grown up immersed in tech. It is hugely important that we harness their talents and put them to good use rather than letting them wander down a path towards criminal online activities.

We must train and engage with the next generation of cyber security experts and is why the NCSC is taking a leading role in promoting a culture where science and technology subjects can flourish within the education system. Their CyberFirst programme identifies and nurtures young talent through a series of summer workshops and competitions. In addition, their CyberUK 2018 programme focuses on encouraging more women to enter into the technology industry, a sector that is largely seen as male-dominated.

There is a great effort across Government and law enforcement to pursue online criminals, prevent those that are headed on a path towards criminal activity, protect the public and prepare for the many threats we face online. We will continue to invest in law enforcement capabilities at a national, regional and local level to ensure agencies have the capacity to deal with the increasing threat from cyber crime.

However, this is not a threat that we can tackle alone. It is everybody's responsibility, from top to bottom, to follow the guidance provided and increase their awareness of cyber security in order to create a safe space to communicate and conduct business online.

The National Cyber Security Centre's chief executive Ciaran Martin and technical director Ian Levy talk to Rohan Banerjee about demystifying the digital landscape and how best to manage risk

"Hollywood hasn't done us any favours"

For a long time, the term "cyber security" might have been mistaken as a motif of science fiction, but now, according to Ciaran Martin, it occupies a "crucial and relevant space across government, business and industry". It is fitting, then, that GCHQ decided to commit to the establishment of the National Cyber Security Centre – a subsidiary tasked with limiting and countering the threats posed, as Martin puts it, "by the simple reality that the whole world is getting more digital." He explains: "There are now more devices connected to the internet than there are people and with the growth of our dependence on technology comes an increased risk. We need to get away from the idea that cyber security is a mystical, impossible subject, and improve the understanding around it. Hollywood hasn't done us any favours."

In stark contrast to the GCHQ base in Cheltenham – which is the size of Wembley Stadium, patrolled by armed guards and with barbed wire fences around its perimeter – the NCSC headquarters in London is decidedly less conspicuous. Located a stone's throw from Victoria Station, two floors of a glass-walled office building, house some of the United Kingdom's foremost cyber security experts. To the average passer-by, it probably looks like countless other glass-walled office buildings. This, Martin says, is a suitable quirk of concept. "Cyber security is an issue for individuals and organisations alike. I think as people start to realise cyber risks in ways that are directly relevant to them – maybe a compromised database of a thousand people here or a couple of hundred pounds defrauded there – then they will see that it's not something that you can afford to overlook. These are everyday crimes, everyday problems."

In the first year of its operation, the NCSC has logged 1,131 incident reports with around 600 being classed as

NATIONAL CYBER SECURITY CENTRE

"Everyday crimes, everyday problems"

"significant". Are there any patterns or common themes in the vulnerabilities exposed by these breaches? Martin says: "I suppose what we've learnt is that cyber security represents both a high-end issue of national security – there are indeed adversarial state-level actors – and a potential to do immediate economic harm. The commonality that we've seen is that most attacks are facilitated by a very basic level of exploitation. You can have attacks that are of low sophistication but have a potentially high impact. This could be down to outdated software, human error or a poor monitoring of network data." What constitutes as a significant attack? "Sometimes the identity of the attacker alone is enough to class it as significant – particularly if it's a hostile state actor – and sometimes the identity of the attacker can be irrelevant but the breach's potential to impact the wider public can be huge."

In May, the NCSC faced one such significant attack – the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding payments in Bitcoin. The attack began on Friday 12th May and within a day was reported to have infected more than 230,000 computers in 150 countries, including those in 47 NHS trusts. The NCSC worked with NHS England's emergency response teams, the Department of Health, NHS Digital and NHS Improvement to coordinate actions. Martin says: "The NCSC reacted quickly to offer victim support and advice on the day of the attack, updating our own ransomware guidance. Experts from the NCSC were deployed to Barts Hospital Trust and we continue today to work and support government departments in identifying vulnerabilities and what data matters and should be backed up."

The NCSC, its technical director Ian Levy points out, is not an exclusively reactive operation. "We're not waiting for attacks to happen; we are creating dynamic solutions to prevent as many as possible from getting through in the first place." In addition to leading the UK response to the WannaCry incident, the NCSC has created a website to provide easy to understand advice and information to the public. It has hosted 2,300 delegates and 173 speakers at the CyberUK conference in Liverpool; seen a 42 per cent increase in visits (4,000 per month) to the Cyber Security Information Sharing Partnership (CiSP); produced 200,000 physical items for 190 customer departments through the UK Key Production Authority, securing and protecting vital communications for, amongst others, the armed forces; and helped nurture the next generation of cyber experts by enrolling more than 1,000 young people in CyberFirst courses.

Levy sent shockwaves across the tech sector at Symantec's Crystal Ball event in September, when he suggested that a more serious incident than WannaCry was "inevitable" but insists that the

"People can't remember a 600-digit number"

comment wasn't defeatist, simply realistic. "I stand by it. Unless we do something differently, the investigations will say it was an unprecedented attack and two guys will get blamed for it because they're charged with doing an impossible amount of security on their own. The NCSC is trying to make a difference by designing systems so that people can use them better."

User-friendliness, Levy argues, represents the bedrock of improved cyber security. "Passwords are my favourite example. If you use a different password for every system, service or account, you're told to make it complicated and change it often. Weigh up the average number of accounts and passwords and it roughly translates to saying that you need to remember a different 600-digit number every month. People can't do that so they build coping strategies, like using the same password for everything or storing them on a text file on the desktop. Those coping mechanisms show that we've got the design of our systems wrong." So, how do we make them better? "Firstly, let's put into perspective that your email account is different. It's the key to your kingdom. Whenever you get a password reset for something, where does it go? It's the source. Let's protect that better and use a password manager to help people understand. In the long run, though, you want different sorts of authentication. The NCSC wants you to be able to log on without a password, using commodity technologies. It could be your Apple pay, your Fitbit or whatever, so you don't have to worry about always remembering a hundred-odd passwords."

Jeremy Fleming, the head of GCHQ, wrote in an op-ed for the *Daily Telegraph* recently that the NCSC has helped the intelligence organisation to "come out of the shadows". What's it like being the public-facing wing of a traditionally secretive entity? While Martin stresses that all sensitive information remains protected by a need-to-know basis – and some very thick walls – he comments that the NCSC is "enjoying letting people

know what they need to know, too. We're trying to make a positive difference by empowering people through knowledge."

When the Prime Minister called a snap general election earlier this year, he adds, it was important to brief all stakeholders on the potential cyber risks involved. "When we did the election protection work, what was fantastic is that we were able to get hundreds of people from political parties, local government and the like to come in. We developed electoral software and had service providers in a room downstairs. While we weren't going to talk about the classified basis of our knowledge, we showed them the threat as we saw it and the easy things they could do to deal with it. We were able to get that rolled out within days."

The same Jeremy Fleming op-ed also addresses one of cyber security's hot

potatoes: encryption. "Hostile states, terrorists and criminals," the former deputy director-general of MI5 warned, "use those same features – instant connectivity and encrypted communications – to undermine our national security, attack our interests and, increasingly, commit crime." Does the NCSC support the idea of inserting "backdoors" into encrypted messaging platforms to enhance surveillance of suspicious actors? "We need to get away from this language about backdoors. The Investigatory Powers Act is clear about lawful access to data in strictly controlled circumstances. We are in favour of strong encryption for all and no one in UK government wants to weaken that encryption. But it is a fact that encrypted services are abused by certain groups, including terrorists and those who commit serious crimes. The government doesn't want unfettered access but we do need to ensure that the service providers can give targeted exceptional access to law enforcement."

It's vital that regulation isn't seen as "punitive"

One of the biggest problems in UK cyber security is attackers spoofing the government to send fake emails. Domain-based Message Authentication, Reporting and Conformance protocol, better known as DMARC, helps to verify whether the communications come from the said sender. Levy explains: "The concept is pretty simple. The most common way to expose victims' systems is to attack is through email spoofing and spear-phishing [where emails are tailored to increase the chance of the recipient clicking on a malicious link]. So we have built the 'Mail Check' service that monitors the adoption of the standard and provides data on trends. DMARC has already stopped a lot of potential attacks, for example blocking at least 120,000 emails from a spoof '@gov.uk' address. Authentication markers that the sender can't control – big ticks and big crosses – those are how you can make it clear what's to be trusted."

Ultimately, reflecting on one year of the NCSC, both Martin and Levy agree that awareness must be at the heart of any cyber security strategy. It's vital that regulation isn't viewed as "punitive", Levy says, but rather as a way of "getting people and businesses to do the right thing by default. We don't want to disadvantage the SMEs. You have to address those different company types in different ways. Our small business guide presents five simple steps as an infographic. We want to be able to present cyber security in a way that it can be consumed easily and by the right audience." Cyber security, Martin reiterates, can no longer be viewed as an issue for a company's IT department alone. The breaches at Equifax, Yahoo and TalkTalk, he says, have caused lasting reputational damage, well beyond the initial loss of data. Should every person and every company, then, be doing more to improve their cyber security? "Absolutely."

No, cyber security is not just a problem for IT!

Assessing, transitioning and refining cyber security strategy has become core to any business, writes **William Brennan**, UK/Europe director of global cyber defence at Leidos

The pace, breadth and impact of threats in the cyber domain continue to accelerate. Global ramifications from cyber incidents have been felt early and often in 2017. A group known as the "Shadow Brokers" released tools that disrupted businesses and impacted markets. Their actions led to a major disruption at the UK National Health Service from the Wannacry outbreak. A month later, Petya ransomware affected industries from pharmaceuticals (Merck) to transport (Maersk) through to oil and gas (Russian energy giant Rosneft). In early September, Equifax announced a major data breach which potentially affected the personally identifiable information (PII) of more than 143m people.

Cyber threats, however, did not stop with businesses. National elections in France were reportedly impacted by a massive data disclosure days before voters went to the polls. In the United States, 198m voter records were found on an unsecured cloud server. Alarmingly, these massive cyber attacks are occurring with greater frequency. In response, it is imperative for all organisations to assess their cyber posture and risk tolerance.

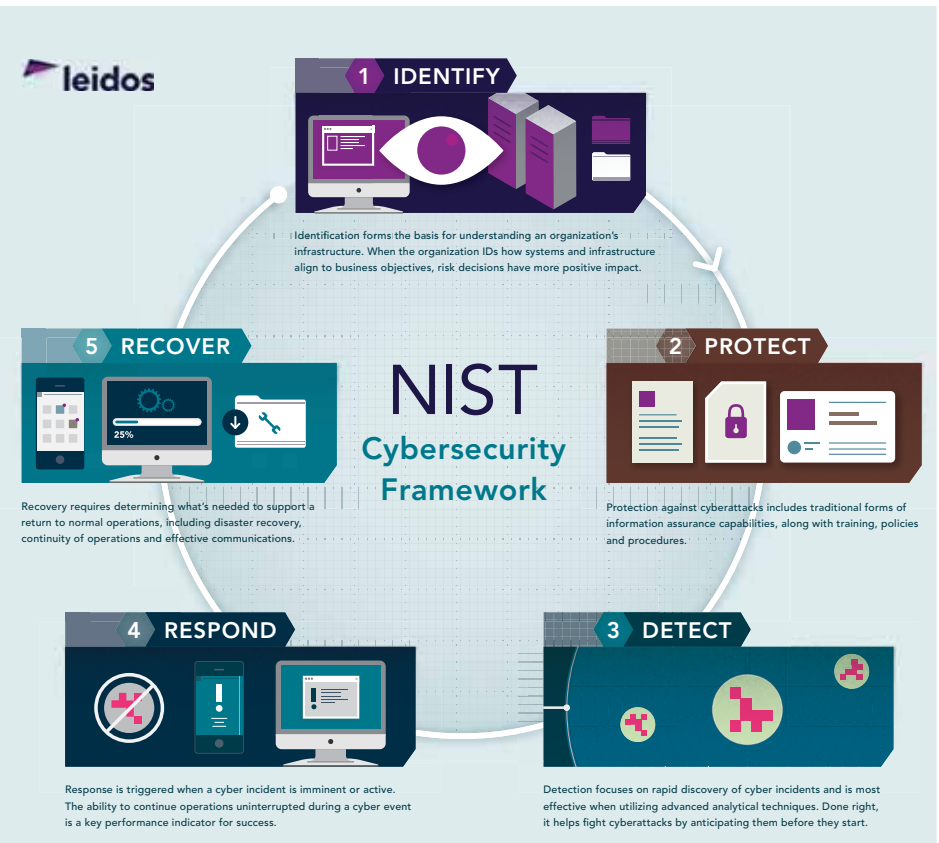
These action steps can be summarised as the practice of good "cyber hygiene", i.e. doing the basics of information assurance and cyber defence well. This includes patching systems that are known to be vulnerable, securing data wherever it resides, and ensuring that networks are actively monitored. When the basics are executed well, companies can focus on defending their organisations from more advanced cyber threats.

Nations around the world are coming to grips with the potential impacts of cyber attacks on their critical national infrastructure. Disruption to citizen services, or worse, has become an issue of national sovereignty. This has led countries to create their own versions of cyber hygiene best practices to guide and advise organisations on how to enhance their resiliency.

In the US, this guidance is best summarised in the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF). The RMF was released in 2014 in response to an executive order. The framework provides cyber risk management guidance to US critical national infrastructure providers. The framework is built around five core functions that, when used in concert, provide the best ability to manage cyber risk. These are offered not as a checklist or an exercise in compliance, but as a set of best practices divided by categories for implementation.

When fully implemented, the framework provides an understanding of residual cyber risk, which can then optimise organisational investments in people, process and/or technology to continually reduce risk, and increase resiliency and defensive agility. With RMF gaining worldwide acceptance, organisations without an extensive

LEIDOS



cybersecurity posture can turn to practitioner partners and service providers such as Leidos for implementation guidance and support.

In the UK, the National Cyber Security Centre (NCSC) provides excellent guidance to the public, government and commercial organisations alike. The NCSC's "10 steps to cyber security" summarises the key elements of good cyber hygiene that, if adopted, can lead to enhanced cyber resiliency. The guidance encourages organisations to understand risk tolerance and coordinate cyber investments appropriately. This NCSC investment provides the framework from which policies can be created, cyber intelligence acquired, and defensive actions taken.

In Australia, meanwhile, the Australian Signals Directorate (ASD) published what they call the "Essential Eight." These encompass the ASD-recommended core strategies to mitigate cyber incidents. While the ASD's key elements of cyber hygiene have significant overlap with strategies from the U.S. and UK, they have taken it a step further. The Australian Government provides a complementary maturity model to allow businesses to assess their implementation of the Essential Eight. Essentially, understanding where an organisation is in its transformation becomes another key element to risk management.

Regardless of the framework, guidance or combination of recommendations an organisation adopts, increasing cyber defence is becoming a core business necessity. At Leidos, we have more than 30 years of experience in transforming and improving the cyber resiliency of our customers across three key areas: assessment, transition and refinement.

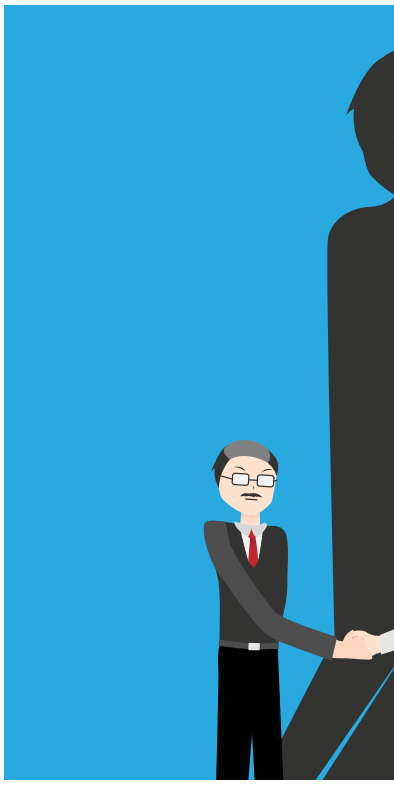
First, an organisation must assess its current cyber defence capability to identify, respond and adapt to cyber risk. It must prioritise key information assets, understand the threats against those assets and align security investments accordingly. Those investments must create resiliency within the technology architecture to adapt to cyber threats not previously conceived. Many enterprises have too many non-aligned security technologies and poor policies supporting their cyber defences. Understanding what you have and where mitigation efforts need to be taken is essential in building a better security posture.

Second, organisations must transition to make cyber hygiene and security integral parts of an organisation's culture. Today's advanced attacks exploit weaknesses in enterprise cyber defences to penetrate enterprise networks, obtain administrative control and accomplish their mission. The increasing need for constant connectivity with vendors, partners, and customers – and future Internet-connected devices on personal, corporate, medical, and industrial networks – will only make this problem worse. A culture of cyber hygiene has to be created in the organisation so that people can identify potential breaches and poor practices in the workplace. Organisations need to ensure the basics are right before considering anything more advanced.

Finally, cyber defence is not something done once. Instead, it is ongoing and requires continual investment in skills, organisational focus and refinement. This is achieved by building an internal team to perform operational activities, or by engaging a partner to help build resilient solutions or even take over these operations directly. Using a partner can insulate an organisation from the challenge of finding skilled cyber professionals. Regardless of the approach, an organisation needs to adjust processes to continually manage risk and use intelligence to inform their decisions.

For more information, please visit: www.leidos.com/uk

Keep your enemies close and your friends closer



The reality of human frailties means you shouldn't rely on anyone completely, says **Joe Jouhal**, CEO at Avatu

If Theresa May knows anything, she knows it's beneficial to keep her enemies close but her "friends" closer. Since the snap election in June, her main threat hasn't come from Jeremy Corbyn or the Labour Party. Her biggest risk has been closer to home. She's known for a long time if Boris Johnson – and others from the cabinet or the backbenches – were to turn renegade, her authority would soon fade away.

When it comes to the security of an organisation, it is imperative you protect yourself from your potential enemies on the outside who might try to attack you, lock up your files or steal your valuable data. However, your biggest assets are also your biggest risk: your employees, your contractors, your partners. In every organisation, absolutely every organisation, people can change their allegiance; loyal people can make mistakes or try to cut corners.

Indeed, according to the Verizon Data Breach Incident report, 90 per cent of security incidents are caused by insiders. And of these, 29 per cent are done deliberately by people with malicious intent but 71 per cent are from mistakes, where humans have simply cocked up or have been manipulated.

But even if there's no big bad monster – no Edward Snowden with *WikiLeaks* on speed dial waiting to share your secrets; no disgruntled employee ready to give your customers' sensitive data to the highest bidder on the Dark Web, or share your IP with your biggest competitor, you will have people within your organisations that make mistakes. Because you employ humans you will have people who are tempted to click on phishing links, containing malware or ransomware, that infect your systems and disrupt your business.

You will have people who fall for the ploy of opening attachments identified as overdue "invoices" that the boss has asked them to pay. Those that intend

SHUTTERSTOCK/GRITSALAK KARALAK

IN ASSOCIATION WITH

avatu

to do you harm are using social engineering techniques to take advantage of people's natural instincts.

You will have people who try to do things outside of policy or protocol and send out unprotected sensitive data to other people, or to the wrong people (to the wrong John Smith for example). You will have people who put your security at risk, and not because they are rogue or self-serving, but just misguided or misinformed.

The savviest of leaders and security professionals, however, employ technology to compensate for the frailties of the humans they have working for them. If you take your business seriously – and we assume you do because you're reading this – you have to take insider threats seriously and invest appropriately too.

Your enemies may be plotting against you but your friends are the ones who will inadvertently help them or just make genuine mistakes. A healthy dose of scepticism and some innovative technologies could just save you from your friends' good intentions, and from yourself.

Six places where technology can make up for malicious intent and human frailties

1. It deals with email attachments properly – Email can be a real headache for security teams. It's a constant source of malware dressed up in a way that insiders let in. It is easy, however, with innovative technology to plug this whole area – and still have access to legitimate documents in a way you can use them properly (where you can keep Excel or Word files, for example, as Excel and Word files, and you don't need to turn them into unworkable PDFs).

2. It only gives people access to the information they need for their job – It seems simple but you'd be surprised how many organisations still allow too much access to too many people. Simple technology can sort this out and seriously limit your insider risk.

3. It protects data at source – If you protect your IP or other files at source with special software, you can pull the plug remotely if it gets stolen or shared by mistake and it will no longer be accessible to anyone that's not authorised to see it.

4. It reinforces security training – Security training is essential for all organisations, but like most training, as soon people leave the training room it starts to be forgotten, unless it becomes everyday practice. Technology can remind people what they should be doing and continues to educate them if they err from the safe path you've set.

5. It can monitor what people are doing – Even trustworthy employees, vendors and consultants need to be monitored to make sure they don't unintentionally – or on purpose – do things that will harm your business. Technology can alert employees in real time of potentially harmful actions and policy violations, and change their behaviour. It can alert security and IT teams of potentially harmful actions and it can maintain irrefutable logs and video recordings to support investigations.

6. It can introduce a robust last line of defence – We all know that traditional perimeter methods will only protect organisations and their information so far. When you are making up for the failings of your people, you can also make up for the failings of your perimeter defences with more sophisticated technology, which detected every threat thrown at it during the rigorous NSS Labs Breach Detection Systems test, without generating any false positives.

For more information, you can email: cybersecurity@avatu.co.uk or phone: 01296 621121

When WannaCry ransomware struck the NHS in May, the government pledged new targets and funding for the health service's IT systems. But will this shield hospitals from another strike? Oscar Williams asked NHS insiders and cyber security experts

Is the NHS prepared for future attacks, or is it a cyber sitting duck?

It was a Friday in May, and "Sam" – a senior administrator at a major English hospital trust – was preparing to leave for work. When she picked up her phone, she noticed that her inbox had ballooned: "I had all these concerned messages from people I didn't know."

The cause of the panic became clear when Sam arrived at the trust. "They had switched off the computer networks; you couldn't access any of the systems." She was called into a meeting with the hospital's senior management who declared a "business continuity incident". Like 39 other NHS trusts around the country, Sam's had been paralysed by WannaCry ransomware.

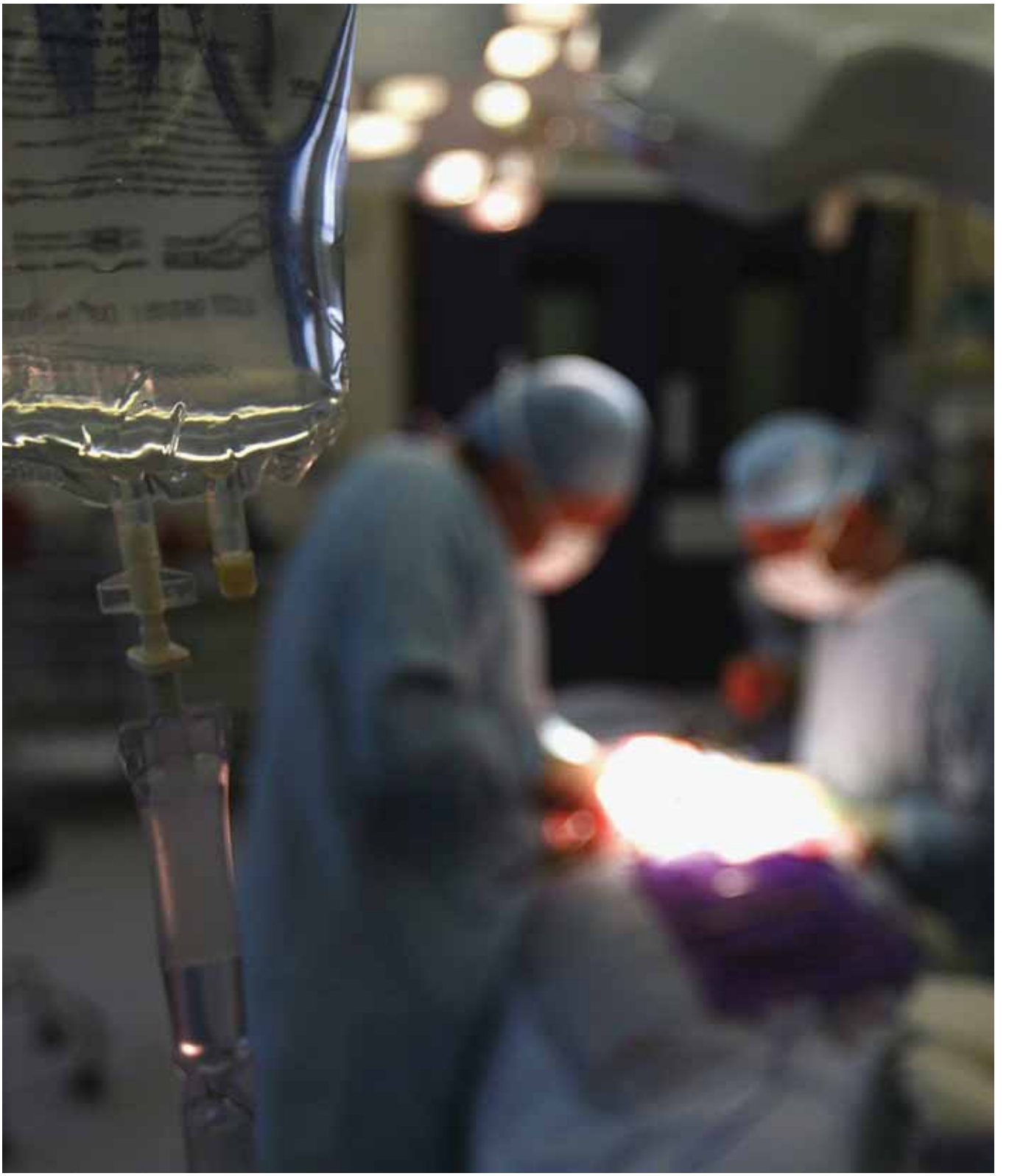
In the months following the attack, British and American intelligence officials traced the computer virus to hackers in North Korea. Their bug had spread indiscriminately through thousands of organisations' networks and was designed, most cyber security experts now believe, not to generate money, but simply to cause chaos.

"'Business continuity status' means everything has to go back to paper," says Sam, whose name has been changed to protect her identity. "We were already full so we had no beds and had to keep sketching the ward layouts. You suddenly realise how reliant you are on technology."

It was feared the NHS Mail system had been compromised and that confidential patient data would be leaked. Staff at Sam's trust were forced to abandon the platform. With no other system to share patient data electronically, her team took the decision to cancel all non-emergency and non-maternity appointments and operations for a week.

"I suppose you could say we could've gone ahead without access to the electronic systems, but it only takes it to go wrong for one person," Sam reflects. "I wasn't confident that patients weren't being put at risk. You don't want anyone going in for any sort of invasive treatment if the surgeon and anaesthetist haven't got the full story."

Between five and seven thousand patients in Sam's department alone are



CHRISTOPHER FURLONG / GETTY IMAGES

Over 200 trusts missed out on extra cyber funding

thought to have been affected during the course of that week. Around the country, tens of thousands more faced cancellations. "Because we had no way to communicate electronically and securely, you're risking cancer diagnosis," Sam explains. "You're risking delaying people's treatment, which can be fatal."

The tragic reality – as it later emerged – was that it was an unnecessary precaution.

Chris Flynn, the security lead for NHS Digital, told delegates at the UK Health Show last month that his organisation had failed to explain the limitations of the virus. "We didn't tell people specifically that NHS Mail was safe," he said. "We didn't say it wasn't, but we didn't say it was. And we know that people pulled connections."

The communication failure was one of several reasons the virus hit the health service so hard. While NHS Digital had issued a patch to fix the vulnerability in affected Windows software, a number of hospital trusts' IT teams had failed to implement it, leaving them exposed when WannaCry started spreading. It was only when then 22-year-old Marcus Hutchins, also known as Malware Tech, accidentally identified a kill-switch that the virus was contained.

In the wake of WannaCry, the government has pledged to spend £50m on improving cyber security and patient data in the NHS, which includes the creation of a £21m fund for the UK's 27 major trauma centres. NHS Digital has also recently started searching for a supplier of a new cyber security centre to improve the service it offers hospital trusts.

When the government announced the new funding in July, the health minister Lord O'Shaughnessy said: "The NHS has a long history of safeguarding confidential data, but with the growing threat of cyber-attacks including the WannaCry ransomware attack in May, this government has acted to protect information across the NHS.

"Only by leading cultural change and backing organisations to drive up security standards across the health and social care system can we build the resilience the NHS needs in the face of a global threat."

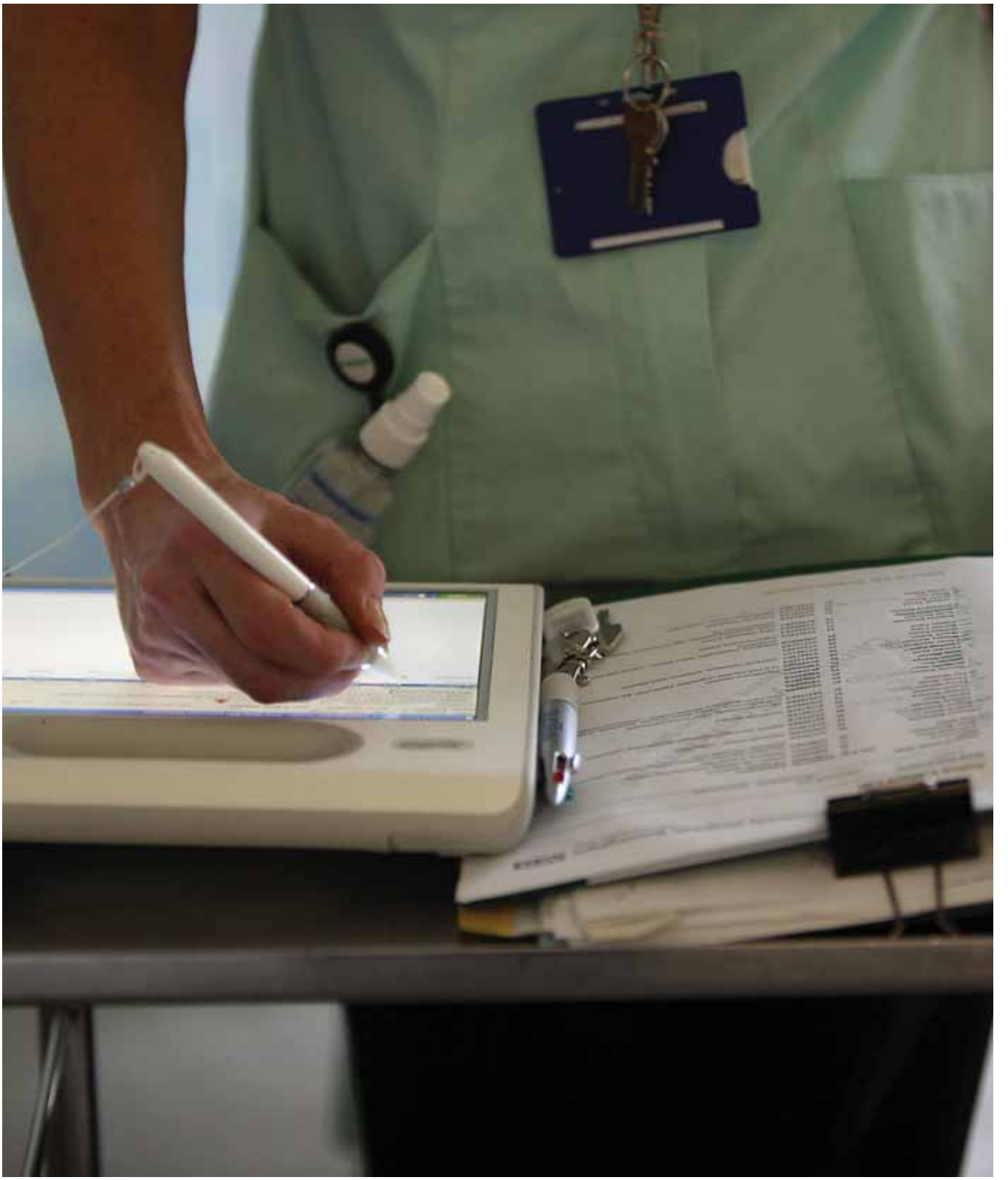
But while the additional funding was broadly welcomed, some experts have cast doubt on whether it will be enough to transform the cyber security of a distributed behemoth that has underfunded its IT provision for decades.

David Evans, the Chartered Institute for IT's policy director, questioned the logic in providing extra cyber security funding for major trauma centres, but not for the rest of the NHS's 240 trusts: "The additional funding will be welcomed by NHS CIOs at major trauma sites, but the rest will have to consider cuts to other areas of budgets to shore up cyber security."

Aside from the funding, the government has also set strict new targets for trusts. The headline requirement is that they must issue software patches for bugs within 48 hours of NHS Digital making them available. When the Network and Information Systems (NIS) Directive comes into force in May, critical service providers such as hospitals will also be liable to fines of up to 4 per cent of their annual turnover if they fall victim to attacks and fail to prove they have followed guidelines for good cyber hygiene.

Professor Alan Woodward, a cyber security researcher at the University of Surrey, describes the two-day deadline as a classic example of overzealous centralised management: "If you don't have the resources, it's like saying everyone needs to be seen in A&E within four hours. If you haven't got the clinicians, it doesn't help you. It just gives you a stick to beat people with, and all they do is they find a way of changing the targets."

Additional support for NHS Digital or the National Cyber Security Centre will not instantly solve the problem, argues Woodward. "If you look at what actually happened in WannaCry, the problem wasn't actually in the centre," he says. "NHS Digital had an update ready for this that would've stopped it. The problem was the lack of resources out in the individual trusts, so individual trusts either didn't have the people or the



CHRISTOPHER FURLONG / GETTY IMAGES

"The NHS isn't fiscally able to keep up with cyber threats"

people with the skills to actually roll this out in time."

NHS Digital's Dan Taylor says the organisation provides an advisory service to trusts: "We support providers by giving free data security assessments to identify their strengths and weaknesses, to help them understand the nature of the potential threats they face and the steps they need to take to enhance their preparedness. We also provide some consultancy services following these visits to help address any areas of concern."

It might be easy to update a computer at home, but it's significantly more difficult in a corporate environment, especially one as complicated as a hospital. "You have to make sure that you don't mess up all the other applications you have," explains Woodward. "Although it's called a National Health Service, there isn't a National Health Service IT. Every trust is different. They've got their own mix of applications and so every trust has to look and make sure they don't mess up their IT."

One of the solutions, Woodward says, is to be found in Scotland, where a number of trusts have already invested in technology that simplifies the rollout of software updates: "Rather than have a man in a van with a USB stick upgrading everything, they can do it laterally, they can send all of the updates out."

Evan and Woodward's concerns about funding are shared by the health service's IT leaders. In June, just weeks after the WannaCry virus struck, cloud computing provider VMware surveyed more than a hundred NHS IT decision-makers. Seventy per cent said the NHS was not allocating enough funding to cyber security. Over a quarter had been forced to cancel or postpone appointments due to cyber incidents, and nearly a third said they were certain that electronic patient data had been infiltrated by hackers.

Despite the government's plans for improving hospitals' cyber security, Sam isn't convinced that WannaCry will be the last strike to cause significant disruption in the health service: "I would like to say it will be, but I don't think we can reliably say that. Until we're in the situation where a critical service is properly resourced in every way it needs to be, in terms of people, infrastructure and estates, we're always going to be running at a risk. Technology moves so quickly and the NHS does not. It's too big and it's not in the fiscal situation to keep up."

DANIEL LEAL-OLIVAS / GETTYIMAGES

Now is not the time to let your guard down

All organisations, whether big or small, need to invest and train in order to keep pace with the evolution of cyber risks, explains Mark Lewis, director at Secure Thought Ltd

Since joining the Royal Air Force in the late 1980s as a telecommunications operator, my work life has been driven by the need for security. The main concept of military communication was based on compartmentalisation, security classification and data handling. Assurance was maintained by the formal nature of legacy military communication systems and the need for communications centres to transmit and receive information.

Fast-forward to early 2000s, and the IT community had just survived the biggest IT crisis the world has encountered to date, and everyone was motivated to looking for the next great thing. Defence mobilised to increase its capability in cyber security and cyber defence and it started the internal recruiting process. The main requirements for entry were: a strong understanding of security, a strong understanding of IT and a willingness to learn.

The one thing that wasn't acknowledged was that you needed to be prepared to change your life. Why? Because security is an all-encompassing and enthralling task, that will consume everything that you throw at it. Over the next six years, the investment in training, self-motivated education and the time needed to support your military commitments was unprecedented. If it wasn't for the support and motivation of all the team, I'm not sure any of us would have succeeded in setting the foundations for MOD cyber defence.

I retired after 22 years, spending the later period surrounded by the smartest people I have ever met and travelling the world working with our defence partners collaborating on "follow the sun" cyber defence capabilities and strategies.
At this point, I had the opportunity to collaborate with an emerging company called Computer Network Defence to support a security delivery for the MOD. I had secured my first consultancy role and my path was set. Over the next five years we spent time in the space industry supporting the security delivery for the Galileo Programme, working on a European-led programme that is set to deliver the future of GPS and meeting all the challenges of an EU-led programme. We are now supporting the delivery of the next generation emergency service network.

As a small business supplying security consultancy we mainly operate at the corporate level. To do this we need to push past the glass wall that exists around companies such as KPMG and Deloitte and the confidence that comes with their history and pedigree. Are we overachieving? I think we are, which is reflected in our vision statement that sets the agenda for the next three years.

We take our corporate customers on a journey through the cyber security landscape, ensuring that they meet the ever present and changing threat to their cyber beachheads.

I have often been told that we should stick with the small business end of the market, however we have never operated in this area. All our clients over the past 10 years have been large companies, where we operate at the mid to senior management level. In most cases we act as the facilitator to improve security strategy and communication between the senior managers and the board. We spend most of our time in this area demonstrating the need for an effective corporate operational picture as well as a effective security-focused operational picture. We are an effective company setting up for the cyber challenges of the future. We work with large organisations to ensure that they understand the over-the-horizon threat to their business operations.

IN ASSOCIATION WITH

SECURE Thought Ltd

A failure to manage risk is risky business

Cyber security affects companies' credibility and capacity to operate in the digital world, explains **Sam Jones**, project development executive at BGi.uk

Cyber crime is one of the biggest threats facing the world today. Yet in a constant stream of warnings and advice, we are still seeing a disjointed approach to mitigating and managing the risks businesses face through being connected to, and operating in, the digital world.

Research by Zurich stated half of SMEs will not invest more than £1,000 on cyber security. Whilst there is no silver bullet, if you suffer a cyber attack or failure it is evident that the more resilient you and your business are, the more likely you will survive the event. Cyber protection requires investment of financial and intellectual resources. This is risk management.

Data is at risk from thieves, hackers and, of course, it can be accidentally lost or damaged. What in your cyber world has a value to you or others? With the introduction of the General Data Protection Regulation (GDPR) the data you hold comes with a huge responsibility, and indeed, is a liability. You need to consider what is likely to be targeted, where the value is in your system and where you are vulnerable.

The data on your system will be composed of information on your staff and suppliers as well as the day-to-day details of your business operations. Not only must a business protect the systems where data is used and collected, but also backing up the data to secure servers should be a priority.

The ability to recover lost or damaged files is key to managing risk and increasing resilience. A market leading service such as Datto can restore data within hours and recovering your data expediently will enable you to carry on your activities and processes – more or less without interruption.

Of course, a data breach is just one of the threats facing businesses. Ransomware can block systems,

SHUTTERSTOCK/ZENZEN

IN ASSOCIATION WITH

denying access and interrupting trade. We all know the old adage that time is money and not only are profits hit but reputational damage can be long-lasting and hard work to repair.

Businesses have a responsibility to all stakeholders to act in a safe manner and secure systems and data accordingly. The increased connectivity on the internet-enabled world means malware can spread to suppliers and clients. A company's reputation, and value, can rapidly diminish from a poorly managed data breach through social media and 24-hour news reporting. Business will need to ask themselves if they have done all they can because if they have not then they have failed those trusting in their services.

Effective implementation of data protection regulations will help develop your cyber risk management strategy and protocols. While complying with regulation can seem an onerous and costly task, it can also be viewed as a good foundation toward improving your resilience to cyber misfortune. Encrypting data, appointing a Data Protection Officer and implementing a data breach monitoring process are all required for GDPR. These are good starting points. Efficient implementation should reduce your investment costs on compulsory compliance while enhancing your security credentials.

The human factor is often the weakest link in the chain but with the right training an improvement in individual online behaviour can dramatically reduce the chances of a security breach. Key to risk management is increasing awareness and education at every level of the organisation; particularly its management and directors as they invariably have access to most parts of the system, the greatest amount of information to lose – and the authority to break the rules. Cyber security is not just an IT department problem.

The recent data breach at Deloitte was described as a "sophisticated hack" when in reality it came through an account with administrative privileges protected by just one password. No two-step factor authentication, just someone's wedding anniversary or child's date of birth. If every employee is shown how to (and encouraged to) take care of "their bit" you will have a more secure environment.

If your security process and systems fail you will want to consider insurance. This does not and cannot provide a total solution to cyber risk but it is the support given after one has taken all reasonable risk management precautions to avoid or minimise the value of an incident. However, buying cyber insurance (like any other insurance) both frees up resources and removes the uncertainty that would otherwise prevail.

To ensure that any business can survive a cyber incident it is critical that the business has in place a continuity plan. An insurance policy will be an integral part of this plan, helping to ease the financial difficulty an incident can cause. If the business does not have the in-house resources to create a business continuity plan they should seek external assistance, and work with their broker or insurer.

While many insurers now provide management and risk management tools with a plethora of differing insurance contracts, the cyber policy, as a necessity, comes equipped with a team of experts who are able to assist with the policyholder's response to a cyber event. For example, the policy coverage can and does include assistance from forensic experts, IT specialists and a PR team to protect the company's ongoing reputation.

There is no one-size-fits-all approach to cyber risk management but common sense, clear and concise planning, continual training and testing, all backed by insurance, are key steps in being cyber resilient.

For more information, please visit: www.bgi.uk.com/cyber

The most successful chess player in history is now the chairman of the Human Rights Foundation, an outspoken critic of Vladimir Putin and a regular speaker on cyber security. Garry Kasparov tells Will Dunn why it's important that liberal democracies protect their freedom in the digital realm

"This is the new front line"

SHUTTERSTOCK/ALEX ALEKSEEV FLICKR/ACE KINDREDZEN LUCKY

Sometimes, before Garry Kasparov answers a question, he rests his elbows on the table in front of him, pinches the bridge of his nose, and very briefly closes his eyes. It is one of those attitudes – see also the hand clasping the forehead, and the chin resting on the bunched fist – that chess players adopt when they are searching for their next move, waiting for one of the hundreds of imagined possibilities behind their eyelids to present itself as the solution to the puzzle on the board.

When answering a journalist's questions he only needs to consider the answer for an instant. In 1996, when he played the IBM supercomputer Deep Blue, he sat like this for minutes at a time while the machine across the room analysed 200 million positions per second. Garry Kasparov was one of the first, and arguably the most brilliant, person to experience what an increasing number of people believe will happen to us all in the future: being outsmarted by a machine.

"Chess," he explains, "was viewed as potentially the ultimate test for a machine's intelligence from the dawn of computer science, by Alan Turing and Claude Shannon and Norbert Weiner." Kasparov first played against computers in the 1970s, but describes the machines in those days as "laughably weak". Even of Deep Thought, the precursor to Deep Blue that he faced in 1989, Kasparov says: "I won quite easily. It was primitive - but if you look back… machines were already making enough progress then for us to realise that it was basically a matter of time."

By the mid-90s, Moore's Law had held

"Humans make mistakes, even the best humans"

true for three decades. As in so many areas, the machines appeared to be little more than a novelty until, following the curve of exponential growth, their power became suddenly apparent. "The whole idea that if we had enough time, we would avoid making mistakes," says Kasparov, "was ignorant. Humans are poised to make mistakes, even the best humans. And the whole story of human-machine competition is that the machines - first it's impossible [that they could play], then the machines are laughably weak, then they are competing, for a brief time, and then, forever after, they are superior."

But the inevitability of the machines' success, says Kasparov, is not a matter of brute force, but of reliability. "Machines have a steady hand. It's not that machines can *solve* the game" – the number of possible moves is so high that, even calculating at 200 million moves per second, it would have taken Deep Blue longer than the life of its opponent, or the solar system or quite possibly the universe itself, to calculate them all – "it's about making moves that are of a higher average quality than humans." The machine, says Kasparov, need never fear losing its concentration because it can never feel fear and it has no concentration to lose. "It doesn't bother about making a mistake in the previous move. Humans are by definition emotional. Even the top experts, whether it be in chess, or video games, or science - we are prisoners of our emotions. That makes us easy prey for machines, in a closed system."

In 1997, Kasparov played his second match (he had won the first) against the IBM supercomputer Deep Blue and lost in the deciding game. He had been the World Champion since 1985, and would remain the world's highest-rated human player until his retirement in 2005. He found losing to a machine to be "a shocking experience," although this was partly, of course, because "I haven't lost many games… Now, two decades later, I realise it was a natural process."

But Kasparov does not think humans are about to be replaced entirely by machines. Even in cyber security, where automation and machine learning are necessary, "It's not a closed system, because there are no written rules. Actually, it's one of the areas where human-machine collaboration will have a decisive effect. I think it's naïve to assume that machines could be totally dominant, because the angle of attack can change. There are so many things that can change. It's an unlimited combination of patterns that can be manipulated."

He is optimistic about technological development because "I read history books, and I know that it's happened before. It's a cycle. New technology always destroys jobs and industries, before it creates new ones. So if we try to slow down AI development, it will still kill jobs, but it will slow down

"Each industry must feel the pressure of innovation"

the creation of new industries. It will prevent us from generating enough income to think about the people who have been left behind."

"We can learn from history that there were negative effects when automation killed millions of manufacturing jobs; 100 years ago, 30 per cent of the American population worked in agriculture. Now it's two per cent. The only difference is, that today, machines are going after people with degrees, political influence and Twitter accounts. So now it's a big story. But it's a natural process; each industry must feel the pressure of innovation."

For Kasparov, the need for governments to embrace technological change is more than simply an economic issue. As the chairman of the Human Rights Foundation he works with dissidents around the world to promote human rights and liberal democracy, and as a Russian he composes strategy against a singularly dangerous opponent: Vladimir Putin. The antidote to the Russian president's powerful campaigns of espionage and disinformation, he says, is a combination of computing power and human intuition.

"The fake news industry isn't about selling you a hard product. It's not about communism, or fascism. It's selling you doubt. That's why I call Putin a 'merchant of doubt'. Truth is relative; how can a machine operate in an environment where truth is relative? That's why, suddenly, we enter the stage where human leadership is required."

We should realise that it's not the Cold War, where you had… the Berlin Wall" - he divides the table with a flat hand and points to either side of it – "free, unfree. We are dealing with a world of very blurry lines. Governments in the UK, in France, in Germany, in the US, must recognise that this threat does exist. In Germany, for three years since the beginning of the refugee crisis, Putin's propaganda has been beefing up the AfD. Giving them support. They [the German government] knew about it. But because German businesses are in Russia, the Social Democrats are part of the coalition – Merkel did nothing. The end result? Ninety-four neo-Nazis in the parliament."

What's most frustrating to Kasparov is that "it's not that we lack the means to respond. It's about political will. We have to recognise that there will always be people who will try to use [cybercrime] against the free world, so we always have to be one step ahead. It's not about slowing down the competition - we're actually speeding it up, just to make sure we are at the cutting edge. I believe in the winning spirit, the pioneer spirit, of the people of the free world. There will always be ideas coming in - we have to make sure that the influx of ideas doesn't stop."

Kasparov describes China as "a more long-term threat. It doesn't meddle in elections. It is stealing – not for immediate use, but maybe later on. But you have so many other potential players, weaker players that could say 'Putin did it, why don't we do that?'"

"The key issue for me," says Kasparov, is "the correlation between privacy and security… I was born and raised in the Soviet Union. I lived in Putin's Russia. I am very suspicious of government authority, and I could see many times how exceeding authority was turning into abuse of power." In major cybercrimes such as the recent Equifax hack, which investigators have said bears the hallmarks of a state actor, he says that "nation states, like Russia or China, look for easy prey. But that's as a result of negligence, so we have to hold our administrations, in America or Europe, responsible for not paying enough attention to defend this data. Millions of personal files have been stolen in America? How come? This is supposed to be the leading country, it has Google and Microsoft and Facebook, and it doesn't know how to defend itself. It's because governments are way behind. The free world has been very slow in recognising that this is the new front line. This is where you have to fight, this is where you have to invest."

Spotlight thanks Avast, for which Garry Kasparov is an ambassador, and IPEXPOEurope for arranging this interview.

FLICKR/ACE KINDREDZEN LUCKY

Complying to compete: how to stay on top of regulation

Companies must factor GDPR and NISD regulations into their cyber security or risk being hit by hefty fines, warns Atkins' **Ian Buffey**

UK and European organisations will soon face fines of up to €20m or 4 per cent of global turnover, whichever is greater, if they fail to take measures to prevent cyber attacks that could result in the loss of personal data or a major disruption to services. This is a result of the General Data Protection Regulation (GDPR) and the Network Information Systems Directive (NISD) that take effect from May 2018. These will force organisations of all sizes, in all industries, to put good information security practices at the heart of what they do.

What is GDPR?

Although GDPR can be regarded as an evolution of the Data Protection Act, Information Commissioner Elizabeth Denham has said this is the "biggest change to data protection law for a generation". Whilst organisations within the UK have become accustomed to working within the current data protection legislation, the six Principles of GDPR go much further than anything before, introducing significant changes to ensure the rights of the data subject are protected.

GDPR is all about personal data, ensuring that people are clear about what data are being collected, the purposes for which it will be used, giving the option to opt out, ensuring that data will only be retained for as long as it needs to be and making sure that proper security is in place when data is stored and transmitted.

The changes range from how data can be collected, to a significant increase in fines which can be levied on Data Controllers and Processors for violations of the GDPR principles which lead to an incident. While these changes present significant challenges, they are also an opportunity for organisations to create a more robust cyber security environment and build greater trust with their customers.

SHUTTERSTOCK/MAKSIM KABAKOU

What is NISD?

The NISD has many common features with GDPR, including the level of fines which can be levied if failure to conform to the directive results in an incident – again this is 4 per cent of global revenue. The focus of the directive is on Operators of Essential Services (OES) such as power, water and transportation companies, as well as Digital Service Providers (DSPs). The latter include suppliers of Infrastructure as a Service, Software as a Service, as well as more fundamental services such as Domain Name Service (DNS) providers, although there is still some debate around the definition of a DSP.

The directive seeks to protect the UK from the loss of critical services, such as power and water supplies, and thresholds have been set to determine if companies are covered by the directive or not, based on the amount of power, water, transportation customers etc. handled by that organisation.

The risk of double jeopardy

The proposals for GDPR and NISD both include the concept of a "competent authority", although the term "supervisory authority" is used for GDPR. For GDPR the authority is the Information Commissioner's Office (ICO), while for NISD, there are multiple competent authorities such as the Department for Business, Energy and Industrial Strategy (DBEIS) for energy, Department for Environment, Food and Rural Affairs (DEFRA) for water, and Department for Transport (DfT) for transportation.

However, as the competent authority for Digital Service Providers is the ICO, there are concerns that organisations could face a double jeopardy and be prosecuted under both GDPR and NISD if a cyber event caused both a loss of personal data and an interruption to an essential service. The chances of this happening are significant as most organisations have connections between the IT systems which typically handle personal data and the Operational Technology (OT) systems which control physical processes such as water and energy production.

How GDPR and NISD compare

A common feature of GDPR and NISD is that incident reporting is compulsory and must take place within 72 hours of it becoming known that an incident has occurred. An incident occurs when a cyber related event causes compromise of personal data or an impact to an essential service. Reporting of events which do not cause a real-world effect (i.e. near misses) are to be reported on a voluntary basis. GDPR incidents will be reported to the ICO whereas NISD incidents will be reported to the UK National Cyber Security Centre (NCSC). The NCSC will liaise with the appropriate competent authority so that the causes of incidents can be understood.

The intention is to base the security requirements for the NIS Directive on a number of security principles similar to those previously proposed by the European Union Agency for Network and Information Security (ENISA), so they will not come as a surprise to most organisations.

The deadline is fast approaching

One of the most notable differences between GDPR and NISD is the level of awareness and readiness for the two initiatives. It is difficult to look at any cyber security related website or even one's email inbox without seeing articles on GDPR, including offers of training and services. EU certification is available for GDPR practitioners so buyers know that the services they are offered are reputable. However, for NISD, the cybersecurity ecosystem is much less mature. It is still quite common for an Operator of Essential Services to be unaware of the scope and demands of NISD and so be at risk of falling foul of the regulations when they become law.

May 2018 is fast approaching and it appears likely that many organisations will not have everything in place by then. There has been some talk of a "soft introduction" and it seems unlikely that competent authorities will be pushing for fines of 4 per cent of global revenue when the first incident occurs. However, there is nothing defined for this soft introduction, so companies need to plan to have everything in place by the time GDPR and NISD become law. A lot of work will be required between now and May 2018 if this is to happen – many companies will not have enough appropriate resource to be fully compliant with the regulations.

At Atkins, we have been following the development of GDPR and NISD closely so that we are ideally placed to help our clients respond to the requirements of the upcoming legislation. Fortunately, the cyber security requirements of both pieces of legislation align well with advice we have been giving to our clients for some time.

For more information, please visit: www.atkinsglobal.com/cyber

Oliver Gower, deputy director of the National Crime Agency's National Cyber Crime Unit, explains why the sharing of information between different parties is crucial for solving cyber crime

How to catch a cyber criminal

The cyber threat to the UK economy is growing in scale and complexity. To keep the UK a safe and prosperous place to live and do business, law enforcement, government and the private sector work in partnership. At the National Crime Agency (NCA) we believe this collaboration is vital to protect the public from serious and organised cyber crime. We really are all in this together.

We co-operate very successfully with industry in many areas. For instance, our joint prevention activity directs young people with cyber skills away from crime and towards fulfilling and often lucrative careers; NCA and police ranks are bolstered by private sector digital experts who volunteer as special constables, and the NCA and the police are prosecuting criminals who target business.

But we can always improve. We can get better at sharing information. It's a concerning fact that many firms attacked by cyber criminals do not report the crime, which means the NCA or police forces cannot prosecute the offender. Despite estimates that more than half of organisations were attacked in 2016, a small fraction of these crimes are reported to law enforcement.

Though there are routes to report attacks without engaging the criminal justice system, companies don't always use them. This can leave gaps in what we know about the type, frequency and seriousness of these offences.

The information deficit is driven by a number factors, with responsibility shared by the private sector and by law enforcement. In our conversations with industry, we've noticed three common themes. Firstly, some firms mistakenly believe reporting crime has little impact, which is a myth we and our colleagues in policing must bust. Secondly, boards sometimes do not wish to further

SHUTTERSTOCK / CIRCLEPHOTO

publicise breaches in their defences by pursuing offenders through the courts. Thirdly, not all companies engage as proactively as they might in sharing intelligence with the broader cyber security community.

The NCA coordinates law enforcement's pursuit of organised criminals responsible for serious cyber attacks on individuals and businesses. The agency's National Cyber Crime Unit uses advanced skills and technical tools to detect offenders and bring them before the courts. It works closely with police forces to share expertise and resources.

It's a myth that reporting cyber crime has no impact

To secure the full trust and support of the private sector, we and our partners must kill off the perception that cyber criminals are free to get away with their crimes. The mistake is understandable: our investigations in this area are long due to their complexity and it can take years to identify a suspect and bring them to court. Our officers work with reams of complex data, cross-border offending and criminals who employ dense layers of obfuscation.

But we are succeeding in bringing offenders to justice. In September, five men were convicted of laundering money on behalf of the operators of a malware variant called Dyre. In the same month we charged a man with alleged cyber attacks on Lloyds and Barclays banks. Along with our partners in police regional organised crime units, we are running more than 100 investigations into serious cyber criminality. You will see more results of our hard work in the courts in the coming months and years. This activity is forcing offenders to see that cyber crime is a risky business. Our officers are skilled and determined. Cyber criminals will be found.

We also succeed by disrupting criminal infrastructure. We were proud to support the international operation which saw the dark web marketplace AlphaBay taken offline this year. All of this activity makes life harder for cyber criminals and makes us safer.

To help us, reporting crime is vital. Our officers are most effective when armed with good intelligence. Private sector organisations who fall victim to cyber criminals possess a wealth of useful knowledge. For instance, what

The chance of prosecution is higher when data is shared

method of attack was used? What did the code look like? Do we know where it originated? This kind of data is of real value and enables us to protect the public most effectively.

The NCA recognises business's need to maintain shareholder confidence. But by reporting an offence (and breaches must in any case be reported to the Information Commissioner's Office) an organisation adopts a principled and pro-active public stance. We work discreetly with businesses right up to the point we charge and name our suspects. By then, vulnerabilities are usually patched and systems back up and running. Reputational damage can be limited or non-existent.

Of course, the NCA also seeks to prevent crime. If we and the private sector share the most up-to-date intelligence, we vastly improve our chances.

Outside of crime reporting, law enforcement, government and industry share information about threats in real time via CiSP, a joint exchange hosted by the National Cyber Security Centre. While many major firms are diligent users of the service, others neglect it. There's real scope to increase CiSP's power if we have input from all organisations which depend on secure computer networks.

The benefits to law enforcement from sharing information in this way are obvious, but this is a two-way relationship. The NCA's intelligence picture holds powerful insights into the cyber threat which no organisation holds alone. In 2016, we and the NCSC published the *Cyber Threat to UK Industry* report, clarifying the threat picture and helping boards to implement targeted security improvements. The UK's resilience to the cyber threat is among the world's best but even so, we're exploiting only a fraction of the information that's out there. We could do so much more.

A truly successful partnership between law enforcement and the private sector relies on sharing detailed information about the threat and total commitment to protecting the country's prosperity. A UK which is digitally resilient empowers us all. The more we work together, the stronger we become.

SHUTTERSTOCK/PAVEL L PHOTO AND VIDEO

Cyber security is not confined to dry land, writes Lord Callanan, parliamentary under-secretary of state for aviation, international relations and security

Fighting the new piracy

In today's interconnected global economy, shipping provides the arteries through which the lifeblood of our economy flows. Historically, the vast seas have been vulnerable to criminal activity – from piracy, drugs and arms smuggling, to illegal immigration. But today there's a new and evolving threat to the industry from cyberspace.

Cyber attacks pose a threat to almost every modern business. But the potential damage and disruption an attack could inflict on maritime is a particular concern since shipping carries 95 per cent of Britain's foreign trade. From port operations to navigation, the smooth flow of goods in and out of the country relies on effective digital communications. Yet in some areas, the shipping industry is still dependent on dated computer technology. To add to the challenge, many new maritime technologies – such as autonomous vessels, or complex digital systems which link fleets around the world – require increasingly sophisticated cyber security regimes to protect them from destructive attacks.

The implications for shipping can be profound. In June, the NotPetya ransomware outbreak which surfaced in Ukraine infected the world's largest container shipping business, Maersk. The cost of the attack on Maersk was estimated to be up to $300m, with disruptions at 76 different port terminals around the world.

The NotPetya outbreak showed that even the biggest players in the shipping industry are still vulnerable to cyber threats. But on a smaller scale, compromised maritime systems can play havoc with an industry that requires order and reliability around the clock to operate efficiently and profitably.

In August last year a hacker gained access to the website of a port in Oman, releasing customer information and exposing weaknesses in the port's online operations. And just the month before that, a cyber activist group targeted three separate maritime companies and leaked confidential documents, from import and export details to lists of the company employees.

Cargo theft is another area of growing concern. There is increasing evidence that hackers and criminal groups are working together to access detailed information on the exact location of containers on board cargo ships. Preventing hackers from accessing online systems is absolutely critical. That is why the government is committed to helping the industry protect its digital assets, with robust security plans to maintain resilience in the face of growing threats.

In recent years we have demonstrated how seriously we take the risk of cyber attacks. The 2015 National Security Strategy reaffirmed cyber as a Tier One risk to UK interests. Then in 2016 we established the National Cyber Security Centre. Within its first year, the centre prevented over a thousand cyber attacks on UK interests, and managed the response to hundreds of individual incidents.

Today we have teams across Whitehall departments dedicated to tackling the cyber threat. Within the Department for Transport we are tightening cyber security in aviation, connected and autonomous vehicles, rail and maritime.

The maritime team is working with

SHUTTERSTOCK / PRES PANAYOTOV

Cyber security should be core to maritime management

SHUTTERSTOCK / SHEILA FITZGERALD

the industry, including port operators and vessels traffic services, to understand the evolving cyber threat, and where the sector might be exposed to attacks, both in the short and longer-term future. As part of this they are looking to promote a wider, security-conscious culture across the shipping industry. In the event of an incident, it is crucial that appropriate plans and actions are in place. And to do so ship owners and operators need to understand cyber security and raise awareness of the subject with their staff and business partners.

To support the British maritime industry, we have published a new cyber security code of practice for ships in partnership with the MOD's Defence, Science and Technology Laboratory, and the Institution of Engineering and Technology. Available on the gov.uk website, the code of practice is aimed at ship operators, owners and crew members. It is designed to help businesses of all sizes to assess risks, devise the most appropriate reactive measures, and manage security in the event of an attack.

The code explains why cyber security should be an integral part of maritime management through a ship's lifecycle, and delivered cost effectively as part of mainstream business.

It also highlights the national and international standards and regulations that should be followed. It will therefore complement the work being done by the International Maritime Organisation (IMO)to raise awareness of cyber threats.

Last year we published a similar code of practice on cyber security for ports. All this guidance is crucial, because the dangers posed by cyber attackers are not going away. One shipping magazine has claimed that maritime is now one of the most heavily targeted industries in the world for cyber attackers. And that is likely to pose an enduring challenge for many years to come.

But that is a challenge we have to meet. As an island nation, our shipping and ports industry is immensely important, and keeping it working smoothly and efficiently is therefore a top priority. So as the techniques and knowledge of cyber attackers get stronger and more sophisticated, our response too will evolve and grow.

Are you aware of the impact that NISD will have on your business?

ATKINS
Member of the SNC-Lavalin Group

From May 2018, UK and European Critical National Infrastructure organisations will face fines of up to €20m or 4% of global turnover if they fail to take measures to prevent cyber-attacks that could result in major disruption to services.

We can help organisations like yours to become compliant with the requirements of the new Network and Information Systems Directive (NISD) legislation.

Contact one of our experts today to discuss how you can ensure that you are 'NISD ready'.

cyber@atkinsglobal.com
www.atkinsglobal.com/cyber

Why is beer more valuable than data?

Cloud technology must not foster complacency and customer information ought to be sacrosanct, according to Stuart Green, managing director of SJG Digital

To prove a point, I took a client for a drink the other day. We'd been having a conversation about data protection and they just didn't get it. "It's IT's problem, not ours"; "It's all in the Cloud"; "We don't have anything that matters" and various other all too common phrases were being thrown around the room with abandon, so we had to look at this particular problem slightly differently. So we went to the local pub.

Fortunately, the pub was packed with hordes of delegates from an event nearby so we found some space that was awkward to get to, quite a distance from the bar and I went to get the drinks. The return journey was interesting and I was watching the client watching me to ensure that I didn't spill their pints (I live dangerously and never use a tray). Various comments ran around the table as I placed all four pint glasses down and hadn't spilt any, much to my own amusement.

As one of the client's party picked up their glass, someone pushed past their arm and caused them to do that strange dance-wiggle-gyration that one does during such occasions, trying to keep the glass straight and level in space, as though parts of your body are gyro-stabilised. A small amount of beer left the glass. Angry glances were exchanged. Apologies were issued. Life continued. Conversations resumed.

The point here was to highlight the problem that we have with data. In this case the data was beer and the device the data was held in was a pint glass. With this particular type of data, we can see it, we can touch it, we can taste it, we can feel it refreshing us and its calming effects as its component parts enter our bloodstream. We can also see the data leaking out of the device if things go wrong.

It was my data that I'd brought back from the bar and then I gave it to someone else for safe keeping. Whilst entrusted in their care, other factors affected them that they couldn't predict and they tried to prevent leakage from the device but they couldn't. Some leakage was inevitable. I had no control over that. I'd lost control of my data and, despite best efforts, the party I'd entrusted with my data was powerless to do anything about it.

Time and time again we see breaches of organisations and there's always a story about data leaking out somehow. We've seen this very recently with Equifax and Deloitte. We've also seen this in the past with cloud providers like Dropbox and Adobe. It always seems to surprise people when organisations leak this data out because they've been told "the cloud" is "totally secure".

We've seen a massive increase in so-called Cloud computing as less "stuff" is held on-premise and more "stuff" put into the Cloud. How many of those decision makers, however, have substituted the words "the Cloud" for "someone else's computer" in the sentence? Does "we're going to store all of our sensitive personal data on someone else's computer" really inspire confidence?

Don't get me wrong, I'm not "anti-Cloud" but I am "anti-breach". Having had my own personal data leaked out in various breaches around the world, I grow less sympathetic to the plight of organisations who leak it out because they clearly don't take security as seriously as their post-breach statement says they do. The sooner we learn to care more about data than we do about beer, the sooner we'll be in a far better place.

For more information, please visit: www.sjgdigital.com
Or call: 01673 898001

IN ASSOCIATION WITH

Stuart J. Green digital engineering

People want to know that they're in safe hands

Implementing better cyber security practices can help businesses to thrive, writes Carl Foster, managing director at Foster Environmental Limited

Just over two years ago, if you'd told me that we could build stronger relationships with our suppliers and customers by doing a "computer upgrade", I'd have looked at you as though you were a mad man. I've always enjoyed good relationships with whoever we work with and most of our supplier-customer relationships are long-standing. I think that's testament to the way we work and, of course, the people that we work with. Recently, though, if feels like our relationships have started to grow stronger and it seems that the reason behind that is we all feel safer together as we're working towards a secure supply chain.

When we started on our journey of boosting our resilience, it seemed more like regime change than anything else. Going through the processes of Cyber Essentials, Cyber Essentials Plus, IASME, and ISO27001 has certainly paid dividends in ways that some may feel are unfathomable, but we've seen real benefits in these.

For example, the people who are on our team are our last line of defence and we need them to be as robust as possible. We've achieved that with a little assistance from our trusted partners and we've now got a situation where the team can just sense when something isn't right and take the appropriate action. Yes, we've got technology helping us out but when there's a human element in the defence plan, that's a great place to be. Humans can ask questions or trust a gut feeling, while technological devices are limited.

Getting the team there has been a challenging and rewarding experience. We've held regular training days where small parts of the team spend an hour or so learning some new "stuff" – all in bite-size chunks. They've learned why things happen the way they do when it comes to cyber crime and what the bad guys want to achieve. Understanding of the threat has been vital and we've catered for a range of ages and abilities.

Testing has been important. Knowing how specific people react to changes in the status quo has really helped us understand how the layers of defence work and how we might need to tweak specific layers for specific people just to make things more robust.

The testing of our security posture is always treated like a challenge, like a game – it's almost like cat and mouse. The test is issued randomly so different members of the team get the challenge at different times but the real strength is that people talk about it. They will quickly discuss it between themselves and bat it off. The result is a stronger, more communicable team

Now this really comes in to play when a "real" challenge or issue hits them. It might be a phishing email. It might be a spot of vishing. They are used to being challenged. They have experience to draw upon. The result is a stronger business. Many times over the past year, members of the team have been able to spot something out of the ordinary and have spoken to the external party concerned. When members of our team can offer some support to external parties, that's the real value. Not only has the challenge been accepted and conquered but support has been offered. The result is a stronger supply chain.

So, for some, security is that thing which means you buy some things, plug them in and hope for the best. But the real value of security is in things that every organisation has: the staff, the team, the network defenders, the business protectors. They are our crown jewels and I'm fiercely proud and protective of ours.

For more information, please visit: www.fosterac.co.uk
Or call: 01724 270717

IN ASSOCIATION WITH

foster ENVIRONMENTAL LIMITED

The National Audit Office estimates that online crime is costing the UK public £10bn every year

"Inertia and occasional flourishes of incompetence"

Louise Haigh MP, Shadow Policing and Crime Minister, says the government is failing to give citizens and law enforcement alike the intelligence they need to stay safe online

There is no doubt about the seriousness of the growing threat we face from cyber attacks. Cyber experts at the National Cyber Security Centre are fending off record numbers of attacks on infrastructure and essential systems. But the story of cyber security in the United Kingdom is one marred by indecision, confusion and a basic lack of understanding from the government charged with acting upon it.

In July, we had the annual release of crime figures and the crimes which concern the public the most – violent assault, the use of weapons – have rocketed. But one theme of the annual release was now depressingly familiar: cyber crime is on an almost unstoppable upward trend and the general public feel almost helpless.

This "low-value, high-volume" crime (most incidents involve the theft of a not-insignificant amount of around £250) has soared to over 5m incidents each year. The National Audit Office now estimates that online crime costs the public an astonishing £10bn every year.

And with public awareness so low you would expect the government to fill the gap. But that's not what has happened. Government action has been utterly pitiful and many police forces feel powerless at a local level to stop the rise.

A joint taskforce was set up in February 2016 and so far we are yet to see a single announcement or action from this group. The Prime Minister keeps telling us that cyber crime has to be the priority and that's why bobbies have been taken off the beat yet she's singularly failing to match her words with action.

Such is the shambolic nature of the battle against cyber fraud, when I asked the simple question of how many people are being reached by the government's awareness campaigns, they couldn't give me an answer.

SHUTTERSTOCK/FFOLAS

A shambolic battle against cyber fraud

They cannot afford to be this complacent any longer. We clearly need to build resilience to this growing threat. We've been calling for a proper programme of online education to educate school children on how to stay safe online and to make sure the millions of people without basic digital skills are brought up to speed. But once a crime has been committed the resources the police have to tackle the threat are far too low when compared to the challenge.

It is the most common crime but just one in 150 police officers are there to fight it and we're trying to replicate expertise and capacity on a force-by-force level. Identity theft is a prime example; when a case comes in to a local force it is likely to be complex and the criminal network is more often than not international.

Local forces simply don't have the support to properly investigate. That has to change and it will only change when our over stretched police services are given the resources they need to meet the challenge.

It isn't just about individuals either. We saw this year with a number of high-profile cyber attacks the damage that can be caused by even relatively unsophisticated attempts.

The NHS was forced to use back-up systems and multi-million pound companies were affected. It emerged that hackers had exploited ageing Windows XP computers, which had been left with no protection at all. It is little wonder, then, that the funding squeeze has forced much of the public sector and infrastructure to rely on ageing computers.

This told another story, too. That ransomware virus which caused chaos in the NHS was thought to be similar to one developed by the National Security Agency. The virus was released and spread like wildfire across the world. In the response to the Westminster attack earlier in the year Amber Rudd proposed measures that could have resulted in a similar incident. She wanted to create a back door in end-to-end encryption and insisted this could have enabled our intelligence services to prevent the attack because he sent a Whatsapp message moments before he got in his car.

It was a vivid example of a government failing to understand emerging technology and through knee-jerk reactions reaching a conclusion which threatens our security. You simply cannot create a back door encryption key only for the good guys. Encryption itself would be threatened by such a move, with devastating consequences for consumer and public confidence.

Our individual rights are now so closely intertwined with our digital rights that we have to guard against heavy-handed measures from a government which scarcely understands emerging technology.

Indeed, the Home Secretary herself arrogantly suggested that she doesn't even have to understand it. But nor should government incompetence be an excuse to give social media companies a free pass and to allow them to abdicate

Illegal content is being shared on Facebook

SHUTTERSTOCK/AHMAD FAIZAL YAHYA

their responsibilities.

In the near three decades since the invention of the world wide web, social media has been a tool for the most astonishing change, connecting cultures and empowering communities. Individual moments, like police violence in Catalonia, can be magnified by a global community and change the debate in the blink of an eye. Politicians can be swept in or out of office and entrepreneurs can make or lose a fortune around that power. It has been hailed as a democratising force through which power is decentralised.

Yet the billions of connected individuals rely on a remarkably top-heavy infrastructure. The vast majority of us view content, receive news and communicate on only a handful of major social media platforms. Those same companies are often part of the very infrastructure of the internet itself.

These new behemoths of the digital age have risen out of nowhere in little over a decade to hold incredible sway over all of us. They know who we are, what we like and often know more about us than our closest friends. But they – and we – are still playing catch up when it comes to the responsibility that goes with that power.

Images of child abuse and dangerous extremist content are shared by like-minded individuals — not on far-flung, difficult-to-access corners of the web, but on Facebook, a site used by hundreds of millions every day. The content was almost certainly illegal, it was flagged with Facebook as inappropriate and yet nothing happened to deal with it.

For those of us who embrace the benefits of a digital and connected world, failures like this are galling. They have devastating real-world consequences, they damage trust and they have exposed an online regime which is demonstrably flawed.

For Facebook and similar platforms, who should work in partnership with law enforcement and comply with our laws, the failure to establish an adequate online reporting regime leads to scepticism that they are serious about the risks.

It is vital we build an accountable framework between the government and intermediaries which can keep citizens safe. Regrettably all we are seeing at the moment is inertia punctuated by occasional flourishes of incompetence.

What every business leader should know...

Dr Adrian Davis, managing director, EMEA at (ISC)², says all companies must adopt a more holistic approach to their cyber security

As a non-profit association with over 125,000 certified cyber, information, software and infrastructure security professionals, we work tirelessly with our members to raise awareness of what occurs on the frontline of cyber security practice to ensure a safer and more secure cyber world. The high-profile WannaCry and Petya cyber attacks taking place in recent months have highlighted some very important facts about our dependence on the internet and IT, and organisations' ability to deal with such incidents.

I believe breaches continue to proliferate because information and cyber risk remains poorly understood outside of the information security profession. There is a misguided view that information risk is a technology problem to be managed by the information security and IT functions. Cyber attacks cannot solely be the responsibility of the Chief Information Security Officer and their team. The organisation and its leaders too must work with their security resources to actively gauge their IT dependence, and the risks they face within the context of their business requirements.

This goes beyond the resources of the information security professionals and the small pockets of deeply technical experts that can analyse the threats. Organisations need to apply their business acumen to the assessment and adopt a more holistic understanding of both the nature of the cyber risk that their organisation may face and the potential impact on the business, to guide the necessary treatments.

Breaches can lead to loss of revenue, intellectual property (IP) and customer data, as well as reputational damage and loss of consumer trust. Such broad and varied concerns call for a fundamental realignment in the way business risks are managed and prioritised and a comprehensive assessment right across the business.

(ISC)² has produced a White Paper entitled *What Every Business Leader Should Know About Cyber Risk* which shares our members' and my own perspective on five fundamental areas that will help businesses take back control of cyber risk and be better prepared for the unknown. It offers a guide to motivate the conversations that can ensure cyber risks can be better understood and managed, covering the need to:

1. Accept cyber risk is a business risk
2. Align cyber spending to your risk
3. Create a culture that prevents vulnerability
4. Get control of data
5. Ensure security and privacy are "baked in" to processes

Overall organisations need to be more resilient. Enabling a holistic understanding of cyber risk will lead to robust investment in preventing vulnerability, defending against the inevitable attacks and having the necessary redundancy to keep going when they occur. It is time to acknowledge that all businesses, their customers and their employees rely on the information, systems and software that underpin the products, services and processes now driving our economy. In the current landscape, we must anticipate interruption from cyber attack and develop the ability to keep the lights on, customers served and essential activities going. This is a business concern, one where business leaders need to be at the forefront; it's not just the domain of the technical experts.

To receive a copy of *What Every Business Leader Should Know About Cyber Risk*, please visit: http://edu.isc2.org/cyberrisk/

IN ASSOCIATION WITH

(ISC)²

INSPIRING A SAFE AND SECURE CYBER WORLD.

GDPR will change how personal data is processed

GDPR injects a fresh sense of urgency about cyber security in business, explains Richard Mitchell, director at Digital Training

The European Union's General Data Protection Regulation, or GDPR, will overhaul privacy management dramatically. All connected businesses and organisations across the world, who process, store and transmit information belonging to EU citizens, will be affected. The UK Information Commission Office states that GDPR is an important continuation of data protection law and the UK must comply with the directive, regardless of the eventual outcomes of Brexit negotiations.

The growth of mobile data for all businesses and organisations are in scope to gain full compliance. Organisations' alignment to the existing Data Protection Act currently have eight principles for privacy management best practices, whether as electronic or paper records. Personal data, it says, should be processed: fairly and lawfully; in relation to only one or more specified and lawful purpose or purposes; adequately, relevant and not excessive in relation to the purposes; accurately and kept up to date; retained for no longer than is necessary; in line with the opt-in rights of individuals; securely against accidental loss, destruction or damage and against unauthorised processing; and finally, no data should be transferred internationally to countries outside of the European Economic Area.

A paradigm shift

The six new principles apply to the data controller and data processor that are jointly responsible and liable for compensation claims by individuals. These are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; retention; and integrity and confidentiality.

Accountability, if tacitly, represents a seventh new principle to be aware of. GDPR legislation obligations are far-reaching. The directive applies to not only every EU member state, but also to any companies that are trading with the bloc but are situated elsewhere in the world. Companies must be clear about what data is being collected and what it will be used for. Data subjects can lodge a complaint following a breach to their "supervisory authority". Furthermore, documentation of consent is needed from a data subject to process their data.

Pre-ticked boxes on a form do not constitute as consent; also, the right to withdraw consent must be easy. Similarly, all data subjects have the right for their personal data to be erased and all data subjects can request a copy of any data that is held about them. Personal data can only be kept for a limited time and data subjects should be made aware of this at the time of consent. Third-party controller or processor contracts should be in place, stipulating all stakeholders' responsibilities.

When it comes to data breaches, GDPR requires breaches to be reported in 72 hours and the data subjects affected to be notified. In addition to a maximum fine under the UK Data Protection Act, data breaches will incur a greater fine from the GDPR of €20,000,000 euros or 4 per cent of global revenue.

This brings us neatly to encryption. The regulation advises that encryption should follow the FIPS 140 compliant standards for PII – data including first name or last name – and SPI – data such as a driving licence, national insurance number or NHS number. With regard to international transfers, if the controller intends to transfer data outside of the EU, then these are only legal if the company complies with GDPR's section five.

For more information, please visit: www.digitaltraining.net
Or call: 0116 331 0106

IN ASSOCIATION WITH

DIGITAL TRAINING
www.digitaltraining.net

DIGITAL TRAINING™
www.digitaltraining.net

Contact us to ensure your business is compliant today!

0116 331 0106

NewStatesman

Spotlight

Read more in-depth interviews and features and download full policy reports at:

newstatesman.com/spotlight

How to solve the people problem: mitigating risk

Employee engagement, awareness and wellbeing are all core cyber security issues, write Forensic Control CEO Jonathan Krause, and psychologist Serra Pitts

In a recent survey, passengers at a London railway station were asked what it would take to get them to give up their company's sensitive data. Thirty-seven per cent said they would sell out for a range of incentives, from as little as a good meal, to a £1m cash payment. In every instance, security breaches are the result of human frailties where technical controls can do little to prevent them. From the finance manager unknowingly paying a fraudulent invoice, to the helpful PA who gives the demanding "director" from head office a password to the CEO email account.

For the vast majority of organisations, the hacker-in-a-hoodie scenario, tunnelling into a network to steal confidential data, is extremely unlikely. SMEs are more likely to fall foul to actions from their own staff, often inadvertent, but on occasion malicious. Incidents such as these can affect your organisation's profits and focus. Your company's integrity and reputation can also be swiftly spoiled in the eyes of your stakeholders.

Unfortunately, these threats come from people who have legitimate permission to be in your office, and by necessity have access to all of your data. At a minimum, the security awareness of executives and management is crucial to protecting your company's assets.

While properly configured firewalls and filtering software play a vital role on the perimeter of your network, similar technical controls only protect you to a limited degree within your office. Many businesses say that a more advanced security strategy is too complex, or they simply don't have the resources to manage it. We believe that organisations of every size can benefit from a more effective, rather than more expensive, security strategy.

The most common risk from staff is inadvertent actions; from not checking the new bank details on an invoice, to providing confidential information to unverified parties over the phone, to accidentally deleting project files. Here is where training can raise staff awareness in teaching them about the everyday attempts at scandal they might be faced with. Coupled with an intelligent code of conduct and strong policies around data protection, both internal and external concerns can successfully be addressed.

Dealing with malicious staff, especially those who have elevated network privileges, can be more challenging. For high-risk positions we recommend due diligence that includes rigorous background checks which detail breaks in employment, financial status, criminal history, and mental and physical health. Ongoing "check-ins" with all staff could include the assessment of attitude towards work, performance history and interactions in the workplace.

Malicious employees carry out significant planning prior to their breach. Monitoring staff activity on your network can be important to helping identify anomalous activity, though data protection and privacy rights must be kept in mind. Monitoring programmes should be promoted to staff as a protection that benefits them and their colleagues. Employee wellbeing programmes are another important preventive measure. This shows staff that they are valued by the organisation and lessens the likelihood of disgruntlement.

Above all, insight and awareness are crucial for the prevention and detection of both internal and external threats to your critical assets. A comprehensive strategy that combines technical, organisational and psychological issues into a single actionable framework can pre-empt a security breach, improving your company's resilience.

Will prison deter an autistic teenager from hacking?

Several of the UK's highest-profile hackers have been young autistic men, at risk of extradition and life sentences. Will Dunn asks barrister Ben Cooper if the justice system needs to adapt to these cases

In early 2002, a young man sat at a computer in his girlfriend's aunt's house in north London. The internet connection – using a 56k dial-up modem – was frustratingly slow, but on the screen in front of him, an image began to form. Years later, he would describe seeing "a silvery, cigar-shaped object, with geodesic spheres on either side... the picture was taken presumably by a satellite looking down on it. The object didn't look man-made or anything like what we have created." As he tried to make sense of the image, however, "someone at NASA discovered what I was doing, and I was disconnected".

Weeks later, police officers knocked on the young man's door. His computer was seized and when the officers returned a few months after that, they were joined by colleagues from the National Hi-Tech Crime Unit. By November he had been accused of "the biggest military computer hack of all time", and 18 months later he was facing extradition to the United States, where he faced a trial and up to 70 years in prison.

It took ten years for Gary McKinnon to emerge from the storm caused by his quest for the information he was convinced the US government was hiding on "UFO-related technologies" such as antigravity and free energy. The barrister who defended him from extradition, Ben Cooper, from Doughty St Chambers, tells me McKinnon "didn't do anything" for a decade. "During that period he didn't really work at all, he was very depressed. Life wasn't going anywhere; he was just waiting."

McKinnon chose a poor time to highlight the US military's incompetence. Using basic techniques – McKinnon has said that the only "hacking" required to enter the military computer network was a basic PERL script that searched for passwords that had been left default or blank – he was able to trawl military computer networks, occasionally leaving messages

SHUTTERSTOCK / COLIN HUTCHINGS

Hacker Lauri Love faces indefinite US incarceration

that said things like "your security is crap", and to vandalise key systems for months when, in the wake of the September 11 attacks, security in the US was ostensibly more elevated than at any time in the country's history. The responding threat of an effectively full-life imprisonment, without any chance of repatriation, was seen by some as a way of forcing him to co-operate with the extradition and accept a much shorter sentence of three to four years. But for McKinnon, who is severely affected by both Asperger's Syndrome and depression, either option represented a death sentence.

McKinnon's extradition came perilously close to being realised, after he lost appeals in the House of Lords, the European Court of Human Rights and the High Court. Cooper then brought a judicial review to the High Court, where permission was granted to challenge Theresa May's decision that extradition would not violate his human rights. May eventually accepted that extradition would violate his rights under Article 3 of the ECHR, because of his very high risk of suicide.

Fifteen years after it originally began, the McKinnon episode is being played out again in the case of Lauri Love. Love, a British-Finnish hacker, has been accused of stealing data from the US military and NASA. Like McKinnon, he is threatened with extradition and effectively indefinite incarceration (up to 99 years) in the American prison system and huge fines. Like McKinnon, he suffers from Asperger's Syndrome and depression.

These two cases are far from the only two Ben Cooper has seen. In 2013, Ryan Cleary was sentenced to 32 months in prison, one of the most severe sentences issued from a British court for hacking. Cleary, who was 19 at the time, was diagnosed with Asperger's syndrome and agoraphobia. In the same year, an anti-junkmail service called Spamhaus was hit by the biggest Distributed Denial of Service (DDoS) attack ever seen. The attack flooded Spamhaus with so much data from corrupted computers that large parts of the global internet slowed down. The attacker was eventually identified as Seth Nolan-McDonagh, a British 16-year-old. Nolan-McDonagh had suffered from mental illness, dropped out of school and withdrawn from the outside world. He first became involved in online criminality when he was 13.

Earlier this year, 20-year-old Adam Mudd was jailed for two years for creating and selling Titanium Stresser, a tool that was used by himself and others – it had 112,000 registered users – to perform more than 1.7m attacks on websites and internet services. Like McKinnon, Love and Cleary, he is autistic. Ben Cooper agrees that he fits the autistic hacker personality type. "Generally they're not really thinking consequentially. They get carried away, in the middle of the night, on their computers. Most of them are extremely lonely guys who have no friends, maybe kicked out of school, some of them have

Autism traits can be helpful in computer science

SHUTTERSTOCK / JERRY-RAINEY

mental health problems and are very much on their own, and so this is their one opportunity to have a community."

In daily life, an autistic person's obsession with organisation and repeating patterns can be debilitating, but in computer science it can be a advantage. Alongside the opportunity for contact that's missing in their daily lives, the repetitive logic challenges of programming and systems administration offer these young autistic men a type of work at which they can excel.

In the case of Adam Mudd, the judge in sentencing stated he was satisfied that, at 16 years old, Mudd "knew full well and understood completely this was not a game for fun" when he created his malware. But there is little evidence that the considerable sum of money Mudd made from selling Titanium Stresser – police seized over £386,000 in US dollars and Bitcoins – was to the teenage hacker much more than a high score in a game whose consequences he did not fully appreciate. This is evidenced, says Cooper, by the fact that Mudd didn't use the money to buy anything. "The judge accepted he wasn't financially motivated, he didn't have a lavish lifestyle." The only money Mudd drew from his account, says Cooper, was used to pay tax on some earnings he'd made from another, perfectly legitimate, online business.

Once caught, Mudd again followed a

"There's no evidence the jail sentences deter them"

similar pattern to other autistic hackers whom Ben Cooper has represented or researched. "They generally have stopped everything. Adam Mudd stayed offline for two years. (Once) their parents have found out about it, they're back on their studies. They're kids who do listen, when told."

In sentencing Adam Mudd to two years in prison the judge, Michael Topolski QC, described the power of teenage hackers to damage systems around the world as "terrifying". In refusing to suspend the custodial sentence he added that it must contain a "real element of deterrence", to persuade other would-be hackers that prison time could accompany their actions. This is accepted as a principle in sentencing many kind of crime - but is an autistic hacker likely to consider it? The National Autistic Society lists as one of the key traits of an autistic disorder that the sufferer may have difficulty "predicting the consequences of an action" and that they may be "less able to see the whole picture", preferring to focus very closely on details. "What evidence is there," asks Ben Cooper, "that people with autism actually think 'I mustn't do this'? They aren't generally on the same wavelength as the rest of us, so there's no evidence that these deterrent sentences actually achieve anything."

"When they're that young," he continues, "it's questionable whether it's right in principle to pass a deterrent sentence, when actually the focus is normally on their welfare and rehabilitation, because of their age."

It is easy to forget that the internet itself is barely older than these teenage hackers, and its ethics may be even less developed. For gifted, socially abnormal young men with stunted moral faculties, the web's darker corners are instantly accessible. Both Ryan Cleary and Seth Nolan-McDonagh were found to have hundreds of indecent images of children on their computers, and Cleary has been placed on the sex offenders register for five years. Junaid Hussein, another teenage hacker, was jailed for six months in 2012 after purportedly gaining access to the private data of individuals including Tony Blair and Nicholas Sarkozy. "The judge accepted that he wasn't a terrorist or a jihadi," remembers Cooper. "There was no prosecution based on that suggestion." But, after about five weeks in Feltham prison, "he came out and joined ISIS. He went to Syria. He'd just done his A-levels, he had a place at university and he had good parents." It is not clear whether Hussein was radicalised before or after his punishment, but he quickly became a key figure in the terrorist network. "He was making a lot of money for ISIS, through cyber fraud." As a valuable fundraiser and propagandist, Hussein became a key target. He was killed in a drone strike in 2015, aged 21.

It is the shameful truth of the digital age that a technology that has revolutionised many areas of commerce and communication has, at the same time, been instrumental in the spread of child abuse, terrorism, disinformation and hatred. In dealing with the autistic-hacker personality type, internet safety and cyber security become the same thing – guiding and protecting these people removes a cohort of gifted hackers from the internet. With the right guidance, it may be that the best kind of rehabilitation for this kind of young, socially or developmentally impaired hacker is found in very similar activity to that which first got them into trouble – but on the right side of the law.

There are plenty of success stories of hackers who turn from poacher to gamekeeper; among the best security researchers are former prisoners. Cooper has seen signs of this already –Adam Mudd was offered a job by a cyber security firm in Newcastle before he was sentenced, while Seth Nolan-McDonagh, having been sentenced to community service, is to proceed with his A-levels. "There have been moves towards exploring how these kids could do cyber security work as part of a community sentence or probation, but nothing has yet been formalised, which is unfortunate because it would give the best form of rehabilitation."

Optimising cyber strategy for the SME

SMEs need a tailored roadmap for cyber security, according to Graham Horne, director at Amwell Information Security

If you are a board member of a medium-sized company, the founder of a start-up, or a trustee of a charity then you know that cyber security is important. Increased public awareness of cyber security means that any breach poses a serious reputational risk. In addition to the direct costs of responding to an incident, the regulatory framework in the UK means that your organisation is at risk of fines and adverse publicity if you don't have adequate safeguards in place. The scale of those potential fines is about to go through a step-change in May 2018, with the incorporation of GDPR into UK law. And the impact on the individuals responsible for cyber security can also be significant, as we have seen in the wake of the recent breach at Equifax.

Larger organisations are likely to have the support of a substantial team of specialists in departments such as Information Technology or Compliance. In a smaller organisation, this level of in-house experience is unusual. You may use a managed services company for your IT provision, but they are unlikely to be experts in cyber security. This means that you need to find your own way through complicated cyber security jargon, confusing messages about what needs to be done and competing claims from product vendors.

At Amwell, we recognise the problems this situation poses for smaller organisations. Our approach is to work with you to chart a route through this complicated world, using recognised security certification frameworks as our guide.

If you don't currently hold any security certifications, we usually recommend you start by certifying with the government-backed Cyber Essentials scheme. This scheme focuses on five technical controls which are designed to deal with around 80 per cent of internet-borne threats. Even if you already implement these five technical controls, the certification is still valuable as it provides clear, publicly verifiable evidence that you are serious about your cyber security responsibilities.

The next stage in maturing your cyber security strategy is to move towards a full-management system for information security. We recommend the IASME Governance certification from The IASME Consortium which defines a risk-based management system that is tailored for smaller organisations and has been recognised by the government as the most appropriate for them. The certification also includes an optional assessment against the requirements of the upcoming GDPR regulations.

A risk of fines and adverse publicity

Rather than being a one-off examination, the scheme requires you to put in place management systems which mean that you can actively and continuously manage information security risk, in the same way that you manage other aspects of your business. If you do not have all the required systems in place immediately, the risk-based approach guides you in deciding where to prioritise your efforts. Over time, your systems will mature to the point where you can apply for certification, which proves you have taken your cyber security to the next level.

For more information, please visit: amwellis.co.uk

IN ASSOCIATION WITH

Amwell INFORMATION SECURITY

All computers are broken

Knowing your enemy is the first step to beating them, argues Jennifer Arcuri, CEO and founder of Hacker House

Between the dependency on critical infrastructure, the rise of connected devices, and all the talk of increased cyber attacks, everyone has an interest in cyber security. It's a rare day where there isn't some big "hack" that's cost companies millions in losses, someone's identity has been stolen, or some indecent exposure has taken place online. This isn't about weak passwords, out-of-date software, another intrusion detection system, anti-virus, or firewall. Automate and introduce managed services all you want, but at the end of the day, we absolutely need more cyber skill.

Why is this? All computers are broken. Inherently, computers are susceptible to an increasing number of threats, advances in attacking has made cybercrime easier to perform and harder to defend against. Every system can be hacked. There is not a company, network or software that cannot be compromised in some way. It's time for us to embrace the problem-solving abilities of hacking and embrace it as part of the solution. Knowing how your adversary works and attacks allows for better targeting of resources, models like the cyber kill chain have helped pave the way for companies to better understand their risks.

Isn't it time we heard from the hackers? Our team has consistently breached security of devices, from the latest "ransomware-proof" computers to "security appliances" meant to prevent advanced attacks. Exploit developers and purveyors of the art of hacking; our team embodies the hacker spirit to show you what your adversary already knows.

One of the biggest reasons companies are failing at security is because they don't have the right skills on the team. Even if they hired an outside consultant, there is still no guarantee that the "patches" pointed out are now secure and that the company is indeed protected from further attack. The cyber consultancy model is flawed. Companies can't afford to keep up with the "ask" for security budget if there is no one on the team who can think as an attacker would.

The result is a shift in industry. Hackers are now essential. Companies invest in hackers on their team rather than "wait" to be made a target. These cyber skills are invaluable to the business because it better prepares companies to handle more of their own internal breaches with a better incident response management. Having an on-site resource who can make sense of cyber security and the tools used can be a huge asset.

Hacker House has developed a Hands on Hacking course to give companies those real-world simulations of what happens with their systems are attacked. It is designed to teach skills used by ethical hackers to conduct a variety of assessment activities. Hands on Hacking allows companies to quickly train and scale their security teams. Rather than pay for expensive theory-based content and out-of-date information, companies are looking for real hackers to train their teams to respond to attacks.

The Hands on Hacking course is made up of modules where students are presented a topic and are taught how to launch an attack upon completion of each lesson. The course can be taken in a classroom environment or online through the on-demand portal. Once the course is completed, students retain access to all lab work; a virtual hacking lab is set up for a live 365 environment to hone their skills and better prepare defences for attacks.

Hacker House teaches the core concepts used in many cyber security-related job roles from intelligence analysts to penetration testing. Whatever your job in technology, isn't it time you learned how to protect yourself?

For more information, please visit: https://hacker.house/training

IN ASSOCIATION WITH

HACKER HOUSE
MAKE. BREAK. DO

United we stand, divided we fall

When it comes to cyber security, companies can't afford to be carrying any passengers on the staff, warns **Simon Townsend**, chief technologist EMEA at Ivanti

SHUTTERSTOCK/G-STOCKSTUDIO

IN ASSOCIATION WITH

ivanti

Cyber attacks have taken the world by storm this year, with the press divulging a new breach or ransomware attack on what feels like a weekly basis. In fact, the NCSC's annual report claimed that 1,131 attacks took place in the United Kingdom alone – that's equivalent to two significant attacks per day. Many of these attacks have been incredibly high-profile, resulting in a knock to both reputation and share prices of giant corporations like Maersk, WPP and, recently, Equifax.

What happened to Equifax?

Equifax, an American credit reporting company with links to UK brands like BT and Capital One, has been the victim of a cyber attack which compromised the PII (Personally Identifiable Information – names, email addresses, birthdays and social security numbers) of 145.5m consumers. Equifax are also in trouble because they reported the breach 40 days after they first discovered it in July. Worse still, this was two months after the breach itself infiltrated the organisation. The breach itself took place when cyber criminals exploited a software vulnerability first identified in March, for which a patch (software update which gets rid of vulnerabilities in the code) was issued within a week.

So, why didn't Equifax patch this vulnerability straight away? Ask anyone who works in cyber security or IT and they should tell you that patching is the bedrock of an effective cyber crime defence strategy. Yet, ex-CEO of Equifax, Richard Smith cited "human error and technology failures" as the reason the breach took place. This is not a valid excuse. Smith also claimed that the 40-day delay in reporting the breach was to prevent an onslaught of copycat attacks from also exploiting the vulnerability. Taking this long to report a breach is unacceptable in today's world – and will become even more

financially punitive with the introduction of the European Union's GDPR (General Data Protection Regulation) in May 2018. When the GDPR comes into force, breaches must be reported inside 72 hours.

I believe that the delay most probably came down to a common challenge that many organisations face when IT teams and the business are not aligned when it comes to technology, processes and workflows. Verizon's 2017 Data Breach Investigations Report found that across multiple industries, cyber security attacks can compromise networks in seconds, but discovery and remediation of incidents and threats can take weeks, months, or even years. IT is typically a siloed set of departments and groups: the web team is separate from the info-security team, etc. Siloed themselves, using separate tools and platforms, and also often very siloed from the business, IT has grown over many years to become what is arguably very far from unified.

GDPR is trying to help organisations realise the importance of data protection and while there are many technologies which can help solve tactical points across the many articles contained in the regulation, the real message here is around changing technology, people and processes to create a more unified approach. If you're not part of the IT department, this is not a cue for you to stop reading; just think about the public perception at stake.

A layered approach to security

A critical element of the unified IT vision is that it is fortified with multiple layers of cyber security measures that defend the organisation from attack. I can't stress enough the importance of a so-called "defence-in-depth" approach so that there can be no single point of failure. For example, Anti-Virus (AV) is great at preventing many threats. However, when the WannaCry ransomware attack hit it took several days for AV vendors to consistently detect and block the attack's spread. Other ransomware variants take time to be detected properly, which can result in many machines being infected globally before AV alone can be an effective measure to prevent infection.

This makes patching a cyber security team's number one priority, simply because it reduces a networks attack surface. This doesn't mean that you should run down to your cyber-security department straight after reading this article so that you can crack the whip. Patching immediately isn't always achievable, but I reckon a doable "time to patch" goal should be around two weeks from the date that a security update is released by a software vendor. After patching should come application control (blocking or restricting unauthorised applications from executing in ways that put data at risk) to help mitigate the threat from as-yet-unknown vulnerabilities. Some argue that application control is cumbersome and can cause disruption to users, but there are more dynamic, "just in time" approaches available that provide adequate security without major drawbacks.

There are other layers to your cyber security defences to consider. User education is vital to preventing those initial – potentially malware-laden – phishing emails from getting in, while regular back-ups will mitigate the risk of data loss. Correctly configuring Windows firewalls can also help to halt the spread of ransomware within the organisation. However, patching and application control should be first on the list for all organisations looking to fortify their organisation against attack.

Hackers' techniques and technologies are growing in sophistication. We all need to fight back by ensuring that our organisations' have a layered approach to security in place, and are ultimately working towards a shared vision of unified IT.

For more information, please visit: www.ivanti.co.uk

Defending the digital world

Rapidly advancing technology is changing our society and we need new thinking to ensure security, writes **James Hatch**, director of cyber services at BAE Systems

SHUTTERSTOCK/JAMESTOHART

Discussion of digital technology has focussed on the internet but our new world is built on a much broader range of technology. Miniaturisation of electronics continues to drive adoption as new applications become more cost-effective. And so we are adding digital instrumentation to many aspects of our lives from smart meters in our homes to GPS-equipped smartphones in our pockets.

The reusability of software is adding intelligence and decision-making through automation and machine learning. And behind the scenes, cloud technology and mega-scale data centres are enabling collection and analysis of masses of data to provide services, operate businesses and government, conduct research, tackle crime and also target consumers with more personalised advertising.

The economic impact has long been recognised, particularly through online retail – a higher proportion of the UK's economy than other major nations. And digital technology is allowing Uber and Airbnb to transform the fundamentally physical taxi and hotel industries.

Digital technology allows us to spend more time engaging with people who are like us rather than near us. And we increasingly rely on digital media for our information. Facebook is the world's largest distributor of news.

As data-targeted campaigning and grassroots online organisation have increased and political debate becomes fragmented among social media echo chambers, it is harder to understand and forecast the intentions of voters. And the public can see the potential for hacking, leaking and other information operations to influence elections.

Connected devices allow us to create smart homes. Driverless cars are just around the corner. Industrial companies are seeking productivity improvements with initiatives such as digital oilfields and the digital railway.

The end of physical distance

Mental models of security have not kept up with these changes for most people. Established models have worked on a division of responsibility best understood in physical terms. As organisations and individuals, we protect our property using risk management – usually informally. We decide how much to spend based on the value of assets and the threat we perceive in their environment. A jewellers shop in a big city will spend more on security than a bakery in the country.

When criminals break through these protections and we are burgled or robbed, we call law enforcement. We expect government to help when something goes wrong but we accept it is our job to ensure our property is properly protected.

There is also the whole separate world of national security. We expect governments to maintain the intelligence and surveillance capability to know what is going on globally and the military capability to deter or deal with aggression that comes from beyond our borders. Businesses and individuals rely on physical distance to keep these two worlds apart and on governments to manage global threats. We have concentrated on local protection and this thinking persists in approaches to cyber security.

Now digital technology is making physical distance irrelevant. Security officials believe that hackers in North Korea were responsible for the attack that crippled parts of the NHS earlier this year. Security still relies on protection, enforcement, intelligence and military domains but the domains increasingly overlap.

Implications for business and government

Firstly, our new security model changes the division of responsibility between businesses and government. Protecting business assets has been entirely the responsibility of the owning business, but there is an increasing willingness by government to support protection, particularly where they can do so effectively by working on improving core digital infrastructure.

In the UK, the creation of the National Cyber Security Centre is a bold step taking part of GCHQ out of the intelligence world and giving it a broad public role in cyber protection. Meanwhile, China has just introduced its first cyber security law with the stated aim of shielding domestic data from foreign espionage.

Conversely, financial services and technology companies can take on online enforcement. A victim of fraud on Amazon is less likely to call the police and more likely to seek a refund through Amazon or their bank. And security companies like BAE Systems can use digital technology to provide significant intelligence, often identifying developments in criminal and national activity from targeted research and work on breaches.

Secondly, we need to reconcile defence of global business networks and technology platforms with the national focus of governments. Governments understandably prioritise their own countries when it comes to security, whereas technology, infrastructure and financial systems are all fundamentally international. Law enforcement has evolved from a primarily territorial remit. This complicates collaboration even within countries but leads to real problems internationally. Investigators need to navigate differences of legal structures and approaches, never mind language and culture.

There are major efforts at improving international collaboration between law enforcement and security organisations. Work is underway to develop a new "architecture" for enforcement bringing in parts of the private sector. But government fundamentally works at right angles to much of the digital world. A complete solution needs a more radical transformation that works independently of local and national authorities but with their agreement and support.

Defending your organisation

Businesses can no longer rely on distance and governments to insulate them from international risk. We need active business defence to protect our businesses. Business defence uses intelligence on adversaries, technical vulnerabilities and the organisation itself to build an understanding of the situation and prioritise resources to dealing with those risks that are most significant. Business defence engineers organisations to be robust in their systems, process and people so the overall business can continue even in the face of a local compromise. And business defence maintains the vigilance to identify problems early and the readiness to deal with them before they cause serious damage. In this way, we can ensure our organisations thrive in the rapidly changing digital world.

For more information, please visit: www.baesystems.com/businessdefence


BGi.UK
Cyber-risk Management
Cyber-risk Management
Key to Making You More Resilient
Training
Storage
Encryption
Insurance
01367 246130 | cyber@BGi.uk.com | BGi.uk.com/cyber

A Sideways View on IT Security

Would you dance if I asked you to dance?
Would you run and never look back?
Would you cry if you saw me crying?
Would you save my data tonight?

Would you tremble if I touched your servers?
Would you laugh? Oh, please tell me this.
Now would you die for just one mistake?
Do pay attention, tonight.

In this article I am going to avoid using the 'C' word.
It's everywhere.
Overkill. None the less, it's important.
Critically important.

Have you ever lost data – or simply mislaid it?
Have you ever let others into your shell?
Have you ever moved money without first checking the recipient?
Have you ever uploaded your daughter's homework?

Would you tremble if your fire walls were breached?
Would you laugh? Oh please tell me this.
Would you survive a simple attack?
Would you share your data tonight?

The following are real events. Which of these events might have been you?

Technology Company – System Hack
Total Cost: £250,000
A Client was notified of an intrusion on their systems and the Insurers IT forensic experts discovered a significant amount of malware had been deployed.

Retail Company – Distributed Denial of Service (DDOS)
Total Costs: £144,000
Data centre hosting a website was subject to a DDOS attack through hacked Internet of Things (IOT) devices. Website was inaccessible for 6 hours before back up could restore functionality.

Charity – Care Home Sector
Total Costs: not measurable
Staff member uploaded her daughter's homework for printing – and shut down the business's systems for six days.

Recruitment Firm – Funds Transfer Fraud
Total Cost: £20,000
Hackers altered an email that was sent from the MD to accounts team with an invoice to a supplier. Accounts team followed 'MD's instructions' and paid monies into the hackers account.

Publishers – Held to Ransom
Total Cost: £60,000
An employee opened a phishing email, which contained the Crypt locker virus. The client's operating system was blocked and client files encrypted. A ransom of £400 in Bitcoins was demanded. Only 90% of files were recovered. The business was unable to trade at all for two days and was compromised for a further two weeks.

Payroll Company (small business) – Held to Ransom
Total cost: one twelfth of annual revenue + costs
Victim opened a payroll file from a regular client. The file was contaminated and prevented access to all current data which had to re-built from the last tape back-up. This took nearly three weeks.

Basic Risk Management can remove many of these risks. Once in place, Insurance can add a layer of security.

So, avoiding for a moment the overused keyword 'C' word – do take care.
Call BGi.uk for assistance

So can we save your data tonight?

01367 246130 | cyber@BGi.uk.com | BGi.uk.com/cyber

Don't let GDPR be a dirty word. Just do it the easier way

The best companies use innovative technology to manage regulation, explains **Rob Savage**, head of professional services at Avatu

IN ASSOCIATION WITH

avatu

Did you almost jump all over this story because it mentioned GDPR? Yes, well I don't think you're alone. GDPR has been so prevalent in business circles – for the last year or so – that while some people have faced the challenge head-on, others have become somewhat GDPR-blind, and are only just getting to grips with it now. Either way, when it comes to the leaders who are dealing with the GDPR requirements, the best are seeing it as a business opportunity rather than a compliance exercise and are using innovation to short-circuit the challenge, as suggested by the GDPR wording itself.

Ground-breaking technologies, mainly in the communications field, have changed the way we do business, including how we store and use personal information. And they have also been the catalyst for the introduction of the GDPR.

Practices and policies have to change but the legislation also advises that technology is used, where possible, to provide the solutions. There are many options for organisations. But to be compliant before May next year, they need to get advice and act now or run the risk of being left behind.

Information Commissioner Elizabeth Denham has told businesses there's no time to delay in preparing for "the biggest change to data protection law for a generation".

Data protection by design

One of the most significant parts of the GDPR is "data protection by default and design" and this is one area where technology can take away the burden of some of the GDPR requirements.

Technologies are available which allow users to control a document at source. The document owner can easily set permissions on who can see what, and for how long they can have access. It can also restrict editing, printing, copying and screen captures. Outsourcing is such an integral part of

SHUTTERSTOCK/WKio03MIKE

business models today that most enterprises simply choose to live with its third-party security risks – or just turn a blind eye. But to achieve GDPR compliance this needs to be taken more seriously. This technology will help reduce the risk from this channel too.

Technology which controls access to information and constantly reinforces staff training and company policies is available and will reduce the risk of a data breach. Technologies that are inbuilt into your systems mean that your team members only have access to the data they need for their job – no more, no less.

One of the most vulnerable routes to your valuable data is malware hidden in email attachments. Technologies which reduce the risk of this being successful should be deployed. Ground-breaking technologies which mean that successful cyber attacks are caught quickly (in minutes instead of months) will limit the damage that data thieves can do .

Understanding your data

GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act. In various articles (including 15, 16, 17 and 18), the GDPR provides rights for individuals. These include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability and the right to object.

It's very difficult, however, to satisfy these commitments if you don't know and understand your data.

Technologies can help you fully understand what you've got, where it's held and how you can deal with any individual requests under the GDPR.

Organisations will require technology to help them manage their data to:

- Connect individuals with their personal data.
- Correctly categorise it and understand how it's held and used

Search and retrieve it.

- Put things right, introduce the correct future activities and make sure you've found everything.
- Make it available to the individual (if necessary). This same technology will also help you with data protection impact assessments.

Responding to a breach

Well-run organisations will introduce the technologies I've mentioned in other sections. But as all business professionals know, there is no such thing as total protection. The risk will only ever be managed and reduced, it will never be eradicated.

With this in mind, the GDPR also expects organisations to prepare to deal with a data breach and introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases to the individuals affected, within 72 hours of the breach being discovered.

According to the GDPR, a breach is more than just losing personal data. It says: "A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

It requires an organisation to do prevention activities with its obligations to "regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of testing." And if a breach is discovered the notification to the ICO must be made within 72 hours of discovery and must cover:

- The nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer (if your organisation has one) or another contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Because of the tight timescales, it's essential to have robust, tried and tested breach detection, investigation and internal reporting procedures in place, in which technology will have an important role. If a breach happens:

- Previously deployed technology will provide an audit trail which is easy to find and follow.
- Previously deployed technologies will reduce the access thieves have to your data and systems.
- Digital forensic technologies will help discover who did what, show where you introduced mitigation (and show you have limited exposure), help you assess your vulnerabilities for the future.

For more information, you can email: cybersecurity@avatu.co.uk or phone: 01296 621121

BY THE NUMBERS

What does a cyber attack mean for a large company?

£27.3bn

Deloitte, which reported £27.3bn revenue in 2016, had its server hacked, compromising the privacy of an estimated 350 clients, including four United States government departments.

£60m

Following the breach at TalkTalk which saw details of more than 150,000 customers stolen, the company lost 95,000 subscribers, costing it £60m.

3bn

Embattled web giant Yahoo revealed this month that all of its 3bn accounts were breached in its 2013 hack.

145.5m

The global information solutions company, Equifax, reported a major incident earlier this year, in which the personal details of 145.5m consumers in the United States were stolen.

26,000

A malware attack in early May exposed the credit card details and personal data of 26,000 Debenhams Flowers' customers. The breach was through an e-commerce service, Ecomnova, which runs online stores for a number of retailers.

£2.5m

In November 2016, Tesco Bank had to reimburse £2.5m to over 9,000 customers after Tesco was forced to suspend online and contactless transactions.

KEEP YOUR ENEMIES CLOSE BUT YOUR FRIENDS EVEN CLOSER

Insider threats are a **challenge for every organisation** but the answer to the problem is in your own hands.

There are simple techniques you can adopt, or you can use something more complex and far-reaching.

We can help you start from scratch - develop your insider threat strategy and introduce you to a variety of innovative technologies to review - or we can help plug a specific gap in your protection plan.

It's up to you...

The insider threat technologies and training recommended by our R&D team include:

- Email protection
- Privilege management
- Digital rights management
- Behavioural analytics and behavioural management
- Advanced malware protection

Give our security team a call today on 01296 621121 to get the conversation rolling.

Avatu – infosecurity advisors to inspiring companies

avatu

www.avatu.co.uk