NewStatesman

Spotlight

CYBER SECURITY DISRUPTING DIPLOMACY

Russia's next election hack The European Union
The red net China's cyber strategy
Snowden's razor When security isn't safe

Could you say - hand on reputation - that your data is properly protected?

Cybersecurity is a fast-moving world which always has something new up its sleeve.

Ever-changing threats can leave businesses feeling like they're constantly chasing a moving target.

But you can **stop chasing shadows**, and **second guessing hackers** and insider threats,w with a data-centric (and not systems focused) approach to security.

Call us now if you're not sure you're protected as well as you should be.

WE'LL HELP YOU PROTECT THE DATA YOU CAN'T AFFORD TO LOSE - AND PUT YOU BACK IN CONTROL.

Call our cybersecurity advisors today on 01296 621121 or email cybersecurity@avatu.co.uk and find out more.

Avatu – cybersecurity advisors to inspiring companies

avatu

www.avatu.co.uk

A state-level issue

When asked last week if he thought a time would come when a state would invoke Article Five of the North Atlantic Treaty in response to a cyberattack, the new chief executive of the National Cyber Security Centre, Ciaran Martin, echoed the response of the former US Director of National Intelligence, James Clapper, who had been asked "pretty much the same question" a few weeks earlier: "He said, that wasn't a judgement people for people like us to make." But someone is going to have to make that judgement, and soon. It is not enough to say that a cyberweapon is only made from information. The last (and only) time Article Five was invoked, in 2001, it followed the actions of a foe who, it is thought, had been armed with nothing more sophisticated than a utility knife. In a specific situation, a piece of data or a utility knife can represent a devastating opportunity for control.

The difference is that information is far more capable in this respect. It can be transported invisibly, it can pass through any number of locked doors,and it can do its work independently of human action. In the development of cyberweapons by nations, we are seeing the weaponisation of information itself, and the opportunities for control – of another nation's energy grid, its media, its financial system, its elections or its aeroplanes – are multiplying at speed. The idea of a state's nuclear weapons programme being hacked is not science fiction. It first took place almost 10 years ago.

The huge effort and investment being put into facing this newly emerged and unpredictable risk is encouraging, but pitting technology against technology is only part of the solution. As any cyber security expert will tell you, human intention remains the deciding factor.

NewStatesman
2nd Floor
71-73 Carter Lane
London EC4V 5EQ
Tel 020 7936 6400
Subscription inquiries:
Stephen Brasher
sbrasher@newstatesman.co.uk
0800 731 8496

Special Projects Editor
Will Dunn
Special Projects Writer
Rohan Banerjee
Design and Production
Leon Parks

Commercial Director
Peter Coombs
+44 (0)20 3096 2268
Account Director
Penny Gonshaw
+44 (0)20 3096 2269

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 24 Feb 2017.

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

Inside cyber security's new nerve centre

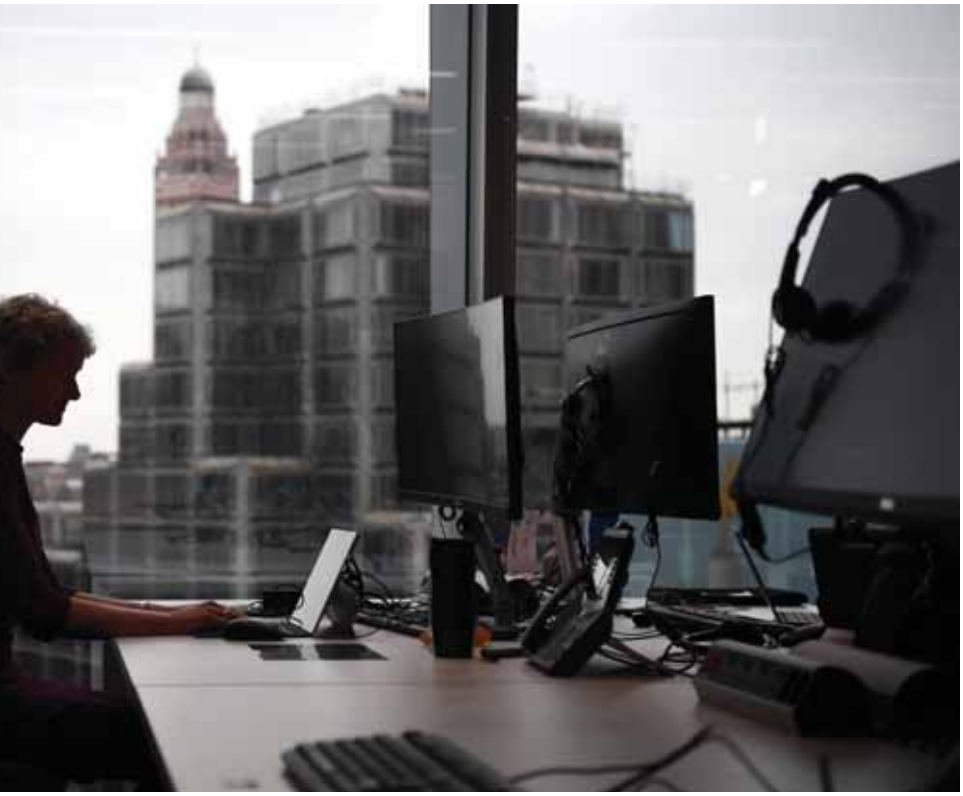
The new chief executive of the National Cyber Security Centre, Ciaran Martin, and other senior members of NCSC staff talk to Will Dunn about the need for a more open, more outgoing arm of GCHQ

The GCHQ base in Cheltenham is a building the size of Wembley stadium, bristling with security cameras, patrolled by armed guards and surrounded by tall fences that are topped with razor wire. The organisation's new London headquarters, however – the National Cyber Security Centre – occupies two floors of a glass-walled office building in Victoria. It's a very smart, new office building, but there is a distinct lack of razor wire, and none of the receptionists appear to be carrying automatic weapons.

The NCSC's open environment is illustrative of its approach, particularly where businesses are concerned. While much of its operational work will remain classified, the NCSC will invite people from the private sector to train within its walls. Following an official opening by the Queen, Philip Hammond delivers a speech in which the digital economy is mentioned before national security, and in more detail.

"The private sector is piling in extensively here today," agrees Ciaran Martin, the NCSC's chief executive. "We're getting 100 private sector people in to work here," he adds, referring to the Industry 100 initiative, which will "embed" 100 workers from across the private sector in the NCSC to share expertise. "It's not one of those areas where the private sector is telling the government to back off – they're asking to work with us, and we've got plenty to learn from them."

The NCSC will also be heavily involved in securing the public sector, too, helping to co-ordinate cyber defences across bodies from the MoD to the smallest local council. "Local government is a major concern for the NCSC," says Martin, "but let me be nice to local government. They are under significant financial pressure, they've got all sorts of obligations, and this can be quite complex stuff. There are 380-odd local authorities in Great Britain. Some of them, like Birmingham, are the size of decent-sized companies, and some of them are very small. If you're a small local authority, I think that in the past, organisations like mine have been slightly too lecturing towards you about what you're not doing right, and not sympathetic enough to the fact that if



"In the past, organisations have been a bit too lecturing"

you're trying run, for example, a small rural local authority, you've got lots of citizen data but you've got lots of other responsibilities, and it's quite hard to get the right people and the right tools in place. It's quite hard to even know where you can look for help."

Martin aims to change that by introducing simple, effective tools that will help public bodies of all sizes secure themselves. "One of the things that we're proudest of, which we'll be rolling out later this year – and which has been exhibited in front of the Queen today – is WebCHeck. What WebCHeck does is, it scans websites for vulnerabilities and it says "here's where you're good, here's where you're bad, here's where your certificates are out of date." It gives you a report that's automatically generated, and it tells you how to fix it. We're giving that to local government for free."

These NCSC-developed tools will also become available to small businesses, too. The centre recently built a tool to eliminate spoof emails that appeared to be from HMRC; "The code that we used to stop HMRC spoofing, we're making freely available today. That means that if you run a small business with an internet domain address, you can work out who, if anybody, is spoofing you and what you might be able to do to thwart them. We're trying to do things that make it that little bit simpler for people who may not have the resources and time of a larger government or private sector organisation, just to make it a little bit easier to take sensible, risk-based decisions and make the improvements that will help. Because every little helps, in cyberspace – if you raise the bar a little bit, attackers can go elsewhere."

The NCSC's technical director, Dr Ian Levy, says blunt instruments are still too effective in cyberspace. "It's important to differentiate the sophistication of the attack with the level of the impact. The two are not correlated; you can have a really, really simple attack that causes a lot of national impact. Take TalkTalk as an example – a very, very simple attack had a huge effect across a large number of people. Whether it should have done is another discussion, but it did. It changed the public consciousness; a lot of the very sophisticated attacks don't have that same sort of impact on a large number of people. Some of them are not about disclosing large amounts of personal data, or stealing, or making money – they're about traditional statecraft, and that has a much lower impact on your average population. It can have a national security impact, but one of the things we need to change the narrative of is the difference between the sophistication of an attack and the impact of that attack."

State-level attacks

While much of the NCSC's work will be in making the UK a "hard target", as Martin describes it, for cybercriminals of all kinds, the centre remains a part of GCHQ. Its work will also encompass the new possibilities digital technology has opened up for espionage, diplomacy and war. At the centre of one of the exhibits shown to the Queen and other visitors on the opening day is a grey box, about the size of a biscuit tin, a few lights blinking on its front. Easily ignored by the passing dignitaries,

GCHQ tracked attempts to influence the 2015 election

this box is of particular significance in security circles. It is a programmable logic controller, or PLC. These controllers are found everywhere moving parts need to be automated and controlled – in factories, power stations, aeroplanes, trains, and automatic doors. In 2010, a mysterious and highly sophisticated piece of malware appeared that targeted one specific model of PLC, in a very specific configuration, and caused it to malfunction, causing serious damage to the equipment it controlled. The equipment it targeted was later identified as the enrichment technology used in the Iranian nuclear programme.

The display also contains a laptop. Tap a button, execute a command through the malware on it, and a light on the PLC changes from green to amber. In December 2015, an unknown hacker tapped just such a button. Moments later, the lights in 230,000 Ukrainian homes went off.

A member of NCSC staff who declined to be named said that his greatest worry with regard to this type of attack was that it could be used on the gas grid. "If the gas network was depressurised," he told me, "it could take up to a year to get it back." These are the more worrying scenarios the NCSC must imagine and plan for; a winter without central heating would bring the NHS to its knees, at the very least.

Jacqui Chard, the NCSC's Deputy Director for Defence and National Security, says that a national security level cyber incident could take many forms. "It's about the impact across government or across citizens," she explains, adding that at the most serious level, the NCSC helps to plan against and prevent attacks that would cause "serious damage, loss or disruption of critical services or systems for the nation – which could be critical national infrastructure, the parliamentary system, defence, our finance institutions, or our transport system."

"From a defence point of view," Chard says, the most serious type of cyberattack would be one that looks like an enemy preparing the battlefield,

that "impacts on the strategic planning for our military forces. Or, if we were subject to attacks on our soil, how we're going to co-ordinate – so, if communications between government at the highest level were affected. That's where we're focusing for the biggest risks for the country at the moment."

While attacks of this type are fortunately still mostly theoretical, it does look increasingly as if cyberweapons are capable of causing loss of life on a similar scale to the kinds of weapons that are bound by international treaties. Steps in this direction were taken in 2015, when the Chinese government agreed with the US and UK "not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information" (in the words of the China-UK statement). Asked why she thinks this statement did not include a statement on national security, Chard replies that "The business agreements that we've made are a matter of national security. They're for our prosperity as a country, so we absolutely see those as part of that."

The NCSC is housed within a relatively conventional office building

The new diplomacy

With the growing power of cyberattacks to cause devastating consequences across borders comes the thorny issue of determining where an attack has originated, who ordered it, and if a government was involved. It is likely that the difficulty of attribution will have profound effects on diplomacy in the future, and a key role for the NCSC will be to provide evidence of the involvement of other nation states.

Both Ciaran Martin and Michael Fallon have spoken publicly about a "step change" in Russian cyber aggression, but Martin says certainty is still hard to come by. "Attribution can be very difficult, and a lot of the detection work on state attacks is in the classified area of where we work, even though we work a lot in the open. But in general terms, in my three years of looking at these [incidents], sometimes you have direct evidence of named individuals with pictures, and sometimes you have very little clue as to even what country an attack might be coming from." Furthermore, "attacks could be coming from within a particular country, but that's not necessarily the same thing as being sponsored by that country, or even tolerated by the government of that country."

What makes international relations even more complex is that increasingly, and especially with regard to Russia, technology allows other "actors" to expose secrets and disseminate lies at scale. This is particularly effective when it comes to elections. The extent to which Russia may have been able to influence the US presidential election is the subject of furious debate, but the UK's political system is not immune to intervention either. Last year, GCHQ revealed that it had tracked and thwarted what Martin calls "activity" with regard to Whitehall servers. "There was activity we noticed," he says, "because we notice activity all the time, that was in and around institutions that may or may not be related to the possibility of an attack on the election."

Governments and political parties are going to have to recognise the threat this "activity" represents. Martin says no formal requests have been made by specific parties for help, but that he expects these requests to be made.

Ultimately, he advises that to safeguard British politics, "you need to look at the system as a whole, all the way through from government institutions to parliament, to institutions that are influential in political life, like the media, like think tanks – way beyond political parties, even to high-profile individuals whose views are of interest. It's about the totality of that. So we'll publish data and recommendations about how to mitigate these sorts of attacks, and we'll look at the most aggressive actors and try to find out what they're targeting. That's probably better than trying to predict the precise route of attack on the British political system."

For a more detailed investigation of election hacking, turn to p14.

The rise of ransomware and how to avoid being held hostage

Don't fuel the fire, says Avatu CEO **Joe Jouhal**, it only creates more victims

IN ASSOCIATION WITH

avatu

Four years ago, ransomware didn't even exist, not officially anyway. The new word was only added to the Oxford English Dictionary in 2012. At the time, it was mainly a problem for individuals who'd have their private files locked down and only released when a few hundred pounds worth of Bitcoin were paid. Although the general style of the attack has changed little in the last few years, the problem has grown, almost unimaginably, in scale. Today, ransomware is big business, thought to be worth a staggering £1bn-a-year and rising

It's a very lucrative organised crime, which is increasingly a thumping headache for businesses and other organisations, both large and small. A *Guardian* report said 40 per cent of businesses are thought to have been attacked last year, and one third lost revenue. Ransomware has been blamed for a variety of issues, including potentially putting lives at risk by crippling NHS hospital computer systems and causing thousands of operations to be cancelled, and shutting down all the payment machines linked to a whole city's public transport system.

More than 638 million attacks were registered last year, up from 2015's 3.8m. Last year, one single ransomware distributor was understood to be paid more than £1m for attacks it sent out.

But most worrying of all, a lot of organisations – almost three quarters of those infected, according to a recent IBM report – paid the money requested to unlock their data, and 70 per cent found the price of freedom was a five-figure sum, of up to £35,000. In a quarter of cases, the blackmailer's laughter echoed on; for even when money was paid, the release key didn't actually work.

In another sinister twist, thieves have started sharing between themselves the names of easy targets who've

BEE BRIGHT/SHUTTERSTOCK

previously paid up. This means if you're hit once, and you pay, you improve your chances of being a target again.

The police and security teams such as ours understand the motivation of people who pay ransom demands but we feel it's simply not the answer. It's a short-sighted approach. The more you feed the monster, the bigger it will become and more bites it will take.While we totally understand the desire of people to just pay up and quickly get their data and systems back under their control, it is neither the sustainable nor moral way of doing things.

The best way to stop ransomware being the weapon of choice requires organisations to stop being soft targets. This means doing the obvious: using the preventive methods, the firewalls, the AV software, installing updates quickly and having regular back-ups. But when it's impossible to always anticipate the thieves' next step, you need to concentrate on what you *can* control.

The best way to protect your data is to place it at the centre of your strategy. Make it your focus; know what you've got and where it's held. Understand how valuable and vulnerable it is and you will start making the best decisions.

Our long experience working with most UK police forces and many corporate investigators has given us deep understanding of what technologies and techniques are needed to stop cyber criminals and insiders doing damage in the first place.

Behaviour management systems can stop people doing wrong or risky things that are against company policy and it can teach them to be more careful at the same time. As half of all ransomware attacks come through email, the risk-savvy approach is to introduce measures to plug this route, and we've sourced innovative technology which does just that.

But this kind of action doesn't just improve your chances of warding off a ransomware attack, this investment and data-centric approach has benefits in other ways too. If you protect against ransomware, you also protect against many other types of damaging malware, threats from social engineering and you even prepare yourself to deal with the requirements of new data protection rules within GDPR. Getting GDPR wrong can cost up to €20m in fines.

It also keeps the money out of the pockets of organised crime gangs, who can be associated with everything from financing terrorists to supporting the drug trade. Not paying up and improving your data protection is both the sensible and sustainable business approach, and the moral thing to do.

The many faces of ransomware

- Ransomware is a problem for many different organisations. UK schools have recently been warned about ransomware being sent to head teachers cruelly pretending to be sensitive mental health advice for children or exam questions.
- Recruitment teams are being hit with ransomware masquerading as CVs.
- The National Crime Agency (NCA) recently warned about a tidal wave of convincing looking emails containing ransomware being sent to small and medium-sized companies, pretending to be from banks and building societies. More than half of all ransomware attacks are hidden in emails or their attachments.
- Ransomware has been hidden in 'fake news' updates and often disguised as online adverts.
- Thieves have created 'pyramid infecting'. They give people the key to locked files free, if they've purposely passed on the infection to other people in their network.
- Ransom demands of up to £54,000 each are known to have been paid in 2016.

For more information please visit: www.avatu.co.uk

End the victim culture – learn how to fight back against ransomware

Avatu has recently run a webinar on how to tackle ransomware, especially when it comes through email. Email is the most frequently used route for a ransomware infection.

Call **01296 621121** or email **cybersecurity@avatu.co.uk** to sign up to view the ransomware session or to arrange a call back to discuss your own ransomware defences and challenges.

China's strategy to become the world's strongest cyber power

Nigel Inkster, former operations and intelligence director of MI6, analyses China's efforts to impose order on its vast online community

When just over two years ago I began researching a book on China's cyber power, mainstream western media were full of stories about China's alleged programme of state-sponsored cyber industrial espionage directed against US and other western corporations. Following an agreement between Presidents Xi Jinping and Barack Obama in December 2015 that "that neither the US nor the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage" that story dropped out of the headlines. But the importance of China as a cyber power has not diminished and understanding China's capabilities and objectives in the cyber domain has become a key element in understanding its global strategic objectives. It is also an important prism through which to understand China's long struggle to achieve modernisation whilst retaining its cultural and political self-esteem.

China came out of the Cultural Revolution in a state of economic and technological backwardness that demanded urgent attention. Its new leadership was seized of the important role modern ICT would play. Although the internet did not become accessible to ordinary Chinese citizens until 1996, the subsequent take-up has been dramatic. China has over 700 million "netizens", the majority of whom access online service through smartphones. In 2015, the total value of online sales was $581bn, making China the world's largest digital marketplace. The Chinese government has ambitious plans to switch from an export-dominated

Mobile networks have helped bring internet access to more than 700 million Chinese people

HUMPHERY/SHUTTERSTOCK

China's online market is worth $581bn

economic model to one based on domestic consumption; and to move up the value chain to break free of a middle-income trap. A key enabler will be an Internet Plus strategy that aims to integrate the real-world and digital economies.

In pursuing this, China's government had to confront two vulnerabilities. The first is the potential of the internet to serve as a vector for subversive influences that challenge the Communist Party's legitimacy. The second is a high level of dependence on western – largely US – technologies and software, seen as a security threat. From the outset China's authorities sought to control online content through a combination of firewalls to filter externally generated content, regulation of service providers and censorship; the latter becoming ever more technologically enabled but still reliant on large numbers of censors and pro-government activists who promote and defend official views on social media sites such as Weibo.

The result has been a cat-and-mouse game in which China's netizens have sought to bypass censorship by relying on the infinite capacity of the Chinese language to generate homonyms for terms which are banned, giving rise to a rich lexicography of online dissidence. But it is a game the authorities are winning thanks to technology dominance and the huge manpower resources devoted to an issue seen by the leadership as existential. This is not to say that the Chinese internet is characterised by an atmosphere of sterile ideological conformity; in many respects it is more vibrant and anarchic than its western equivalent and has been used to good effect by its citizenry to hold officialdom to account. But first under Hu Jintao and ever more under Xi Jinping a climate of greater political and cultural conformity has led to popular bloggers –so-called Big Vs – being shut down. And China is unapologetic about asserting an approach to the internet based on the concept of cyber sovereignty, in effect its right to determine what its citizenry can access.

Meanwhile, China is pursuing a policy of indigenous innovation to reduce dependence on western technologies. Dependence on western ICT is such that when in 2014 Microsoft announced that it would cease supporting Windows XP it subsequently had to make an exception for China, such was its reliance on that system. That dependence will take time to erode. But there is a growing number of indigenous Chinese software companies, Chinese smartphones and other devices are increasingly competitive with western equivalents and Chinese entrepreneurs have shown considerable ingenuity in developing

China spent $22bn on western tech start-ups in 2014 alone

and marketing a range of online services. As the Chinese state seeks to impose greater order on what to date has been an anarchic and insecure Chinese cyber environment, new laws have imposed greater demands on western companies such as the provision of source code. China is seeking to leapfrog the west in key areas of ICT including artificial intelligence (AI), quantum encryption and quantum computing. And the Chinese government is facilitating the purchase by Chinese companies of western technology start-ups. In 2014, $22bn had been spent on such deals, which have significant medium-term implications for the competitiveness of advanced industrial economies including the UK, France and Germany.

The global outlook of China's leadership is dominated by the so-called Century of Humiliation covering the period from the mid-19th century up to the founding of the People's Republic in 1949 during which China was virtually colonised by the west. The determination not to repeat this experience has translated into a transformation of China's defence posture from a land-based, low-tech, mass-mobilisation force to one that is increasingly based on a capacity for naval force projection with a view to securing China's supply lines and protecting its growing range of overseas interests. Digitisation is seen as critical for China's efforts to develop armed forces on a par with its only real comparator, the United States. This is exemplified by an ambitious reorganisation at the end of 2015 which led to the creation of a new Strategic Support Force that combines signals intelligence, electronic warfare and information warfare capabilities within a single organisation that also has responsibilities for space-based activities. After a long period of coyness PLA officers now talk openly of China developing offensive cyber capabilities albeit at a "moderate rate" and in response to the activities of states such as the US.

This posture also translates into a more assertive foreign policy, no longer merely concerned as until recently with ensuring peace and stability to permit economic development. China probably does not aspire to replace the US as, in their words, "global hegemony". But it does wish to move from a global governance system dominated by the US and its allies to a world that is multi-polar and which respects different political and cultural systems. And to transition to a "new security concept" which while broadly respectful of international institutions like the United Nations, also subordinates customary international law to the interests of major powers. Here too the cyber domain plays a major role with China championing its vision of a global cyber governance and security order where the USA is no longer predominant. This vision enjoys some support in the developing world, not least due to the activities of national champions such as Huawei and ZTE who are building and operating core backbone IT infrastructure systems in countries that would otherwise remain on the wrong side of the digital divide.

To revert to cyber espionage, it is now clear that US threats of financial sanctions against Chinese companies deemed to have benefited from the theft of US intellectual property (IP) persuaded China's leaders that this particular game was no longer worth the candle. The "noisy" reduplicative exploits that characterised so many cyber-attacks emanating from China are now much less in evidence. But cyber capabilities have become a major enabler of Chinese statecraft and are inter alia reducing the space within which overseas-based opponents of the regime can operate. For better or worse China is transitioning from becoming a large cyber power to a strong cyber power and can be expected to play an increasingly prominent role in this space.

The west will have to get used to living in a world in which it no longer enjoys the unquestioned technology dominance to which it has long been accustomed.

The bigger they are, the harder they fall

Even the largest companies have got their approach to cyber security wrong, writes CEO of ECSC Group plc Ian Mann

In terms of cyber security, there is no such thing as too big to fail. Across politics and business, we have seen even supposedly tech-savvy institutions like TalkTalk and Yahoo fall victim to serious breaches of their organisations.

From hobby hackers to elite internet criminals and foreign intelligence agencies, who have honed their skills purposefully to topple the top, against a backdrop of digitalisation any and all companies are facing a threat they cannot afford to ignore.

The lines, it seems, between perception and reality are blurred. TalkTalk is a very large technology enterprise with £1.8bn revenue. The leap to assume, then, that it should have both the technical resources and management focus to be protecting its customers and its own sensitive information, does not seem a far one to make. However, the reality for large technology companies driven by profit expectations and a faster moving technology and service change road map, is that they struggle with even the basics of security.

A year on from TalkTalk's major breach, the report from the Information Commissioner's Office (ICO) didn't tell a story of some malignant mastermind, capable of advanced internet espionage. Rather, it said: "TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate (its) systems with ease. Yes, hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action."

With over 15 years' experience in dealing with cyber security incidents, we here at the ECSC Group plc agree. TalkTalk's oversight is symptomatic of a concerning industry-wide ham-handedness: the out-of-date software, lack of encryption for customer data and lack of response to previous known incidents.

If there is any lingering doubt as to the gravitas of the impact that poor cyber security can have on a company, consider that TalkTalk was fined the near maximum £400,000 for its lapse in judgement which led to the theft of personal data of close to 157,000 customers. How many companies could survive such a breach? The risk is not just to their bank balance, but to their reputation and capacity to draw future business as well.

It is worth noting that under the new General Data Protection Regulation (GDPR), an EU Regulation set to become law in May 2018, TalkTalk's fine could actually have been as high as £72million.

Still, however clumsily complicit, it would be disingenuous to suggest that TalkTalk actively intended on its failure. The root cause of many security breaches for companies lies in a lack of awareness, from the boardroom down. Frontline staff are trained insufficiently to identify risks from the offset and those wielding the budget are often floored by the smokescreen of a sales pitch by security product vendors. Not all security is effective security; it's worth remembering that.

One important truth remains: in 15 years of ECSC incident responses, only a handful have ever reached the public domain - most incidents are contained and kept secret. However, in addition to significantly higher fines, the GDPR requires all incidents to be reported to the ICO within 72 hours - so there will be no hiding incidents from 2018.

For more information please visit: www.ecsc.co.uk

Delude and conquer: inside the Russian messaging strategy

Cyberattacks, leaks and fake news have changed the electoral landscape. Will Dunn asks Dr Lucas Kello and Philipp von Saldern if, this year, Russia will win every election in Europe

The French television network TV5 Monde is the Francophone equivalent of CNN or BBC World News – a global, 24-hour current affairs network. It claims to be one of the three most widely available TV networks in the world. On 8 April 2015, without warning, all of TV5's international channels went off-air.

It quickly became clear that the outage was the result of a cyberattack. Responsibility for the hack was claimed almost immediately by a group called the 'Cyber Caliphate', ostensibly from the Islamic State; the group also hacked TV5's website and Facebook page, where it posted jihadist propaganda. However, the sophisticated methods used – systems were compromised weeks in advance using espionage techniques, custom software was written to target the encoders used by the TV station – pointed elsewhere. French and US security services found that the most likely perpetrator was a group that had previously launched cyberattacks on the White House and other NATO governments. The hackers collectively referred to themselves at the time as "Pawn Storm" or "APT28". More recently, the group has identified itself by another name: Fancy Bear.

Following its actions against the World Anti-Doping Agency, the Democratic National Congress, and the governments of the Netherlands, Germany and the Ukraine, Fancy Bear has been linked by security researchers to Russian foreign intelligence, with a number of security firms stating publicly that it is likely to be sponsored by the Russian government.

At the time, the motive for the TV5 hack was unclear. It was suggested that Russia – if it was Russia – may have been testing its capabilities. In the light of other attacks, however, it could be viewed as having been a test not only of Fancy Bear's ability to disable a major TV network, but also of its ability to push a message – about immigration and French

SHUTTERSTOCK / BESTPHOTOPLUS

The FSB headquarters in Moscow. Vladimir Putin once said that "there is no such thing as a former KGB agent."

This year's elections offer the chance to help dismantle the EU

military involvement in Syria – into other media and social networks.

Since TV5, other major cyberattacks have displayed this two-pronged form. The theft of data from the servers of the Democratic National Congress prior to the US presidential election was not just a theft; the stolen emails and documents were not exploited privately but released publicly, in a manner and to a schedule that benefited Russia's preferred candidate in the US presidential election. A declassified version of the findings of the CIA, FBI and NSA recognised the two-pronged approach, stating that it "blends covert intelligence operations—such as cyber activity—with overt efforts by Russian government agencies, state-funded media, third-party intermediaries, and paid social media users".

It is impossible to say exactly how many votes were decided by the "Russian messaging strategy," described in the US intelligence community's report. But it is certainly true that Moscow's preferred candidate won.

Towards the end of the intelligence report, the Russian messaging strategy is described as "the new normal". Following its (real or perceived) success in the US, "Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide." This year, the Russian messaging strategy could bring down a target more valuable to Putin than even the US presidency: the EU.

In March and April, the Dutch and French elections offer the chance for Russia to "boost", in the language of social media marketing, candidates that would call referendums on their EU membership.

"There are at least four ways in which a foreign adversary can subvert the democratic elective process", says Dr Lucas Kello, senior lecturer in international relations and director of the Cyber Studies programme at Oxford University. An adversary can manipulate voters using an overt public message – "disseminating unfavourable news, real or fake, about the target candidate to diminish his or her popular support," or "by unobstructively but demonstrably penetrating voting or registration machines with malware in order to erode public confidence in the voting outcome." They can affect how many people vote, "by attacking voter registration systems to diminish turnout among sectors of the electorate that tend to favour the target candidate," and, finally, they can directly compromise the result by "attacking voting or vote counting machines with malware to alter the voting results."

In Holland, voter confidence may already have been eroded. Earlier this month, the interior minister Ronald Plasterk announced that all votes in the March election will be counted by hand. Elections become more complicated under the Russian messaging strategy; a government that protects itself against one of the attacks Kello describes automatically calls into question the integrity of its own electoral process.

In France, ANSSI director Guillaume Poupard described last month "a real strategy that includes cyberattacks, interference and leaked information." The current favourite – strongly pro-European candidate Emmanuel Macron – has become the main target. Macron's campaign manager, Richard Ferrand, said this month that "hundreds and even thousands" of direct hacking attempts had been made from within Russia. At the same time, Macron has been subject to a deluge of unsubstantiated coverage, including reports that he is an "agent of the American banking system", and that he is backed by a "very rich, gay lobby". Wikileaks – the website that released the hacked emails of the DNC – claims to have thousands of hacked documents on Macron. If this is true, it is likely that they will be released at a time designed to cause maximum damage to his campaign. Votes that do not go to Macron may then head further right, to the vociferously anti-EU Marine Le Pen.

One of the things that makes the Russian messaging strategy so effective

What Russia is doing may not be illegal

is that it is at least partly legal. As Dr Lucas Kello points out, "International law does not prohibit interstate espionage. Although almost all domestic penal codes criminalise the unauthorised access to a computer system to seize its data, no international treaty forbids this activity. Disruptive or destructive cyberattacks may breach treaty obligations, but only if they produce consequences that are similar to an act of war or a use of force." This, says Kello, is new territory for diplomacy. For the first time, one nation can replace another's government without invading. "One of the distinguishing features of virtual weapons is that they can significantly affect national security – for example, if they alter electoral outcomes – without satisfying those rigid legal criteria."

Following the Dutch and French elections, the grand prize for the Russian messaging strategy will become available in September, when Germany elects its next Chancellor.

The relationship between Angela Merkel and Vladimir Putin has never warmed beyond a frosty mutual tolerance. Merkel grew up behind the Iron Curtain in East Germany. In a Stasi document from 1984, an informant described the young Merkel as "very critical" of the Soviet Union, which she saw as "a dictatorship". Putin was an agent of that dictatorship, as a KGB agent in Dresden. As heads of state, the tone for their meetings was set in 2007, when Putin had his large black labrador brought into a meeting with Merkel – who is known to have a profound phobia of dogs. The German Chancellor's response was withering. "He's afraid of his own weakness," she explained of the incident, reflecting that "Russia has nothing, no successful politics or economy. All they have is this." As the most powerful woman in the EU, Merkel presided over an economy 13 times the size of Russia and enjoyed a strong relationship with the US. A decade later, with a pro-Putin president installed in the White House and the EU's second-largest economy preparing to leave, Merkel does not hold so many aces.

"There is a serious threat of interference in our upcoming federal elections," agrees Phillipp von Saldern, President of the Cyber Security Council of Germany. "But, and this is very important, such attempts can come from everywhere. Different parties could be interested in attacking our elections. These could be private actors - script-kiddies, hacker-syndicates, criminal organisations or even companies. On the other hand we have other states or organisations with strong ties to a state."

The first step in protecting elections against attacks, says von Saldern, is to consider "every attacker, no matter what background he has. To avoid direct attacks as the one on our Bundestag, we have to keep our security-measures as up-to-date as possible. This requires constant knowledge transfer between different authorities on a federal level, as well as with our "Länder"[local government] authorities, but also with our economy and with international partners."

"Protection against fake news," he adds, "is just possible, if we cooperate with the platforms where they are posted, such as Twitter or Facebook, and if we find clear regulations about their responsibilities. We also need to sensitise our society to the subject of fake news, so that our citizens proof properly what they read and are willing to report suspicious information."

Facebook and Twitter, he says, have "a responsibility to prevent [fake news]. Major platforms, such as Facebook currently have already announced, that they will do more to prevent fake news on their pages, but it is still unclear how this should work. To my opinion the only way to hold such online-platforms to their responsibility are clear regulations from our state."

"Time is running out," he concludes. "It is very urgent that our government acts here as soon as possible."

Dr Lucas Kello is director of the Cyber Studies programme at Oxford University. His book, The Virtual Weapon and International Order, will be published by Yale University Press later this year.

No fake news is good news

Stories that can't stand up to scrutiny have no place on the internet, writes Digital Assurance's Jordan Orlebar

The internet enables huge swathes of conversation and access to intellectual material. In the shadow of this uprising we are beginning to see the darker side of sharing. The algorithms behind content propagation elevate not only the most applicable to our current online lens, but also the most popular, and sometimes the most damaging. At its best fake news is a freight train of amusement, distraction and disruption to debate. More recently it has even been a vehicle to balkanise political support. At its worst it's life endangering. In December last year, Edgar Maddison Welch fired an assault rifle inside a pizza restaurant in Washington, D.C. Welch was convinced by a conspiracy theory purported through online media that the establishment was harbouring children, as well as conducting indecent and illegal business.

Technological giants Facebook and Google have pledged to aid in the reduction of fake news prominently appearing in our online spheres. Google has proposed to remove the ad-revenue from articles and sites found to be purporting fake news. Facebook has followed suit. Facebook also previously applied for a patent outlining a new set of algorithms to leverage machine-learning in order to flag and remove "objectionable content" more easily. This algorithmic solution will allow people to submit content to be moderated, which will then be filtered through an automated decision making process and if applicable passed on to human moderators to sustain or overrule the objection of it.

Unfortunately machine-learning is as fallible as the information it is given. Any system that weighs user input can be gamed, and any system that trusts user input implicitly can be abused. Handing the results of the system over to a human moderator does not help in solving the problem either, it simply moves it. The whole effort is circularly redundant. An 'AI' solution in the middle will only filter down content from the totally objectionable to the questionable, leaving us back at square one albeit it with a lesser amount of content to judge.

A better solution would be to give people easy ways to assess the source of the information itself (e.g. where is the information from, who authored it, how long has the site been around, does the site have any agenda now or historically, has content been rebuked or supported before by third party adjudicators etc.). Facebook's potential solution intends to select content for moderation based in part on attributes of the user that flagged it. The suggestion here is to move the attribute selection from the user to the content and let individuals decide based on the facts.

Both Google and Facebook's proposed plans have their flaws. Removing ad-revenue from fake news producers will only quell the most inflammatory of stories. The actors in this play that rely on subtlety to sway their victims will continue to be Iago in the eyes and ears of those that dwell in the warmth of their echo chambers. Furthermore asking people to vote on content sounds democratic but critically ignores all of the information that gets lost as a result of a binary decision.

We all must ensure that independent thought and legitimate information continue to be valued and discussed even if they do not align with our own personal beliefs. Enabling people to make their own decisions when given the entire scope of the information at hand is the way forward and can only be achieved if we are persistent enough to make it a reality. Therefore before you share that next sensational link, give a little thought as to who wrote it and why.

As the chief legal advisor to Edward Snowden, Ben Wizner works at the forefront of civil liberties and technology. He speaks to Will Dunn about mass surveillance and the threat it represents

Databases of ruin

A Skype call with Edward Snowden's lawyer is different from other Skype calls. Beneath the introductions and the courtesies sits the question of who else is listening. Among the NSA data released by Snowden in 2013 was a training document which confirmed that "sustained Skype collection began in February 2011". Since that date, the NSA has been able to listen to and record any Skype call. Does Ben Wizner think they're listening, right now?

"I guess I would say… probably not." Wizner is not one for dramatic speculation. He first sued his government for torturing its own citizens more than a decade ago; his work is dramatic with embellishment. Wizner joined the ACLU months before 9/11. Ten years later, he became the director of the Speech, Privacy, and Technology Project. In 2013, he became principal legal advisor to the world's most wanted man. In his defence of Snowden and his work for the ACLU, Wizner works at the point where civil liberties and national security meet. Increasingly, he says, it is hard for the legislation that protects civil liberties to keep up with the methods available to those who would infringe them.

"The fundamental issue," says Wizner, "is simply that surveillance used to be expensive, and now it's cheap. That's something that we have to confront, centrally, as one of the main challenges of our time. It used to be that our privacy was protected more by cost than by law, but that cost protection is gone. If governments wanted to know where you were, a generation ago, they

National Security Agency headquarters, Fort Meade, Maryland

had to assign a team of agents to track you 24 hours a day. There was no real legal barrier to doing that, but there was a huge resource barrier. There had to be a pretty good reason for it. Now, our technological systems are passively collecting all of this intimate information about all of us. The cost of storing it, forever, has plunged from being very expensive to almost trivially cheap. So we're going to need law and policy in places where we didn't need it before. We're going to need to figure out what role law needs to play in a world where governments have the financial and technological capability to record and store virtually complete records of our lives."

Many technologists have observed that the advances in computing and communication of the past few decades have allowed us to sleepwalk into an almost perfectly pervasive surveillance state. Wizner advises viewing any argument for extension of these powers with extreme caution. " I think the way to understand this is that even people who seem willing to exchange personal privacy for a measure of safety wouldn't want video cameras throughout their house, including in their bedrooms, on at all hours of the day. They wouldn't want drones with sophisticated cameras hovering over their homes and communities, 24 hours a day, recording every movement in the streets. But mass metadata surveillance achieves almost the same effect. If the police can know, without any legal restriction, where your phone is at any hour of the day, what other phones are with it at any hour of the day, and they can get months of this information and put it together, they can paint a remarkably intimate picture of your life. Who you're sleeping with, whether you pray, whether you drink, if you've had an abortion. All of this information can be very easily reconstructed from the metadata that we leak on a daily basis now."

The argument for further extension of government surveillance almost justifies its means by the threat of terrorism. Wizner calls this a "bait-and-switch" – a ruse, to secure powerful surveillance in the name of preventing extremist attacks, but then to pass these powers on to other authorities. Against terrorists, he points out, "mass surveillance is not terribly effective as a predictive measure. Collecting billions of communications in order to predict extremely rare events is not effective. The system gets overwhelmed with false positives, no matter what measure you're using. That's why the investigatory groups that were put together following the Snowden revelations uniformly reached the conclusion that collection of the metadata for all US phone calls didn't lead to either the prevention or the discovery of any terrorist attack or activity."

For domestic law enforcement, however, vast databases of the details of citizens' lives represents a goldmine. Wizner calls it "a kind of surveillance time machine. They would be able to hit rewind on the database, and to reconstruct all kinds of things that had happened. Because they could be extremely useful for solving crimes, the capabilities will migrate from intelligence into law enforcement. And then, our societies are going to feel very different – when every police officer with a smartphone has access to the kind of information that the NSA and GCHQ collect."

In the UK, Wizner's forecast has already precipitated. Under the Investigatory Powers Act, the communications data of any UK citizen is now collected by default and may be provided, without a warrant, to any police force. The data is also available, again without a warrant, to most government departments, as well as to such well-known anti-terrorist forces as the Food Standards Agency and the Welsh Ambulance Service.

What kind of state does Wizner think this will lead us into? "Here, I like to quote the security technologist Bruce Schneier, who asks 'how do you feel when a police car is driving right next to you? Imagine having that feeling all the time.' Some people might say, 'oh, I just feel safer'. But most of us don't just feel safer. We feel nervous, we feel watched, scrutinised. It absolutely would affect our willingness to take risks, to engage in behaviour that's not fully sanctioned – the kinds of things that free societies need to grow and develop."

Whether the unprecedented mass surveillance now being conducted by the governments of the UK, US and other nations on their own citizens will lead inevitably to totalitarianism is debatable. What is inevitable is that when governments collect data on their citizens, it falls into other hands. In 2015, it was revealed that councils in the UK suffered data breaches at an average of almost four per day, losing the personal data of children on 658 occasions in three years. In 2012, the NHS lost 1.8 million patient records. In 2008, HMRC lost the

Snowden says computing has reached its "atomic moment"

personal data of 25 million taxpayers. The list of incidents in which the UK government has lost, stolen and carelessly handled databases of its subjects' data is thousands of items long.

"We've already seen networks of hackers obtain vast amounts of personal information, and convert it into profit," agrees Wizner. It is absolutely the case that we're going to have to come to see that aggregated data is not just something that has beneficial uses, but something that creates real liabilities for us."

However, Wizner says we should not compare the data being collected on us by mass surveillance to traditional government records. It is more personal than that. The data breaches that will result will be closer to the 2015 data breach of Ashley Madison, a dating website that enabled people to have extramarital affairs. Publishing of the site's user database was linked to suicides in two countries. Wizner says he and his colleagues refer to such deeply personal information as "databases of ruin", because "they contain within them the seeds to ruin any of us."

That a government database could contain the seeds of your ruin – the means to impersonate you, jeapordise your position or make public the evidence of anything you've done which you'd rather wasn't publicly known – is not, says Wizner, a paranoid idea about the future. "That information sits in government databases today. And not just our own government. The Chinese government was able to breach the database the Office of Personnel Management, which does all of the background checks for people who work in sensitive jobs in the United States. Millions of records, of the most sensitive kinds of information, are now available to a foreign government."

Wizner says last year's dispute between the FBI and Apple, in which the technology giant refused to crack the security on its iPhone in order to aid the agency's investigation of the San Bernardino terrorists, is a good example of law enforcement's failure to recognise that data security can be more important than forensic capability.

"Many former high-level NSA officials actually took Apple's side in that dispute. They argued that it was actually more important for Apple to be able to create government-proof security on a global scale than it was for US law enforcement to be able to break into this one phone. They know that if Apple has to engineer its product to allow the FBI in, then it will also have to allow in the Chinese military, and Russian intelligence, and other governments."

So how can civil liberties be protected in this emerging state of cheaply available, barely regulated surveillance? "There are two parallel reform conversations that need to take place. One is about what kind of laws we need to pass, and how our courts can act as a check on government. The other is on the technology side - how can we build up our defences. The answer to the second [question] is encryption."

The great benefit of encryption is that "it can assist citizens even in authoritarian states. We could have the best surveillance reform imaginable in the US – we haven't, but we could – and it wouldn't protect anybody in Russia or China. On the other hand, if the technology platforms that we're using make it difficult or impossible for governments to engage in mass surveillance, that's something that could be a benefit everywhere."

Wizner says it's crucial that these issues of privacy and security are seen as international, because the means are so easily to sell and transport that one country's surveillance capabilities soon become another's. "It would be a mistake if everyone in the world viewed the Snowden revelations as a story about the NSA's activities and capabilities. Snowden likes to say that we have reached the 'atomic moment' for computer science. But proliferation is much faster; it doesn't require all of the complexity that nuclear proliferation has required. So now is the time for us to be developing laws about how we're going to deploy those technologies against each other."

Successful cyber security can't be cloned

Effective protection must be specialised, not standardised, writes Secure Thought director Mark Lewis

Secure Thought Ltd was established in 2007 as an independent security consultancy on the back of my experience as a leading member of the then MOD Defence Computer Incident Response Team based at Corsham, Wiltshire. My work has taken me all over the world and I have had the pleasure of meeting and working with some of the world's leading experts in the cyber security field. This specialist group spent time studying the technical specifics of sophisticated attacks and producing the tools and processes to detect, react to and prevent many that we know today as the APT. This was my training ground, at the centre of the discovery and categorisation of cyber warfare in the form that we understand today.

My early experience has formed the basis of many of my security philosophies, mainly, "it's only a mater of pressing the right keys, in the right order to gain malicious access to any system." If a threat actor wants to gain access to your corporate system and they have the motivation; it is only a matter of time.

In today's cyber world organisations are still reliant on a security industry that follow two basic rules:

1. Identify as malware, attack vectors and viruses as possible.

2. Concentrate on mainstream, known events and attacks.

Many organisations have become reliant on this methodology, as it covers the known battle ground and is accepted as industry best practice. We are now in a world where the industry's best practice has become the standard for security, but are we right to accept this as the modern cyber defence strategy? These days, the cyber security industry is driven by the need to prove that they are doing the best they can. Usually by gaining certifications that show they meet the level of security maturity in their specific industry. My main concern for the future of cyber security is whether the need for standardisation has had a detrimental impact.

The term industry best practice has become the driver for many organisations' security strategies. However, these best practices only form a security baseline, which leads to minimum investment in the cyber industry as a whole. The drive to invest in education, equipment and capability is now based on the minimum the industry needs to achieve to certify and standardise the cyber market place.

The past decade has seen many individuals drawn to the industry by the massive investment from both government and corporate business. In an attempt to reduce the skills gap, we have built the cyber security clone. Many of the early specialists in this area set up training companies to meet the demand. The syllabi became standardised and receptive, churning out cyber security clones at a massive rate. We have created a workforce who can work at an operational level, who are fully dependent on the security tools that have been given to them.

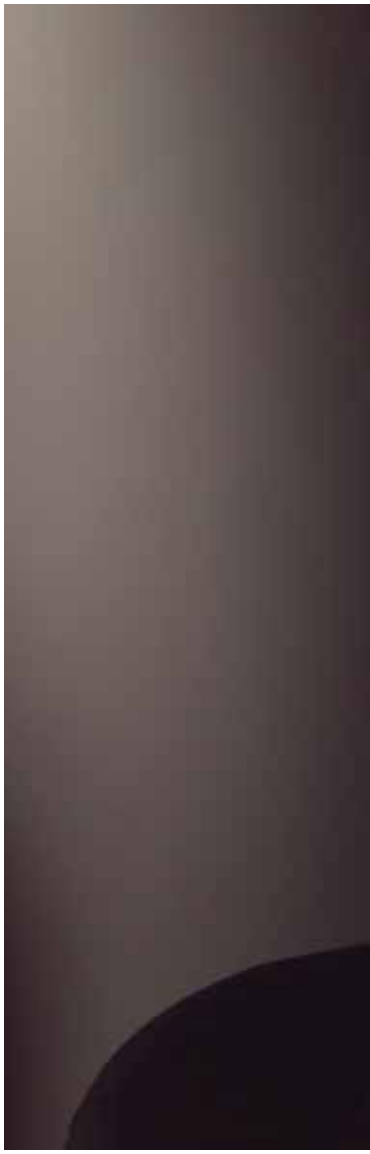
It was too late, the world had accepted that this was how the cyber security industry should look. A world of cyber clones that only completed their basic training, using best industry practice as a baseline for their understanding and experience.

As specialists, we need to understand the limitations we have placed on the collective cyber security industries' capabilities to protect cyberspace from future attack methodologies. The realisation is organisations are basing their security and risk modeling on an generalised security industry driven by a mass-market business philosophy.

IN ASSOCIATION WITH

SECURE Thought Ltd

Online deception can be a threat to people's mental and physical health, warns Professor Monica Whitty, cyberpsychologist at the University of Warwick



Hacking the heart: the psychology of scams

Con artists have been scamming victims for centuries. However, because the internet allows criminals to target many more victims, in the last 10 years we have witnessed scams on a global scale. In the UK in 2016, it was reported in the National Crime Survey that citizens are 10 times more likely to be robbed while at their computer by a criminal based overseas than to fall victim of physical theft (Office for National Statistics, 2016). In my work in the Cyber Security Centre at the University of Warwick, WMG, I have been leading inter-disciplinary projects that attempt to understand the psychology of scams and find effective methods to detect and prevent them. In particular, we have focused on mass-marketing frauds (MMFs).

Not all readers will be familiar with the term MMF; however, most would have encountered at least one of these in their lifetime. MMF is a serious, complex and organised crime. Examples include foreign lotteries and sweepstakes (in which the victim believes they have won money from a lottery and are told to pay a fee in order to release the funds); '419' scams (advance-fee fraud, in which

JOANA LOPES/SHUTTERSTOCK

victims believe that for a small amount of money they will make a large fortune); and romance scams (taken in by a fake online dating persona, in which the victim sends the fake persona money). Some MMFs are low-value, one-off scams on large numbers of victims, whilst others involve developing a relationship (e.g romantic, business, friendship) where money is defrauded over time, again with simultaneous or sequential victims.

Victims of MMF suffer both financial losses and psychological impacts, with the latter sometimes outweighing the former, even when large sums of money are lost. One of our motivations to investigate this particular cyber crime is the severity of this psychological harm – in some cases victims have been known to commit suicide. Common reacions to being scammed include shame, guilt, embarrassment, depression, grief, anxiety and loss of trust.

Catching and prosecuting MMF criminals is difficult, for three main reasons. Firstly, the criminals often live in a different country to the victims. Secondly, the methods they use make them difficult to trace, and thirdly, prosecution is very time-consuming, owing to the large amounts of online data that need to be analysed to establish evidence.

Although disruption tactics are important, we have taken a more victim-oriented approach to protect users from MMF. Our work has involved interviewing victims of MMF to gain a greater understanding of why they believed they were tricked and persuaded to give money to fraudsters as well as to map out the anatomy of these scams.

In my work, I have argued that

Many victims find it hard to delete scam messages

criminals are able to exploit the media they are communicating within to develop hyper-personal relationships with victims (especially victims of a romance scam). Communicating in online spaces can potentially isolate victims from friends and family to allow the criminal to become the dominant person in the victim's life. A synchronous and long-distance communication in the form of emails, texts and instant messenger allows criminals to be very strategic in the stories they create and the messages they send, creating the perfect online lover. In fact, many of the victims of romance scams that I have spoken to find it difficult to delete messages and photographs sent by the criminal, even after it has been revealed to them that they have been deceived.

We have also researched the victimology of different types of scams, considering demographic as well as psychological factors. Our research is finding that different types of people are susceptible to different types of scams. Many romance scam victims, for instance, have been found to be middle-aged, educated women who score highly on psychological measures such as impulsivity, addictive disposition and trustworthiness.

One of the novel methods we are currently researching to detect and prevent MMF involves a team of computer scientists: Professor Rashid, Dr Stringhini, an expert in human-computer interaction; Professor Sasse, a criminologist; Professor Levi; and a philosopher, Professor Sorell. The work we are undertaking involves developing a proof-of-concept automated agent to identify communication with a potential scammer and hoping to do so prior to the 'sting' taking place. The agent will need to make decisions about the probability of a victim communicating with a scammer by drawing upon their personal data.

One of the challenges in our research is the human element. MMFs, unlike phishing or even spear phishing, are especially a challenge to detect because they typically involve communication with another person, rather than a bot – this means that scripts can vary and are more complex. Often the criminal is developing a relationship that appears authentic to the users (romantic, friendship, working relationship) over a long-period of time prior to asking for money, and they can vary the communication when a user demonstrates a lack of trust. They can also use multiple media channels to communicate with the user.

The research being undertaken in our project is drawing from psychology, media and communications, criminology and linguistics to help identify deception and persuasive communication, and evidence of the "grooming" often found in MMFs. We are also interested in identifying the online identities, other communication and online behaviours typical of scammers as well as victims. By examining socio-technical features such as the use of the same profile photographs, descriptions across multiple profiles and patterns of interaction and contact with other users (e.g. login times), we can help to spot MMF earlier.

Importantly, we will be considering the ethical and social challenges associated with detecting and preventing MMF. For example, questioning the ethics of drawing in personal data from genuine and disingenuous people to assist in decisions regarding the identity and authenticity of another user. Moreover, we are interested in considering the ethics involved in how we ought to treat victims who cross the line and knowingly become "money mules" in order to recoup their losses. Should they also be treated as criminals?

As we produce papers we will present our latest findings on the DAPM website, and we are looking for volunteers to help us with our research. If we're successful, we hope prevent some of the most damaging and upsetting cyber crime.

Can the UK deliver where it needs to in digital skills?

Cohesion between industry and academia is key to training future generations in cyber security, says Bournemouth University's Dr Christopher Richardson

Our hyper-connected world, as a pervasive network of socio-technical systems, digital services and applications, has an expansive, active and evolving cyber threat to e-commerce, privacy, data protection, intellectual property, political interference and is raked by a plethora of fake news.

The National Crime Agency's (NCA) 2016 report said that: "The long-term impact of a cyber attack could include substantial loss of revenue and margin, of valuable data, and of other company assets," and "the impact of litigation costs (and, with the arrival of new regulations, potential fines), the loss of confidence from reputational damage and possible executive-level dismissals could also result in immediate and material loss of shareholder value."

It was essential, therefore, that the 2016-21 government's National Cyber Security Strategy's own development programme has galvanised the Department for Culture, Media and Sport (DCMS) to create this recently announced Cyber Schools Programme "to find, finesse and fast-track tomorrow's online security experts."

Government, businesses and individuals are all beginning to realise the damage unsolicited man or machine cyber threats can cause. They can disrupt, corrupt or endanger our society and it comes with little surprise that there is a critical shortage of cyber security professionals.

With the £20million available (from the £1.9billion budget committed to cyber security by former Chancellor George Osborne in 2015); DCMS wants to deliver an extracurricular school programme for at least 5,700 students. DCMS wants "an army of expert external instructors teaching, testing and training teenagers selected for the programme, with a comprehensive cyber curriculum expected to mix classroom and online teaching with real-world challenges and hands-on work experience."

The programme, though, cannot achieve its aim in isolation. It's going to take a multi-sectorial, collective effort to deliver this vision. The eventual provider will have the flexibility to decide an appropriate way to deliver the DCMS Cyber Schools Programme with its target to start with secondary school pupils to complete a four-year course, probably utilising NQF Level-2 (Certificate) and Level-3 (National Diploma) qualifications supplemented by recognised security skills qualifications with its pilot beginning in September 2017.

Since 2007, with the National Information Assurance Strategy, Objective 4 of the 2010 National Cyber Security Strategy and now with the well-funded 2016-21 Strategy, we have seen a desire to professionalise the security of our digital services and economy. To meet this demand, DCMS, The National Cyber Security Centre (NCSC), GCHQ/CESG, Cyber Security Challenge UK, NCA, CREST, The Tech Partnership (formally e-skills), IISP and The Office of Cyber Security and Information Assurance (within the Cabinet Office) all have a part to play, but it's going to have to be a public (academia and schools) and private (corporations and SMEs) collaboration that will have to deliver this essential component to our national defence and skills capability.

Better liaison and outreach of universities with further education colleges and mainstream schools, with better cyber laboratories, virtual learning environments, peer-to-peer skill training supported by industry academies will provide the initial impetus to bringing this opportunity to learn necessary cutting edge cyber security skills to students.

WHAT WOULD YOU DO?

BE PROACTIVE!

Prevent
with Cyber Essentials and IntaForensics

Cyber Essentials is a Government-backed, industry supported foundation for basic cyber security hygiene. The Scheme has been carefully designed to guide organisations of any size in protecting themselves against cyber threats.

React
with Incident Response Support from IntaForensics

If an incident occurs, you cannot afford to bury your head in the sand and hope that it will go away. A rapid, decisive and professional Incident Response could be the saviour of your business.

Investigate
with IntaForensics PFI Specialists

The faster an Organisation responds to a potential breach, the lower the likely impact will be. Deal with a company which has substantial resources to deploy quickly to identify the causes and methods by which your cardholder data has been compromised.

Stay Secure
with IntaForensics Qualified Security Assessors

IntaForensics are accredited to offer specialist consultancy for compulsory Payment Card Industry Data Security Standard (PCI DSS) compliance and offer in-house technical expertise to further improve network and information security.

IntaForensics

+44 (0) 247 771 7780
www.intaforensics.com
cybersecurity@intaforensics.com

PCI Security Standards Council
PCI FORENSIC INVESTIGATOR™

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

CYBER ESSENTIALS
IASME Consortium
GOLD

GDPR is the foundation for future strategy

UK plc is failing to appreciate or finance data protection requirements, according to Dr Adrian Davis, managing director at EMEA, (ISC)²

The United Kingdom may be preparing for Brexit, but it appears committed to EU regulation when it comes to its cyber security strategy. The UK government's cyber security regulation and incentives review, published late last year, concluded that the EU General Data Protection Regulation (GDPR), with its reporting requirements and financial penalties, represents a significant call to action for industry and a prerequisite for doing business in the UK. It also suggests that GDPR provides a solid basis to demonstrate cyber security by declaring that there is no need for new cyber security regulation.

The government can be applauded for its position, while companies should welcome it as an opportunity to demonstrate commitment and the ability to manage cyber risk. Let's hope the opportunity is taken. Experience to date, however, gives reason to worry that it won't be.

As a non-profit organisation of certified cyber, information, software and infrastructure security professionals, (ISC)² and its EMEA Advisory Council have established an international GDPR Task Force of certified information and cyber security professionals actively charged with implementing GDPR to track and curate frontline experience with the regulation. First observations from the group are that a current lack of business buy-in is preventing implementation projects from getting off the ground. Business leaders are not appreciating the requirements placed on them, are unclear about their role in the process and not anticipating the resources (both human and financial) required. Progress that is being made tends to be linked to the rollout of new initiatives, leaving gaps in addressing existing systems and processes.

The UK government has made it clear that they expect organisations to manage their own risk in respect to sensitive data and online presence. Their review acknowledges that each organisation and its IT is unique, and states that mandating specific controls would not work as they would become out of date very quickly.

Given this, GDPR cannot be treated as a tick-box exercise or even a compliance issue. The requirements are too broad and expectations too high for companies to adopt such an approach.

Organisations must become proactive and agile in their efforts to deal with the requirements of the regulation and the dynamic and ever-changing cyber risk landscape that organisations find themselves in. Significant resources and budgets must be allocated to the review of all processes, security controls (managerial, technical and procedural) as well as approaches for data collection and storage.

For cyber security professionals, the government's review supports our desire to be trusted to get on with the job and deliver. We can be expected to highlight its results – and the emphasis placed on GDPR – to our boards, our CIOs and legal functions to help us gain the support needed and to convince business to recognise their role in such an enormous task.

The window of opportunity to show that we can deliver may not be open for long. The UK government has reserved the right to re-examine whether further regulation is required in the future. A massive breach, or failure to embrace the requirements of GDPR across UK industry, could be scenarios that trigger another review and more regulation.

For more information about (ISC)² and its EMEA Advisory Council please visit: www.isc2.org/eac-volunteering

Federated identity: tailoring the user experience

Introducing industry-wide standards for biometrics will improve data protection, says Salvatore Sinno, chief security architect at Global Security, Unisys

IN ASSOCIATION WITH

UNISYS | Securing Your Tomorrow™

The biometric market is booming and is set to reach $15.1bn by 2025, according to a recent study by Tractica. Biometrics could be the key to enabling a digital onboarding and ongoing verification process with drastically improved transaction security and a better customer experience.

To delve deeper into the progression and market adoption of biometric security methods, Unisys conducted comprehensive research into biometrics in banking, in collaboration with students from the BI Norwegian Business School. What initially began as an investigation into the banking sector developed into assessing both the government and retail sector's integration and perception of the technology.

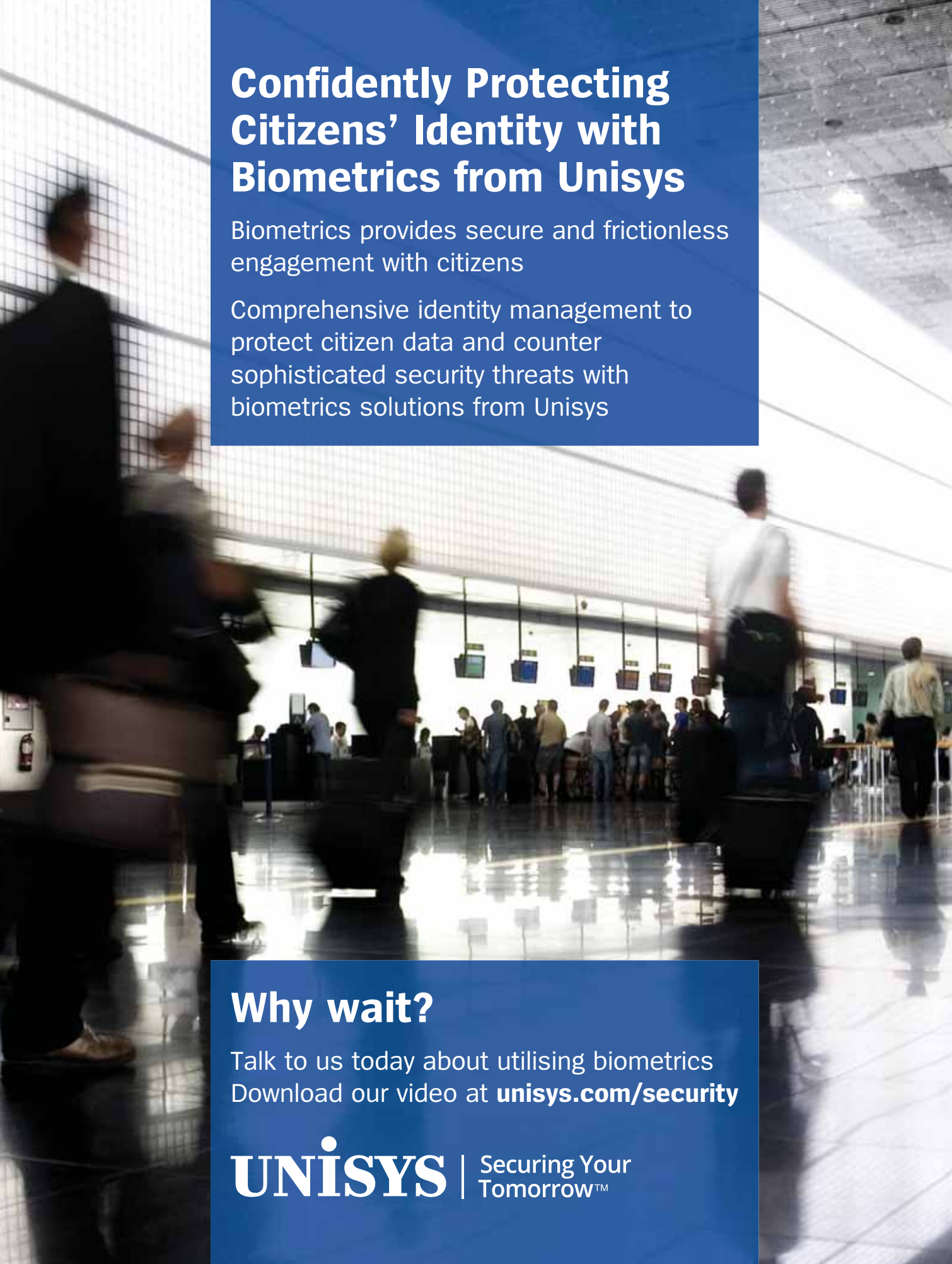
The banking sector was an early adopter of the technology and has already integrated some functions into the services they offer to customers. For example, we have seen Nationwide team up with Unisys and BehavioSec to begin utilising behavioural biometrics within their mobile application. Everyone holds and interacts with their mobile device in a different way and this biometric solution monitors the patterns and habits that are unique to each mobile banking user, to improve security while improving customer experience. On the other hand HSBC has begun working with partners such as Nuance Communications to offer voice biometrics as well as integrating their mobile application with Apple's Touch ID. However, the adoption and widespread market success of the solutions has been hindered due to many leading banks developing bespoke identity management solutions with or without biometrics.

Without an established common standard, whether set by the industry or government, organisations will continue to create biometric identity management services in accordance to their own security objectives. This might cause compliance and security issues when considering regulation of data security. It will also degrade the overall customer experience; increasingly customers juggle a number of online accounts, and while each individual one might provide a good user experience the aggregate experience of bouncing back and forth between them will be poor. Open and scalable standards can increase the development speed of this technology and allow federated identity to come into play.

Federated identity in this scenario would allow biometric credentials integrated to a single identity management service to be used when accessing multiple online services in the marketplace. This would not only improve the individual customer experience involved with a certain service, but also the aggregate online customer experience; not to mention improve security overall whilst reducing friction.

It is strongly recommended that organisations and governments alike should refrain from creating standards and solutions from scratch, and instead utilise leading standards and platforms that have already been created and evolve these dependent on the use case. This would allow a small number of profoundly successful and secure identity management infrastructures leveraging biometrics, to be utilised by whole markets with a regulated and tested security and operational underpinning.

It goes without saying that driving standards will foster the use of biometrics and the correct use of federated identity can only be a positive in a world where threats to consumer data, their personal accounts and online services are growing daily.



Confidently Protecting Citizens' Identity with Biometrics from Unisys

Biometrics provides secure and frictionless engagement with citizens

Comprehensive identity management to protect citizen data and counter sophisticated security threats with biometrics solutions from Unisys

Why wait?

Talk to us today about utilising biometrics
Download our video at **unisys.com/security**

UNISYS | Securing Your Tomorrow™

What makes an effective cyber security policy?

A 'one size fits all' approach leads to disaster, warns **Anish Chauhan**, managing director at Equilibrium Security Services

Hilary Clinton's presidential campaign chairman John Podesta had a series of emails leaked from his personal account last year

Whether it is for an SME, a FTSE or for the UK's new £1.9 billion investment plan, it is essential that your cyber security policy is completely indestructible.

Regardless of the size of an organisation, a cyber security policy should always be tailored to the unique needs of the individual business. High-risk areas need to be to be assessed so that intelligent firewalls can be set up to safeguard your most sensitive data.

Considering that 70 per cent of breaches are caused by employee error, the best cyber security strategies should always incorporate cyber awareness training for staff.

Set to wage war against the cyber crime epidemic, the government plan to invest a colossal £1.9bn into a new cyber security strategy, but what is it they are proposing to safeguard the UK from these relentlessly sophisticated and evolving intrusions?

The government are keen to outline that cyber attacks will be treated with the same urgency and consequence as any other serious criminal offence. In the hope they will remove the invisibility cloak of the cyber villain, they plan to hire a team of 50 criminal investigators who will work alongside the National Cyber Crime unit.

But is deterrence really a feasible measure to combat the criminal who can easily conceal their identity? Though the NCSC will undoubtedly prosecute a percentage of the less sophisticated criminals who fail to cover their tracks, there were 5.8 million incidents of cyber crime within the first half 2016 alone.

How are the government planning to control this level of criminality?

It is often difficult to even locate the country that a malicious hack originates, let alone to incriminate an individual. Although it is essential that we convict these cyber crooks, the

CENTER FOR AMERICAN PROGRESS/FLICKR CREATIVE COMMONS

IN ASSOCIATION WITH

EQUILIBRIUM CYBER SECURITY SERVICES

emphasis should lie with creating intelligent security systems that force the hacker into redundancy.

As 2017 is predicted to be the year of the 'creative hacker', it is important that the UK learns from other countries' approaches to cyber security; 2016 became the year that the USA fell victim to numerous and humiliating cyber breaches. Unfortunately, their failure boiled down to an ashamedly amateur approach to tackling the global crisis.

Rather than hiring a team of specialists that could protect their most valuable data, the USA relied heavily upon cyber deterrence as the fundamental ammunition to keep hackers at bay. In true Uncle Sam form, the USA aimed to protect themselves the only way they knew how – by threatening military action.

During Hilary Clinton's presidential campaign, the Democrats suffered a devastating email hack which was subsequently posted on *WikiLeaks*. To add insult to injury it recently came to light that campaign chairman John Podesta allegedly used the security word 'password' which he gave out in a false phishing email.

In an age where most five-year-olds are tech-savvy, Podesta has no excuse for lacking the most basic understanding of password security. It is common knowledge that a safe password should be eight to 10 characters long, contain numbers, upper and lowercase letters and must not contain easily guessed information. So how did Podesta conclude 'password' would be a safe choice?

Not only this, the Democrats had seemingly not educated their party on how to recognise a phishing attack. It is unnerving that the potential leaders of such a powerful country could oversee this damaging loophole in their IT infrastructure. Donald Trump's rise to the country's presidency is shrouded in suspicion for this very reason.

Over in the UK we had our own cyber unrest to contend with

In particular, the past 12 months have been host to an unprecedented number of attacks against NHS Trusts. In October of 2016, the Lincolnshire NHS Trust was forced to shut down all of its major systems after a malware attack. This resulted in all patient appointments being cancelled; women in labour and extreme trauma cases were advised to go to alternative hospitals, causing extreme overcrowding and long delays.

Mark Brassington, chief operating officer at ULHT, reportedly said: "The biggest impact on the trust [was] processing of blood tests, access to historical test results and availability of blood for blood transfusions." Evidently, these criminals lack a moral compass, as these NHS attacks affect real life and death situations. But the question is, are they conscious of the potentially fatal aftermath of their actions or is it more of a detached and impersonal business transaction?

With the UK professing to having a cyber crisis on its hands, GDPR are set to change data protection regulations for businesses which will launch in 2018.

As it stands, there are noticeably blurred lines around data protection laws for cybercrime. However, when the new rules are put in place next year, failure to follow compliance could lead to a fine of up to 4 per cent of a company's annual turnover.

How can Equilibrium help?

There is clearly a dire need for security professionals to protect UK businesses. Thankfully, here at Equilibrium Security we are first and foremost cyber security experts. We pride ourselves on not only offering the most cutting edge security solutions on the market but also on providing outstanding security expertise for our clients.

Our Phishing Simulation service aims to put your employees to the test by using well-known brands to simulate realistic cyber attacks. We monitor the click through rate of the employees who are successfully duped and then redirect them to training videos and interactive quizzes which provide awareness of how to recognise a phishing attack. Another service we offer is Ransomware Protect, this works off an intelligent cloud-based application called Cisco Umbrella which analyses historic and global internet activity. It can address ransomware and other malware threats before they have even taken hold.

We do not abide by the 'one size fits all' mentality, we take time to understand exactly what your business needs and then deliver it with nothing short of industry excellence.

For more information please visit: www.equilibrium-security.co.uk

Email: info@equilibrium-security.co.uk
Telephone: 0121 663 0055
Or follow us on Twitter: @EquilibriumSS

The clock is ticking...are you ready for GDPR?

The General Data Protection Regulation is changing the way organisations – both large and small - need to look after information, writes Avatu's **Ashley Page**

IN ASSOCIATION WITH

avatu

When the GDPR rules were added to British law and the UK was given two years to get it right before penalties began, some companies realised the dawn of a new era had arrived. It was time to get serious about looking after their own business information and their customers' personal data.

Others, however, shrugged their shoulders and decided to kick the can down the road, thinking :(a) GDPR didn't concern them, (b) the EU regulation could be repealed before it became actively enforced, or at least soon afterwards, or (c) they'd sort it out later.

Unfortunately, for these people, the message is now a tough one. If you do business in the UK, or the wider EU, and you keep personal data (anything from IP addresses to bank details), it does affect you.The British government hasn't repealed it and isn't likely to any day soon. Time is running out; the deadline to have your beefed-up data protection policies and practices in place is just over a year away. If you don't, you could be running the risk of the enormous penalties and perhaps the ignominy of being one of the first to fall foul of the new rules; which is why it's important to act now.

Renewed focus

Whilst GDPR has been introduced to better protect EU citizens' data and to standardise legislation throughout Europe – and its implementation may disrupt the way many organisations operate – it should be considered good for business. It will help you manage risk effectively, understand security dangers and protect your brand.

Companies should solve data security issues by approaching them from a business point of view. The introduction of GDPR has provided organisations with an opportunity (if not a wake-up call) to take full control of their data and re-evaluate security systems that are no longer suitable.

20 million reasons to get it right

Organisations who collect or handle EU citizen records should be aware of a couple of headline items. Firstly, people

MOPIC/SHUTTERSTOCK

who intentionally or negligently break the rules may be liable for fines of up to €20m or 4 per cent of annual turnover, whichever is greater. Secondly, organisations must notify a breach to their supervisory authority within 72 hours of it happening. It is critial – because of these increased sanctions – that key stakeholders within the business fully understand the final legislative text.

GDPR compliance: the five steps

1.Identify

To develop an effective defence strategy the first step is to be clear if your organisation is a data controller or a data processor when it comes to Personal Identifying Information (PII). PII is any data that can potentially identify someone. Organisations should regularly review existing and new processes around PII. They can determine where this data resides, and importantly, whether it is at-rest, in-motion and/or in-use. Knowing this will help them to understand how this data is/should be protected.

2. Protect

Having identified data as PII it is vital that it is secured. Common control standards include encryption and access control. But there is still much more that can be done. Monitoring of data leakage, from negligent or malicious employees, and external data theft are all important considerations. Password sharing puts organisations at risk of data loss because people use passwords that are all too easy to crack.

To demonstrate compliance with GDPR, alternative solutions will need to be adopted. Technology which reduces the chance of breaches happening through email can significantly reduce the risk. Programmes which routinely control who sees what information and what they can do with it is another layer of mitigation.Tools which educate employees and stop them making data vulnerable can also limit exposure.

3. Detect

When data loss occurs, it's critical that the breach is detected quickly so you can know if any PII records were lost or stolen. If they were, speed of discovery is paramount. Notifications must be sent to the relevant authorities within 72 hours of the discovery and a full investigation needs to be started.

Organisations need to design protection strategies for the differing levels of sensitivity. They need tools that will not only protect the organisation's 'crown jewels', but also minimise the chance of a data leak.

It is widely acknowledged that it takes an average of 247 days for organisations to discover that they have indeed been breached, and the UK average is believed to be more like 400 days, according to recent government research. This is mainly because the industry focus has traditionally been on creating perimeter defences such as anti-virus and sand-box technologies. Unfortunately, these will only help to defend against known threats.

4. Respond

GDPR means that security breaches can no longer be swept under the carpet. Incident response is a crucial element when it comes to protecting the data. On top of the mandatory data breach notification requirement, organisations must also make sure they've implemented and tested an effective incident response plan. With a plan in place, organisations have a better chance of reducing the risk and impact of data breaches.

Next generation tools that use 'deep inspection' techniques to detect all breaches in real-time, enable quicker response and reduce the impact. And digital forensics are an important part of finding out what has happened and who is responsible, and provide intelligence to improve future protection.

5. Recover

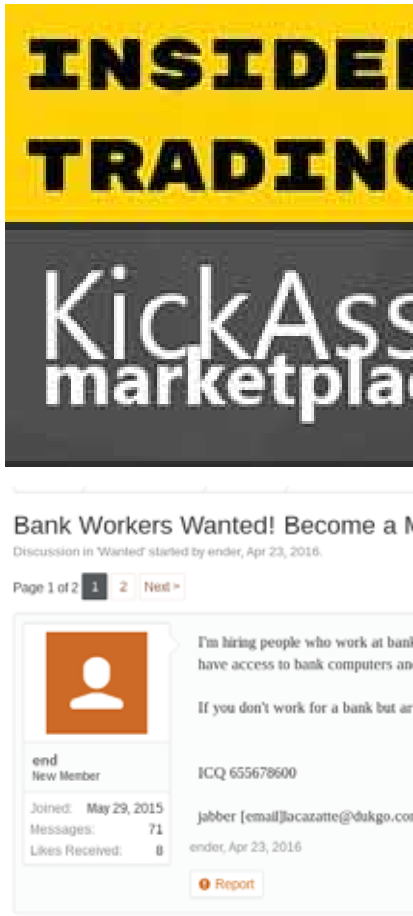
The final step for businesses that fall victim to a data breach is to continue ongoing communication with the authorities and the customers affected. This makes sure any losses are managed and those who have been directly affected are regularly kept informed. During the recovery process, organisations will learn the lessons of why things went wrong, and use this to improve their future arrangements.

Still unclear about GDPR and how it affects you?

Anyone who has questions about GDPR, or who's unclear about their readiness for the new rules, can arrange a special assessment with Avatu or can sign up for an Avatu GDPR webinar briefing.

Phone 01296 621121 or email **cybersecurity@avatu.co.uk**

Encrypted corners of the internet have become a marketplace for company secrets. IntSights' Ido Wulkan and Red Owl Analytics' Tim Condello talk to Rohan Banerjee about solving the problem



What can you find on the eBay of secrets?

Keep your friends close but your enemies closer. This mob maxim from *The Godfather Part II* takes on a twisted new meaning on the dark web. The dark web, for those in the dark, is a collection of websites that exist on an encrypted network and cannot be found using traditional search engines or browsers. Dark web users are afforded, therefore, a cloak of anonymity and unknown location. For this reason, the dark web become a hotbed for insider trading, converting friends into enemies for the right price.

Ido Wulkan, intelligence team leader at IntSights, and Tim Condello, technical account manager at Red Owl Analytics co-authored a special report on this phenomenon – *Monetizing the Insider* – last month. Wulkan, who terms these dark web sites as a "sort of eBay of secrets", explains how they have evolved over time. "What it does is give cyber criminals a new variety of products that before now no one thought were available online. It started off as a place to sell drugs and other such illegal merchandise, but gradually as the dark web has become more popular, more readily accessible, the market has evolved." What kind of thing are people selling now? "Information. There is a concrete and prominent market for insider insight and information." Like what? Condello pitches in: "What the report found was that dark web criminals enlist people who work and have insider knowledge at banks and financial institutions. It means they can steal or transfer money; we found the dark web being used a lot to manipulate stocks."

It seems fair to say, then, that the criminals on the dark web are setting

Dark web forums have become a hotbed for insider trading

In January, the exchange rate of 1 BTC was US$895

their sights a little higher than soap opera spoilers. Wulkan continues: "With the insider's information, the threat actor attempts to profit with a more educated action, maybe a stock market bet, and the insider receives a commission.
The dark web facilitates illicit trading activity by providing anonymity, making actors difficult to identify. All of the transactions are in Bitcoin (a type of digital currency that uses encryption) so it's harder to trace them." As of January 2017, the exchange rate of 1 BTC was US$895.

The dark web's insider trading racket, Condello is keen to stress, is pronounced. He says: "The insider trading forums we investigated were exclusive. They were like clubs. Though some activity may be happening in generic black markets, it appears that the most potent information and sophisticated actors are in small, elite groups. These groups require those who apply for membership to prove their capabilities and/or access to knowledge by sharing real inside information, which is then thoroughly checked and confirmed."

The KickAss marketplace, a dark web forum which the report case studied, is a hub for such groups. The forum's managers claimed to enforce high standards by reviewing every user's post for accuracy. In return for this high bar, they also charge a significant 1 BTC membership fee. The forum is fairly active with around five posts and a total of 40 BTC in transactions (US$35,800 per week); according to the report, there are members who make more than $5,000 a month using the leaked information.

Recruitment of insiders on the dark web is growing. Research found that

"Hackers will capitalise on a person who is dissatisfied with their life"

forum discussions on insiders nearly doubled from 2015 to 2016. What are the reasons behind this? While Condello accepts that in some circumstances, employees of organisations can be duped or let down by their own lack of appreciation for the sensitivity of the information they are privy to, he suggests that the most common cause is disillusionment. "I suppose you get some cases where people are roped in, but there are plenty of people who do end up seeking out this kind of activity themselves. The hackers will capitalise on the sort of person who needs money or is maybe dissatisfied with their status in life or position in the company. Insider trading is a way for them to make some money out of their situation."

Indeed, dark web criminals have targeted collusion with some lower-level employees of organisations who are more receptive to the promise of a cash reward. The report featured examples of a dark web forum member approaching a cashier in a large chain to help purchase iPhones and another to relay credit card details.

But why are people willing to risk their jobs? Wulkan adds: "Well, if they are that unhappy then is it something they're going to lose? I think people are more willing to take risks because it is easier to stay hidden."

Is there any light at the end of the dark web tunnel? Yes, there is; and both Wulkan and Condello insist that companies must do their utmost to reach it. According to the pair, the response to insider trading should be three-fold: cultural, human and technological. The cultural dimension, recommends Condello, relates to "creating an environment to mitigate from the threat of disgruntled employees. So it's important that companies start understanding the relationship between their human and technological resources. There needs to be a holistic approach to training and a message that we're all in this together. If people are happier in their work, they are less likely to want to sabotage it."

Further to this, the human aspect, Wulkan points out, means treating the two as one and the same is misguided. He says: "Treating insiders as a technological problem ignores the human side of their motivation and behaviour. Security teams must monitor employee behaviour across a broad array of channels that identify suspicious activity and also help understand negative employee sentiment."

Despite the focus of Wulkan and Condello's comments being on the less technical elements of the problem, neither are naïve as to the pertaining need for advanced technology. Condello concedes: "Regardless of what you might manage with your culture or staff, you've got to prepare for the case that it might not work too; so you need an effective insider threat programme. This means a foundational capability to see across all employee activity and spotlight any unwanted behaviour, while still respecting employee privacy."

How can surveillance still respect employee privacy? Given that employees are ultimately using a work system, Condello considers any charge of encroachment philosophically. He says that monitoring is a "last line of defence" and more concerned with "patterns of work" than scraping the barrel of email content.

Underestimating the capacity for internal threats has, according to Wulkan and Condello, themed a worrying amount of companies' capabilities for cyber security. Ironically, 80 per cent of security services studied in the report focused on perimeter defences, while fewer than half of organisations had budgeted for insider threat programmes. "The threat landscape," Condello reiterates, "is not something that's exclusively external and companies need to realise that." The cost to productivity and – arguably more damaging – reputation, is a risk factor that no company can afford to take lightly. Wulkan concludes: "We're not only talking about protecting the company and the brand; it's about protecting the customers as well."

Be prepared: insurance in the digital age

Modern companies must not underestimate the threat of cyber attacks and train their staff accordingly, says BGi.UK's Samuel Jones

There is a confused approach towards the management of cyber risks with a lack of clear standards, a varied and technically heavy language and rapidly evolving threat landscape leading to a 'head in the sand' attitude within many organisations. The insurance industry is well placed to take a strong lead in the development and management of cyber risks. The costs of a cyber attack can be crippling for many organisations where some relatively simple and cost-effective measures could have prevented or mitigated the lasting effects of an attack.

Given that insurers are working with and protecting clients against cyber risks, they are well positioned to provide leadership and dialogue with various other stakeholders, notably the government to assist on developing future strategies and schemes such as Cyber Essentials. Professionals throughout the insurance industry need to continue developing their IT security knowledge, keeping abreast of the developments which will alter underwriting approaches and risk management practices.

BGi.uk have developed a risk management package providing not just insurance covers but also secure online backup systems and training package for clients' staff. Phishing, social engineering and ransomware are preventable threats but only if staff are aware of what they are and how to handle them.

Increasing awareness and training of staff is going to be pivotal in protecting organisations. This process has to be led by the C-Suite and they must adopt the stance that cyber security is not the just the domain of the IT department but something every connected member of the organisation has a responsibility toward. A knowledgeable broker is ideally situated to assist their clients with adopting a strong risk management protocol if it is not in place already.

Brokers should provide knowledgeable advice and, where possible, the tools to help their clients who have placed their other business risks, and much trust, in them. Insurers and brokers need to demonstrate an understanding of the risks facing clients and also ensure that clients fully comprehend these risks. Whilst the news can be filled with stories of large businesses and hospitals getting hacked too many organisations are taking a chance when it comes to securing themselves. The monetary costs and lost production time when dealing with an attack is lost value not only to the organisation but to the overall economy.

Transfer of the risk is a major tool in managing cyber risks but organisations need to first understand and then take ownership. The nature of business and the supplier cycle means that insurance is becoming more of a requirement than an optional cover. Insurers therefore need to be clear with the cover that is provided. The Insurance Act 2015 has altered the way insurance is presented, sold and written. Buyers of insurance must be aware of and understand what it is they are purchasing and the exclusions and limitations of such cover. So ask more from your brokers and insurers; we have the knowledge and resources to help manage and mitigate your risks.

Given the reliance of the world on the internet to communicate, operate business, society requires a multi-tiered approach to cyber risk management. Whilst the government can lead in the development of national strategies some sectors such as insurance must provide leadership and knowledge to implement the basic level of security which will help protect from an insecure internet service. It is a service that might be difficult to live with but one that we cannot live without.

IN ASSOCIATION WITH

BGi.UK Insurance | Risk Management

The pillars of durable national cyber security

A long-term strategy for digital skills and risk management is vital to any country's economy, says **Adi Dar**, CEO at Cyberbit

SATIT_SRIHIN/SHUTTERSTOCK

International cyber espionage has reached new peaks. The world is reeling at the audacity of alleged attacks by one nation on the free, democratic elections of another via online data theft. The commercial sector, meanwhile, has been hit with a new level of breaches including giant corporations such as Sony, Tesco and TalkTalk.

While these attacks may have taken the general public by surprise, state and military leaders responsible for the UK's national cyber security have been aware of these threats for some time. Full awareness of the threat landscape is the first step, and the government has certainly taken that step by publishing the National Cyber Security Strategy 2016 – 2021 report. Now, we must devise and execute the strategy. This article will outline the three critical pillars for strengthening our nation's cyber security: securing critical infrastructure, establishing a national cyber security standard and developing a highly skilled workforce.

Securing critical infrastructure

Cyber attacks on power plants have already begun. Kiev was hit twice last year with breaches that led to loss of power to several portions of Ukraine's capital city. Other countries have also suffered mysterious massive outages that have raised the suspicions of leading cyber security experts. We've known for decades that Britain's critical infrastructure is considered a prime target for enemy actors.

To understand how to protect critical infrastructure we must first understand why they are so vulnerable. Utilities and heavy industry use operational networks called SCADA (supervisory control and data acquisition). SCADA systems are used to monitor and control equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and

transportation. They have local sensors distributed throughout the plant that gather, store and relay information to a central command centre. Many of the sensors also have computational abilities and can analyse data, detect irregularities and make decisions about how to remedy them.

This means that these remote sensor units are capable of sending commands that affect the physical operation of the plant. If hacked by malicious actors, the results could be catastrophic. In Kiev the supply of power was cut off, but the potential damage for SCADA attacks could be much worse. For example, in a nuclear power plant, SCADA systems monitor and control speed (RPM) and vibrations of the centrifuges. If hacked, malicious commands can be sent to change the speed and cause debilitating physical damage. Hackers could cause destruction of billions of pounds worth of equipment, explosions, fires or worse.

While most utilities and manufacturing plants have excellent physical security on site, most have next to nil cyber security in place. This simply lies outside the industry's expertise. Furthermore, there are limited commercially available solutions tailored for the unique needs of SCADA systems, that can effectively secure the interconnected IT and OT (operational) networks. Some hold the belief that they can keep operational networks safe by completely separating the two, so that the regular IT network cannot be used to compromise the OT network, an approach known as air-gapping.

But in today's modern plants, air-gapping is a myth. The IT and OT networks have completely converged and are intertwined. Therefore, effective defence requires and integrated approach. This kind of expertise is the dominion of the military and defence sectors who have been responsible for protecting the world's most sensitive critical infrastructure targets. The military and intelligence community must take the lead in protecting national critical infrastructure and partner with the very best international experts.

National cyber security standard

Cyber security is no longer just a cost-benefit consideration for individual organisations to weight on their own. The interconnectivity of the internet means that a breach in one network could be used to damage another. For example, user credentials stolen from web email accounts can be used to gain access to banking or credit card details. The repercussions of cyber attacks will be felt beyond the specific breached organisations and threaten to undermine confidence in the nation's commercial sector. The government must take a proactive leadership role in establishing clear, binding standards for cyber products.

A national standard that outlines product classes, specifies required capabilities and certifies products have been tested and found suitable is critical. Over 15 years ago, the United States government initiated a partnership between its National Security Agency (NSA) and National Institute of Standards and Technology (NIST) to develop a cost-effective way to establish a credible standard for the testing, evaluation and validation of information security products. This joint programme, the National Information Assurance Partnership (NIAP), champions the development and use of national and international standards for IT security (Common Criteria) and fosters research and development in IT security requirements definition, test methods, tools, techniques and assurance metrics. We recommend establishing a joint agency for partnership between the Government Communications Headquarters (GCHQ) and British Standards Group (BSI) to develop, promote and verify excellence in cyber security products and training.

A highly skilled workforce

The most imminent challenge we are facing is recruiting and training the 'boots on the ground' for the new cyber battlefront. The future of Britain's cyber defence depends on a highly skilled workforce of cyber security experts in all branches of the military, law enforcement, government and commercial industry.

The demand for well trained professionals is already outpacing supply. If the professional training goal is set high and energetically pursued, the UK stands to emerge as a global leader in cyber security and contribute significantly to the health of our nation's economy.

The training of a highly skilled cyber security workforce can be achieved by establishing excellent training centres and programmes for secondary school through to university level as well as professional trade schools and military and law enforcement academies. The courses must all contain theoretically studies and ample realistic training to gain the experience and prowess to necessary to effectively confront a variety of aggressive attack scenarios.

Ensuring infrastructure cyber resilience

Organisations must not fall for snake-oil salesmen and should instead seek expert advice, writes Atkins' **Andy Wall**

Digital technology is part of the fabric of modern society. What was science fiction a decade ago is reality today. The penetration of connected technology, from computers and tablets to smartphones and internet-enabled household equipment, is transforming our lives. Technology is also spreading rapidly into the industrial machinery and control systems that keep modern society operating in areas such as power, transport and water.

The ability to harness this technology offers the allure of huge potential efficiencies: smart sensors automating reporting via mobile or internet links could save human time and cost while improving the accuracy and frequency of checks; process alerting through portable devices could improve response capability and safety. While this transformation has benefits, there are also significant risks as industry goes digital. More devices, more connectivity, more computer controls means more opportunity for attackers, as well as a greater reliance on technology and automation.

High profile incidents underline the importance of protecting the UK's cyberspace from cyber crime, activists and nation states. Attacks on TalkTalk, Tesco and the NHS have impacted the lives of thousands of people, leading to loss of connectivity, bank fraud, cancelled operations or demands for cash by criminals.

Critical National Infrastructure (CNI) and the Defence sectors are not immune to these threats. Within the last 14 months, Ukrainian power networks have been attacked twice, causing significant blackouts. Malicious software has been found on the United States' electricity grid. The UK government has acknowledged that there are hostile foreign actors developing techniques that threaten the country's electrical grid and airports, and MI5 has disclosed that Russia is performing cyber attacks.

IN ASSOCIATION WITH

ATKINS

Our own research, undertaken in October 2016, highlighted concerns about such attacks, revealing that senior CNI figures have low confidence in the cyber security of supply chains and that an organisation's staff are considered to be one of its greatest cyber resilience weaknesses.

While the IT industry has generally developed a good understanding of cyber risk, the same cannot be said for the Operational Technology (OT) within CNI, which, with some notable exceptions, lags significantly behind in risk understanding and secure implementations. Yet organisations increasingly want to link these two worlds together and join the physical with the digital. An IT risk understanding that is focused on information and money clearly does not easily translate into one where risk has tangible physical consequences such as the loss or damage of electricity, oil and gas supplies and many other utilities, as well as potential health and safety risks and environmental damage.

This would appear to be a grim assessment. It is a sad fact that old style hacks and tactics still frequently seem to work. Undertaking regular maintenance on systems in the form of updates, patching and hardening goes a long way towards shutting off avenues of attack, but often even these simple measures are not being applied by default or in a timely manner.

We believe that effective cyber security should align organisational security approaches with the threat faced and what they are trying to protect in asset and safety terms: their staff, reputation, operations, and data. This has the potential to blend technical, people and process controls into a truly holistic protective regime.

However, this is where it starts to get interesting. Cue the snake-oil sellers, intent on seducing organisations into fix-all purchases and solutions that offer a panacea. The advice from many technology companies is to buy more 'stuff' - firewalls, anti-virus, anti-ransomware and encryption – so that they will be protected.

The point is that newer, smaller, bigger, faster technology is not generally the answer to the question posed by the business. Buying 'stuff' without understanding its purpose is simply the wrong approach.

This is critical for CNI organisations where the impact of attacks extends beyond the organisation to society, consuming citizens and their way of life. The Ukraine power attack could have been stopped by better trained staff with an understanding of what was happening and the capability to respond more quickly.

This brings me to a critical aspect of cyber security in CNI. Despite face-value similarities in technology, networks and process, OT is not the same as IT. The mistake is to treat it as if this were the case. Plant control systems are fully engineered for potential decades of use and are umbilically linked to the machinery they control and monitor. They operate valves and pumps; they read and report sensor data; they need perfect operational availability with resilience to match. The data types and flows need careful handling and processing.

The common IT practice of scanning for systems connected to a network is more likely to crash legacy industrial control systems than find them.

A reboot is not a recovery option.

Cyber security in CNI environments needs this engineering lens to evaluate proper risk and accurately generate the most appropriate security countermeasures that best fit the engineering organisational approach and culture.

Put simply, IT-based cyber security advisers rarely understand this engineering world and the control systems CNI operators employ. If they do not design and commission these facilities then what grounds do they have for thinking that they can develop the solutions to secure them?

What CNI organisations really need is advisers who have this real-world engineering and plant systems knowledge together with the cyber security skills to develop the sensitive and effective cyber controls required. The cyber security response in this context is a demanding one for CNI organisations as it must:

- Cover all engineering-security dimensions: technical, people, process and physical
- Integrate security into the engineering design from inception through to operation and decommissioning
- Range across the whole supply chain
- Embed security awareness from board level through to plant operators
- Prevent attacks, but also consider the response and recovery measures required to provide true resilience.

CNI organisations need advisers steeped in the engineering world who can offer solutions and approaches, smooth the journey through the design and implementation of cyber resilience strategies and offer assurance for live system service running.

Are we really prepared in the event of a security breach?

UK government and industry must collaborate on cyber strategy, according to Meg Hillier MP, Chair of the Public Accounts Committee

The cyber attacks on the Democrats in the US presidential election highlighted the steps those with an agenda wanting to exert influence will take. They have confirmed the reality of modern espionage and that insecure servers are the back door to those who mean harm. And if anyone had any remaining doubts about who was behind this, Michael Fallon's speech at St Andrews spotlighted the specific threat from Russia.

Data security breaches at Tesco, Northern Lincolnshire and Goole NHS Trust, Sage and TalkTalk have recently thrown the challenge of protecting information into focus. The NHS attack also underlined that such attacks aren't simply about hacking but that disruption is a new weapon for hackers as ransomware is on the rise. And the impact on patients is potentially catastrophic if building systems are shut down by a cyber attack.

All this is happening against the backdrop of a mission to use digital to reform public services. More and more of our important data is online and these systems are interconnected. Forgot your password for your tax return? No worries, you can provide personal data to have your identity verified by a third party organisation and connect back into HMRC's system.

There's a benefit to UK productivity as overheads are reduced and many interactions are automated. Nevertheless, we are sharing extraordinary amounts of personal data including financial information as a matter of routine. The benefits of our digitally connected world are here to stay. But the threats and hacking incidence don't just undermine our capacity to deliver government services or deliver on business objectives, they also undermine public confidence.

Consider health: the whole system relies on patients trusting that information is secure but can be used to help us through the health system when we need it. And yet there was a huge backlash when the government tried to introduce the electronic health record and share anonymous patient data.

In Sweden, there is a minister for digital health. Using digital effectively in healthcare could be the basis of massive

DEFENCE IMAGES/FLICKR CREATIVE COMMONS

In 2015, Government Communications Headquarters (GCHQ) was alerted to 200 cyber security breaches per month

"Hacking undermines our services and public confidence"

patient empowerment to take control of their lives. The prizes from well-designed digital systems to improve our health and connect our disjointed health system are potentially great. But these benefits need to be sold to sceptical consumers.

The rise in the threat and the government's response was the subject of the recent Public Accounts Committee report on how well prepared the government is in the event of a serious cyber attack. In 2010, the government ranked cyber security as one of the top four security threats to the UK. The preparedness of individual Whitehall departments is patchy. And each department determines what it considers to be a data protection breach and records this data differently, leading to a chaotic approach which the centre of government cannot monitor.

Senior ministers have been clear about the challenge. Former Chancellor George Osborne criticised the complex "alphabet soup" of agencies involved in cyber security and heralded the launch of the National Cyber Security Centre. Threats to cyber security are growing rapidly – with 200 incidents a month which were serious enough to alert GCHQ in 2015, up from 100 a month in 2014. But it has taken government too long to consolidate and coordinate its response to protecting the UK.

As recently as April last year there were at least 12 separate organisations in the centre of government with a role in protecting information. The establishment of the National Cyber Security Centre is a welcome step in beginning to bring these bodies together and act as a bridge between government and business.

It has been established to provide a unified source of advice, guidance and support, including the management of critical cyber security incidents. But there is a lot still to do to make sure that the new centre lives up to expectation.

It is not clear how a hospital, local authority or business would be able to ascertain whether a cyber breach needed to be escalated. An area of real concern, and one harder to tackle in the short term, is the recruitment of staff with the right skills to tackle the problem. The skills problem is a challenge for all sectors but too often the private sector can outbid government rates of pay. In 2013, the Cabinet Office established a security profession to develop the skills of civil servants working in this field. And it is attempting to paper over the cracks by setting up large clusters where civil servants can share their skills - amalgamating 40 different departmental security teams into four larger clusters.

There are patches of good practice in Whitehall. The DWP has done some thorough work to ensure that staff at all levels understand and buy into their role in maintaining security. The National Archives is leading the pack and providing training courses for civil servants from across Whitehall.

But cyber security relies on us all – individuals, private companies, public bodies and government. The fact that Britain ranks below Brazil, South Africa and China in keeping phones and laptops secure is sobering.

The government has to make sure it has the capability to provide the appropriate support in the event of an attack. A hospital with systems that won't work, loss of sensitive passwords or a virus in one part of an interconnected IT system could lead to chaos for individuals or institutions.

The National Cyber Security Centre has the potential to provide national leadership, but it is only just making its first baby steps in 2017 despite the government committing to take action in 2010. We are seven years off the pace.

Government has a vital role to play but it needs to raise its game. Its approach to handling basic data breaches is chaotic and my committee did not have confidence in its ability to take swift, coordinated and effective action in the event of an attack.

The UK was ahead of the game in the past – Bletchley Park and Alan Turing won us the war. We need to be this good again, but we have some work to do before this is reality.

David Beckham's own goal is a warning shot to the world

It's not just celebrities who need to be cautious about their cyber security, writes Avatu CEO **Joe Jouhal**

It was hardly an act of high treason, but it seems safe to assume that David Beckham would have preferred his calling the Royal Honours Committee "unappreciative c***s" to have stayed under wraps. The former England captain, allegedly aggrieved at the decision not to award him a knighthood for his charity work, is the latest high-profile victim of a breach in cyber security. Hacked emails between Beckham and Simon Oliveira, his publicist at Doyen Global, found their way into the public domain after the ex-Manchester United winger's camp refused to accept the hackers' £1million blackmail demands.

Responding to the controversy a spokesperson for Beckham told *The Daily Telegraph*: "This story is based on outdated material taken out of context from hacked and doctored private emails from a third party server and gives a deliberately inaccurate picture." Context, though, is a courtesy that no hacker is likely to afford. While Beckham's reputation might be in question, that of Doyen Global's is in ruins.

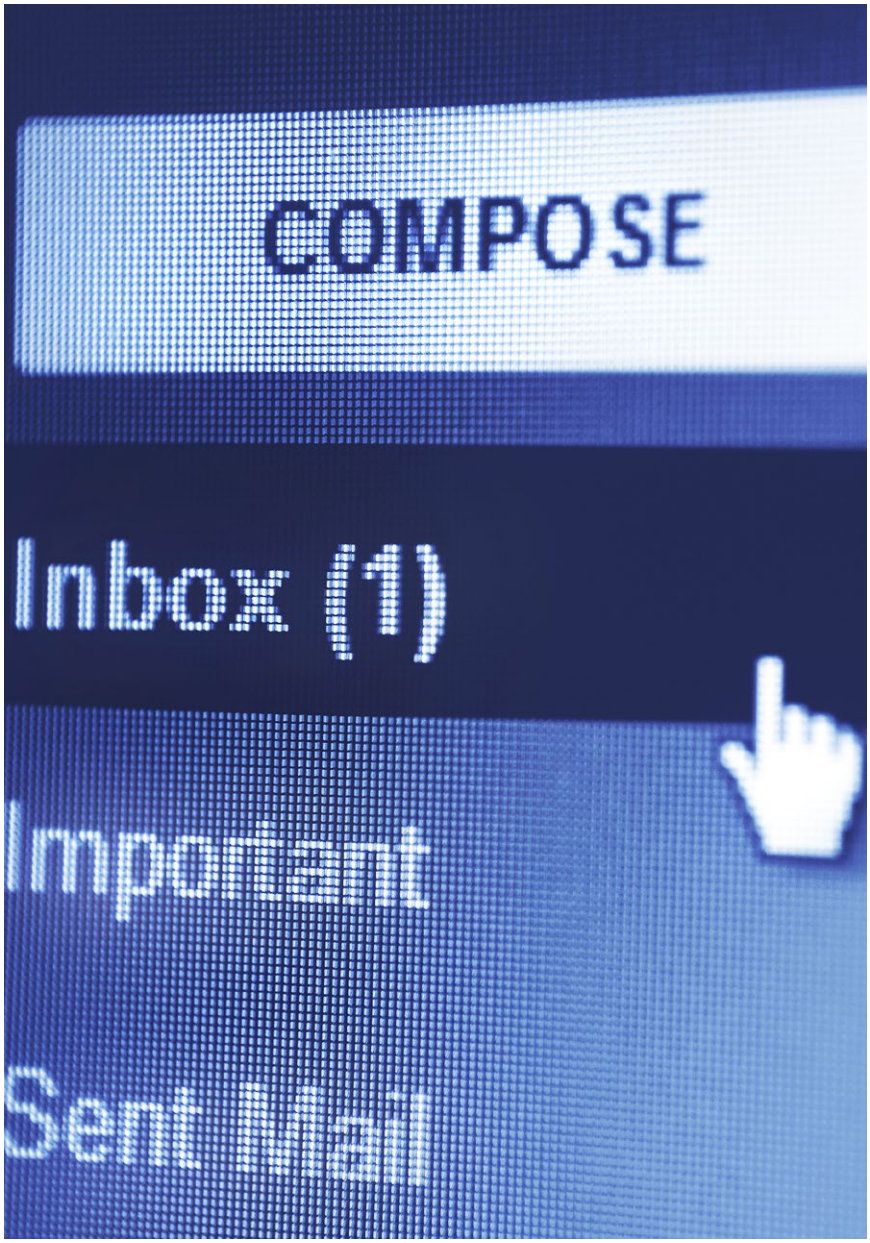
It's worth noting, of course, that hacking victims needn't have done anything wrong. In 2014, actress Jennifer Lawrence had nude photographs of herself shared over the internet after hackers accessed her iCloud files.

The risk faced by individuals, such as Beckham and Lawrence, can be applicable to businesses too – whether big or small. The fact of the matter is, we as a society, as a species even, exist online. Reputation management is tithed to the internet and cyber threats are very real pressures on privacy, productivity and, perhaps most crucially, public perception. Certainly, the variance between what is said publicly and what is said privately can suggest hypocrisy and undo good work and investment elsewhere.

Convenience, it seems, has led to a dangerous culture of complacency. That we are able to access information at the touch of a button should not supplant the pressing need for security. You don't have to be a celebrity to have information that you might not want out in the open – that joke from last night, that gossip from last week, might just be your last hurrah.

Every company, every person, values their right to confidentiality. It's why we have locks on doors; it's why we wear towels round our waists; it's why we have passwords on computers. Yet, too often, in the haste to achieve instant delivery, people and companies are willing to take shortcuts. TalkTalk's lack of encryption of customer data, for example, could have proved even more catastrophic than it did.

Across industries, there has been a worrying abdication of personal and professional responsibility. The concern is that companies don't attach as much importance to their cyber security strategy as they do to, say, their building insurance. While a building burnt to



AARON SHOLL/FLICKR CREATIVE COMMONS

the ground can ultimately be rebuilt; it is more difficult to say that for a company or person's social standing.

Naturally, appropriate investment can only come as a result of appropriate awareness and it is here we find our biggest barrier to suitable cyber security – education. The status quo surrounding cyber security is largely curative; it would do well to be preventive.

While perimeter defences have their merits, they are limited. A multi-layered, preventive approach, meanwhile, which includes education and re-education, guards against both external, and the oft-overlooked, internal threats.

Many security breaches are the result of an individual's error – they are usually more clumsy than complicit – and the training of staff must become a priority for any sized company. Fortunately, very effective technologies are available that can make sure employees know, understand and use policies and procedures outside the training room too. By working with employees and through the logging and monitoring of staff's online behaviour, problems can be nipped in the bud for both issues caused by carelessness and those caused by intent.

Computer-centric risks require preventive technologies. This recognises that the majority of breaches to companies' security come through compromised email attachments and there is advanced software available which ensures only the sending and receipt of clean, safe and compliant files. Users can be protected, therefore, from sophisticated malware, such as ransomware and zero-day attacks, that bypass conventional anti-virus and sandbox defences in the form currently deployed by organisations.

Furthermore, irrespective of the United Kingdom's decision to leave the European Union, companies will need to comply with the General Data Protection Regulations (GDPR) set to become law from May 2018. It significantly strengthens data protection rules for all EU countries, and for any organisation – anywhere in the world – that wants to do business with the EU.

The most forward-thinking companies are becoming GDPR-ready, even if they only work within the UK. Why? Because it encourages organisations to take data security more seriously, with a minimum 72-hour incident report policy, regular vetting and financial penalties in place to keep standards high. Such sobering fines can be up to €20m, or 4 per cent of global turnover, which ever is higher.

There is no such thing as a typical victim when it comes to hacking.David Beckham's indiscretion might have cost him a knighthood; a company's might cost it its business.

For more information please contact Avatu on 01296 621121

The secret policeman's crystal ball

Privacy, online or otherwise, is a basic human right, argue 44Con's **Malcolm Tuffet** and **Tor Signell**

BLUEBAY/SHUTTERSTOCK

Inside an isolationist, hermit kingdom, belligerent to its closest neighbours and with one questionably reliable close ally in the region, elite cadres exercise control over its populace through one of the world's most pervasive surveillance states. Power is concentrated in the hands of a select few. Access to the internet is arbitrarily and tightly controlled.

There are secret arrests, secret trials, secret prisons, state-supported torture and immigration detention centres.

An unaccountable and pervasive surveillance state keeps the state safe from vague, shifting threats from 'terrorists' and 'foreign powers', invoking war imagery to justify its belligerency to its neighbours.

The state can spy on your home through your internet gadgets, smart TV or security cameras with impunity. Unaccountable automated tools decide whether you need further investigation.

You might think we're talking about North Korea, but welcome to the Democratic People's United Kingdom (DPUK). It's not a hyperbolic dark vision of the future, it's the world we live in as of November 2016.

The DPUK keeps detailed Internet Connection Records (ICRs) of all digital communications. Collecting all of this data is an expensive task, so the government gets mobile and broadband Internet Service Providers (ISPs) to do it for them, and provide access to this data through a new IT system called a Request Filter, allowing the authorities to perform complex automated searches across multiple sources.

For example, Google keeps records of all of your account activity and you can see some of it at the Google MyActivity website. Imagine this for everything you do, wherever you do it, on whatever device you use. Now imagine it being trawled through by thousands of officials, in different government departments, most of which you have

IN ASSOCIATION WITH

44CON

nothing to do with.

ISPs assure us that they take security seriously, but suffer regular and major breaches that they fail to address properly. To suggest that Request Filters won't be successfully attacked by organised criminals and state sponsored hackers would be naive.You might think it's reasonable that the police and health services have legitimate reason for access, but what about the food standards services, and health and safety executive, and over 40 other departments, quangos and their contractors?

Between 2011 and 2015 the police experienced over 2000 data breaches. The NHS, beleaguered by breaches itself also has access to the Request Filter. Over a three-month period in 2016, the Information Commissioner's Office fined two police forces and two NHS trusts at total of £595,000 for breaches ranging from posting 6574 staff members' personal data on the internet, to sending a domestic abuse case suspect a copy of all data on his alleged victim's phone.

You might think that you have nothing to hide. After all, you're not a criminal. However, ICRs must be retained for at least a year. That means that should the law change, government agencies can investigate your internet activity retrospectively.

Under the Act, the DPUK can gain permission to hack into anyone's device, regardless of whether the individual is the subject of an investigation. If you're on the same bus as a person of interest, the government might decide to hack the phones and home internet connections of everyone who shares the same bus. Or just hack all the phones it can, just in case.

Let's pretend for a moment that you use the world's most secure ISP, that your home is a digital fortress and that you encrypt everything so strongly not even you can read your own email. Allow us to introduce the most fiendish part of the DPUK's surveillance legislation – the Technical Capability Notice. A Technical Capability Notice is a secret notice that forces a "telecommunications operator" to do whatever the government thinks is necessary to make surveillance easier. In plain English, this means that anyone that the government can claim provides a telecommunications service (such as your employer, ISP, Google, Microsoft, or a hotel wi-fi network) can be compelled to implement any backdoor or other changes the government determine suitable.

The orders are secret; once issued with one you can't disclose the contents or even the existence of it, at risk of prosecution. Microsoft, Apple and Google have all condemned this, along with human rights experts, technical specialists and lawyers, but the DPUK has "had enough of experts." Worse still, assuming such backdoors will remain secret is optimistic at best, so ordinary criminals are likely to exploit them as well as the DPUK elite.

Of course the government tells us that these powers are needed to stop serious crime and terrorism, but criminals and terrorists are already breaking the law, therefore they'll continue to use encryption as they always have. These powers are really about gaining and keeping access to your information, and ensuring that the state retains the ability to watch the general public, unhampered by encryption and other security measures.

So what can you do to stop all this? Sadly, that ship sailed some time ago. We were all repeatedly warned of this, and foolishly didn't do enough. Instead of telling you to use technical measures, we're now left unplugging devices and removing batteries if you want to talk privately and to leave mobile phones at home as though we're living in a spy novel. The European Union has struck down similar laws before, but that will only work until we leave EU human rights obligations behind.

Now that both the government's wishes and the law are stacked against you, your only hope is to act, act now, and act continuously. Engage the political process. Write to your MP once a month about the issues that matter to you. Write about the fact you're being spied on. Write about how holding legitimate political views risks you being branded an extremist and targeted for surveillance.

Nobody wants to stop the security services and law enforcement from doing their jobs in keeping us safe. Nobody wants to stop the police from fighting crime. But to do so we must have transparency, accountability and openness, and we must accept in a functioning democracy, a clear line must separate legitimate investigation from spying on everyone. We all have a right to privacy as enshrined in the European Convention of Human Rights, the Human Rights Act and the UN's Universal Declaration of Human Rights. We must hold our government to account in order for them to honour it.

To find out more visit: www.44con.com
The UK's premier security conference
September 13th-15th, ILEC London

Why encryption is the best strategy

Data protection, wherever it resides, must form the core of companies' security systems, says **Colin Tankard**, managing director at Digital Pathways

MORROWIND/SHUTTERSTOCK

Encryption, in which information is converted from a readable format into one that obscures its meaning from those without the authorisation or ability to decipher it, has long been used to protect sensitive information from prying eyes.

Data security as a pressing concern

In recent years, ensuring the security, confidentiality and integrity of data has become an ever more pressing concern. Information and data produced and collected by organisations, including intellectual property and personally identifiable information related to customers, employees and business partners, is valuable not just to the organisation concerned, but also to criminals who can use it for financial gain.

According to recent research by Vormetric, 91 per cent of IT executives state that they feel vulnerable to data security threats; and with good reason since data breaches are everyday news and can impact any organisation, no matter its size or line of business. A recent government survey found that whilst 65 per cent of large firms reported having suffered a data breach in the past year, more than half of medium-sized firms and one-third of small organisations had been breached, showing that no one is immune. Gemalto has released a report that showed that businesses in the UK suffer the highest level of breaches in Europe, and are second only globally to the USA.

According to Breach Level Index, almost 5 billion data records have been lost or stolen since 2013, but only 4 per cent of those records were encrypted. Any data breach can cost the organisation that was involved dearly, both in terms of lost revenues and damage to its brand and reputation. The Department for Business, Innovation and Skills states that cyber security is a

growing threat for all organisations, costing large businesses an average of £1.5 million, up from £600,000 in 2014, whilst the average cost for SMEs has doubled to £310,800.

The key role of encryption

Encryption has a key role to play in keeping sensitive and confidential information safe from criminals and prying eyes. The use of encryption is the best strategy for any organisation for maintaining security for any information when it is in storage or is being transmitted, such as over email. Originally considered to be a complex technology to deploy and manage, the technology has moved on and can now be easily used by anyone.

But it is not just a good strategy to choose to encrypt sensitive data, it may also be required. Organisations face a wide range of regulations and industry standards that they must adhere to and that are increasingly strict with regard to protecting sensitive data. In the USA, the majority of states have laws regarding data breach notification and those doing business in Europe will face similar pressures when the General Data Protection Regulation (GDPR) becomes law in May 2018. As with most directives and regulations produced by the EU, the GDPR is not particularly prescriptive in terms of technology to be used, with the exception of encryption and pseudonymisation, which are specifically 'called out' as suitable, appropriate safeguards for protecting data.

A safe harbour where encryption is used

What many of these regulations and industry standards such as PCI-DSS for protecting payment card information have in common, is that they provide a safe harbour when encryption has been implemented. For example, the majority of laws that mandate data breach notification contain clauses whereby notification is not required where data that has been lost or stolen has been encrypted, since the data cannot be compromised unless the encryption code or method is also compromised.

Encryption in overall security strategy

Encryption by itself is not the only technology that organisations should have in place to protect sensitive data, but should be a strategic part of the entire security system, alongside complementary technologies such as access controls, monitoring systems, and auditing and reporting capabilities.

Of particular importance is that the actions of privileged users are tightly controlled in terms of what they can access and what they do with information. This is necessary owing to the need to counter insider threats, which are estimated to account for 43 per cent of all breaches, many of which are attributed to actions by privileged users. Not all insider threats are caused by malicious intentions, as accidents can occur such as inadvertently sending information to a recipient other than that which was intended; but insider threats can be the most damaging since internal users can have access to the most sensitive and valuable information that an organisation possesses. These controls should be tightly integrated so that there are no security gaps that could be exploited so that organisations are better able to both 'ward off' advanced threats and meet their compliance objectives.

Encryption should be applied across all areas, devices and cloud services. The latter can be achieved with the use of a cloud encryption gateway that provides robust, persistent controls, detailed visibility regarding data access and the ability to detect unencrypted files. Such technology not only ensures that risks are reduced, but also provides full auditability so that compliance requirements can be met and proven.

Another core capability is cryptographic key management, which should be centralised to ensure that policies can be consistently applied across all data, both when in transit and when at rest. Efficient key management can be achieved through use of a physical or virtual appliance or, increasingly can be provided as a service, especially for cloud applications.

Encryption as a baseline

The importance of having such controls in place to protect sensitive data is only set to grow. Organisations that have not yet started preparing for compliance with the GDPR should be looking to do so now as there is only just over a year to go before compliance is mandatory. In comparison to previous data protection laws it is considerably more stringent and impacts a wider range of organisations than before.

Encryption should be considered to be a core part of any data security strategy that organisations develop, both for data at rest and in motion. For both data security needs and for achieving regulatory compliance, encryption should be considered to be a baseline.

How to catch a hacker

Dr Jim Kent, advisor to the United Nations on cyber security and co-author of the government's best practice guide for digital investigation, gives an introduction to digital forensics

About 10 years ago, I was called to a job in a very prestigious part of London, by a company that traded in aluminium. They told me they thought something was wrong, but they weren't quite sure. They were in litigation against another business, and it appeared that when they were preparing their legal documents, the responses coming back from the other side were very rapid, almost as if the other side were seeing what happened before the letters were even sent. The responses were coming pretty much instantaneously. The litigation was worth millions of dollars.

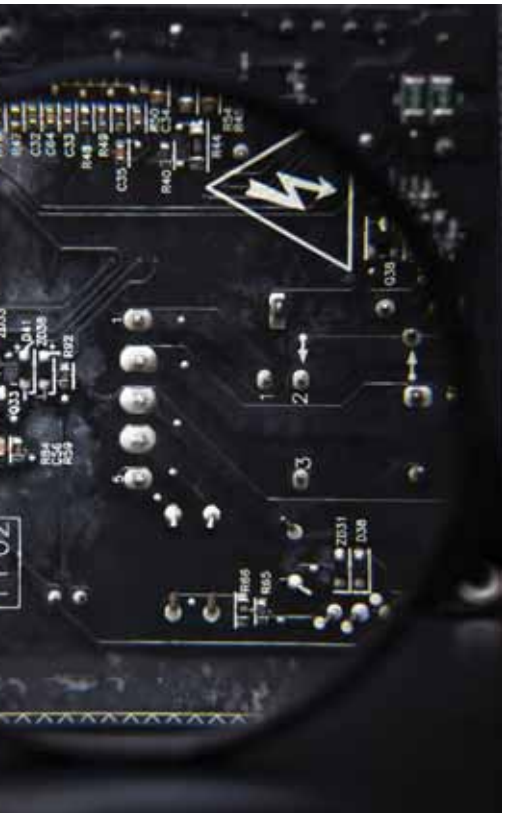
It transpired that the other organisation had crafted an email to the secretary of my client's CEO. The email was crafted as if it was from one of her friends, who they were able to impersonate using insider information, and they sent her an email saying "here's your tarot cards, double-click this and it'll tell you your future." She clicked, of course. It told her the future, and she closed it and didn't think anything more of it.

In the background, a payload had been delivered when she doubled-clicked, installing a keystroke logger onto her machine. The keystroke logger started catching data and sending it back to whoever was listening, it also slowed down her machine. So she called IT, who logged in on her machine as an administrator, and then the keystroke logger captured the administrator's password. At that point, the outsiders could log in with the administrator's account, make themselves new accounts, and trawl all the way through everything in the company environment.

Arriving at the scene as an investigator, the same forensic principles apply as with any other crime scene. The first concern is, don't destroy any evidence. Fortunately with digital forensics, it's possible to make a perfect copy of the crime scene. A forensic copy is not just a matter of copying files, it's a bit-for-bit image.

Once you've done that, you can start investigating and correlating. Again, just like in any other crime scene, you look for anomalies. A changed IP address, a user account that has been created, a bogus user account, with a bogus

SHUTTERSTOCK \ PJARUWAN



“It’s very difficult to completely destroy information”

time. Random files with random dates on. You’re looking for threads you can pull on. Our pen-testers, or “ethical hackers”, will probe an environment from the outside, trying the doors and windows, if you like, to see what opens and what data is coming out. In the case of the trading company, we could see just by looking at certain ports that were coming out of the firewall that this thing was trying to talk home. So every now and then a door would open and a load of stuff would run out and the door would shut.Then you start to follow these clues up – so, the IP address or a port could tell you how they got in and also help you trace where that data went. You can start to look at where they were on a map and find people, objects and events.

This is where an investigation starts to develop more dimensions. You’re no longer looking at oh I could be digitally investigating a phone or a hard drive; the phones and the laptops are part of the metadata of a human story. So you’ve got to start looking at things in context, to rebuild the storyboard.

Sometimes there are no breadcrumbs. Smart criminals will do counter-forensics, and wipe the machine completely, but it’s very difficult to completely destroy information. We’ve recovered data from a drive that’s been in a river for years. A thumb drive or an SSD that’s heavily encrypted is harder. You might know everything is pointing there, you’re actually holding the evidence, but you can’t get to it.

It’s also true that you can’t always say who is pressing the keys on the keyboard, so we might need supporting evidence – when was a file made? What other activity was happening? If there was web browsing history, if they logged into a bank account or Facebook, you can place someone at a keyboard at a certain time. The records from phone masts have been good at placing people in certain locations in the past, but now there’s lots of data available freely on the web that can help to place people.

Digital tracing can also be a big part of the job. If you look at airports, they have contractors coming in and out, and you know what they all door swipe in and out. They all have IDs. All of these are digital artefacts which come together so you can start working out what, who, why. If you know if one person has four different identities, you’re onto them. We live in such a digitally rich world that everything is there if you know where to look at you’ve got the right tools to look for it. And that’s the key. Sometimes it takes a bit of time, of course, and there are some very clever people out there, but if you take your time, everyone trips up.

Finally, you can look at where the stolen goods have gone. Tracking is very interesting. Validating can be fraught, sometimes, but with comparative analysis on the data, it’s no different to getting an art expert to validate a stolen oil painting.

I can honestly say that I love investigating this type of crime. I love it when a machine is infected with something new and we find a piece of malware and take it apart, reverse engineer it and look at what it does. You catch people that way, too – they can’t help but put a little bit of kudos for themselves in it, so they hide something stupid in there.

While it’s true that we are always going to be chasing the bad guys, we’re also looking at how we can build things to protect people. That’s where investigating really comes into its own, because you can start using the things you’ve learned and pushing that intelligence back out, to build better defences. Building a better understanding of cyber crime is the real crux of what we do.

Dr Jim Kent is the Global Head of Security and Intelligence at Nuix

The British Bulldog is well and truly back

Cyber threats might have evolved but so too has Britain's capacity to deal with them, says SJG Digital CEO Stuart Green

Another year on and here we are, once again, writing for another cyber security supplement and I'd love to be waxing lyrical about how much the landscape has changed and what a wonderful world it has become.

Well, there hasn't been a massive landslip where UK plc has galvanised themselves in to action; the bad guys have got more savvy and their numbers have swollen but one thing is for certain, for those business leaders that want to, they can do a heck of a lot more to keep the bad guys out. All it takes is the will and for that inspirational CEO in your organisation to ask one question: "What is really happening on our network?".

For some CEOs, this is a daunting question because it could potentially open a rather large can of worms. For others, they know that they are going to be hit by an avalanche of "geek speak" which they don't really understand. For an enlightened few, however, asking this question results in the normal "state of the nation" report that is discussed at every board meeting. So what's so different about that? Well, that enlightened few is growing in number as more and more organisations adopt the Cyber Essentials standard and insist on only dealing with organisations in their supply chain that have it. It is a small but significant step in the right direction.

In the past year, we've seen the United Kingdom make its mark on the world in a number of ways. Never mind Brexit, look at what we have achieved by standing up the National Cyber Security Centre. Law enforcement are tackling the problem head on with revamped Action Fraud reporting and Regional Cyber Protect Officers dedicated to helping businesses. With so many resources available freely to us all, we've now got something that few nations can turn to should the worst happen.

Vendors, too, are producing more and more clever things that can help to make us more resilient. It is simply not the case of technology getting in the way when security is implemented; now we have that time where technology is enabling us to do things in a secure way, gently nudging us in the right direction and silently keeping the bad stuff out. Buzz words and terms like Next Generation Threat Extraction, Behavioural Attack Detection and Zero Day Attack Protection are all creeping in to organisations and we've even arrived at the point in time where devices on a network will speak to the network infrastructure to reassure them that they are free from infection.

For those of us using these devices some of us are getting awareness training to elevate our knowledge in terms of how to stop bad things happening and work safely. Some of us even have access to NCSC's CiSP to inform us of the pertinent threats in our area or sector and what to do to combat them. We can even run free tests such as Check Me from Check Point to help us answer the difficult questions and see that the defences we have are working without the need for technical know-how or involvement.

So, this time last year, we asked that business leaders stand up, be counted and fly the flag of resilience. Many took the plunge and are rebuilding their business networks with the whole "cyber thing" central to their operations. Those who did take the plunge are seeing their culture become stronger, their staff more informed and their supply chains more robust. More significantly, they are growing, they are prospering. When we've got forward-thinking business leaders tackling cyber attacks head on by changing their business culture, we're proving that UK plc is still a great place to be.

The inconvenient truth about data breaches

Anomaly detection can be just as important as preventive technology, according to Alex Moyes, UK country manager at LightCyber

Why is it data breaches continue to rise in volume and magnitude without any sign of stopping or slowing down? During 2016, cyber crime overtook physical crime in the UK, and all indicators point to increasing loss and damage in this coming year. Law firms in England and Wales alone lost £85m in disclosed breaches over the past 18 months and vastly more than that in ones not reported or made public. Even UK charities have been hit by cyber criminals. Cyber crime seemingly knows no bounds.

The success rate for cyber crime is extraordinarily high. If an attacker is motivated and reasonably adept and equipped, there is a high probability they will be able to accomplish their goals before being detected. The flipside is also true: the success rate for an organisation to find an active network attacker before theft or damage is extraordinarily low. One reason why traditional security has largely failed to stop the problem is that compounded misunderstandings have prevented practitioners from addressing the core issues.

First, there is a fundamental disconnect between knowing that attackers will get into a network and what one must do in response. Today, attackers can gain access to any given network, most likely through compromising a user's computer or network account. It's a certainty, and it's often touted by law enforcement agencies around the world, professional organisations like SANS and industry analyst groups such as Gartner. The best white hat pen testers guarantee they can do this within two days. So, if intrusion is a certainty, the question is: "Can you find an active attacker on your network?" Here is the disconnect—the gap between recognition that attackers can and will get into a network and the action of doing something about it. Few top executives ask the question about being able to find an active attacker on the network, and few security professionals gear their thinking in terms of what they need to do differently to gain that ability.

For more than two decades, security has focused on prevention—keeping the bad guys out. Admitting they can get in and shifting some focus to detecting them represents a foundational shift. Preventive security is still important and likely deflects the vast majority of attacks, but it can no longer prevent them all. The task, then, is not a real-time identification of the intrusion, but spotting the attacker once they have landed in a network and started their work of exploring the network, locating assets and moving across the network to gain control of them. Make no mistake, this is a human-driven process that is iterative and designed to stay under the radar.

These operational steps utilise many familiar administrator tools and procedures. They rarely use malware, so security based solely on malware detection will prove mostly fruitless in detecting an attacker. Although attacker activities blend in with legitimate use of such tools, they can be readily identified if one knows what normal looks like for each user and device on the network and can then discern anomalies.

Anomaly detection alone is not enough. To successfully detect an active network attacker early in their process requires high fidelity and precision. Flooding security operators with high volumes of alerts that do not reflect attacker activities will only bury a needle in a haystack and make it unlikely to be found. Security teams need a new type of vision that can uncover an attacker at work and stop them immediately.

Cyber strategy: adopting the Airline model

Companies must be wise to the evolving complexity of digital risks and use a flexible defence system, says Wavestone's **Florian Pouchet**

Cloud-based services, digital transformation and open systems are placing ever greater demands on cyber security professionals. We need to evolve beyond traditional models (usually referred to as Fortress and Airport) towards a new agile Airline model, based on a decentralised information system.

The evolution of cyber security models

In the older Fortress model, information systems were protected by a strong security wall.This was based on only one entry point. Once inside, users could circulate freely. However, this centralised information system can no longer deal with the scale of change in data and connections, as users have multiple access options across a variety of devices.

The next evolution in security was the Airport model, based on an increasingly open information system, consisting of different zones with different levels of security, similar to an airport.

Cyber attacks are increasingly sophisticated and current security practices cannot keep pace with new cloud-based IT operating models for critical business applications. These information systems are typically hosted in multiple locations. This new level of complexity requires organisations to manage this whole environment, which makes it more challenging for the Fortress and Airport models to mitigate the security risks.

To respond to this complexity, organisations need to adopt a more innovative cyber security model: the Airline model.

Key principles of the Airline model

This concept draws parallels with aircraft and passengers of an airline that are present at multiple destinations. The airline securely transports passengers using trusted airports via

MAXIM GAIGUL/SHUTTERSTOCK

secure routes. Its Operations Centre is responsible for monitoring the movement of its fleet and managing incidents or crises.

The first principle of the Airline model is knowing the most critical assets that have the highest security requirements. Organisations are continually managing an increasing amount of data accessed from multiple points. It is no longer feasible to maintain similar levels of security across the whole system. So you need to involve the relevant senior executives to identify the most critical assets and apply strict security protocols/encryption.

You also need to learn how to manage and share encryption keys through services such as Certificate as a Service (CertaaS), Key Management Service (KMS) and Blockchain.

Since data flows through a variety of access points, the second principle is to develop trusted data applications. Validating your own environment and being clear about your service and security level agreements with cloud providers is critical to ensure that applications and data are protected. Organisations can establish secure environments by assessing the trustworthiness of hosts with standard security metrics.

Bringing on board a security specialist into agile project teams (so-called 'pizza' teams) enables the prioritisation of risks and critical assets and helps to mitigate the highest threats first. This approach brings security controls closer to the developers and reduces time to resolve issues.

This model requires organisations to continuously integrate security in the environment. This could for instance be used for patch management, by releasing security fixes in a continuous and integrated way, as cutting-edge operating systems do. Organisations are encouraged to 'attack themselves' to test for potential gaps in their own security systems. To optimise testing efficiency, purple teaming can be used to merge both offensive (red) and defensive (blue) tactics.

The third key principle is to ensure secure movement of data across channels. Despite not being in control of the applications or data flow, organisations still need to adopt a dynamic security model. An Operations Centre can identify and allow secure access levels to user devices. Organisations can build reference tables for devices and servers, to validate ownership and security levels statically or dynamically. The checks vary on a case-by-case assessment of trust levels between the device, network and the application.

Challenges in implementing the Airline model

Dealing with legacy infrastructure shouldn't hinder the adoption of the Airline model. CISOs must acknowledge that they can't initiate a complete migration of the organisation's system for the sole reason of security. So they should find ways to adopt the Airline model with the understanding that legacy systems will eventually shrink by themselves. Security must be kept at the heart of the migration process.

A human workforce is no longer capable of keeping up with the volume of cyber threats, hence the need for automated security. The main implementation challenge is the positioning and timing of cyber security automation. Organisations can focus on three areas:

- Introduce automated security roll-outs that scale protection to the evolving information system needs. This includes deployment of cloud security packages and utilising Software Defined (SD) Security.
- Introduce automated detection and response to enhance and match the detection speeds to that of the attackers. This could include End-point Security Automation, Incident Response Automation, and use of Machine or Deep Learning principles to eliminate false positives.
- Introduce enhanced threat intelligence to share threat information for the common good, through trusted platforms – authorities, regulators, ISACs, etc.

Finally, successful adoption of the Airline model requires a team with the right skill sets. It is not only about reacting to risk mitigation but also the ability to think innovatively about the defence mechanism. New team structures need to be introduced including new roles such as Data Scientist and Agile Security Champion.

With organisations adopting cloud-based delivery models and committing to digital transformation, the traditional Fortress and Airport cyber security models are unsustainable.

Against the backdrop of relentless digitalisation, cyber threats are growing in volume and the nature of the threats is continuously evolving. As a result, it is vital for organisations to adopt the next generation Airline model to protect their data, infrastructure and reputation.

For more information please visit: www.wavestone.com/uk

A united front: defence in a digital world

Industry collaboration is key to effective cyber security, according to BAE Systems' **Robin Oldham**

BEE BRIGHT/SHUTTERSTOCK

Over the past few years, cyber security has steadily climbed up the business and political agenda. Putting the right protection and protocols in place to defend against cyber risk is now front of mind for senior leaders around the world.

We conducted a global survey of business leaders and IT decision makers (ITDMs) in eight counties to discover the thoughts, aspirations and challenges of businesses today when it comes to the cyber security of their organisation.

This research confirms the importance that business leaders place on the cyber security of their organisations. However, it also shows a disparity between the views of our C-suite respondents and those of the ITDMs. Both groups understand that they face threats, but their understanding of the nature of these threats, and of the way they translate into business and technological risks, can be very different. Perhaps it is no surprise, then, that 71 per cent of the C-suite executives who took part in our survey told us that cyber security represents their most significant business challenge, and that 72 per cent of ITDMs expect to be targeted by a cyber attack over the next year.

However, when it comes to their organisation's defences against a cyber attack, confidence among both these groups is very high. Our research reveals that C-suites believe a tenth of their organisation's IT budget is spent on cyber security and defence, and among ITDMs, this figure is 15 per cent. This constant spending – often year-on-year – must offer reassurance that businesses have at least something in place. But despite confidence in their people and process, many of those surveyed expected that human error by an employee would be the reason an attack on their business would succeed.

A staggering 83 per cent of ITDMs say they have a Security Operation Centre

(SOC) within their organisation to detect and prevent breaches, demonstrating that most businesses are taking the issue of cyber security seriously. At the same time, both ITDMs and C-suites confirm that the level of alerts these teams are seeing is on the rise.

A breakdown in communication

Our research revealed a marked disconnect between the views of the C-suite and those of ITDMs when it comes to their organisation's defence strategy. Both groups understand they face threats, but their thinking when it comes to the nature of these threats, and of the way they translate into business and technological risks, can be very different. This is largely down to their priorities; one group mitigates business risk, the other delivers effective IT that supports the aims of the business.

This disconnect is not the cause of discontent; ITDMs report feeling supported and believe they have the right information to tackle cyber threats. 79 per cent of ITDMs said their organisation's Board of Directors took the risks associated with a cyber attack seriously, and just over three quarters felt they had enough information to make informed decisions on cyber security. Still, while these two groups agree on many things, they often have very different perspectives on the issues, displaying a lack of clear communication. This is shaping how and when companies go about defending themselves and whether they can do so effectively.

Both groups are worried about falling victim to a cyber attack. However, senior executives, charged with assessing and managing business risk, are worried about the theft of sensitive information and customer personal data. In contrast, IT managers are concerned with a broader set of potential losses, some of which are operational. Yet many concerns reflect a more mature understanding of the consequences of a successful attack.

What's more, views varied around the nature of the threat their organisation was facing. Almost half of C-suites (49 per cent) think the most likely attackers are hobbyist hackers, while only a third of ITDMs agree, with more (46 per cent) thinking that professionals present a greater threat. The two groups also differed in their assessment of the cost of an attack: C-level executives estimated $11.6 million, while ITDMs averaged out at $19.2 million.

Perhaps the biggest disconnect is who's to blame in the event of a successful attack. While both groups expect human error by employees to be the root cause of a security breach, responsibility for the failure is where the C-suite and ITDMs point the finger at each other.

Changing regulation

Regulations around how personal data is stored, processed and controlled is a reflection of societal concerns with data privacy, and may also account for differing opinions on cloud usage.

With measures such as the General Data Protection Regulation approved across all EU states from the 25th May 2018, it's likely the wishes of those surveyed who saw regulation as a key means of combatting potential attacks may be fulfilled.

Regulation of this sort places obligations on businesses to protect data – which in itself isn't going to stop someone bent on breaking the law. What such regulation does do is create baselines of behaviour for companies to follow: rules that govern how to protect data, penalties for failures to do so, and a significant industry of organisations willing to help companies attain and maintain compliance.

Businesses also see increased knowledge-sharing – with peers, law enforcement, governments or IT security firms – as vital to supplementing their defences against cyber crime. In an ever-more connected world, it is no longer possible for businesses to work effectively in silos.

Partnerships such as the Joint Money Laundering Intelligence Taskforce and the National Cyber Security Centre in the UK, as well as the sorts of working relationships we build with organisations like the secure financial message provider, SWIFT, are vital.

What can I do?

Our research shows that the majority of respondents expect the number and severity of cyber attacks to rise in the year ahead. To counter this, they plan to devote more time and other resources to cyber security. However, the biggest positive change an organisation can make, it seems, is not necessarily to buy the latest and greatest security product, but to first improve its own internal communications.

A diversity of opinion tied to common goals is a symptom of strength in an organisation. Effective collaboration, communication and intelligence sharing are the bedrock on which effective defences are built.

Know your enemy: aware means able

Companies can't be complacent about training their staff, according to **Matthew Olney**, communications and content executive at PGI

SMATEJ KASTELIC/HUTTERSTOCK

A wealth of articles and reports have been released highlighting the cyber threats faced by companies and organisations in 2017. The language used in many of these is that of fear, but is that an effective way to promote the need for cyber security?

The answer is no. It has been several years since the issue of cyber security entered the public domain and yet we find that many people have still not got the message. If you ask people on the street what cyber security is, most folks' eyes glaze over or offer some vague recognition of the phrase. They know it has something to do with computers and they know it's something to consider, but beyond that the message just doesn't seem to be getting through.

Time and time again the media is filled with stories of breaches that occurred as a result of things like clicking on malicious links or because the victim used a weak password. Warnings of such attacks are delivered on a daily basis. Just set up a Twitter feed that looks for the cyber security hashtag and you will see that hundreds of companies and government organisations push out warnings continuously. So why are people still making such basic mistakes?

Is it because they are overloaded with dire warnings and scare stories? Is it because the very word we use to describe the issue is an instant turn off for the people on the street? Ask yourself this: what do you think about when you hear the word 'cyber'? For many people they instantly relate it to something that is necessarily negative and this is understandable.

Consider these terms: cyber terrorism, cyber war, cyber bullying, cyber attack, cyber crime, cyber hacking. Note that all are negative and are contrary to the benefits that we hope to promote from a digital experience.

In business and government worlds this lack of understanding continues to

IN ASSOCIATION WITH

PGI

be exploited by an IT security industry who perpetuate the concept of dramatic and increasingly apocalyptic consequences if their new security technology is not adopted. The industry continues to use the same complicated language that they used in the run-up to the millennium that dented its credibility and confidence in its integrity.

As a result, people are now afraid of it and this has given cyber criminals an advantage. Instead of using fear perhaps we need to promote why being cyber secure is a positive thing. Moreover, we need to normalise it.

Warning fatigue

In January, security experts released data on the most commonly used passwords of 2016 and needless to say it makes for some pretty depressing reading. Keeper examined over 10 million passwords that were released to the public following cyber security breaches and discovered that a staggering 17 per cent of those passwords were "12345".

Compared to last year the list hasn't changed much at all despite the increased media attention on all things cyber security and the huge increase in government spending aimed at tackling the issue. The worrying thing about these statistics is that it is clear people either remain completely oblivious to the fact passwords can be broken in less than a second by a hacker using basic tools or email providers aren't doing enough to stop spammers from setting up lots of dummy accounts.

Or, perhaps it is just down to the fact that people are lazy. According to the list, it is pretty clear that people want simplicity rather than actually having to go to the effort of remembering more complex passwords that can keep their data safe.

Is there a lack of understanding?

The Office for National Statistics (ONS) data released in January showed that there were 2 million computer misuse offences recorded by the police in 2016. In reality, this figure is likely to be far higher as many of these types of crime go unreported.

There has never been so much information out there about cyber security and yet we continue to see the number of incidents rise. The ease with which a person can launch an attack has never been greater but does that hold up when governments are investing billions into countering the threat?

The growing security threat from an insider's report created by Dimensional Research on behalf of Pre-empt shows that the majority of IT professionals surveyed were concerned about naïve individuals and employees. The report also shows that of the companies surveyed, 95 per cent provide end user security training, however, and very few said they believe the training is very effective. In-house training is obviously not working for many organisations highlighting the need for proper training.

The cyber skills gap

Michael Keen, head of cyber training at PGI said: "The global workforce's knowledge gap means it is largely unaware of cyber vulnerabilities, causing an unnecessarily large number of avoidable, damaging incidents requiring response and reparation – (in turn) requiring a need to transform working culture to acknowledge that all stakeholders are potential victims.

"The skills gap means a shortage of trained and demonstrably qualified people to respond effectively, be qualified to do so and be prepared adequately to help mitigate identified organisational risk. PGI help to address these shortfalls by tailoring cyber training after conducting effective training needs analysis and deep consultation with our clients to understand where they are now and where they want to be in an ever evolving digital environment, with the increasing challenges of remaining secure."

The courses taught by PGI are designed specifically to educate the right people and deliver hands on learning. With GCHQ-accredited trainers delivering bespoke courses designed to fit an organisation's needs, we can help you dramatically reduce the threat.

Being prepared

All of the evidence proves that the increased media attention and constant warnings aren't working as effectively as we would might have hoped. Instead, we need to encourage organisations to deliver better awareness and skills training.

Only hands-on, real-world experience will hammer home the importance of taking cyber security seriously. The "I'll worry about it when I get hacked" mentality remains in the mind-set of many. Only seeing the consequences and how a cyber breach can impact them and their business will they be shaken out of their apathy.

For more information please visit: www.pgitl.com

Why "wait and see" isn't acceptable anymore

The right cyber security advice is out there; it's up to companies to listen to it, writes **Damian Walton**, director of professional services at IntaForensics

I suspect that the vast majority of technology users must be at saturation point with the daily barrage of news and media articles regarding the unceasing tirade of cyber attacks being perpetrated against high street names and current celebrities. The perception may be that the threat is interesting, even worrying. Most people leave it there, and never take any concrete steps to reduce or manage the risks. For consumers that is their personal choice.

For a business, however, the effect of data breaches is subject to a "multiplier effect" where a single event can have a serious impact throughout the ecosystem of stakeholders dependent on that business – including employees and their families, suppliers, customers or service users, financial institutions, insurance companies; the list goes on.

An often quoted statistic is that 80 per cent of cyber security risks can be tackled by 20 simple to implement preventative steps. Our experience suggests that organisations undertaking a structured and supported programme improve their security significantly. The UK government introduced a relatively simple "light touch" assessment process in the form of Cyber Essentials and Cyber Essentials Plus in 2014. Having supported companies of all types around the UK, we can attest that this programme proves that even companies with a modest budget can significantly improve their chances of being secure in the face of growing cyber threats.

Being aware and then being prepared to take steps – even modest small first steps – are a far better strategy for most than "wait and see" or designing the cyber equivalent of the Maginot Line with complex and expensive technical solutions, and are crucial to any company.

Changing technology = changing threats

We live in an era of perpetually accelerating change observed by

FOTOGESTOEBER/SHUTTERSTOCK

IN ASSOCIATION WITH

IntaForensics
www.intaforensics.com

mathematician Vernor Vinge. Nowhere is this more visible that in information systems and interconnectivity. We are witnessing the electronic equivalent of the post-war arms race, with the rewards being unimaginably vast. Unfortunately, basic security is frequently an afterthought and our desire to create an environment where our every need can be achieved by the press of a button or the downloading of an app is undoubtedly exposing us to financial, moral and, occasionally, physical danger.

This new world has created a new language – 'Internet of Things' (IoT) has become a common phrase. In very simple terms, it refers to the expanding ecosystem of common 'appliances' that now have the ability to connect to the internet – think kettles, heating systems, doorbells and cars, although the list is constantly being added to.

In a similar vein to the maxim "what goes up, must come down", if a device is capable of network connectivity, the obvious corollary is that the network enables connections to the device; meaning that the device can be attacked, hijacked and used for nefarious purposes. It may simply be targeted as a means to an end, i.e. as the vulnerable gateway into a much larger organisation, or it may be the specific object of a hacker's attention such as a mechanism by which to deliver a ransomware demand.

What can we do?

Businesses can take several tangible steps to protect themselves and their stakeholders:

- Understand potential internal and external threats.
- Think "security by design" when designing processes or implementing new technologies.
- Design and test your security arrangements – consider penetration testing of your networks, run business recovery planning and appoint a retained incident response partner.

It is also important to remember that you don't have to do this all on your own. You are not alone, there are experts out there who are willing, able and equipped to provide individuals, businesses and private organisations with a range of support activity, incident response and post-attack investigation services.

Security versus compliance

Some business sectors are already a long way ahead in their efforts to remain secure. The major payment card brands mandate that all entities who store, process or transmit cardholder data must be compliant with the requirements of the Payment Card Industry Security Standards Council (PCI SSC) Data Security Standards (DSS). Depending on the transaction volumes of the organisation, this compliance might take the form of a self-assessment or may require independent auditing and validation from an accredited Qualified Security Assessor (QSA). The actual requirements reflect current threats identified against payment card environments and a substantial number of the requirements are fundamental common-sense processes, i.e. complex password enforcement, firewall configuration and a "least-privilege" access regime.

If, however, a business is attacked and payment card data is stolen, a thorough investigation will be required and can only be conducted by an accredited PCI Forensic Investigator (PFI) company of which there are currently only 22 in the world. In addition to the financial cost of the investigation, consideration must also be given to the other intangible expense – loss of productivity, reputational damage and long-term effects on the business. In such cases, it is vitally important to secure the services of a professional, diligent and empathetic PFI company.

It is no use simply treating the PCI DSS requirements as a compliance checklist. The whole essence of the Standard is security. Think security, implement security and maintain security.

Don't bury your head in the sand

Some simple guidance in conclusion must include:

- Plan ahead – if the worst happens, it is far better to have a planned response ready to go.
- If you need help planning, understanding the risks or ensuring the right technical responses are in place, ensure you get help.
- Retain what external assistance you might require in the event of an incident and get contracts or arrangements in place before any incident occurs

If you suspect that such an incident has occurred, you have the opportunity to engage a specialist digital forensics service provider who will conduct a post-incident investigation. Their actions might include deleted data recovery, examination of access log files and timeline analysis to establish culpability.

Cyber security for dummies: keep it simple

The modern CTO needs to know more about business than technology, writes Protective Intelligence director Vince Warrington

A few years ago, I sat in the headquarters of a multi-national consumer goods business as it unveiled its new Chief Technology Officer (CTO). He, in turn, had something to reveal – a surprising confession for someone in his position. He had very little interest in technology. He didn't even own a smart phone.

Once the swathe of disbelief had subsided, the CTO explained: "I don't need to know about technology – that's your job. Mine is to get the board to support the department, and if you can explain to this Luddite how your project is going to help the company's bottom line, then I'll be able to sell it to them."

Now, the company's technology had stagnated for some time, as previous CTOs failed to make their case sufficiently. As a result, the company had fallen behind its competitors in terms of digital stakes. The board was growing tired of technical jargon and were after someone who could translate and talk to them on a level they understood.

The role of Chief Information Security Officer (CISO) fits such a description. In an era so definitively digital, no business can afford to overlook the issue of cyber security. Even a company's greatest asset – its people – can expose, lose, corrupt or render vital data inaccessible, whether intentional or not. So, if you've decided you need someone to manage these risks for you, how do you go about selecting a really good CISO?

Many of the CISOs around today are highly experienced in the world of IT and technical security. They have numerous IT security accreditations (such as CISSP), have good contacts with a variety of security vendors and could, if asked, still roll-up their sleeves and start coding, or analysing the logs from a firewall. In the modern climate, however, they need a more business-focused set of skills.

Crucially, they need to be able to explain cyber security concepts to a wide range of people, who are perhaps less tech-savvy, in a language they understand. Your CSIO also needs to understand how you operate, what your risk appetite is, and what special conditions you work under – especially if these are regulatory in nature.

'One size fits all' is not an appropriate approach to cyber security, and what one business might consider far too risky might be absolutely essential in another. Indeed, this might be true for different areas of the same organisation (such as allowing the use of USB flash drives).

For all the gravitas of cyber security as a term, what it really boils down to is risk management. A CISO needs to be able to understand risk, how it applies to your organisation and how to mitigate against it. It's one of the reasons many of the new breed of CISO come from non-IT backgrounds, such as the finance and legal professions.

In many ways, the role of the CISO is a thankless one. Unlike other positions at C-Level, they don't bring in any sales nor, at face value at least, save the company money. They're only likely to only be in the spotlight if there's a problem. You need to find someone who can cope with these demands and recognise that while their contribution is crucial, it should be kept behind the scenes.

Ultimately, your CISO needs to bring the entire organisation – from the board to the cleaners, and even your suppliers – along the journey to security. They should be personable and approachable. Being an inspiring leader, after all, is more important than knowing how to configure a firewall.

For more information please visit: www.protectiveintelligence.co.uk

We're all going to have to change the way we think about data protection

Elizabeth Denham, UK Information Commissioner, says companies must get wise about the new GDPR or risk paying with their reputations

The General Data Protection Regulation (GDPR) is coming. On 25 May 2018, the UK adopts a modern law for a growing digital economy. Data security breach reporting becomes mandatory, data breaches including cyber attacks where personal information is lost or stolen could carry fines of up to four per cent of a company's global turnover, not to mention the damage to a reputation.

The GDPR builds on the previous Data Protection Act, but provides more protections for consumers and more privacy considerations for organisations. It brings a more 21st-century approach to the processing of personal data and it puts a responsibility on businesses to change their entire ethos.

It gives consumers more control over their data. Consumers and citizens have stronger rights to be informed about how organisations use their personal data. They'll have the right to request that personal data be deleted or removed if there's no compelling reason for an organisation to carry on processing it. And they'll have the brand new right to data portability – to obtain and port their personal data for their own purposes across different services.

Businesses will have to report data breaches that pose a risk to individuals to the ICO, and in some cases to the individuals affected. They'll have to ensure that specific protections are in place for transferring data to countries that haven't been listed by the European Commission as providing adequate protection, like Japan and India. Consent will need to be freely given, specific, informed and unambiguous, and businesses will need to be able to prove they have it if they rely on it for processing data.

For the most serious violations of the law, the ICO will have the power to fine companies up to twenty million Euros or four per cent of a company's total annual worldwide turnover for the preceding year. The GDPR gives regulators the power to enforce in the context of accountability too – data protection by design, failure to conduct a data protection impact assessment, DPOs and documentation. If a business can't show that good data protection is a cornerstone of their practices, they're leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation significantly.

The ICO remains committed to helping organisations to improve their practices and prepare for the GDPR. We've recently published an update setting out what guidance organisations can expect. It's essential reading, as it will help you plan what areas to address across the next twelve months.

Consistency across the EU is one of the key drivers of the GDPR, and the Article 29 Working Party – the body that currently brings together the DP authorities across Europe – is leading the way developing guidelines on some of the key aspects of the law. As the UK member of the Article 29 Working Party, we're inputting into this process and taking a lead role on a number of priority guidelines aimed at organisations.

Could you say - hand on heart - that you're ready for GDPR?

There will soon be 20m reasons to get it right

GDPR* is changing the way organisations - large and small - need to look after their data.

Big penalties of **up to €20m** can be handed out to organisations that get things wrong.

Don't be one of them.

Time is running out before the new rules - and penalties - come into force.

Call us now for **sensible, risk-savvy, cost-effective advice** on how to properly protect your data - and stay in control.

Phone 01296 621121 or email cybersecurity@avatu.co.uk

Avatu – cybersecurity advisors to inspiring companies

avatu

www.avatu.co.uk

* GDPR - General Data Protection Regulation