NewStatesman

Spotlight

CYBER SECURITY / WHAT EVERY CONNECTED PERSON NEEDS TO KNOW

Dido Harding / Chi Onwurah MP / Tiffany Rad / Stuart Aston

In association with

avatu

Ignorance is no longer an option

While politicians have a history of saying boneheaded things about technology in general – and cyber security in particular – Donald Trump's comments this month bear repeating. "You know," said the man who would like to be in control of the world's second-largest nuclear arsenal, "cyber is becoming so big today. It's becoming something that a number of years ago, a short number of years ago, wasn't even a word. And now the cyber is so big."

While it's bleakly amusing when a presidential candidate struggles to form a coherent sentence about cyber security, more worrying – and more revealing – are the statements in which Trump has hinted at a desire to profit from cyber crime: on Twitter and at a press conference, he has openly invited Russian hackers to direct their efforts at President Obama and Hillary Clinton. Trump has since claimed – perhaps after his legal team read the Computer Fraud and Abuse Act – that these comments were 'sarcastic', but they reveal something important about cyber crime: those who don't understand it see it as remote, virtual, not morally equivalent to real crime – and for this reason, potentially useful.

Trump's failure to take seriously the ethics and consequences of cyber security are far from unique, in politics or in business. In fact it signifies a global trend; at every level there is now a need for education and participation, from the experts who run our national infrastructure to the millions of small businesses that depend upon technology to run efficiently in modern Britain. It is no longer sufficient to hope that we will remain unaffected: the only question is how best to manage the threat.

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

Supplement edited by
Will Dunn
Guy Clapperton
Zoe Grunewald
Design and Production
Leon Parks
Sub-Editor
Tracey Beresford

Commercial Director
Peter Coombs
+44 (0)20 3096 2268
Account Director
Penny Gonshaw
+44 (0)20 3096 5269

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 6-12 May 2016. © New Statesman Ltd. All rights reserved. Registered as a newspaper in the UK and US.

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

COVER ILLUSTRATION BY SAM FALCONER

Cyber security for government and big business is well funded. But, speaking to Will Dunn, shadow minister for culture and the digital economy Chi Onwurah says the needs of Britain's 5.4 million small businesses are being dangerously overlooked

"We are only as strong as our weakest link"

The link between a parliamentarian and their appointed subject can be tenuous – Andrea Leadsom, then climate change minister, famously asked in 2015 if climate change was real – and this disparity becomes more apparent the more technical the portfolio. The current digital minister, Matt Hancock, does have some tech experience – he worked briefly for his father's computer company – but his opposite number, Chi Onwurah, is that rare thing: a politician who is also a highly qualified engineer.

"Engineers are definitely under-represented in government," agrees Onwurah. "And they're under-represented in the Civil Service, because the Civil Service has had an emphasis on generalism. That basically meant not being an engineer. It meant having a first in classics or medieval history, and there haven't been career paths for engineers and technical specialists. The Civil Service says it's addressing that, and I hope it is."

She adds: "We are under-represented in political parties, too, because the routes by which most MPs become MPs do not include engineering. We've got lawyers, spads [special advisers], PR people, journalists, but we don't have engineers.

"I joined the Labour Party when I was 16. I wanted to become an engineer or scientist from the age of about nine. I looked to politics and technology as the two ways of changing the world for the better, and first of all I thought I wanted to be an engineer, as that was also what interested me – making things work, building things, so I went into engineering. It was a fantastic career and

“I’m coming to the conclusion we need to scare people”

I’d recommend it to anyone and everyone. Particularly during my time working in Africa as an engineer, and later at Ofcom, it really highlighted to me the importance of public and government policy in making technology accessible.

“I could design the best broadband network in the world – I still think I could,” she says, with the confidence of someone who has clearly not quite given up being a telecoms engineer, “but only if people had the right income, the right skills, the necessary rights to lay cables, to actually get to use that fantastic technology. And so when it was announced that the MP for the bit of Newcastle where I grew up was standing down, I thought, ‘Let’s see if we can.’ ”

It was in Onwurah’s pre-political career that she first encountered cyber security. “Quite early in my career, as an engineer for Northern Telecom, or Nortel, we were looking at how access to telecoms switches were password-protected or not. We didn’t call it cyber security then; it was just security. The first time I encountered it as a citizen issue was ten years ago at Ofcom, when I was asked to write a report on malware.

“I went back to Ofcom’s senior board with all these tales of black hats, honeypots and viruses, and they thought I’d been playing *Dungeons & Dragons*. A lot of the terms I used then have changed but the actual threats and challenges, whether they’re to mobile telephony or fixed lines or desktop PCs, are still there. I remember learning about honeypots and bot networks long before these terms had any common understanding.”

Onwurah also has plenty of experience of battling to make the case for cyber security. In 2005, she says, even the Ofcom board was slow to appreciate the risk. “They were sceptical, I think, about whether we needed to invest real resource then. Ten years on, those threats are very, very real – they’re part of the daily, lived experience of everyone who’s online.”

Reluctance to address this risk, she says, persists today: “I’m still very surprised at the level of complacency. Ed Vaizey [digital minister in the Cameron government] used to talk with great pride about putting over £600m into cyber security, but that had almost all gone into the security services – MI5 and MI6 – and critical national infrastructure. It hadn’t gone to the police force, to deal with the day-to-day rising tide. And they’re totally under-resourced, so I think there’s still huge complacency.

“We’ve just seen today, and I’ve asked for an urgent question on it, that GCHQ has raised security questions about Universal Credit, and that’s one of the reasons it’s been delayed. I’ve been raising security questions about Universal Credit since about 2012, because they didn’t design security into it from the start, and you’ve got millions of vulnerable people with low digital skills, which creates a huge potential for fraud.

“I don’t want to put people off

technology. I'm a tech evangelist – I think it can do amazing things for us and make our world better – but obviously it can also be used for scams, IP theft and more, and it's a real dilemma about how we raise the profile of the threat without scaring everybody silly. But I'm coming to the conclusion that we need to scare people, because it's not being taken seriously."

Onwurah even has the dubious honour – increasingly common among public figures – of having been hacked. She found the experience informative: "It was a very good demonstration of the risks small businesses face. Our office is about the size of a small business. From the investigation that was done, we know that one of my staff had gone on to a perfectly legitimate website in the course of their work, where there had been an ad that had downloaded malware on to their computer. That had spread over the course of about three days on to our servers, and then the ransomware locked up our files and demanded a ransom."

For Onwurah's well-supported team, this wasn't a huge problem. "We have a big department supporting us. We also had all our casework on a separate server, which meant there was no compromise of constituents' data. Our digital services identified the virus, cleaned up our systems and restored us to the day before the virus was downloaded – we lost a couple of days' work. But if we had been a small business, we wouldn't have had access to that kind of support, and it could have put us out of action for a lot longer."

What many small businesses may not realise is that their cyber security constitutes a responsibility not only to themselves, but to others. The law takes a dim view of businesses that do not protect their customers' data.

"We have a duty of care, which is why it was so important that our constituent data wasn't compromised, but a small business could find themselves liable in that respect. Also, small businesses are in the supply chains of large businesses. I'm really keen to emphasise to large businesses and government that protecting the big boys is all very well, but actually small businesses are part of everyone's supply chain, as well as having access to important data. We're only as secure as the weakest link."

"Almost all the £600m went into national security"

Is an institution such as the new National Cyber Security Centre (NCSC) solely for the big boys, then? "To be honest, small businesses generally don't have the resources themselves to seek out the right sort of support," Onwurah says. "The NCSC is focused on the financial sector, and the financial sector is hugely important, but it clearly doesn't see it as its role to raise the overall standard of cyber security."

So who is there to help the little people? "That's the key question. The government put in place the Cyber Essentials programme of accreditation for small businesses but it's had very low take-up – just over 2,100 when I last

Fortress GCHQ: while security services are well funded, Chi Onwurah says this is at the expense of programmes to improve cyber security for small businesses

asked." From the UK's more than 5.4 million SMEs, that represents a take-up rate of 0.0004 per cent.

"One of the things I want to look at," she adds, "and one I know the Institute of Chartered Accountants in England and Wales, for example, are looking at, is linking insurance to cyber skills. So you get a discount on your insurance if you've trained in cyber skills."

Should small businesses have to display their cyber credentials, as restaurants display their hygiene certificates? "There is a level of cyber hygiene that we need to be promoting and enforcing," Onwurah says, "but part of the challenge is having the skills for enforcement. That is one of the things Cyber Essentials was supposed to address, but I don't think it has."

She believes that cyber security is too important to be left unenforced: "Government should recognise that it has a real role to play here, that it's not enough to say, as they have, that the market will deal with it, and that people have recourse to the small claims court if they feel that their data have been mishandled. Government should be much more proactive. It should be working with insurance companies, to look at driving the incentives by linking premiums to cyber security knowledge, and looking at kitemarks and standards.

"There isn't cyber-security support in a box. We need to look at stimulating the small-business cyber-security market, so that there are more products and better services out there. And yes, there should be ways of making that more visible to consumers. Look at the role that the fire brigade plays in helping small businesses with their fire alarms – there are many examples where the state intervenes to ensure a level of security, because it's in the interests of everyone, but this government hasn't recognised that cyber security is just like that."

Like many others, Onwurah is dissatisfied with the low level of reporting of cyber-security incidents. "One of the issues with reporting is that people often feel stupid – they don't want to report it; it's not good for business – so the level of reporting may not yet match the level of the issue. But now that cyber statistics have been added to the police crime statistics, we've seen a huge rise in reporting, and I think we're going to see that in small businesses as well."

We should, she says, see this as a chance for Britain to become a leader in cyber security: "There's a huge opportunity here."

So: what does Brexit really mean for cyber security?

Avatu's **Joe Jouhal** says that in or out, the best-run organisations will still shake their security all about and make sure they're ready for new data protection rules they simply can't afford to break

We're off - but is your company packing GDPR protection?

IN ASSOCIATION WITH

avatu

As everyone knows, the outcome of the EU referendum has made life a little more uncertain. Organisations have had to take a long hard look at their business activities and investment and growth plans as they second guess the new world future.

Before the referendum, cyber security had started to pick up some impetus in the best-run, most forward-thinking organisations.

Leaders in these places have already acknowledged that cyber security is a serious business challenge, rather than something that applies only to the IT department, and are, consequently, giving it the right focus, investment and priority.

The government's new Cyber Security Centre, which is due to be operational later this year, will also build more confidence.

And, in theory, so should the EU's new, far-reaching, General Data Protection Regulations (GDPR) with their extra security requirements and big penalties. Or this was the case, until Brexit somewhat muddied the waters.

The landscape – before the vote for Brexit

Earlier this year, all EU countries adopted as law the GDPR. This is something of a game-changer when it comes to data and cyber security.

The new law significantly strengthens data protection rules for all EU countries, and for any organisation – anywhere in the world – that wants to do business within the EU, regardless of whether it holds personal or sensitive data or not.

While the regulations came into force on 24 May this year, there's a two-year grace period for organisations to get their houses in order before penalties

SHUTTERSTOCK

begin to apply. Fundamentally, GDPR means, from May 2018:

- Organisations will have to report data breaches to the individual people affected, and the national regulator, within 72 hours of discovery. This means they will need to be prepared for fast action after a breach is uncovered and aware that news of a breach will always be public information, and plan accordingly.
- EU citizens have a 'right to erasure', which means an organisation may have to delete every record they have on a particular person (this is a significant challenge for many, as they don't actually know what data they have and where every piece is held).
- Some companies will need to have a dedicated data protection officer – but not all will.
- Organisations need to show they have a sound, risk-based approach to data protection and a privacy strategy.
- Penalties for rule breaches can be up to €20 million, or 4% of global turnover (this is perhaps the most sobering part of the new rules).

The landscape – after the Brexit vote

No one yet knows when the UK will leave the EU. But we do know it won't be before January 2019 – at least eight months after GDPR comes into play.

The government hasn't yet given an indication on the future fate of GDPR or if it will stay UK law; there are bigger fish to be fried first. But the consensus among many experts is that nothing is likely to change – or if it does, it may not change for quite some time.

What we do know for sure is:

- If you have clients or market in any part of the EU outside the UK, GDPR will definitely apply to you no matter what happens within the UK – so you need to prepare now.
- UK Select Committee MPs are also urging companies to penalise CEOs for data breaches that happen in their firms. The Culture Committee – which has responsibility for cyber security and the digital economy - wants to make sure digital security is a priority for chief executives by linking it to their pay. This means the issue of data security is hotting up in the UK, too.

The best advice: just do it anyway

Regardless of Brexit, the most forward-thinking organisations are becoming GDPR-ready, even if they work only in the UK.

It's a good idea for any business to comply with the principles of the new law, because it encourages organisations to take data security more seriously, and ensures they are less vulnerable to cyber attacks and data breaches caused by insiders.

It doesn't have to be complicated or massively expensive process. Organisations can improve their security relatively easily.

Think about it: even without the risk of a GDPR penalty, could you say – hand on heart – that your organisation is prepared for, and could cope with, a data breach, and the associated fallout?

If the answer's no, you don't need to wait for clarity on this aspect of the law. You need to take advice and act now; Brexit is merely a distraction.

Keep on top of cyber security, data protection and Brexit

We're running a series of briefing sessions to keep people up-to-date with the latest developments on GDPR, cyber and data security and Brexit. They will include a leadership briefing event, a webinar and email updates.

To find out more or join the mailing list email: **cybersecurity@avatu.co.uk** or call **01296 621121**.

Could you say - hand-on-heart - you are prepared for a data breach?

If the answer to this question is no, and you need help now, call our security advisors on **01296 621121** or email **cybersecurity@avatu.co.uk**

We can help you assess how effective your security arrangements are right now, develop a plan to improve them for the future, and keep you in control.

ADVERTORIAL

Biometrics and the new state of security

Mission Impossible-like systems are becoming a reality but they need standardisation, says Fred Svedman, public sector director for Unisys

As people have become more accustomed to using online and digital services, they have also had to become more used to increasingly advanced security methods. Once, not too long ago, online services were accessed only by passwords. However, as data breaches have become more pernicious, many providers have now implemented two-factor verification.

There is a lot of work being undertaken to develop the next stage in authentication protection, and we at Unisys believe it to be biometrics. Already great strides have taken place to bring *Mission Impossible*-like systems into reality, and there are a wide variety of companies that offer solutions and are committed to extensive and exciting R&D.

A number of public sector organisations have already invested in implementing biometric authentication systems, as the technology can be used by government departments to verify the identity of citizens accessing public services both online and via the telephone.

Over the past year or so we have also seen biometric authentication technology introduced on mobile devices such as laptops and smartphones, available directly to the general public. This means that there is not only a logical case to be made for biometrics, but a growing expectancy from the wider user base that the technology will become widespread.

As organisations seek to update their authentication systems, they appear to invest in several different solutions so that they are able to capitalise on the best opportunities available. However, what we're seeing is that almost every provider is using its own protocols and standards – meaning that for every organisation there are differing biometric systems, some that are able to work together and others that aren't. This is causing huge inefficiencies both in costs and IT infrastructure, and when you consider the scale of government departments these complexities are multiplied exponentially.

Between service providers, biometric technology suppliers, identity service providers, consumers and smartphone manufacturers there is little or no coordination. As such, government and businesses either sit and wait or make their own investments in something that might only be suitable temporarily.

More generally, there are a number of other concerns that arise from a deeply fragmented and unregulated biometrics market. The most pressing is to do with the data itself, how it is stored and accessed. With such a huge amount of sensitive information about specific individuals, it is of the utmost importance that any and all personal data is securely stored and that the identity register is owned by a reputable and trustworthy provider.

That being the case, now is the time for all parties who have an interest in biometrics to act and collaborate in order to develop industry-wide standards. Doing so will mean that consumers and businesses have more confidence in using the technology.

The industry needs to work together to create maximum value before it becomes too complicated and diverse. Only in this way will government departments and businesses be able to offer their citizens and customers digital services with the latest biometric technology of their choice, in the knowledge that it is safe.

For more information, see unisys.com

IN ASSOCIATION WITH

UNISYS

"The first ransom demand was not a good moment"

Dido Harding, chief executive of TalkTalk, speaks candidly about how she managed every CEO's nightmare: a cyber attack that compromised 157,000 customer accounts

The hack may have begun weeks or months before – it is still subject to a criminal investigation – but the first telltale warning emerged on the morning of 21 October last year, when TalkTalk's engineers noticed a latency in the company's sales and service site. While this is not a rare occurrence, it can be an expensive one.

"A priority-one technical incident," Harding explains, "because customers couldn't access the website fast enough. I saw that had happened, mid-morning. Often when websites start running slowly, it's because they're under some form of attack."

Harding returned from a lunch meeting to find the problem ongoing, and becoming more serious. "Our escalation process is to immediately put the executive committee together if there's something very serious. On that call, the team talked us through that there was indeed a live attack and that, at that stage, we believed that the attackers had breached through one defence into an online database."

It was during this meeting that the true scale of the hack became evident – not from TalkTalk's security team, but from the hackers themselves. Harding recalls: "Roughly three or four minutes into that call – I was sitting in a meeting room in Farringdon [in central London] – I received the first ransom demand from someone purporting to be the hacker.

"That," she adds, "was not a good moment. It's not a normal thing to receive a ransom demand in your in-box. I felt physically sick."

Due to the ongoing criminal investigation, Harding can't go into detail about the contents of that email, but she says that "it was very clear that it was credible". For the chief executive of a national telecoms company with four million customers, there was an immediate necessity: "I asked my security director to get hold of GCHQ, straight away."

A foreign land

"At that point," says Harding, "we immediately went into serious incident management. It was very quick: we flipped from a normal business objective to 'hold on, this is a proper crisis'. That's a very different prism through which to run your organisation.

"I've had 20 years, 25 years of running business. I've been well trained by a number of amazing organisations and I've got a lot of implicit, subconscious pattern recognition on how to make business decisions. [But] what we discovered in the cyber attack, from that moment of getting the ransom demand onwards, was that none of us had been prepared to live in this world of spooks. We very quickly started to do what we normally did – to rely on gut instinct – until we realised that our gut instincts were based on having watched *Spooks* and James Bond.

"You can't rely on your intuition and your instincts if you don't have years of pattern recognition, if you haven't lived in that world before. We had to very quickly rely more on data and evidence, and listen more to the experts from the different security services.

"Likewise, we'd had a long-standing relationship with BAE Systems, who ran our security operations centre, and I was on the phone to multiple board directors – including the chairman – of BAE, asking their advice, because of course they do live in that world. In that sense we knew very quickly that we were in a foreign land."

One of the defining characteristics of a major cyber attack is uncertainty. "If somebody breaks into your shop," Harding explains, "you know who it is. If a foreign army has just invaded your

▶

“Once it becomes mandatory to report that you’ve had data stolen, blackmailing you is a waste of time”

▶ shop, it’s pretty visible, and if it’s a local gang, it’s pretty visible. In a cyber attack, in the initial period of knowing you’ve been attacked but not knowing what’s been taken or who’s done the taking, you really genuinely don’t know if you’re in the territory of a state actor – a foreign state – or one individual acting maliciously from inside the business, or a few people from outside. You just don’t know. That makes it terrifying, in the heat of the moment.”

What’s missing?

As the day progressed, GCHQ put the TalkTalk team in touch with the right people at the National Crime Agency and the police. Harding continues: “That afternoon, the case was passed to the Met police, who immediately kicked off their investigation. We’d already taken the decision to bring down all of our systems, which is the safest way to act to protect your customers’ data, so the urgent thing for us, that afternoon, was to work out what might have been stolen.”

As evening drew in, this became a global effort. “We used, that first night, a team from BAE based in the US, so you’re trying to use the time zones in your favour to get analysts and computer programmers immediately mobilised to start looking through lines of code to see what’s happened. [The aim is] that overnight you get to a place where, first thing in the morning, you can have a view of what’s actually been taken.

“I probably slept quite easily on that Wednesday night,” Harding recalls. “I didn’t quite know what was ahead of me. I knew that there was an issue. I knew we had all the right people working on it. I’d had great advice from the law enforcement agencies on what to do, and I was expecting that someone would give me, first thing in the morning, quite a black and white view of what had been stolen and what hadn’t. What I now know is that that was a very naive hope.”

Going public

The following morning brought no such certainty. “At 8am on the Thursday, we had another incident call with the executive leadership team, and they took us through what they knew. What they told us was that it was going to take quite a long time to figure out which customers had been affected and what data had been stolen.”

Harding and her team now faced a difficult decision: try to solve the

problem quietly, or go public. "That was the biggest decision we took – if we had chosen not to warn our customers that day, but instead had waited two weeks and said 157,000 customers had been affected – it wouldn't have been news. The actual number affected was quite small. What was different was that we thought we could protect our customers, at that moment in time, by warning all of them."

The decision to go public was partly informed by TalkTalk's knowledge of its customers. "What we suspected then, and we know in spades now, is that having somebody steal your bank account details, in and of itself, isn't dangerous. The problem is that the criminals then use that data to prey on the most vulnerable in society. That's not just happening to TalkTalk customers – it's happening in the UK and globally. The concern we had is that we serve a lot of those most vulnerable groups in society. We're a value provider – a lot of people getting a broadband connection for the very first time get it from us – and we worried that they would be the most easily conned by these criminals pretending to be TalkTalk."

Does Harding believe other companies have kept their own data breaches quiet, and avoided the headlines that have plagued TalkTalk for the past year?

"I don't know for sure, but I think so. The awful truth is that the actual data isn't very valuable on the dark web any more. What is valuable is people being afraid of their brand reputations. So I think this is quite a popular crime, and it's one of the reasons we think it ought to be mandatory for businesses that experience a successful cyber attack to have to tell not just the Information Commissioner's Office, but to tell their customers. Not least because it's actually the only way to give people the confidence to trade online.

"It never used to be mandatory to report health and safety incidents on oil rigs, until after the Piper Alpha disaster. Once it was mandatory to report it, health and safety got a lot better. Once it becomes mandatory to report that you've had data stolen, blackmailing you is a waste of time. Blackmailing you to keep quiet – you can't, because you've got a legal obligation to tell everyone."

While the security team continued to search for answers, Harding focused her other teams on providing TalkTalk's customers with information. But not everyone was eager to tell the press: "When we talked to the police around lunchtime, they were really adamant that they didn't want us to go public. We ended up having a long conference call with the Metropolitan police's hostage negotiation team, where we felt like we were almost from scratch trying to work through whether or not you should treat a digital ransom demand in the same way that you would a physical one.

"[The police] were incredibly professional and always very supportive, but in the end, their objective is to catch the bad guys. Our objective was to protect our customers. If I could change anything, I would have gone out at lunchtime or mid-afternoon in a much more measured way. It would have ▶

▶ been better for our customers if there had been a more ordered communication through that Thursday afternoon.

"I've heard other CEOs since – with me in the room – say that it's important not to go too soon and to wait until you know the scale. I couldn't disagree more. If you can protect your customers by warning them of a potential threat, then you should do it."

The recovery plan

Harding spent the Thursday evening appearing on news outlets. First thing on the Friday morning she was interrogated by "a very grumpy John Humphrys". In between media appearances, she began planning TalkTalk's recovery.

"I was setting up the operation of the company to be able to run what became, for several months, the most important thing that the business was doing. I pulled out my group change director on the Thursday night and made him the programme director for the recovery from the cyber attack, and I asked him to mobilise all his best programme managers and project managers, to assign them to workstreams.

"So we had a workstream to work out what data had been stolen, how they got in. We had a workstream for communicating with customers and managing customer contact. There was a big workstream dealing with all the big law enforcement agencies, which we called the 'cops and robbers' workstream – jokingly. You need to have a sense of humour to survive these situations."

A powerful lesson

As the weekend arrived, one of the main priorities was to reassure four million anxious customers. "We started polling our customers, that first weekend, running statistically significant consumer research to understand how they felt about what was going on.

"We tracked whether or not the messages were getting through, and whether or not we were building trust in what we did. What we saw, throughout the first three weeks, was that the more communication we engaged in, the more customers thought we were looking after them. Absolutely contrary to what a lot of commentators at the time were saying, we were using customer insight to drive how we supported our customers. It was such a powerful lesson for the whole company, that if you ask your customers what they think and act on what they tell you, things work out OK."

Have they worked out OK, then? Is TalkTalk back in control?

"That might still be a work in progress," Harding says. "On the Sunday night after the attack, I scribbled down one slide to present to my board, with three phases: one to two weeks to be off the front pages of the papers and to get the call centres under control. Then we said we were going to take until Christmas to stabilise the business, and a further three months reviewing what this meant for the strategy of the business. That is exactly what we did."

Harding's advice for others in this situation is to get involved. "The temptation is to assume that if you're not an engineer – and I'm not – you don't really understand this stuff enough to know the risks you're taking. Businesses and leaders want to ask the question 'Are we safe now?', and that is entirely the wrong question to ask, because the only answer you can give is no. No organisation is going to be completely safe from cyber attack.

"You need to ask what risks you're taking today by trading online, and what risks would you mitigate if you did more, and what risks would grow if you did less. You don't need a PhD in electronics to do that. So the biggest piece of advice I give to people now is to stop asking 'Are we safe now?', and instead get your engineers and technologists to tell you what business risks you're exposed to, based on where your security programme is today.

"You'll find they find it incredibly difficult to answer the question, and the more you push them, the more you will realise you don't need a computer science degree to understand the answer. And then you are taking business decisions while knowing the risks."

She was grilled by "a very grumpy John Humphrys"

How to win gold-standard cyber security

There may not be a bike or a boat in sight but the success of Team GB in the last two Olympics has many lessons for forward-thinking companies, says Joe Jouhal

Team GB's success this summer was remarkable in many ways. But when you look a little closer, it was unremarkable in many more. Those medals weren't won exclusively in Rio; they were won in meeting rooms and science labs, on cold February mornings on the road, the track and in the gym, over many years.

In 1996, Britain reached an Olympic low by winning just one gold medal in Atlanta. A rethink was needed, as was investment. In came National Lottery funding, and a new mindset.

That's where I see many parallels with developing information security strategies: there are so many different elements to prepare for, and there are so many different things that can go wrong. You can never say you won't lose. But by taking the right approach – and funding it correctly – you can reduce the chance of that happening, and the impact it has if things go wrong.

Leading analysts and think tanks, such as Gartner, agree that in today's world, to aim for total prevention is futile. They advocate an information-focused, people-centric approach to cyber security – exactly the approach that Team GB took in preparation for each of the last two Olympics.

There are seven areas where gold-medal cyber security and Team GB overlap:

1. **Prepare to be radical**. If you've won one gold medal in Atlanta or if you're still relying on firewalls and antivirus software as your main cyber security defence, you need a rethink.

2. **Decide what matters most**, and then focus on this. For Team GB, this is winning medals, because it underpins funding, and they can't afford to lose it. For cyber security, this should be protecting your most valuable data – which you can't afford to lose, either.

3. **See the problem as a whole**, but break things down to component parts and look at each one separately. Where are your weak points? Where are the one per cent gains that collectively make a big difference? The Team GB boxing team realised that 20 minutes a night of extra sleep could be gained with longer, wider beds at their training centre. By doing just four simple things you can stop 85% of common security threats. Simple, inexpensive new email technology can stop 94% of successful malware attacks.

4. **Look carefully at your people** and the things they do. Think about their minds and their learnt or natural behaviours. What can you do to make up for habits or frailties, such as clicking on dodgy links or accidently leaving laptops on the train? Somewhat ironically, the Team GB cycling team banned their Rio bound teams from having a 'Brazilian' or shaving or waxing at all, and had no more trouble with saddle soreness.

5. **Get in the best tech you can**. Technology can provide you with an edge and make up for the mistakes people make.

6. **Analyse things as you go along**. Find out what happened and why. Analytics and digital forensic tools are increasingly an important part of cyber security.

7. **Keep an eye on the prize**. Focus on the things you can control (all of the above) and don't waste time, money and energy on the rest (such as the performance of the other teams, or trying to second-guess where the threat will come from next. Here, you can never win).

Joe Jouhal is CEO with Avatu, security and digital forensics advisors to forward-thinking companies

This woman can hack prisons… and that's a good thing

She can, in theory, open the doors in any prison in the US from her computer. Thankfully, Tiffany Rad is a "white hat", an expert who uses the tools of the hacking trade to find cyber-security weaknesses before the bad guys do

In the state of Virginia, possessing lock-picking tools is a criminal offence. Why else, Virginian law asks, would you have lock-picking tools if you don't intend to pick a lock? And why would you pick a lock if you don't have criminal intent?

For many in the hacking community, this train of thought falls short of rationality. Tiffany Rad, a practising lawyer who is also a "white-hat" hacker and penetration tester, tells me that her father taught her to pick locks as a child, and that she will be teaching her own children the same skill. "It teaches problem-solving," she says, "but also understanding how something works, how it can be broken and what would make this lock harder to pick."

Helpfully, she has a lock to hand. "In this example we're doing, it would be more pins within the lock, picking the pins at different angles, using different tools that would make it harder."

She points out that, in the UK, an organisation called Toool teaches people how to pick locks – "and then many go on to become locksmiths".

White-hat hackers could perhaps be considered the locksmiths of the cyber-security world. They search for weaknesses and vulnerabilities within a company's system and bring it to the attention of the organisation, for the good of their security. "Hacking" may be a term that gets a bad press, but the key difference between "good" and "bad" hacking, Rad argues, is intent. White hats intend to cause good, helping companies to improve their security from the perspective of a potential "black-hat" hacker. Just as a locksmith may carry his lock-picking equipment on his person with no harmful intent, a white hat may use their hacking capabilities to make gateways stronger. Ability doesn't equate to criminality.

In 2013, the Turner Guilford Knight Correctional Center in Miami, Florida experienced a potentially catastrophic security breach when the cell doors in the maximum security wing of the prison simultaneously opened, allowing prisoners to leave their cells unguarded. Although the incident was never proven to have been the work of a third party, or black hats, concerns were raised that it might have been an attack orchestrated from the outside. Video footage seemed to suggest that one of the inmates had anticipated the opening of the doors, proceeding to carry out an attack on another inmate. In the years since, the spectre of a hack on a maximum security prison has overshadowed discussions about the future of cyber security.

The Miami prison episode inspired Tiffany, and her father, the security consultant and engineer John Strauchs, to see if it was possible to hack an industrial control system in such a way, and to shed some light on whether what had happened at the prison could have been the work of sinister forces.

"I had the idea for this project initially because I was studying the mechanics of the Stuxnet worm," Rad explains.

Stuxnet was a computer worm that collected information and compromised the centrifuges in the Iranian nuclear programme, causing them to self-destruct. Although speculation remains about who was actually behind it, there is little doubt about the severity of the hacking: a fifth of the centrifuges were destroyed and huge damage caused to Iran's nuclear programme.

Stuxnet specifically targeted the programmable logic controllers (PLCs) within the system. PLCs are commonly used in prisons and other industrial facilities such as power plants. "The programmable controller acts as a simple junction," says Rad. "One wire can go back to the control centre instead of having tons of copper wire going through

INTERVIEW: WILL DUNN, WORDS: ZOE GRUNEWALD

these facilities. So that type of controller is used in a lot of places.

She continues: "We wrote an exploit [the software] in just two weeks. We had purchased a programmable logic controller on eBay. The fact that we were able to create a project like this in two weeks [made it] evident to us that the bad guys already know how to do this – and they have a lot more funding and time than we have."

The discovery was vital security information, because although the system was known to be hackable, the fact that it had been so easily infiltrated by outsiders raised considerable concern.

"I think there had been other people talking about industrial control-system vulnerabilities before," says Rad. "This wasn't a surprise. What was a surprise is that we could do it in two weeks and hire equipment off eBay, and if we didn't want to pay for the appropriate legal licence it would have a cost $500 plus the cost of an export writer.

"Where do we hear that these facilities are not connected to the internet but there would be a huge national security risk if something actually happened? We found so many places. It wasn't just correctional facilities – it was public transit, heating and air conditioning. In the middle of summer when it's very hot, you can do significant destruction to the computer if you turn up the heat and turn down the AC."

Despite the benefits gained from their expertise, attitudes towards white hats are still somewhat hostile. The Wassenaar Arrangement, a multilateral agreement intended to strengthen international security, has disadvantages for the cyber-security industry, Rad argues. Amended in 2013, it now includes the control of intrusion software, which she says makes the job of white hats harder: "When you're hired as a penetration tester, you need to have a good set of tools. And when there is legislation that affects your ability to collect these tools, create them, buy them, sell them, trade them with other people that do this kind of work, that's not good."

Some organisations are more grateful to white hats than others, Rad says. "As an attorney I get calls frequently from those doing security research that want to tell the company about their vulnerability. They want to disclose it to them but they're afraid they're going to turn around and get sued.

"So, I help facilitate that information trade-off while protecting that person's identity. As an attorney, I get a special privilege where I don't have to tell anyone who my client is. I can just say, 'You need to know this information. I'm protecting them. They are a client of mine. I'm going to give you the information, but please let's not turn it around.' Most of them [her clients] are white-hat security researchers who have stumbled on something and want them to fix it."

The situation for these people is improving, she adds. "I'm glad to say that it's changed over the years. When I first started ten years ago it used to be very confrontational. I'd call [and say], 'I'd like to speak to a security engineer.' Sometimes that didn't exist – I'd be put through to IT, and IT is not the same. Then they would say, 'We're going to have you talk to our attorneys.' It's not a good way [to respond] because the researcher gets very nervous and the other side makes you tell them who did this, and it's just not right.

"It's a trade-off, and nowadays you need to welcome this type of information. You want to hear it from someone who is a white hat before you read it in the paper that someone else with malicious intent just took all your data and put it in the bin."

Indeed, it is in the company's best interests to respond with gratitude to any security breach by a white hat, as Rad makes clear: "Because if I know about it, chances are a lot of people do too." These people may not necessarily be the locksmiths.

It's not just companies and industries that need the help of white-hat hackers. White hats can also identify threats to their country's national security. In 2015, a man claimed that he had hacked into ▶

Warning Langley: Rad's findings earned her team a meeting with the CIA

the entertainment system while on a United Airlines passenger jet, and had subsequently turned the aircraft on its side by putting its computer system into "climb mode".

"If what he did was true, that's pretty irresponsible," Rad says. "But if he was able to do this, then the aviation service has some vulnerabilities."

Whether someone could hack a plane is undoubtedly a question for national security. "It's hard to say, because the newer ones have different networks but, saying that, the older ones will be up in the air for a while."

Ultimately, Rad argues, the key to preventing attacks is not trying to speculate whether they could happen, but using penetrative and offensive testing to actively simulate security breaches. If we are to do that, we need to listen to and encourage the white hats. "I want to believe that the aviation industry looks at things from a hacker's perspective."

She adds: "I'm also a dual [US-Latvian] citizen. Latvia and the Baltic States are very nervous about Russia's capabilities – it's the future, I think. Every government is going to need to have these [cyber-security] capabilities and if you make it illegal for your citizens to create or design these, you are going to be stifling your own defence."

The Pentagon this year launched its first "bug bounty" programme, in which it challenged the white hacker community to penetrate its systems to try to find vulnerabilities within them. It received 138 legitimate reports of vulnerabilities, which were then patched up.

If the Pentagon has come to understand the benefits of white hats, why do we continue to legislate against them? It comes back to the Wassenaar Arrangement, Rad says. "I don't think it was intended to be written that way, but that was the consequence of that."

However, she remains optimistic: "There are some people I know who cannot work for the military or US federal government. They don't want to but they're very good at writing these exploits. They just don't want 9-5 jobs. The way that they work and their personality is not the same as everyone else in the army or the navy. But the [armed services] would like these people to share some of the information they have with them."

In fact, the Pentagon has in recent years recruited software writers, she says. "They need people with these skills, and you don't have to wear a suit every day."

Overall, as with many things, the key lies in education and greater public awareness, so that hacking is more widely seen as a beneficial tool.

Rad concludes: "Hopefully the next generation will be telling employers: 'We need to design this with security in mind because here's an example of when this didn't go right. Let's not do this again.'"

"The armed services need hackers"

Achieving diversity in cyber security

Closing the gender gap will help the industry evolve beyond a narrow focus on bits and bytes, says Lyndsay Turley, director of communications and public affairs for EMEA at (ISC)^2

The cyber-security skills gap is widely publicised but we also need to focus on the cyber gender divide, and recognise that the two issues are intertwined. Women comprise just 10 per cent of the global information security workforce, according to the (ISC)^2 2015 Global Information Security Workforce Study, and in the UK only 6 per cent.

With more than three-quarters of UK chief information officers warning of increased cyber attacks resulting from a shortage of information security professionals, the industry's failure to recruit from 50 per cent of the population is now an economic and security threat.

So why do men continue to dominate to such an extent, and what can be done to widen the industry's recruitment net?

Part of the reason is that information security employers tend to recruit people with backgrounds in science, technology, engineering and maths (Stem) subjects, which men are more likely to study than women. In computing science degrees alone, there are 17,000 more male than female undergraduates in UK universities. The job specs for many cyber-security roles are also heavily technical, which deters people with non-technical degrees, inadvertently filtering out many women at the entry stage.

Yet it is unnecessary to recruit solely from Stem graduates. While technical know-how will always be integral to our profession, cyber security is evolving beyond its roots as a profession dominated by bits and bytes. As every aspect of our economy becomes connected, cyber security is an increasingly multidisciplinary profession, required to influence every aspect of business, from boardroom decisions to HR practices.

For example, our Workforce Study report on Women in Security found that one of the fastest-growing fields of cyber security is governance, risk and compliance (GRC), which requires many "soft" skills, such as defusing emotional conflict, encouraging collaboration across multiple stakeholders, balancing business objectives and managing risk. Evidence shows that women possess key character traits that enable them to succeed in these roles; they already form 20 per cent of the GRC workforce, double the proportion of women in cyber security as a whole.

Lucy Chaplin, manager at KPMG's financial services technology risk consulting practice, says: "Our pool of new graduate hires is often a 50:50 gender split because we recruit equally from Stem and non-technical degree backgrounds. We typically look for three types of recruit: the pure techies, the business management people, and those who can successfully translate between the two."

If we are to improve the situation, cyber security recruiters should broaden their job specs, recruit for specific attributes rather than specific types of degree, and appoint successful female professionals as ambassadors.

As our industry is required to handle issues as wide ranging as regulatory compliance and HR, the growing diversification of cyber security as a profession will help to drive the diversification of the workforce itself.

(ISC)^2's next Global Workforce Study is under way, and will help shed more light on the current gender breakdown when the findings are released in 2017.

For more information, see isc2.org

IN ASSOCIATION WITH

(ISC)^2

INSPIRING A SAFE AND SECURE CYBER WORLD.

ADVERTORIAL

Don’t wait until you need us; you need us now

Small firms, wealthy individuals and family offices are increasingly targeted by hackers. G3’s Malcolm Taylor says everyone needs a defence strategy

“My job is all about trust,” says Jo. “My boss and I have the closest working relationship, and that is central to our success. My role is as much about being her presence back home as it is about the investments and the family.”

Jo’s boss had emailed. She was on holiday and asked Jo to transfer some funds to a new client. This, in itself, wasn’t unusual. “I logged onto our bank and made the transfer,” says Jo. “It was a lot by most people’s standards I suppose – £35,000 – but not out of the ordinary.”

The first thing Jo knew about something going wrong was when her boss texted her to call urgently. There was something wrong with her Mac. She had tried logging on to her work account and couldn’t get in. “Instead she got a message saying that someone had locked all our data down, and we could only get it back by making a payment of $5,000 to a bank account in Bulgaria”.

Cyber criminals had somehow gained access to her boss’s machine. They spent some time learning her email habits, then they copied them and sent the fake email requesting the transfer of funds – and they chose an amount they hoped Jo would transfer without becoming concerned. Sadly, they chose well; the money is gone for good. Second, they launched what is known as ‘ransomware’, which made all the company’s data unavailable by encrypting it.

On the Monday, Jo called a friend who worked in IT and he suggested she get in touch with G3 Cyber, a bespoke consultancy based in Marylebone.

“The situation Jo found herself in, that Sunday, is no longer unusual” says G3’s Head of Cyber Security, Malcolm Taylor, “though it isn’t every day we see two such closely co-ordinated attacks on the same target. We did two things for Jo and her employers. First, we were able to get her data back for her – on the day she called us. We found, fortuitously, a recent enough backup, which meant they lost very much less than they might have done. Second, we did a full security review of their network and company as a whole, which identified a number of vulnerabilities – including how the attackers got in the first place. The attack came from Ukraine, but the attackers are long gone. We don’t know how they identified Jo’s employer as a target – she’s rich, but not particularly high-profile – but once they decided on her, they invested some time in learning about her life. They used common tools to “social engineer” her – LinkedIn, Facebook, and other social media. They knew she was overseas, and they knew how she signed off her emails.”

Identifying vulnerabilities is one thing, of course: fixing them is sometimes another. “We provided Jo with a roadmap to better security, based on our review” Taylor adds, “and then we worked with her and her IT providers to implement our recommendations. Some were absolutely straightforward and cost nothing, whilst others needed more investment. For example, we changed the way the company’s email accounts are set up, which minimises the risk of someone being able to impersonate a member of the company in future, and we implemented a secure communications network, company-wide. They’re much more secure now, but it’s really sad they had to go through all that in the first place. Preparation is the key, but unfortunately so often people only find out when it’s far too late”.

IN ASSOCIATION WITH

G3
GOOD GOVERNANCE GROUP

Beyond the phone scam: how the threat is evolving

Are antivirus developers winning the battle against today's cyber criminals? Microsoft's chief security adviser, Stuart Aston, talks to Will Dunn

Cyber threats have been a reality almost since computers were invented, but they're evolving. People carry their data with them in their pocket. The "Internet of Things" means that apparently inanimate objects can connect and communicate, and some companies are allowing their employees to use their own devices.

You might imagine this would cause the nature of threats to change dramatically. In fact, according to Stuart Aston, Microsoft's chief security adviser, a lot of the dangers are well established. The good news is that a lot of the techniques for fighting back are well established, too; the bad news is that not everyone is adopting them.

First, the new stuff. The Internet of Things isn't actually all that big a deal, believes Aston. "Any time we provide a device with some sort of connectivity, we should think about the security of that device – what it can do, what it's connected to, what it knows and what it doesn't know," he says. "Then we should think about how it's appropriate to secure that in a risk-management way."

In other words, as other contributors have said in this supplement, it's worth assessing what the risk actually is and how dangerous the information a device might hold can become. Smart light bulbs that allow themselves to be turned on and off remotely are undoubtedly connected, Aston points out, but if they're hacked then the consequences are hardly disastrous. "Then the bad guy knows whether my lights are on or not. Is that a big threat? Do I care?"

The answer may well be yes, if the light bulb's connection can be piggybacked to gain access to banking or other confidential details, but it might be completely harmless. The key is applying security technology intelligently, as distinct from the mainstream idea of aiming simply for ubiquitous cover. In business, in particular, it has to be a cold, detached decision.

"If I had a diamond in my house and I didn't have locks on the doors, the bad guys could help themselves," says Aston. "But if the cost of the locks and all the other security was more than the value of the diamond, I have to start asking how badly I want the diamond."

Up in the cloud

The other idea that could provoke some disquiet is that of putting everything into the cloud. This is actually a strength, Aston believes. "We spend something like a billion dollars per year on cyber security at Microsoft, which is a big investment," he says. "I doubt many commercial organisations can afford to spend that much resource on making their own services as secure."

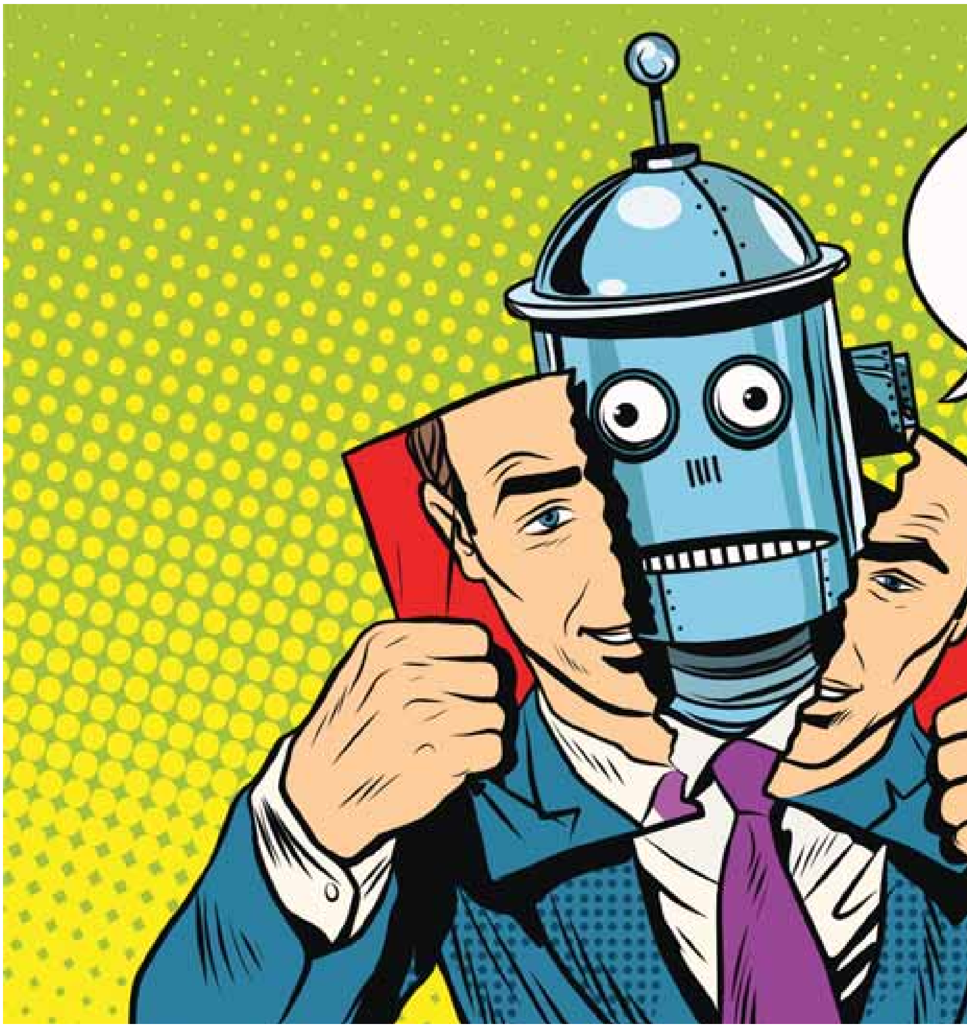
There are follow-on benefits from taking this approach, he believes. You start off with one customer whose installation of, say, Microsoft Office 365 is under attack in the cloud. Microsoft works out what's going on and how to prevent it, and protects not only that customer but all those that use Office 365. "We use highly trained people to look at security events and react to them accordingly," Aston says.

Cloud, when it's done right, also helps companies in sensitive environments. "People know where the information is stored, how it is stored, and then you as the consumer of that cloud service can make a judgement about your risk – it does become a choice, because cloud is about choice. Many consumers are observing that and saying they'll put a portion of their data into the cloud for a well-evidenced resource."

The main documented threats still come from the traditional avenues, Aston explains. These are examples of disguised malware, which might look like an email or a video codec or something else, which the end user – the criminal hopes – will install on their system, believing it to be innocent. It then starts doing something else on the network: "It could install software designed to steal banking information. It could be a Trojan designed to download other malicious programs. It could be a root kit on a PC. It could be there for ransomware. It could be there to spy."

Ransomware is a relatively new development. Frequently delivered by a Trojan, which is just the mechanism, it establishes itself on a system and cuts off access to data unless a ransom is paid. Trojans have declined as a menace over the past year: Microsoft research shows that around 3.5 per cent of computers with reported malware have Trojans, as distinct from 5 per cent a year ago, but longer-term data suggest this risk is fluctuating rather than dying down.

Browser modification is another recent development. Here, a web browser is changed to make it show an unwanted advertisement (which sounds harmless, if annoying); or to record keystrokes (less harmless if you're typing in sensitive passwords); or any number of other things. At the same time, criminals are moving towards "social engineering", observing how someone behaves on social media and when emailing – their signature, their general manner and so forth. They can mimic this behaviour, so that recipients of any messages become convinced they're communicating with a friend or colleague. This friend or colleague then turns out to be stranded at an airport and needs a money transfer, or something similar.



Rise of the robots

The social engineering phenomenon points towards humans being part of the problem. This is true to some extent. Easy-to-guess passwords and default security settings left on phones and other devices are a widespread security risk. (Remember the phone hacking scandal a few years ago – in which phones weren't actually hacked. The criminals simply guessed that the owners wouldn't have changed their voicemail passwords.) Today, people are talking about security more than they used to and are increasingly in the habit of reporting incidents, says Aston, which has to be a positive thing.

"In the Seventies and Eighties there was a spate of [fraudulent] double-glazing sales that were made over the phone," he adds. "The callers asked for credit card details, and people were giving their details over the phone. So the person is also part of the attack." Such scams are less common today, but can still occur.

However, automation is a major part of the equation. "The reality is that you're looking at millions and billions of security events every day," Aston says. "You can't have someone going through all the code by hand and saying, 'That looks a bit fishy.' You have to generate machine-based algorithms to work out what's out there. It turns out those algorithms are about 100 times more efficient than the humans, anyway."

There is a great deal of machine-to-machine learning happening, which helps sharpen the systems' responses. So, logically, does this mean that the criminals can also use machine-to-machine learning? Aston suggests that the cost would be prohibitive, although the theoretical possibility exists. And with state-sponsored cyber crime now well established, it might be asked just

Robot detected: your next security exploit – and your best defence against it – will soon be artifically intelligent

“The reality is that you’re looking at millions and billions of security events every day”

how finite hackers’ financial resources could actually be in some cases.

But fighting the malware remains relatively straightforward, Aston says. Leaving the actual cure for the viruses and other malware to the giants such as Microsoft, there are simple practical steps that individuals can take, and that companies can train their employees to implement. “It’s quite common for identity to be used as part of an attack, and it’s a simple thing to protect against, or at least be aware of,” Aston says. “You can do a number of things. You can use multiple factors of authentication; you can use an authenticator; you can use smartcards or other mechanism.”

Staying up to date

The other thing to do is to ensure that all software is up to date. “Many customers don’t have up-to-date software on their PCs, so the bad guy gets a free pass,” says Aston. “That’s not just from Microsoft’s point of view – every piece of software needs to be kept up to date.” This is normally achieved through automatic patching, although many customers find these facilities annoying and switch them off. This magnifies the problem not only because the security hole is unplugged but because there are known patches to address specific vulnerabilities. The cyber criminal knows there will be systems in the field with that specific problem, so they know where to find the weaknesses.

“It’s like hygiene,” Aston says. “We go to the toilet; we wash our hands. We go to a hospital ward; we wash our hands or give them a spray. The chances of our getting sick are much reduced. It’s the same with updates and generic software.

“What we see for the UK is something like one in eight computers report an encounter with malware over a six-month period. Also in the last quarter, 3.5 per cent had Trojans, down from 4 per cent last year. Browser hijackers were at about 5 per cent for the fourth quarter of 2015.”

The figures might sound low but, given the sheer amount of computers in the wild, they’re not. It’s arguably reassuring that the emergence of cloud, the Internet of Things and other innovations is unlikely to damage security, but it remains the case that the basics around identity are often ignored. Overcome this and, while it’s unrealistic to expect it to go away, the threat will at least be mitigated.

Defending your reputation: the cost of complacency

With negligent executives at risk of criminal conviction, Carolyn Harrison, marketing director of BeCyberSure, looks at what's at stake after a cyber security attack

IN ASSOCIATION WITH

BeCyberSure

In the UK, Europe and beyond, we are living through one of the most uncertain and transformative periods of recent times, and businesses are faced with increasingly challenging issues. The use of the internet and communication networks has revolutionised the way we work, share information and exchange data across a diverse range of organisations.

In the pursuit of the cyber-security silver bullet, the one thing that has often been overlooked is the presence of an overall governance regime, which draws all security stakeholders in an organisation into the same information security (InfoSec) conversation. To some extent, ISO 27001 certification, Cyber Essentials and other similar programmes, plus the news reports of hackers and cyber crime, have exacerbated this situation because they tend to focus almost exclusively on the cyber element of data protection.

However, this itself creates further vulnerability, given that 95 per cent of all breaches (according to IBM) are as a result of human activity.

Cyber security is largely a people problem. Criminals use whatever tools are available to them to gather intelligence for further exploitation, steal information or money, or create routes to more lucrative targets. Your technology, if you allow it, is merely one of those potential tools. The criminals are looking for vulnerabilities to exploit – even your child's phone or Facebook account could be used to get to you. Of course, vulnerabilities don't need to be digital. An open door or a weak procedure is as vulnerable as an unpatched operating system. Recent statistics from the Information Commissioner's Office state that, in most sectors, human error is the biggest factor, often involving things like lost faxes and papers.

Governments and legislators have given up the pretence that they can fight the cyber-crime fight on their own and have begun to demand that companies take responsibility for their own data protection. Big fines and criminal sanctions are starting to be used against executives who fail to meet fairly low required standards. Errors here can be reduced with structured education and training, which raises overall awareness for everyone in the organisation.

Regulatory compliance laws are changing, and punishments getting more severe. The EU's new data law, general data protection regulation (GDPR), will take effect in May 2018, almost certainly before Brexit. GDPR allows for fines of 4 per cent of global turnover (up to €20m) and criminal convictions for executives. We believe that, regardless of the eventual outcome of negotiations to leave the EU, GDPR will be *the* most important law governing data protection for years to come, for any UK company operating in and outside of the UK. In addition to existing requirements, organisations will need to map and archive all data in their possession and receive consent for their use of any individual's personal information.

US law is also something that everyone, regardless of their domicile, has to pay attention to.

A well-constructed governance policy, proactive management, good education and training programmes, and healthy security culture should be at the heart of any information security regime. Effectively executed, this will go far in countering the "insider threat", and lead to a significant reduction in general cyber risk.

For more information, see becybersure.com

Incident response: the first hours after an attack

Any company can be targeted by cyber criminals. The key is to be prepared for when they strike, says Kevin Bailey, vice-president of strategy for BAE Systems

IN ASSOCIATION WITH

BAE SYSTEMS

It is a consequence of our interconnected world that almost every organisation today faces a real possibility of cyber attack. There are lots of technically competent cyber criminals working in the UK, targeting businesses, other organisations and the public, and the threat is ever increasing.

As a result, data breaches are common – it's not if an attack will happen, but when. Therefore, it is more important than ever that businesses prepare so that they can react quickly and efficiently to minimise the impact in the event of a suspected breach. How a business reacts in the first hours after an attack is critical.

Discovering an incident

There are a variety of ways in which a company may become aware of a potential attack, ranging from alerts through security monitoring, a tip-off from an external party, an unexplained bank transfer, or suspected insider activity.

Successful attacks can attract widespread media attention, and stolen data can sometimes be used to aid other online attacks. One potential adverse consequence from an attack is a loss of investor or customer confidence, resulting in a drop in share price or a loss of trade if a company is perceived as not responding correctly.

A planned response

Businesses must prepare to react to successful cyber attacks. Effective plans must be developed to mitigate the impact, because defending the digital perimeter is not enough. Some government departments already assume that their network will be penetrated, meaning that they are focusing on ensuring operations are maintained and that damage from a breach is minimised.

An incident response plan allows an organisation to react quickly to a breach at an appropriate escalation level based on what's at stake. Internally, it allows all business functions, such as HR, communications and legal departments, to react in a co-ordinated way. Externally, companies can establish which experts they will turn to for support and counsel – on issues ranging from reputational management, through to how to ensure key evidence is retained and which authorities should be notified.

Most companies have an incident response plan, but these are sometimes out of date or not specific enough for particular incidents and situations.

Managing a cyber incident

In the event of a breach, time is of the essence, with remedial actions taken in the first few hours critically influencing the eventual income. The correct preparation can have a dramatic impact on the management of an incident. It is a complex task that requires the co-ordination of decisions, resources, tasks and information, so having the right people lined up is critical.

Many businesses waste precious moments during this early phase trying to work out what they need to do and whom they can turn to for help. Increasingly, we are seeing organisations put this support in place in advance, establishing cyber incident response panels to reduce the initial pressure in deciding where to seek help. At BAE Systems, we have a global emergency response team, who can be brought in to manage any crisis and can be contacted around the clock by companies within the group that believe they could have suffered a security breach.

Spend a little now to save a lot when disaster strikes

Cyber security is too often regarded as an expensive extra. **Matthew Olney**, communications and content executive at PGI, says the figures add up

IN ASSOCIATION WITH

PGI

Cyber security is one of the dominant issues faced by business and government. Stories of huge data breaches and the subsequent financial losses that follow often appear in the media, leading to damaged reputations, reduced consumer confidence and knee-jerk responses.

The way the issue is presented by both the media and cyber industry is often alarmist, with the facts confused by buzzwords and hyperbole. Scary headlines sell newspapers and generate clicks for online articles, but what is the security companies' excuse? They know that fear may scare victims into opting for their often very expensive products, which promise to be the much sought-after silver bullet

In reality, there is no one wonder fix for cyber security. Organisations need to implement their security measures systemically and effectively, spending money only where it is necessary and not where it isn't. Safeguarding data and systems doesn't need to be expensive. The simple introduction of basic accreditations such as Cyber Essentials, or basic maturity models, plays a major role in reducing the threat. The education of employees and the introduction of a cyber-aware culture will cause the number of incidents to fall sharply. It is a process that one cannot and should not be panicked into. However, this doesn't mean that businesses should just wait for an incident to happen before doing anything, either.

Under new legislation, organisations face huge fines from government bodies for not having adequate defences in place to protect their own data and those that they hold for others. The outcome of Brexit negotiations will not affect the need to comply with new

SHUTTERSTOCK

EU regulations. All organisations that handle sensitive data must prepare for them, since last-minute rushes will be expensive and inadequate.

ONS figures show scale of cyber crime
According to figures released in July by the Office for National Statistics, cyber crime now accounts for 40 per cent of all crime recorded in the UK. Of the six million cyber-security breaches recorded, two million were the result of computer misuse. This ranged from people opening emails infected with malware to people looking at rogue websites and having their machine infected. This huge figure of misuse is easily eliminated.

It's all about people
The most effective way of reducing risk is to develop a cyber-aware culture that runs right the way through an organisation. From the chief executive to the intern, an organisation's workforce is often cited as the weakest link when it comes to cyber attacks. In many incidents, malware infects an organisation's systems via an email accidently opened by a member of staff, or by someone clicking on a link that downloads and inflicts something nasty on to their businesses networks. To avoid incidents like this, an organisation should invest in cyber-awareness training for its employees and supply chain partners. Education can teach employees the signs of phishing and spear phishing emails, as well as helping people to understand social engineering and how social media can be a route into an organisation for criminals. If everyone in the company knows what to look for and what to avoid, the chances of a breach will fall sharply.

By taking a measured approach to implementing cyber security, an organisation can gradually reduce the threat without causing huge disruption to its operations and balance sheets. It's best to take action now rather than delay until a time when costs and effects are outside your control.

This measured approach will also reduce the impact on your workforce and productivity. If an organisation does suffer a breach and does not have effective cyber security in place, the effects can be extremely debilitating, especially in the case of small or medium-sized enterprises.

Mitigate the cyber threat
PGI helps organisations to implement a cyber-aware culture every step of the way. We can assist in attaining certifications from Cyber Essentials through to ISO 27001, and deliver cyber-awareness training that will be of great assistance in implementing a cyber-aware culture and significantly reducing the risk of attack.

Incident response plans are the first step in mitigating this risk. These plans should consider the current threat intelligence and have a solid understanding of the attackers that threaten organisations. An incident response plan should outline who is responsible for each area that is likely to be involved in a security breach; what steps they should take in this event; what resources they can call on (including external consultants); and whom they should communicate with. It will list the possible types of attack and how best to identify, contain and eradicate these, and how to recover from them with as little impact on business as possible. Incident classification and severity ratings give a basis for a manageable set of procedures to handle security breaches.

Protective Monitoring services ensure that your organisation has an early-warning system in place. Experts keep an eye on your systems and warn of any attempted breaches. The main benefit of this is that it lets you focus on your business operations.

PGI aims to close the skills gap
People wanting employment within the sector are looking for practical training; and organisations need employees with the right skills. PGI aims to be a major contributor in the struggle to close the skills gap. At our state-of-the-art Cyber Academy, based in Bristol, we provide an immersive technical environment to educate people to become the next generation of cyber-security professionals. The academy offers the most sophisticated training on the market in techniques for cyber defence, cyber-threat intelligence analysis and organisational leadership roles, with training delivered both on- and offsite.

From the basic theory to the advanced techniques taught in our Advanced Threat Methodology and Digital Forensics courses, we can educate someone through every stage of their cyber-skills development to externally certified recognised standards.

By investing in the training of their staff, businesses can ensure they have the right people in place to tackle any security issues that may arise in the future. In short, spend a little now to save a lot when disaster strikes.

People can either be the weakness in your cyber armour or your greatest strength, says **Malcolm Taylor**, Head of Cyber Security at G3 Good Governance Group

The best defence? Knowing what an attack looks like

Are you being cloned? Your Facebook and LinkedIn connections can be used to build up a picture that helps hackers spoof your identity

There are a couple of important misconceptions about how cyber attackers select their targets. The first is that you have to be somebody, that you have to be high-profile. You don't - we all have information that can be of value to cyber criminals. The second is that this only happens to tech companies. Actually, the opposite is the case – criminals are less likely to go after tech companies, because they're better protected. Anybody can be a target.

Around 90% of successful attacks come from emails that contain malicious attachments or links - what's known as 'phishing'. These can be sent at random, but the result is a very low hit rate. Over 100,000 emails would get fewer than 10,000 clicks. But if the attackers do their research on you as an individual, they can change the odds from fewer than one in ten to about eight in ten.

This is very simple to do. Everyone uses the internet, and most people use it incautiously. Take Facebook: few people, remarkably, use the right privacy controls, so a lot of information is there for the taking: hobbies, where someone travels, their date of birth, phone numbers, email addresses, friends and family. LinkedIn, too, is a great source of information for hackers. It's outward-facing – it's designed to show strangers your skills, where you've worked and your interests, but it also serves up birthdays, phone numbers, email addresses, photographs, courses you've been on and people who influence you.

So with two quick searches, you can learn a lot about someone. If you spend a week on it, you can build up a very detailed picture. Cyber criminals use this approach to design an attack such that when they send you that email, it seems trustworthy and familiar. It's worth noting that a hacker doesn't need to be able to write a single line of code to do this, or any real technical skill. All that's needed for 'spear phishing', as it's known, are the words you've written

SHUTTERSTOCK

IN ASSOCIATION WITH

G3

GOOD GOVERNANCE GROUP

about yourself online. You give them their ammunition.

A step up from 'spear phishing' is 'whaling': going after a prominent individual or a big company. To steal a celebrity's photos or a company's intellectual property (IP), someone might spend a month or more preparing their attack. Some cases have included physical surveillance in the real world, to understand the target's daily life.

The object is almost always money, ultimately – personal information, names, credit card numbers, National Insurance numbers, all are saleable. You can buy them on the dark web right now, for people like you and me. Ordinary people's details can be had for a dollar, but there's a scale for these things, depending on how much information there is. A study by the Ponemon Institute in 2014 found that some personal information of 47% of US adults – that's over 150 million people - had been exposed by hackers in that year alone.

Companies are the most profitable targets, but people are usually the way in. Often hackers will target finance directors and senior executives - people with the authority to sign off payments – but they don't stop there and will target anyone in any company. The CEO email scam is really common at the moment - hackers use a targeted approach to understand how the company works, then they 'spoof' the CEO's email, sending a request for money to be transferred to an account where the hacker can access it. This can be done from anywhere in the world – the chances of getting that money back are basically nil.

How to stay secure

While people are a security weakness, trained people are a great strength. Senior executives need this training not just because they'll learn important things that will protect them at work and in their private lives, but also because if the CEO is taking this training, everyone else is more likely to sign up, too. It's about creating a security culture.

At the most basic level we'd often start by making sure people have different, strong passwords for every account. We talk about the Leveson Inquiry and 'phone hacking', but it's important to remember that those phones weren't actually hacked in any sophisticated way - it was just that people never changed the default codes on their voicemails. If you bought a new house and the builders said "there's a key under the doormat," you wouldn't just leave the key there.

Secondly, don't ignore software updates. Yes, they mean your phone's out of action for a couple of hours, and it looks exactly the same once you've done it. A lot of our clients say "but I can't afford to be off the phone for two hours!" Well, do it in the middle of the night. Manufacturers don't produce these updates for fun, they do it because someone has found a security flaw.

Thirdly, spend an hour or so targeting yourself, as a hacker might: Google yourself, find out what information is out there about you, and think about how that could be used. I guarantee you will be surprised. Once you've done that, you may want to think about your Facebook and LinkedIn accounts, what's on there, and your privacy settings.

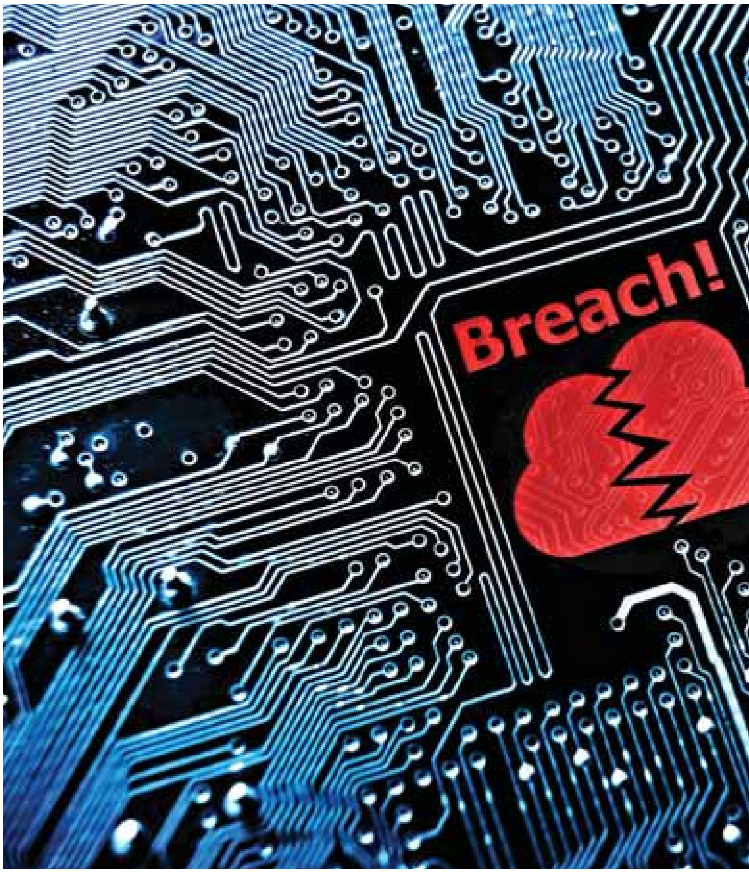
Anybody who runs a company and anybody who is in any sense high profile really should think about investing in expert advice. To be as secure as possible, you've got to stay current. We have a number of clients for whom we provide training as a managed service – each month we'll do some face-to-face training or produce a video or an email with some reminders and hints. We tailor our approach – for example we work for a big Nigerian company and they find cartoons very effective, so every month we produce a cartoon with a key reminder. There's a reason Apple and Microsoft release updates and security patches so often; regular training is the human equivalent.

We also work a lot with high net worth individuals - some very high profile – and family offices, and we've been able to work with them so that they've gone from being very wary of using email, telephones, etc., to being confident again; we've provided them with a secure network with good encryption, proper MDM, and we've simplified their life in that sense. A lot of people in that position, we find, have simply been moving away from using modern communications. We're able to put them back on, with the confidence they need. And a big part of that is understanding the information out there about them – and there can be a lot on prominent people – and so understanding the threat. We regularly produce "digital footprints" for high profile people, and it always helps us improve their security. It surprises them, too, every time.

It's by using this constantly updated approach that we make sure our clients are as secure as they can be. If you're in business, either as individual or as a corporate, this approach takes the risk and the worry out of a threat that nobody seems to be able to avoid.

Speed is of the essence

How long does it take an organisation to respond to a data breach? **Josh Goldfarb**, chief technology officer of FireEye, believes it's almost always too long



SHUTTERSTOCK

How old do you think the news is by the time you read it? A politician makes a speech in the morning; it's online and on the radio bulletins at midday and in the evening, and then reported in the following day's papers. So it's a matter of hours until it's massively important, in which case it may be reprised in the Sunday papers.

Now ask yourself how old the news that "major company A suffers security breach – tens of thousands of customers see their personal details compromised" actually is. A day? A week? A month?

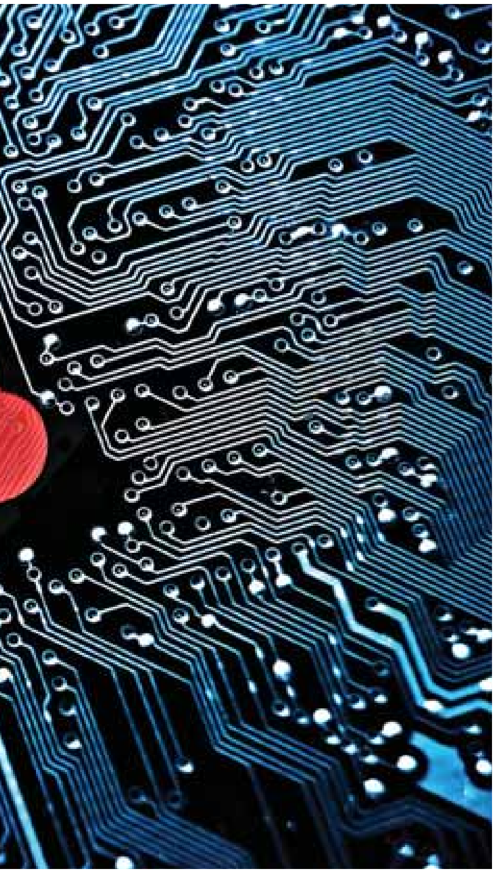
In fact, it's not at all unlikely that the breach is months old, possibly even a year. The actual news is that the breach has come to light; the perpetrators, meanwhile, have had enough time to establish themselves in the system and siphon off enough data to do some damage – and then to be detected. These people are sophisticated; it's not a fast process. But what if companies were geared up to start reacting more quickly and cauterise the wound to stop the flow of data earlier?

Changing to a faster reaction environment would mean a complete change of organisational culture but the results could be worth it. Before we get to that, it's worth considering how organisations typically regard their security at the moment. Essentially it's a matter of preventing anything bad happening to the company, keeping the malware and bad data out.

This is a good start. Everyone should do it. But it's not enough. Consider what you do elsewhere in life: you take care with matches and candles, for example, but houses still

IN ASSOCIATION WITH

FireEye™



catch fire. The fire brigade is never unemployed. In the winter you wash your hands assiduously but people still catch colds. You lock your doors and windows, install an alarm but someone, somewhere, is still going to get robbed.

Yet in terms of cyber security, so many corporations we meet have a view that once they've done their best to secure their perimeters, they have done all that is reasonable.

Poor perception

Bolting the door is an essential but it's only the beginning of a comprehensive strategy. A starting point has to be to get the board to buy into the importance of security and to gain some understanding of it. We have clients wanting to know when their security is "done", and it doesn't work like that. It's an ongoing process.

And it has to happen at board level because customers are increasingly aware that their suppliers should be custodians of their data. FireEye research suggests that 73 per cent of customers – nearly three-quarters – would move away from shopping at a particular retailer not if there were a breach (only a quarter would do so) but if they felt that the board wasn't taking the breach seriously. In other words, the public is sufficiently savvy to understand that stuff happens – a laptop is going to lose some data sometime – but they will punish companies that don't take it seriously. Unfortunately in our experience that's most companies. But for those that do start to take it seriously at board level, the rewards can soon multiply.

Prioritisation and process

The board will analyse risk and prioritisation just as they do every other business issue once it's on their horizon (and once the security professionals have learned to talk to them as board members rather than as if they were IT staff). In the traditional model, a company might have, say, 100 pieces of data. One might be a piece of fake data dummied up in the lab for experimental purposes. Four might include customer data, supplier data, payroll and HR information. A lot of companies would apply the same security focus to all of these pieces of data.

The board-driven, business-led approach would instead say that there is no point spending the same amount of money and human resource protecting the dummy data as is spent on protecting people's real details. So the prioritisation starts and resources get allocated where they're needed.

There are also different sorts of protection available, which is where having an informed partner like FireEye will help. A manufacturer will be subject to different forms of attack compared to, say, a web design agency or a bank. One-size-fits-all doesn't work efficiently. Once again, we tailor security requirements to fit elsewhere in our lives without thinking. If you get on to an aeroplane, the security is very different from that which you would find on a train. A good security partner will have an overview of what has happened to businesses or public sector agencies your size, or in your territory, or in your market. They will recommend security tools and strategies accordingly.

The other thing about board buy-in is that it can facilitate speed.

Speed of reaction can be anything. Consider, as we've established, that a breach is almost certainly going to happen sometime, even to the companies that have taken every sensible precaution. What happens next is vital. An unprepared business, without board buy-in, will have no procedures in place. It may not know whom to notify, whom to call for help, at what stage to call the police or even GCHQ, and it might have no plan in place to keep customers informed. Board members, however, will be focused on procedures and process – it's how they think.

So they put procedures in place. If a laptop is behaving oddly, maybe that's a level-1 alert. If customers are querying transactions as well, that's probably several stages along – but there's a procedure and a clear guide as to what to do next throughout. Ideally this culture goes through the organisation so that people are in the habit of accepting stuff happens and reporting it immediately without fear of blame. There is a very good chance, if people are geared to react immediately, that the leak will be plugged before it does intolerable harm.

A lot of this is about reputation. It's about whether an organisation has the reputation of having ticked the "security" box and is unprepared when the inevitable happens, or whether it knows precisely what to do and whom to call to mitigate the inevitable breaches when someone gets through.

Which description fits your company?

Could you say – hand
on heart – that you
could cope with a data
breach or cyber attack?