
NewStatesman
Cyber Security
The fightback issue
Government initiatives
Security and outsourcing
Beneficial hacking
avatu

avatu

Don't be put off by the hype

Cyber security is simpler and easier than you think, says **Joe Jouhal**, CEO of Avatu

From the headlines you'd be excused for thinking it's unstoppable. "The end is nigh" and all our businesses are about to implode under the cyber criminal's destructive gaze.

But, of course, reality is a little more balanced than that.

In reality:

Yes, there is a serious, growing threat to business. The World Economic Forum's *Global Risk Report* has cyber threats and data theft in its top ten (alongside climate change and large-scale migration) and PricewaterhouseCoopers's recent survey of 100,000 businesses revealed that 38 per cent more security incidents were detected in 2015 than the year before.

Yes, it's impossible to know if you will come under attack, so you have to assume you could.

There is no such thing as a typical data breach victim, as Lincolnshire County Council, TalkTalk and Bettys Tea Rooms can testify. And, as motivation diversifies, it's hard to know why or where the risk will evolve.

And yes, a cyber attack or data leak can be expensive and damaging. TalkTalk said recently its data breach cost it 101,000 customers and £60m.

There is an urgency to assess the risk. But organisations should not be dazzled by the hyperbole or the hype.

Security doesn't need to be a complicated, difficult or vastly expensive business. There is much enterprises can do, simply and easily, to help prepare for, and protect against, a data breach launched over the internet or caused by a rogue insider.

It's a case of fighting on a battleground where you can win and being equipped with the right weapons.

How to fight on a battleground where you can win

1. Don't rely on staying safe with just perimeter protection. Anti-virus software and firewalls will only stop known threats. If you have systems or data that need to be protected, you need to become more sophisticated in your security arrangements.

2. Assess what's most important and sensitive to your organisation – and protect that. You can cover other things as well but start with the most important.

3. Email attachments are a significant weak point in many security plans. But there are new technologies which can automatically strip away worrying content without blocking them completely (so employees never miss important emails that disappear into firewall black holes).

4. Remember, even your friends are also potentially your enemies. Employees and contractors can make silly mistakes or can be tempted to the dark side (sometimes for very small amounts of money). You can, however, limit your exposure by protecting your data at source, making it secure when it's inside – and outside – your organisation, and you can pull the plug remotely if there's a problem.

5. Limit access to the important stuff. This can be done easily with privilege management (where people only have access to things they need for their job). It sounds simple but you'd be amazed at how many people don't already do it.

6. Consider cyber insurance. Not only will it give you a financial cushion if things go wrong, it will help introduce risk-limiting activities and a proactive mindset.

7. Get your security advisers to give you options. No one piece of technology or policy will give you everything you need (indeed, the Government's advisers at GCHQ recommend a layered approach). But you almost certainly will not need every piece of expensive kit on the market.

It's a rapidly changing world where the criminals are on the front foot. But being proactive can vastly improve your chances of winning the war.

Joe Jouhal is the chief executive officer of Avatu, the information security company for inspiring companies

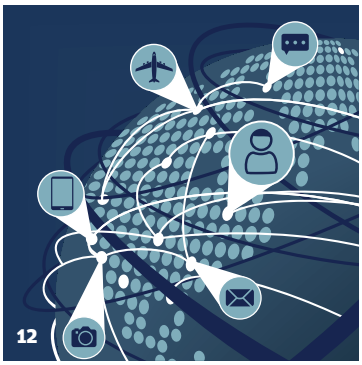
For more information visit: www.avatu.co.uk

New Statesman
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 Editor
Guy Clapperton
Design and Production
Leon Parks
Sub-Editor
Peter Barker

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

4
The Digital Minister is bullish


12
An expanding Internet of Things


16
Being responsibly social

The cyber fightback

The threat to everybody's security from the cyber world is well established. For years publications have been highlighting the dangers, whether these are from hackers, automated bots sending distributed denial of service (DDoS) attacks (which send huge quantities of data that overwhelm a system) or just viruses.

It's possibly time to be a little more positive. This publication won't flinch from the difficulties people are facing in business and as individuals, or even nations. Social media carries its own fresh risks, cloud technologies do the same, and in the long-established trend towards IT outsourcing, the systems subjected to threat might not even belong to the business or public-sector body under attack. However, people are taking action to fight these threats.

There are practical steps to be taken, and those steps are covered in this publication. Company cultural issues such as the acceptance of threats as "normal" and therefore requiring mitigation, rather than regarding them as exceptions, are addressed by one of our contributors; so is the role of the outsourced third party. And have you ever considered hacking might be beneficial? One of our writers describes this area.

Some contributors examine different forms of security precaution. Visual security and integrity of data in an increasingly mobile environment are relatively new concepts but they will become important, so we offer explanations here.

The focus is on the positive and what people are doing, as well as what else organisations can do to reduce their exposure to risks. Ed Vaizey, the Minister for the Digital Economy, offers practical advice (*see page four*) and also sets the scene realistically: the environment has changed, but there are steps a business can take to remain safe as it grows and the threat starts to grow, too. It's not just businesses. Individuals can also put a distance between themselves and the cyber threat by taking sensible precautions, some of which are obvious but are still ignored by many.

No organisation is 100 per cent safe yet, but nobody is guaranteed safety crossing the road. This supplement aims to explain the changing landscape and outline what can be done to mitigate the dangers rather than to sensationalise. That said, there are still a few people who use "P-A-S-S-W-O-R-D" or their pet's name as their passwords online. If that is you, just stop it . . . right now. ●

Guy Clapperton

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

First published as a supplement to the *New Statesman* of 26 February – 3 March 2016. Registered as a newspaper in the UK and US.

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.

COVER: SHUTTERSTOCK/DESIGN BY LEON PARKS

Eyes wide open: complacency and indifference to the threat of cyber crime are a large part of the problem

Staying safe in the digital age

There's a digital revolution happening across the UK economy – and I want to make sure it's a secure one, says **Ed Vaizey**, Minister for the Digital Economy

Our lives are being transformed by digital innovations. New online tools and digital services are making tasks in our work and personal lives easier and more efficient. But in order to benefit fully from this digital revolution we need to get the security aspects right. Businesses in particular are losing too much time and money to cyber crime. So I want to explain what the government is doing about it – and how businesses can help.

Little over ten years ago it would have been hard to imagine the scale of online commerce we see today. UK citizens are Europe's biggest online shoppers, with 79 per cent of people making an online purchase in the past year and e-commerce worth over £557bn. The proportion of business now carried out online is astonishing. But I think we have adapted to this new world surprisingly quickly, particularly so in business. The modern love for digital makes it now routine for businesses to send and receive invoices online, to make payments online, to send sensitive data via email, and to operate

SHUTTERSTOCK

services via the web. In fact, such is the ease of use that it's easy to forget the need to be aware of security.

We are generally happy to punch in passwords and click our way through websites when we're under pressure to get on quickly with the job in hand. Complacency and indifference towards the problem is part of the risk. Indeed, many businesses aren't even aware they have been attacked – until, perhaps, their database appears online and their customers start receiving hundreds of spam emails.

The scale of cyber crime is vast. Just as useful services have moved online, so has a wide range of activity from the criminal world. It's difficult to put a figure on the cost to UK industry, but we suspect it is in the tens of billions of pounds.

We know from the government's annual Information Security Breaches Survey that 69 per cent of large organisations and 38 per cent of small businesses were attacked by an unauthorised outsider in the past year. This can come in many forms: theft of data, theft of money or intellectual property, damage or disruption to computer systems.

If you run a business, it's easy to think everything is all right because you're unlikely to be a target. Hackers are after the money and the banks, right? The truth is that most businesses hold information likely to be of value, such as customer details or commercial data. And much of the criminality we see online is automated.

It may not necessarily be a hacker specifically targeting your business. Instead, they've set literally thousands of traps, in emails and on websites, and they're waiting to pounce when one of your staff clicks on a malicious link or opens a questionable email attachment.

Once your business is exposed you are open to a range of threats, such as theft of money and data. We've seen "crypto-extortion", in which companies' files are rendered useless through encryption, and are unlocked only after payment of a ransom. Even just general disruption to IT systems can be serious: what would the impact to a business be of having no website or email for just a few days?

Our analysis has found that more than 80 per cent of successful cyberattacks target basic weaknesses in IT systems. Businesses are being exploited because they haven't taken simple steps to protect themselves. In effect, criminals are walking in through an unlocked front door. It's actually fairly easy to get the basics in place – even absolute beginners can do it – but not enough businesses are taking action to protect themselves.

This is why the government worked with industry to develop the Cyber Essentials scheme. Cyber Essentials shows how to address those basic vulnerabilities that are commonly exploited. Government suppliers are now required to have a Cyber Essentials certificate in order to sell goods and services to government.

Cyber crime is perhaps one of the greatest threats to national security, which is why we are taking the necessary steps to protect businesses and customers.

What would the impact be to a business of having no website or email?

We need to get real about the threat. I want all businesses operating online to have Cyber Essentials, as a minimum. Many should do even more, but every business should have the basics in place.

The government's Cyber Streetwise campaign urges all small businesses and consumers to use strong passwords, instal security software and always download software updates.

This is a great start for all small businesses. Firms can also use our free guide *What You Need to Know About Cyber Security* and train their staff using our range of free online training modules. All government staff are required to complete this training and I'd like to see all staff in businesses do so, too.

Protecting personal data is a legal responsibility for businesses under the Data Protection Act. Taking action on cyber security is not just the right thing to do, it's also what customers expect. The public is increasingly interested in how its data are used and stored. The latest research suggests 83 per cent of consumers are concerned about which businesses have access to their data and whether they are safe, with over half (58 per cent) saying a cyber breach would discourage them from using a business in the future.

Entrepreneurs and start-ups – particularly those with innovative ideas and intellectual property to protect – may be particularly vulnerable, given their organisations are likely to be new and yet to develop a mature approach to security. We need to protect our knowledge and intellectual property, as this is a key strength that sets the UK apart from others. Earlier this year, when I met the Catapult Centres – the UK's innovation centres to help drive growth and innovation in critical areas – I said I'd like them all to have Cyber Essentials by the end of the year.

So, where are we now? The changes we've put in place during the past five years as part of the £860m National Cyber Security Programme have transformed industry awareness and action.

A wide range of guidance and support is now available: 58 per cent of the top UK firms have used the government's 10 Steps to Cyber Security guidance (up from 40 per cent in 2013) and 88 per cent now include cyber security in their risk register (up from 58 per cent in 2013). There is also increased capability in law enforcement to tackle the threat. To build on this, the Chancellor recently announced a further £1.9bn investment in cyber security to make the UK one of the best-protected countries in the world.

Awareness and action are increasing. But the government can't do it alone: business leaders need to play their part and ensure they protect the companies they have worked so hard to build. Only by doing this together can we fully realise the benefits of the digital economy. ●

Ed Vaizey has served as Minister for the Digital Economy since 2014 and is the MP for Didcot and Wantage (Conservative)

TOP TIPS

My top three online security tips for businesses

1. Get the basics right and train your staff

2. Understand your risks and manage them

3. Adopt the Cyber Essentials scheme

avatu

May the force be with you . . .

Cyber threats are here to stay, and are growing in sophistication. Leaders worth their salt, says **Joe Jouhal**, always face a challenge head on. And this is how.

If there's one thing that a business leader understands, it's risk.

Risk to the share price, risk to the organisation's reputation, risk to his or her career.

It's a universal language understood by all business leaders everywhere until . . . for some (apparently almost inexplicable) reason, they come face-to-face with cyber security.

It's hard to believe, but report after report shows that many business leaders still don't – to the frustration of their security and IT teams – have a handle on their organisation's cyber security liabilities, and the threat their organisation faces because of it.

Indeed, the chair of the Institute of Directors, Lady Barbara Judge, said that cyber security is so overwhelming for many senior execs and boards that they leave it in the "too difficult category", no doubt hoping it will just go out of fashion and melt away.

The question is why? And what can be done about it? It appears – as the IoD has already identified – that many people, even at the highest level, find the subject too complicated and too confusing.

They also expect the solutions to be overly expensive and don't think they'll be affected. They believe the rudimentary perimeter protection they rely on now is enough to combat the evolving threat.

But this finger-in-the-air approach isn't leadership. It's Russian roulette.

A leader can't say his or her organisation doesn't need to be on its guard without first properly analysing the threat.

> Tackling cyber and data security issues can be simple and inexpensive

There is a lot of unnecessary hype and hyperbole. And cyber security is sometimes considered the "new big thing" with a flash of the emperor's new clothes. But the truth is, technology is already ingrained in our business world and it's only going to increase as more and more of our equipment is controlled and monitored over the internet (commonly known as the Internet of Things).

If a business doesn't do it now, it is going to have to do it in the near future.

Its existence means we have to change the way we operate in business. Exactly in the same way we had to accommodate the steam engine, the telephone and strong-armed health and safety directives.

It is something almost all businesses should be taking seriously, merely because the ramifications of getting it wrong can be extremely costly (ask TalkTalk, Sony, Carphone Warehouse, Ashley Madison, Lincolnshire County Council, Bettys Tea Rooms – and the many more who have suffered).

The sooner leaders get to grips with the subject, the sooner layers of mitigation – in the shape of technology, policies and practices – can be introduced to reduce the risk of cyber and insider threats.

Tackling cyber and data security issues can be simple and inexpensive. There are solutions for every pocket and everyone's appetite for risk. But underpinning it all has to be strong leadership to face the subject head on, and risk-based, tried-and-tested, age-old good business sense.

Joe Jouhal is CEO of Avatu, cybersecurity and information security advisers to inspiring companies

Are you asking the right questions?

How to assess your cyber risk

Organisations usually have firewalls and anti-virus software in place – but this doesn't mean they are secure. The government's advisers at GCHQ recommend that organisations adopt a layered approach to protect their business from hackers or insider threats.

To understand the risk they face, leaders need to question what is being done beyond anti-virus.

Questions to ask include:

1. Where is our most sensitive, potentially damaging and most valuable information? Where is every copy of it? (This could be customer information, IP, investment plans, emails between executives . . . and much more). Who has access to it? What special arrangements do we have to protect it within our systems? Is access privilege managed (where people have access to only the things they need)?

2. How do we protect our sensitive data when it's outside our perimeter? How is it protected when it's with our lawyers, accountants, contractors, consultants, etc? How do we stay in control? How do we stop it being seen or shared by unauthorised people, or being made vulnerable by their insufficient security? How can we pull the plug remotely if we need to?

3. How do we protect the multiple devices we all use today (which are called "endpoints" by the IT world)? Are they a potential weak point of access to our systems and data?

4. What do we do about email security beyond anti-virus? Do we employ tools that strip away anything that's potentially damaging but still allows safe information through? Technology for this now exists.

5. Do we KNOW we haven't already been breached? If something sinister has already evaded outdated security, people often don't know it's there until the damage is done. Knowing sooner rather than later can't turn back the clock, but it does give the chance to limit the damage.

Help with the answers is available for innovative and inspiring companies from Avatu on 01296 621 121.

Assess your cyber risk with a 30-day behaviour inspection report

Special offer to New Statesman readers

Is the enemy already within?

Ignorance is not bliss when it comes to cyber security. Actionable intelligence gives you the chance to manage your risk and make informed decisions.

Anti-virus and firewalls stop only known threats. But others can slip through without being noticed – and the longer they stay on your system, the more damage they do.

In many cases, infections and breaches last for several weeks and even months (the average discovery time is more than 200 days), leaving your organisation vulnerable to unauthorised remote access, data theft and espionage.

With our partners, we'll arrange a 30-day behaviour review of your IT network systems.

Our recommended specialist detection and mitigation technologies are used by some of the world's largest and most successful organisations.

For a month, we'll monitor what's happening live on your systems and we'll also let you know if anything risky is already on there which your perimeter defences didn't see and didn't stop.

Call us on 01296 621 121 or email cybersecurity@avatu.co.uk to find out more.

The report will help you assess your overall risk, and decide your priorities.

SANDCASTLES *in* WATERFALLS

NOTHING ENDURES BUT CHANGE

You are the weakest link

People talk a great deal about technology and its vulnerabilities but the culture and human issues are important too, says the technology writer **Stuart Wilkes**

An incorrectly addressed email leading to your company's salary details being emailed to a competitor. A USB stick left on a train that is stuffed with your market-leading intellectual property that then finds its way on to the internet. A disgruntled employee downloading your client list and emailing it to his Gmail account in preparation for a move to a competitor.

Be under no illusion: the human element within a business is the biggest cyber risk it faces. Alternatively, an individual may get duped by a fraudulent email, or hand out a password to a third party. We may try to avert these sorts of issues, these cyber breaches, but we are flawed. We can be tired, lose concentration, we can be in a bad mood, we can be overrun by our emotions, stressed to breaking point and then one moment of human error and a damaging cyber incident has occurred.

Irrespective of the cause, be it accidental or purposeful, the effect on a company can be disastrous, losing it reputation, customers and trust.

All of which will take considerable time and expense to rebuild. In order to prevent such human error, companies need to develop a cyber culture, ensuring that all employees, contractors and suppliers who handle company-sensitive data are aware of their responsibility for its safekeeping coupled with the company's clear understanding of its legal obligations.

This culture needs to be backed by strong human resource guidelines that can be vigorously enforced should a data breach occur.

Let me tell you a little secret: you have been here before. You have had human-related issues in the past and you have addressed them and enforced them, and although some of your employees may see them as onerous and mock them, they have actually improved business for the better. What am I referring to? Health and safety. Two words that continue to get a bad press and that have taken a generation to become part of corporate culture. However, there is no denying that it has improved business.

The lessons can be mirrored when adopting a cyber culture. The difference here is that we are dealing with virtual as opposed to physical risks.

There is a legal requirement for health and safety, which, should companies be complicit, can lead to fines and prosecution if not adhered to. We are at the dawn of a similar transformation regarding cyber security.

To lessen the burden on the individual and to do everything technically possible to prevent human error there is a raft of technology solutions that monitor the threats, monitor all the endpoints on a network and, should they discover any form of cyber attack, will alert the security team and also automatically apply countermeasures. However, they cannot cover all eventualities of human error.

With European legislation coming into force in 2018 that will make mandatory disclosure of any cyber breach, companies are well advised to start developing a culture with regard to the handling of data which mirrors their experience of health and safety.

Luck can no longer be relied on to prevent a cyber breach occurring by human error. Leadership is required.

You've done this before – and you can do it again.

Just do it before anybody gets hurt.

Stuart Wilkes is a specialist technology writer and is also editor-in-chief of a forthcoming technology publication, *Sandcastles in Waterfalls*. The first issue, available in March, examines the topic of cyber security from a range of differing viewpoints. For more information visit: sandcastlesinwaterfalls.com

Digital Pathways

It's a growing internet thing

The Internet of Things is producing security issues all of its own, explains **Colin Tankard**, managing director of Digital Pathways

The Internet of Things (IoT) was first envisaged in the 20th century. It is a vision whereby potentially billions of "things" such as smart devices and sensors are interconnected using machine-to-machine technology, enabled by internet or other IP-based connectivity.

A study by the McKinsey Global Institute estimates that the IoT will have a potential economic impact of US$3.9trn to US$11.1trn per year in 2025 across nine settings: homes, offices, factories, retail environments, work sites, human health, outside environments, cities and vehicles.

Estimates vary widely regarding how many IoT devices will be connected, but one often quoted statistic comes from the technology firm Cisco, which estimates that 50 billion objects and devices will be connected by 2020.

Security issues

While the IoT holds promise, security issues have been uncovered. Such security issues can have grave consequences, causing damage, disruption to operations or, in some scenarios, even loss of life, due to the wide range of sectors involved, and their impact on everyday life.

In smart buildings, where systems ranging from HVAC, lighting and door access controls to video surveillance and elevators are all interconnected, a security threat that is exploited to disrupt power or lighting could cause loss of life – for instance, in a hospital. A range of security risks has been uncovered in the devices that make up the IoT, because many devices are not developed with security in mind. Many contain embedded software, often proprietary firmware, which is problematic to patch and upgrade, leading to vulnerability and configuration management issues.

Solving the security challenges

To solve the security challenges of IoT devices a different stance is needed. Security needs to be built into products by design. It cannot be bolted on afterwards.

Steps organisations should consider

Organisations should look to limit what is allowed in the workplace, considering the risks versus the benefits, as well as looking at how systems are interconnected and, therefore, how risks such as malware infections can be spread.

Our experience has shown that it is time to link physical and network security together to enable a total view of incidents. This has led us to develop our nLiten system to enable organisations to have a manager of managers gathering information from all systems and physical guarding/security. This enables management to make decisions regarding the threat posed and how it can be controlled.

Where any anomalies are uncovered organisations need to have workflow and escalation procedures in place so that managers of security are alerted promptly to any potentially serious security threat or incident. This helps greatly in the time taken for remediating problems, and therefore cost. It is essential that all procedures and processes are documented, completed in a compliant way and an audit trail generated to provide evidence of the effectiveness of actions taken.

Remaining vigilant

While it could be said the IoT is still in its infancy, IoT devices, and increased connectivity, are being seen across a wide range of sectors. Many will be familiar with consumer-oriented, smart, highly connected devices that invade workplaces. Organisations are still grappling with BYOD, creating headaches for many in terms of managing and controlling what sensitive data can be accessed.

But the industrial IoT holds the greatest promise, and threat, and this is being overlooked.

The IoT appears to be an unstoppable force. Until security issues are resolved, organisations need to be vigilant, ensuring that they weigh up the security risks against the benefits to be gained putting appropriate controls and policies in place, as well as keeping a constant eye over what is connected to their network and how devices are performing.

For more info visit: www.digpath.co.uk

Cyber security is like a conspiracy

Cyber security is a mix of people, unknown threats, impending legislation and how they all conspire to make life difficult, says **Andrew Taylor**, CEO of Bronzeye IBRM

Cyber: a word with no settled definition and that sends shivers down the spine of most executives at every company.

Information security (InfoSec): what they usually really mean when they say "cyber security".

According to Microsoft, during 2015, 160 million customer data records were compromised and cyber breaches had an average duration of 229 days before detection (and a similar period to remediate). This helped to destroy $3trn of market value in the process. If each of those dollars was converted to one second of time, it would equate to just over 95,000 years!

In the last year, 84 per cent of large companies and 75 per cent of smaller enterprises have experienced some level of data breach. The average cost of a large breach is over £15m. Yet, despite all of this, executives convince themselves that their company will dodge the bullet. Well, they are almost certainly wrong. NO company is too small to be of interest; hackers will steal or gather intelligence to create a fraud opportunity, ransomware attack, or to find a route to bigger targets.

New cyber laws are being enacted everywhere. Many have cross-border reach; most have far-reaching implications. Increasingly, authorities require companies to bring qualified expertise into the management structure. Increasingly, these regulations contain swingeing negligence and non-compliance penalties. The trend is to single out executives who were responsible for a firm's InfoSec for public sanction. It is advisable to know which legal regime(s) you are accountable to.

Our problem is largely psychological rather than cyber. Disgruntled or distracted insiders are ultimately responsible for an enormous proportion of data breaches. You can be certain that people will drop you in it more frequently than your IT systems ever will. Pressured, late, overworked, distracted, duped, or anything else, it is too easy to make an error.

Hiding in plain sight we have Zero Day or 0-Day threats – technology flaws, unknown to security professionals, which allow stealthy access into systems. Because they are unknown, there are few defences against them. As with their physical cousins Aids and ebola, defeating Zero Day threats is a Sisyphean task in a fast-moving environment.

Every government has prioritised the broad improvement of InfoSec. Criminals seek to exploit flaws.

Top of their interest lists are easily tradable or exploitable data such as financial information, followed by weak processes and flawed procedures.

Create a virtual door, and a virtual criminal will walk through it. We must seek to restrict their options on every level.

InfoSec is at the heart of all good businesses – physical, cyber and personnel security, drawn together with good governance. This must be driven by management and engage all employees. Four in five data breaches at large companies begin in smaller companies.

Criminals exploit weak information security arrangements in the supply chain. Frequently, an attack will begin with a spoofed or hijacked email from a trusted sender which is likely to be accepted and attachments opened by the unsuspecting victim.

Regardless of how strong defences are, companies must ultimately prepare for the worst.

Being ready to respond effectively when (not if) an attack takes place is critical. Reading up on the crisis management instruction manual in the middle of the storm is not an optimal strategy.

Effective planning and preparation for the event increases the chance of identifying, ejecting, mitigating and weathering a cyber breach, improving a victim's ability to get back to business. No plan probably means the opposite – financial and reputational damage, which could prove to be fatal to the business.

Think security, not compliance.

Think people, not cyber.

Your call.

For more info visit: www.becybersure.com

Threats and opportunities

Involving a third party in your IT infrastructure carries its own risks and rewards, says **Malcolm Marshall**, global leader for cyber security at KPMG

While technology may be developing faster than ever, in many cases today companies have IT functions that are capable of supporting their business ten years ago rather than for what their needs will be in ten years' time. A fear of being left behind has created a huge industry of outsourcing companies willing to take the strain of keeping up with innovation while also allowing their clients to focus on what they do best – selling their product.

As a consultant working in the technology industry for many years, I have seen swaths of industry hand over their IT – whether it be their accounting functions or data centres. And this is a good thing. I believe that 95 per cent of a company's technology can and should be outsourced.

Outsourcing companies can generally do things more cheaply and also have the benefit of being able to provide top-level talent to clients. KPMG has conducted many surveys looking into the cyber skills gap in the UK and it is a recurring theme. When using an outsourcing company, clients can also tap in to a wider network of potential learning through client forums and events.

But as with any business decision, there are pitfalls, which is why I am emphatic about 95 per cent rather than everything. Companies need frameworks and safeguards in place before they take this important step.

In recent years, a number of global companies have been reversing previous outsourcing decisions. One major financial services provider, for example, was well known to have been one of the most innovative and enthusiastic in recognising the benefits of sharing the load – outsourcing nearly 80 per cent of its IT work at its height. But fast-forward to 2014, and the new chief information officer talked openly of outsourcing having "gone too far" and how the firm was now insourcing work that it recognised to be of strategic importance.

What it recognised was something other businesses are now realising – you cannot outsource that 5-30 per cent of your company's IT requirement when it is of critical importance to your business. Not only could you risk losing intellectual property, but clearly it would be very possible, certainly in a smaller business, to be reliant on technology that nobody within the organisation understood.

As a personal example of this, my first experience of the Internet of Things was 15 years ago, when an infrastructure operator called me in when they had a new safety system installed. I couldn't understand why they needed me, until I realised the system was internet-enabled and the company was in a mild panic about what that meant. While it makes me nostalgic for the days when equipment was operated with big yellow levers marked "on" and "off", it does make the point that it is quite easy for a company to sleepwalk its way into a situation where it has a lack of control over critical parts of the business.

It was interesting that this year's Davos summit was about the Fourth Industrial Revolution. Many companies still struggle with the Third, and are still learning lessons from being hacked and having suffered other data breaches.

Only in recent years have chief executives started to realise the importance of IT and they are creating governance systems around their accounting systems and putting in risk controls around data and assets. Companies such as retailers and banks, which have close customer engagement, have been under intense pressure to deal with this.

What is bizarre is not that these companies are leading the way in dealing with this but that so many others remain relatively blasé about being hacked when even a humble vending machine is now internet-enabled and transmitting a constant stream of data.

That is not to say that nothing has changed. I have seen companies become more prescriptive about how their security is managed. Typically, businesses

The Internet of Things will throw up risks as well as opportunities

will retain a security function, but we have also seen cases where companies will choose to outsource part of that to an independent supplier so that they still get the comfort of there being third-party oversight of the outsourcer, but without having to have a large in-house team themselves. For large companies, it is not uncommon to have anywhere between five and ten supplier relationships or even more, for various parts of the technology infrastructure, including apps, back office and front office.

But what makes this whole ecosystem work is contract flexibility and a collaborative culture. It is vital that both customer and supplier work hand-in-hand to ensure a constant flow of information, as it can quickly become a nightmare when things go wrong.

A few years ago I was in a situation with a major customer-facing brand where the US-outsourced IT security was going swimmingly but relationships had all but ground to a halt in Europe. What quickly emerged was that the European division had negotiated the supplier down so hard that it had had to cut dangerous corners to keep the contract in profit. It just doesn't work. Like anything in life, you get what you pay for and the best outsourcing relationships are delivered from close and flexible working where everyone understands what is expected of them.

Now clearly this takes planning. Cyber security issues can sometimes sit at the end of a larger contract, or end up being rushed through after a hack or where an internal audit has uncovered a weakness. Again, this can lead to misunderstandings and therefore a breakdown in communications.

It is vital that the in-house team takes the time to take suppliers through a detailed walk-through of its requirements and processes, so that any issues can be identified in advance and expectation gaps are kept narrow.

What is also vital is that everybody – all suppliers, and not just IT – is covered by the same rules. All suppliers need to understand where weaknesses can occur. For example, there was one high-profile attack where the hackers got into the business from the air-conditioning supplier – nothing to do with IT, one might think, but still a bridge to highly sensitive data. The point is that one can have the best IT outsourcing companies in the world but if one has weak processes, passwords or small suppliers who simply don't understand what is expected of them, data, and therefore money, can go missing. And the best contracts in the world will not stop that happening.

We live in an era of vastly changing IT and one in which fraudsters are innovating. While outsourcing can and should absolutely benefit an organisation, it needs to be handled in a thoughtful way, particularly when it comes to security. The best scenario is where companies and suppliers work closely together to resolve issues and where learning is shared. For some, more forward-thinking organisations, they are already leading the way – by hosting seminars for smaller suppliers, for example, to help them understand what is expected of them. This is a fantastic and collaborative approach that should be welcomed and copied. Clearly others will find their own way, but make no mistake: the pressure is on.

PSD PHOTOGRAPHY

PROTECTION GROUP INTERNATIONAL

Unless we normalise the cyber threat we can't manage risk

Education and normalisation are the keys to tackling the cyber threat, says **Matthew Olney**, communications and content executive at PGI

On New Year's Eve 2015, the BBC's website was knocked offline. Immediately social media was abuzz with rumours and it wasn't long before the press got involved. Headlines blamed the so-called Islamic State for the attack. In reality, it turned out to be the handiwork of anti-IS hacktivists who were testing their capabilities. Either way, the question remains whether a simple piece of temporary online vandalism merited the media profile it generated.

People fear what they do not understand

Cyber is a word that can cause the mind to race. A "cyberattack" is as dramatic as whatever an imagination makes it. With the right stimulation, "cyberattacks" make good headlines and great scare stories. The best way to tackle the threat posed by cyber criminals is to educate people so that they understand how such attacks occur and in turn learn how to counter them. If we regard cyber crime in a similar context to, say, burglary, immediately the threat becomes normalised.

Every decision we make in our lives – be it conscious or subconscious – is based upon some kind of risk assessment. Unless an understanding of the "new cyber threat" is thorough and widespread, the associated risk will continue to be seen and treated as extraordinary.

In the 21st century, where technology underpins just about everything we do and use, this is an unsustainable and unaffordable position.

In business and government worlds this lack of understanding continues to be relentlessly exploited by an IT security industry that perpetuates the idea of dramatic and increasingly apocalyptic consequences if its new security technology is not adopted. The industry continues to use the same hi-tech, complicated scare language that it adopted in the run-up to the millennium that burned its credibility and confidence in its integrity.

The real-world consequence of this lack of understanding and consumer scepticism is that the take-up of cyber security risk management is far slower than it should be.

Perhaps, unlike Y2K, there are genuine threats and risks which are, and will continue to be, an inherent and perpetual aspect of adoption of technology. There are always people who will seek to exploit good things for nefarious or criminal means, and technology is no different. But that doesn't undervalue the huge benefits of adopting technology. Nor does it mean – just like with all other security risks – that the threat is anything to fear disproportionately.

For years, law-enforcement agencies have educated the public on how to protect property from would-be thieves, and just like with conventional crime there are measures that people and organisations can take to prevent themselves from becoming victims of a cyber crime.

The risks vary hugely, depending on the environment in which they are considered and, again, just like with other security risks, proportionate treatment of them for the vast majority need not be expensive, complicated or anything other than a normal cost of living and operating in the 21st century. Even for those such as banks, the defence industry, some government departments and other industries where the nature of the threat is more complex and has more impact, effective risk management need not be any more challenging.

Let's tackle crime

Cyber crimes are the most common in, but only one part of, the spectrum of activity referred to as cyberattacks. But such incidents aren't "attacks". They are theft, vandalism, blackmail or ransom – or, indeed, any version of illegal activities that have plagued society for thousands of years. The main differences between "cyber crime" and "conventional" crime is the scale of effect that can be achieved.

Conventional theft is limited by how much swag the perpetrators can physically carry. Cyber crime is not.

Conventional crime, unlike cyber crime, often can be investigated and solved within one national jurisdiction. Cyber criminals can carry out crimes against their victims simultaneously, very cheaply and without necessarily leaving "home".

Does that sound scary? It doesn't have to be. The police and other agencies are very good at thwarting conventional crime. They've had many years to develop new methods of crime-fighting, from taking fingerprints to DNA profiling and other sophisticated techniques.

The same principles apply to cyber terrorism, cyber warfare, online activism, etc – each sits at a different point on the cyberattack spectrum.

Normalising the hacker

The portrayal of hackers in the media conjures up evil masterminds or sophisticated military units based in some secret bunker, and surrounded by racks and racks of highly expensive and sophisticated equipment.

Of course, many do work for nation states, subversive or proscribed organisations or sophisticated international criminal gangs. Yet many hackers are bored teenagers experimenting and operating out of their bedroom or their parents' basement, or they are ordinary, self-taught criminals who find this type of crime somewhat less arduous than others.

Just like any other opportunistic thief, these hackers would rather attempt to steal from an easy target. And just like other types of criminal, they rely on their victims' naivety and carelessness. When looking for a target, a hacker will typically choose something that will not require too much effort to attack.

As with any regular criminal, if they think security is too tight they will move on and seek out easier prey. If every person and organisation puts effective, basic security into place, the number of incidents we see so frequently will fall. By demystifying hackers and their mindset, they won't seem as scary.

Knowledge is strength

To quote one FTSE-100 chief executive: "This debate is controlling us, not vice versa." Effective education, underpinned by informed investment in the right things at the right time, will place control of the debate, as well as the solution, back in the right hands.

PGI aims to be a major contributor in helping to normalise the new cyber security threat.

All of our instructors are established cyber security professional who hold leading industry certificates and have a wealth of real-world experience. They combine their teaching with daily operational activity, keeping their knowledge and training material fully up-to-date and relevant.

Whether you are a small company or a large organisation, we have the skills, experience and expertise to offer businesses and governments tailored solutions that will make the difference in tackling the threats posed by cyber crime.

PGI believes in education and awareness. In addition to training cyber security professionals, cyber security education and training for mainstream IT professionals, users and executives stand at the core of our posture.

To assist with this, PGI opened its Bristol-based Cyber Academy. The Academy is a custom-built, multi-functional learning environment, offering 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.

We hope that increasing awareness and education will lead governments, law-enforcement agencies, businesses and the public to adopt the right posture.

Cyber crime is nothing to be complacent about, but neither is it anything to fear. It is simply one of the modern risks of operating in the 21st century.

www.pgicyber.com
Telephone: 0845 600 44 03
Email: enquiries@pgitl.com

Who's hiding behind your app?

David Emm, principal security researcher at Kaspersky Lab, considers the new risks

Mobile phones have become a ubiquitous technology and an extension of our everyday lives. With the rise of technology came the emergence of various social media platforms and applications designed to make our lives easier and more convenient: for example, online dating apps aiming to help us find companions. However, with our connected culture come great risks, such as identity fraud, harassment and theft. Beyond a handful of pictures, emojis and lighthearted messages, you have very little knowledge of a person's true intentions or motives when they are positioned behind a social media account or dating profile.

Recently, there have been calls to increase awareness of these dangers, as it has been reported that crimes relating to dating apps have increased by 560 per cent in the past two years. In 2015, there were a huge 412 crimes relating to just Grindr and Tinder.

There are clearly dangers associated with consumers sharing too much information on social media using modern dating apps. However, there are also risks businesses need to consider when they have a mobile workforce accessing such applications and using the same devices for work.

Identity fraud

When you've booked a holiday and received your ticket, it is not uncommon to want to post pictures of your boarding pass on the likes of Facebook and Twitter. However, this is one of the fundamental mistakes we make.

Not only are you providing all of your travel details with potential criminals, they also aggregate personal information about you from several places on the internet, which could lead to the fraudsters finding out where you live. And if that is the case, you've just told them that the house will be empty for two weeks.

Additionally, when you post pictures on social media, there is the inherent risk of having your "face" stolen.

Everyone loves to take a "selfie", but posting pictures to Facebook for the world to see opens up a whole new world of problems, considering that the content is accessible by cyber criminals. It is already possible to put on the face of another

SHUTTERSTOCK

person during a video call. In fact, there was an app in 2011 which could easily overlay a face from a photo on to a moving face in a video, dynamically.

With technology available that is already five years old having the ability to "steal your face", precautionary measures should be implemented now in order to combat identity theft.

Unfortunately, the dangers of oversharing information aren't always glaringly obvious, and we're even more likely to be caught off guard when using a smartphone or tablet to go online. These devices haven't often been a target for cyber criminals in the past, so we unknowingly feel secure using them. It's important to avoid a false sense of security when posting information online. There's a good rule to live by to help avoid oversharing information online – if you wouldn't publish something on the front page of a newspaper, don't post it online.

So, how can we do a better job of protecting ourselves online? When using social media, it's important to note that each individual social media platform is a treasure trove for scammers who are able to gather users' personal data. This data is then often used to engage in fraudulent activities. To counteract this, it is always a good idea to check your security settings on the likes of your Facebook, Twitter or even Instagram account.

Social business

There are two aspects one needs to consider when using social media platforms. The first is privacy. It is imperative to understand how you can restrict what someone else can find out about you online. You also need to be aware of what happens to the information you share through a social network – either with others, or with the provider of the service.

Consider who owns the data you publish and how the provider will use it in the future. In the case of a business account, it makes sense to give it a generic name, rather than linking it directly to a person. This immediately distances the account from a specific employee – and makes it less personal if someone directs abuse at the account.

The second aspect that comes into play is security. Use only secure web pages to log into online accounts. Check that the URL starts with "https" and click to check the security certificate.

You should also be careful when accessing an account. Public, untrusted wifi is fine for general surfing, but unsuitable for confidential transactions or sharing private company data. This is due to the danger of accessing rogue hot spots, or of unencrypted data being intercepted. Finally, access sites from secured devices only – devices that are protected using internet security software and patched with the latest security updates.

Dangers of dating apps

Online or offline, meeting strangers will always have inherent risks. The risks become even more prevalent when using online dating apps. As such, it pays to take the same precautions when arranging a real-world meeting with an online date as you would in "real life" – for instance, you wouldn't arrange to meet a real-life first date down a dark alley having told no one where you were going.

Various measures can be taken in order to minimise these risks, and while taking such precautions might not make you totally safe, they limit your exposure to risk.

> There isn't a digital platform in existence that is 100 per cent secure

The first and most obvious measure is not to trust people online automatically. There's no way to identify someone's true appearance or motives through the messages they are exchanging with you. Take the Ashley Madison hack. Of the 37 million registered users, approximately 12,000 of the active accounts turned out to be real women. Most of the others were either men or just bots.

Second, and this relates back to the usage of social media, linking your Facebook or Instagram profile with an online dating app can prove to be problematic, especially in the hands of burglars or fraudsters. If you happen to "match" with someone with ill intent, they are able to gain access to your social media pages, which are likely to include addresses, pictures and more personal information.

There isn't a digital platform in existence that is 100 per cent secure, especially with the likes of dating apps, dating websites and social media being utilised every day by a significant portion of the global population. However, another platform that is equally insecure but often overlooked in terms of security is the messenger app. Research by the Electronic Frontier Foundation (EFF) showed that most popular messengers do not boast high security levels. The highest score that a secure messenger app could get was seven points. Unfortunately, Skype, AIM and BlackBerry Messenger notched up merely one point each, whereas Viber, Google Hangouts, Facebook Messenger and Snapchat scored as high as just two points. Even WhatsApp, which recently announced that more than a billion people use its messaging app, scored no better than two points.

In the case of the Ashley Madison hack, it is clear that hackers are targeting not only individuals, but businesses, too. The company reportedly asks its customers to pay a fee of $19 to erase their profiles if requested. However, their profiles aren't completely wiped as promised.

Since then, the hackers have actually said that because a lot of the members use credit cards as a method of payment, their site records show real names and addresses – which, of course, is the most important information that the site's customers want removed.

Another consideration is that the lines between using mobile devices for leisure and business have also become blurred. Although it's clear that both the general population and businesses around the world are becomingly increasingly aware of BYOD, it is often difficult to translate that into action. With this, the number of consumers accessing certain applications on their smartphones grows for businesses, too. Companies need to ensure that their employees are aware of the threats they may be posing to the organisation.

So, how can we ensure that both businesses and consumers in general are doing the best they can to protect themselves online? It is vital that businesses consider the human dimension of security and ensure they make security awareness an essential part of their IT strategy.

Businesses also need to adopt an in-depth defensive approach, rather than relying on perimeter defences.

In today's mobile business environment, they need to apply a "security wrapper" around every employee – so that they are protected wherever they work and whatever devices they use.

UNISYS

The time is ripe for microsegmentation

Corporate security strategies are failing, so leaders must retool to face the latest cyber threats, says **Tom Patterson**, vice-president (global security) at Unisys

You could say that 2015 was the year cyber crime became mainstream. We saw brands from all over the world including the likes of TalkTalk, JPMorgan Chase and Ashley Madison all come under scrutiny as breaches of their security became global news. It's repeatedly on the news agenda, as it's pervasive and growing in complexity and persistence. Breaches are not only detrimental to business, but major brands also run the risk of reputational damage due to the inconvenience and the exposure their customers are subjected to.

As a result, 2016 is the year when the priority will be to shift tactics to combat the increasing number of hackers by abandoning outdated security strategies to protect intellectual property and other assets. But how can this be achieved?

Security openness

As with all change, the first step is for more security leaders to start admitting that their current processes are falling short, and to look at new strategies and methods that have a more realistic chance of protecting the organisation.

This isn't a new theory by any means, and is something that many experts have been stating for a while.

However, despite the obvious "clean slate" advantages of starting afresh with security solutions, there will still be a large section of CISOs who are unwilling to let go of their sunken costs and to look forward. To succeed, they will need to abandon the old ways of securing the enterprises – with bigger walls and more event tracking – and adopt the new micro strategy, which takes advantage of network virtualisation and Internet Protocol Security (IPsec) to isolate the underlying infrastructure in a much more granular and controlled way.

Year of the micro

The answer to this is microsegmentation, as it allows enterprise managers to quickly and easily divide physical networks into thousands of logical micro segments, without the historic security management overhead.

This approach gives control back to the enterprise networks, without them having to deal with the firewall rules and outdated applications, all the while embracing remote users, cloud-based services and third parties that have all become targets for attack.

This new micro-segmentation model will start giving the good guys the advantage in the fight against cyberattacks.

With new containment strategies, organisations will have the ability to work at the Internet Protocol (IP) packet level, which makes it easier to apply anywhere a company's data goes – from data centres to public clouds, from employees on the move to suppliers around the world.

Microsegmentation is driven by existing identity management systems, so it is simple to establish communities of interest for authorised users across all of these technologies.

It is clear that the impact of the major breaches of 2015, which has been reported as having an average cost of £107 for each corporate record lost or stolen, ensured that security is no longer just a technology issue. Instead it is now seen as a business issue that requires prioritisation from the top down. We will see the security function evolve to no longer report solely to the CIO.

Boards will start to care and take real action and make cyber security expertise a requirement across the C-suite. Security is now a top agenda point in the boardroom as business reputations are once again at risk. Organisations will no longer be allowed to take the position of standing by and watching cyberattacks unfold: they will finally have the power to react rather than prevent.

As a result, "proactivity" will be the key word for 2016, with microsegmentation being a major player and step in the right direction for innovative organisations that are serious about security.

For more info visit: www.unisys.com/offerings/security-solutions

DigitalAssurance
Information Security Services

Watching me, watching you, aha

Security comes in different flavours. **Carl Jordan**, security consultant at Digital Assurance, explains the visual variety

Visual security is the protection of sensitive or private information from physical events and circumstances that could impact the confidentiality, integrity and availability of this data.

As our working environment becomes ever more mobile, data is becoming increasingly exposed to the threat of direct observation techniques such as shoulder surfing. With assets including PINs, passwords and sensitive documentation becoming some of the prime targets, these techniques thrive in crowded areas ranging from commuter trains to office lifts.

High-profile occurrences have caught the attention of media outlets in the past, with a number of public figures having been caught out.

In 2008, a UK civil servant, Zahir Sachak, was pictured working on secret documents, including government policies, on his commute home. Similarly, in 2009, the then senior counterterrorism officer Bob Quick was photographed with briefing papers of a secret anti-terrorism raid designed to foil an alleged al-Qaeda plot to bomb Britain. The latter resulted in Quick's swift resignation.

The cost to businesses of cyber crime continues to grow. A new study by the Ponemon Institute shows average annual losses to companies globally are now in excess of £5m, with some studied companies losing up to £45m. Overall, it is estimated that cyber crime will cost businesses over £1.5trn by 2019. Breaches through visual security are often useful for the reconnaissance phase of these attacks and the unauthorised identification and mapping of vulnerabilities and services.

On a personal level, the simplicity of breaching visual data security and the difficulty in detecting such events should also be of concern to individuals and their privacy. Its very notion and threat to data integrity is echoed by IT professionals. In a study by Digital Assurance, 80 per cent of those asked had minimal confidence that adequate steps were being taken by individuals in an effort to secure their data from malicious onlookers. If you happen to be reading this article in a crowded area, take a look around you. It's more than likely that within a few minutes you will have some form of sensitive data at your perusal. Despite this, the general public awareness of visual security could be enhanced, because it evidently fails to deter individuals from entering PIN codes, reading personal messages or conducting online banking in clear sight of others.

From a corporate perspective, Secure – the European Association for Visual Data Security – offers a broad set of guidelines that organisations should adopt in order to protect themselves.

The steps include:

- Identify sensitive data
- Classify data
- Access control
- Know where your data is
- Monitor access
- Regularly review and manage remote access
- Password-protected screen savers
- Security awareness
- Privacy screens
- Siting of equipment

Secure also recommends that IT security guidance should contain instructions on mitigating these threats: for example, through utilising ISO/IEC 27001, a family of standards that assists organisations in keeping information assets secure. Primarily, employees should be educated on the threats of visual data breaches and cost-efficient solutions such as screen shields or privacy filters should be implemented.

Although this article only scratches the broad surface of visual security, it strives to promote general awareness and highlight an aspect of the industry that is all too often overlooked.

Questions need to be asked as to whether national security agencies, corporations and individuals are doing enough to mitigate some of the threats outlined in this article. You never know who is watching.

For more information visit: www.digitalassurance.com

Why are SOCs failing?

The fightback against security risks is very real – but **Luke Jennings**, head of research and development at Countercept by MWR InfoSecurity, still sees flaws

While definitions vary, generally speaking a security operation centre (SOC) is a central point from where all security issues are dealt with on an organisational and technical level. Typically, it will encompass all the enterprise's information systems – from websites, applications, databases, data centres and servers to networks, desktops and other endpoints, that are monitored, assessed and defended. The problem is that all too often SOCs are failing. When you see organisations spending huge amounts of money on security measures that fail to spot 95 per cent of simulated attacks, it's hard to come to any other conclusion. So, what's going wrong?

The classic mistakes

One of the first mistakes often made is people jumping to a perceived solution without thinking about the problem first. There is often a perception that log aggregation, collected from as many devices as possible and all fed into a commercial SIEM that generates as many different alerts as possible, is a measure of success. Though it is true that centralised log collection can be a beneficial component of an effective attack detection system, it needs to be done right, and even then it is still only one component.

The situation SOCs end up in with this approach is that they have a mountain of data that is very difficult to process, and a huge number of daily alerts, the overwhelming majority of them being false positives. Even when a legitimate attack or compromise is discovered, it can be very difficult to investigate or respond to the problem without additional capabilities. This is also often a very threat intelligence/signature-focused approach (which ultimately is one and the same) and so at best it ends up being a system that can only detect compromises that have been seen before – it won't pick up any advanced, targeted attacks.

The approach outlined above ends up being the virtual equivalent of a security guard with his feet up reading the paper, who occasionally glances up at the CCTV screens he is supposed to be watching.

The data and capabilities required

Instead of jumping to a solution that doesn't work, focus should instead be on what matters and what the requirements are. What specific types of attacks need to be detected? Which parts of the cyber kill chain should be focused on? What type of threat actors need to be deflected?

This should all be done with reference to real attack techniques and so requires good offensive knowledge. Worrying over how many IP addresses port scan a well-secured public facing website every day is pointless when the way many organisations are being compromised is through spear-phishing emails. Remember also that some threats suit detection and others much less so. For example, detecting ransomware is of limited value because the damage is done immediately. Trying to detect ransomware and then to find and power-off the affected system before it encrypts other data is fighting a losing battle. On the other hand, a targeted attack that seeks to gain a foothold on a network, gradually extend access and then maintain that access to information for months or years to come is much more suited to detection. Finding that on the first day or even in the first week is a huge success, compared to it going undetected.

The next question is what key components are needed to support these activities. Log collection was mentioned earlier, but that is just one facet of one major component. Collecting the right logs to support objectives plays a part, but also to discard anything that is of no security value – after all, less is more in this sense. There are two additional major components – endpoint analysis and passive network monitoring. These three major components all address different problems and only when combined create a truly effective attack detection system.

Once these systems are in place, an effective workflow is needed, that is followed every day, and is designed to detect the attack scenarios identified. Alerts on certain types of data from the different data sources collected are one aspect of this but require careful thought and tuning to ensure that the alerts are suitable, manageable and provide enough context to investigate the issue properly. The last thing anyone wants is a mountain of events that can't be actioned.

However, real-time alerts are not the only way to work. Though they have their place, they are arguably much less effective than active data visualisation and review supplemented by anomaly analysis. The idea here is to have set ways of visualising the data, each with a specific intended purpose. Aggregated data pre-

Active data visualisation can help security operation centres work more effectively

sented in the right way and enriched with supporting information is a very effective means of detecting a wide variety of attacks, particularly targeted attacks that have not been seen before.

As a very simple example, being able to visualise every persistent binary across a network in one view, with each unique entry shown only once and counted by the number of hosts, is a very effective technique for quickly discovering that one user laptop seems to have an executable that runs on start-up that no other system on the network has. Is that laptop unique? Or is that just the one system that has a full remote-access trojan installed and set to run on start-up?

The people problem

This one is critical. No matter how good an organisation's technical systems and capabilities, it's all for nothing if the right people to support it are missing. To solve this problem, the job needs to be intellectually stimulating and rewarding and needs to develop experience over time in such a way that it is attractive to capable employees, so that they improve over time and so that they want to remain working there.

As a rule of thumb, smart and capable employees do not like staring at screens of thousands of alerts 24 hours a day and seven days a week that are almost entirely false positives and performing the same monotonous tasks over and over again.

> People are key – the right people, the right experience, the right roles

To make the job interesting, the SOC should take out the grunt work, continually improve and generally not overwhelm analysts with huge amounts of data. This ensures that the job itself can remain interesting and allow focus on the important parts that deliver results and develop experience.

Top tips for success

Having already covered several critical issues for success above, the following gives a summary of a few top tips for success:

- Make sure endpoint analysis, network analysis and log collection are in place – endpoint analysis is particularly important for detecting more advanced targeted attacks.
- Don't be completely reliant on threat intelligence feeds to stay ahead of the curve.
- People are key – the right people, the right experience and the right job roles.
- Real-time alerts can be useful but active data review with anomaly analysis is arguably the more important component.
- Test your SOC. Test that it can detect the attack techniques it claims in practice and, if not, then improve it until it can.
- Less is more – constantly review data sources, workflows and alert cases to eliminate what isn't valuable and further improve what is.

How do you know whether your SOC is delivering good results?

Unless you test and measure the SOC's effectiveness, there is no reason to believe it is of any value at all. To see results, thinking needs to change. Not every compromise can be prevented, but identifying it quickly and acting on that intelligence is the endgame.

SHUTTERSTOCK

NetRisk Ltd

Back to basics

Peter Wenham, director of NetRisk and Trusted Management, looks at some basic tenets of data security

This article is written from the perspective of an independent information security consultant who has been round the block quite a few times – not just InfoSec and IT auditing, but also building private wide area networks (WANs), networking applications and interconnecting private networks to public networks (my first experience of "penetration testing" was in 1989). In that time, I have seen many a bold claim for various "box" solutions but none that delivered a complete solution but generally cost serious money.

What have I learned over the years? First, that any job is not complete until the paperwork is completed (read: comprehensive documentation required).

Second, that any documentation must be maintained and, more importantly, made easily available to staff (read: documentation must not become "shelf" ware) and used (read: operating procedures and practices).

Third, like documentation, software and any firmware *must* be maintained. Security patches are issued for a reason.

Risk-assess any security patches and instal the critical ones soonest, serious ones within a few days of issue and any remaining patches during scheduled system maintenance time but don't leave things too long (three months at most). It should go without saying that there should be a formalised mechanism for monitoring patch notifications, and that mechanism should cover all software, not just operating systems and office applications (word processors, spreadsheets, etc).

Fourth, ensure that any commercially supplied software is maintained at the manufacturer's current support level and for business-critical software ensure that you have an escrow agreement in place covering, at a minimum, supply, documentation and maintenance; and please note that escrow is just as important in cloud environments. My fifth area is change control. It must be a documented and auditable procedure that requires notification (for instance, users, other application owners), back-out and contingency plans and reporting as part of the process.

Moving deeper into InfoSec, my sixth area is data ownership. In many organisations security is thrown over the fence to the IT group without any (useful) business input as to the value or sensitivity of the data/information and who or which groups can create read or modify the data or when data should be archived and for how long. Such input is crucial to the IT group being able to devise and implement a pragmatic set of technical controls.

Also crucial is a clear statement from the business of the organisation's risk appetite, as that will have a bearing on the cost of controls implementation and maintenance. I say technical controls because that is all the IT group can devise and implement; the other key set of controls, that of controlling what the humans in the system do, is outside their remit. And that takes me to my seventh area.

The board, senior managers and all staff need to be aware of their responsibilities to secure company data and of the potential dangers in emails, internet browsing and social media. Awareness training and regular reminders (say, poster campaigns) are required and the messages must be clear and fully supported from the top of an organisation to its bottom-most level. Who should run or control awareness training? The CIO or data protection officer or security manager, or possibly HR.

All this talk about an organisation's data brings me to remind all readers that the EU General Data Protection Regulation (EU-GDPR) have now been formally adopted into law with a two-year grace period for organisations to implement appropriate controls. An internet search will produce quite a few useful hits, with a number of well-known companies offering white papers.

For further information contact @peterwenham or email: peter@netrisk.co.uk

corix partners

The board strikes back

Responding tactically to cyber threats is not sufficient. Boards now need to step up, argues **JC Gaillard**, managing director of Corix Partners

Recent data breaches have scared board members – in particular, the TalkTalk incident of October 2015, and the aggressive media coverage that surrounded it. Losses can easily run into the tens of millions and – more importantly – brand reputation and customer trust can be left irrecoverably damaged by cyberattacks.

Still, even in response to board-level demands, many large organisations continue to focus on IT point solutions, looking for some imaginary tactical silver bullet that would make the problem disappear. However, many recent breaches seem to relate to the absence of security controls that have been regarded as good practice for years and should have been in place. This is consistent with the low levels of cyber security maturity measured by many recent surveys.

In that sense, it is essential to look at the road to digital resilience from the right historical perspective. In spite of decades of spending in the information security space, many large organisations are still struggling today with problems going back to an era where security measures were seen as a necessary evil imposed by regulations – at odds with functionality and preventing innovation and agility.

Where problems are rooted in decades of neglect, underinvestment and adverse prioritisation, there can be no miracle solution, technical or otherwise. Avoiding cyber security breaches, or dealing with them, will require coherent action over time across the whole organisation.

It is also key to focus on driving tangible action, instead of open-ended risk discussions. On their road to digital resilience, large organisations have to accept first that this is no longer about "risks" – in other words, things that may or may not happen – and that security controls are therefore essential. But getting to that realisation after ten to 15 years of complacency, neglect or short-termist "tick-in-the-box" practices will not be simple. Only by identifying and removing the roadblocks that have prevented progress in the past will they establish a genuine and lasting transformation dynamic.

In our opinion, this is a problem deeply rooted in governance, organisational and cultural matters. It requires a fundamental rethinking and rewiring of information security practices, which can be articulated around three dimensions:

First, change must come from the top and, in that context, board involvement is essential, coupled with a true cross-silo corporate approach – looking beyond mere IT matters. The board must be prepared to look at the problem over the long term and be capable of sticking to a long-term plan. In such a sensitive area, changing approach every time a new board member comes in, or every time a serious breach happens elsewhere, is simply a recipe for confusion and failure. The board must also integrate cyber protection into the remuneration packages of key senior executives, alongside other factors such as delivering new products, increasing revenue or cutting costs.

Fundamental to success will be the personal gravitas, political acumen and management skills of the key transformation agent – the CISO in most large organisations. The CISO should not be just a technologist and must have the seniority and experience to make change happen. This means he or she must remain in charge over the necessary period to oversee real change, and they should be encouraged to consider their tenure over a five-to-seven-year horizon in many cases, instead of the more usual two to three years.

Finally, driving real change in that space will require a long-term transformative vision (supported and funded by the board), articulated into a strategic security road map and a sound security governance model – reaching across all corporate silos, major geographies and key partners across the supply chain.

Contact Corix Partners to find out more about developing a strong cyber security practice.

Corix Partners is a boutique management consultancy firm, focused on assisting C-level executives in resolving cyber security strategy, organisation and governance challenges

Where have all the white hat hackers gone?

Can hacking be good for you? Cris Thomas, strategist at Tenable Network Security, thinks it might

Fear of a dark planet: not all hacking serves the dark side

With *The Hateful Eight* and *Forsaken* lighting up the silver screen, the "western" seems to be experiencing a resurgence as a genre. However, this time around, modern westerns have a dirtier, grittier, more realistic feel than the campy and clean movies of the 1930s, such as *Montana Moon*, *Tumbling Tumbleweeds*, *Stagecoach* and *Dodge City*. One theory is that the characters of these earlier films were fairly flat: they were either good or bad, right or wrong, with very little ambiguity. And just in case there was any confusion, the audience was given clues as to the hero and the villain by the colour of their hat. Bad guys wore black hats; good guys wore white hats. Easy.

At some point in the 1980s, the white hat/black hat trope of the American western became associated with the fledgling hacker community. "Good" hackers, who identify a vulnerability and tell the company so they can fix it, became known as "white hats". "Bad" hackers such as the authors of a virus designed to steal banking information became "black hats".

Here's the rub. There is no "good" or "bad" to hacking, there is just hacking. Still, the term "hacker" has been used so often in news media and pop culture as a stand-in for "someone who does bad things with computers" that, to most people, "hacking" is synonymous with breaking the law.

Who wears a hat these days?

People who are technologically adept, those who are skilled at solving complex computer problems, those who understand how computers and the networks

SHUTTERSTOCK

that connect them work – these people collectively are hackers. It's what they do with these skills that determines on which side of the fence they sit.

Lest they be confused with criminals, the "good" hackers wanted to distinguish themselves from their amoral counterparts. This led many to adopt additional monikers such as "ethical" or "white hat" to draw a distinction between them and people who might use similar skills for criminal activities.

The white hat hacker was heralded as a champion for justice, using his or her skills to fight the black hats and save the world from cyber Armageddon. They ride in on their keyboards and network cables to save the "family" server farm from the black-hat-wearing landlord.

However, mud sticks, and as the hacker community transforms into the $170bn global cyber security industry projected for it by 2020, increasing numbers of people are dropping "hacker" from their identity altogether. Those who once might have called themselves white hat hackers now go by corporate-sounding titles such as penetration tester, security researcher, malware reverse engineer, or forensic data analyst.

Incidentally, it's the same thing on the other side of the fence. Despite one of the largest annual security conferences in the world calling itself Black Hat, even black hat hackers are seldom identified that way today. Instead, they are labelled as cyber criminals, malware authors, hacktivists or nation state actors.

It's sad but no one is proud to be called a hacker any longer.

Reward or persecution?

Today, security researchers – who arguably are the most direct heirs to the white hat legacy – often find themselves persecuted by legal threats for trying to do the right thing. The overly broad and vague laws such as the Computer Fraud and Abuse Act in the United States and the Computer Misuse Act in the UK, as well as the intimidation tactics used by some companies, have convinced many to hang up their "hats".

Instead of responding positively to someone who points out a flaw in their product, many companies all too often fall back to a defensive posture and use legal threats and intimidation or simple delay tactics to keep the information about a potential vulnerability from being made public. In fact, so many researchers have found that the risk is just too high that they have stopped doing security research altogether.

A case in point is that of Cisco, which in 2005 took out a court injunction and threatened to sue the security researcher Mike Lynn to prevent him from revealing information about a vulnerability discovered in one of its routers. More recently, in 2015, FireEye obtained a court injunction to stop researchers for the German firm ERNW from disclosing "too much" information about vulnerabilities discovered in one of its security products.

Perhaps this is why some researchers choose to sell their discoveries to the highest bidder, instead of disclosing them to the manufacturer, ignoring the probability that they may be used by nation states as offensive weapons in a potential cyber war.

> White hat hackers now go by corporate-sounding titles

However, there is some light on the horizon. The introduction of "bug bounty" programmes is arguably a positive step forward. These programmes are designed to encourage researchers to spend their time looking for flaws, report them in a responsible manner, and be compensated for their time. The relationship is mutually beneficial, because the vendor ultimately gets a more secure product, at a lower cost of development, without the risk of a public relations nightmare, should a severe vulnerability be discovered and publicised before a patch is available. And everyone benefits from continuously improved, secure programmes.

Unfortunately, the percentage of companies that participate in such schemes is exceedingly low and often there can be ambiguity.

For example, at the start of 2016, General Motors announced its bug bounty programme, which is hosted by Hacker One, but it "forgot" about the bounty element. Instead, it laid out to researchers the provisos that would prevent legal action being taken should a vulnerability be discovered – a novel approach, some might say.

We need hackers, now more than ever.

The challenge we face is that technology isn't standing still. For a start, we're on the cusp of a brave new world with the coming Internet of Things, where everything is connected to the internet.

With the advent of the "connected home", everything now comes with a Bluetooth stack to send data directly to the cloud. From mundane objects, such as televisions, frying pans and speakers, to the less mundane thermostats, smart meters and even rectal thermometers, these devices can be attacked; their data manipulated, or they can be used as launchpads for other attacks. Without being an alarmist, the potential for abuse *is* very scary.

Regrettably, the companies developing these items have demonstrated time and time again that they are not capable of creating devices that cannot be compromised. In some cases, the devices are not even capable of being fixed or updated should they be discovered vulnerable, or should fixes become available. We, as consumers, are left with these insecure ticking time bombs in our homes, further complicated by the fact that in some scenarios, we don't even own the equipment – we only purchased licences to use the items.

We need the hackers, regardless of their hat colour, now more than ever. Whether their hats are white, black or some shade of gray or if they choose not to wear a hat at all, we need them. We need hackers to find the holes and to alert the companies responsible and – when necessary – to alert the public at large. Without the hackers, we, the consumers will be at the mercy of the security afforded by corporations and governments the world over – and all too often that means no security.

Rather than penalise the hackers, let's make sure we recognise the valuable contribution they can make to building a secure world, and that they are motivated to join the forces of good, rather than evil. Otherwise, it really will be cyber Armageddon, with the sheriffs in the saloon, and the rest of us fighting the good fight on our own. ●

Cris Thomas was the editor of the Hacker News Network before joining Tenable Network Security

Bournemouth University

The human landscape to cyber threats

Less than 25 per cent of cyber security applicants are qualified to perform the skills needed for the job, according to the study *State of Cybersecurity: Implications for 2015*. **Dr Christopher Richardson** of Bournemouth University considers the implications

A KPMG survey of UK medium, large and international organisations articulated that most IT and HR executives "face new cyber challenges that required new information security skills, citing data protection and privacy as particular areas where their organisations required more expertise. More than half said they would consider using a hacker to provide inside information to their security teams, or an expert with a criminal record. The primary reason: the skills to combat cyber threats differ from those needed for conventional IT security." Government agencies, law enforcement and small businesses are at risk of losing their cyber security specialists and digital investigators as larger enterprises compete for the best talent.

The demand for cyber security and assurance practitioners is expected "to rise globally to six million by 2019, with a projected shortfall of 1.5 million", stated Michael Brown, Symantec CEO, following from Cisco's 2014 *Annual Security Report*, which had warned that in the worldwide shortage of information security professionals there are over a million current vacancies. This skills gap is seen as a contributory factor to increases in cyberattacks and data breaches each year.

This skill shortage in cyber security and information assurance is distorting the global market, with vacant posts, unqualified practitioners, job churn and mobility, stressed security staff and junior staff filling roles beyond their experience and capability. Even with well-publicised breaches, many organisations still do not recognise this widening capability gap and the threat to their security readiness, or value the need for good practice; many continue to fail to understand that information governance, cyber risk management and compliance starts in the boardroom and across their C-suite.

Conducting business in cyberspace requires a different way to think about safe and secure applications, platforms, networks, the Internet of Things and online digital services. Many security practitioners do not fully understand the business environment they are employed to defend, as technology, advance services and determined threat actors erode their knowledge and experience. For too long, our cyber security posture has been focused on perimeter defence and deploying technology to defending the walls of our corporate castle and yet the inside threat is always present. The human factors that lead to security breaches are equally dangerous to the 10,000's malicious codes generated each day. Persistent advanced threats and advanced adversaries are potentially damaging to us all.

CISOs and their security teams need to analyse the technology data sets against the business processes to manage trust (ultimately corporate reputation) and assure risk. The language of a breach must transform the bits and bytes to exposure of risk and the impact to the business in performance and costs. The Cisco principal Dmitry Kuchynski, of Cisco Security Solutions, encapsulated this, saying: "CISOs must be able to frame the discussion in a strategic way that clearly communicates the potential impact of a data breach on stock price, customer loyalty, customer acquisition, and the brand."

According to a 451 Research study, based on US and EMEA responses from more than 1,000 IT security managers,

there are significant obstacles in implementing desired security projects due to lack of staff expertise (34.5 per cent) and inadequate staffing (26.4 per cent). In the time it takes to train and educate our new security practitioners, the criminal and state-sponsored attackers have transformed the cyber threat landscape, making cyber defence a catch-up race with competition given a headstart by several laps!

Recently, Eddie Schwartz, the international vice-president of the Information Systems Audit and Control Association (Isaca), stated that "in the last five to seven years there's been a dramatic surge in advanced threats and malware; much of it is more sophisticated than reasonable security practices and procedures driven by compliance regimes". This alone should compel us all to review our training, recruitment and retention strategies.

Market reaction to the skills shortage is beginning to incur further costs to security budgets and price practitioners away from SMEs to larger corporations. The need for more cyber security professionals explains why Infosec (cyber and information security) is now considered one of the best career choices for the next seven years. US News & World Report ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015. Furthermore, it also stated the profession will be growing at a rate of 36.5 per cent through 2022.

We need to bring in fresh talent, both from the existing workforce of experienced business executives and service managers and a new crop of able apprentices and graduates. Here at Bournemouth University we frequently see our BSc digital forensic and security students headhunted before graduation.

Our new 2015-16 BSc cyber security management degree at Bournemouth has attracted a 300 per cent increase in Ucas applications for 2016-17, and we are now working on a suite of new BSc programmes for the degree apprenticeships encompassing cyber analytics with digital investigations, disaster management, financial security, secure programming and digital health care.

An important aspect of marketing cyber degrees and improving both the gender and skills gap for cyber security is to induce more female applications, to increase the number of women in security. We are aware that early awareness of career options generates interest and influences syllabus choices and BUCSU promotes wider participation of cyber to a variety of school-year-group classrooms and in particular to business, psychology and English classes, to demonstrate that the wide variety of skills needed within the security industry is to be found not just within computer sciences.

The UK has a pool of talented individuals, unaware of the opportunities within cyber security and information assurance. Exploiting this capacity with new skills from research-led education will provide this country with an improved capability to defend its information assets and valued export income from knowledge transfer to a world demanding skilled cyber security practitioners.

For more information on this topic or to speak to a business consultant, contact the Bournemouth University Cyber Security Unit on 01202 962 557 or email us at: bucsu@bournemouth.ac.uk

Reality check for new EU security laws

The laws around security change constantly but need scrutiny, says **Dr Adrian Davis**, CISSP, managing director for Europe, Middle East and Africa at (ISC)²®

This year opened with the declaration of an agreement on Europe's long-debated General Data Protection Regulation (GDPR), quickly followed by a new Network Information Security Directive (NIS). Few truly understand the cost and level of change needed to comply with these regulations, but there is little doubt they will have a significant impact on how business can be conducted in the European Union.

Whether we agree with them or not, new rules, rights and responsibilities have been articulated across the 28 member states that require levels of co-operation and investment in areas that society is recognising should have been considerations in the first place. As an international body of cyber, information, software and infrastructure security professionals, with nearly 20,000 members across the region, (ISC)²®, guided by its regional EMEA Advisory Council, recognises a real need to help everyone understand what compliance with these measures means.

The years of debate that led up to this point highlighted varied concerns that will continue to challenge us. Many requirements will prove difficult to translate into current business and technology operations. The removal of data from servers to ensure our new "right to erasure", for example, is not an easy task for companies forging ahead with cloud and mobile technologies which are built to enable the free movement of data internationally. We must be prepared to recognise that supplier contracts may not be viable. Whole industries or business lines could be at risk.

This comes at a time when consumers are waking up to new risks, and innovators are being called upon to think more thoroughly as they march forward with initiatives such as the Internet of Things (IoT) and Industry 4.0. As members of society continue to download applications without hesitation and rely on them for everyday tasks, consumers are beginning to understand how much they are owned by the online ecosystems they choose. The legislation offers consumers leverage, with the "right to data portability" outlined in the GDPR, for example, which requires rival companies to co-operate and invest in mechanisms to achieve it. Hefty penalties for non-compliance – 4 per cent of international (not just EU) revenue within GDPR – should mean companies take note.

Looking at the NIS, all public administrations, critical infrastructure operators (including health-care providers and energy firms) and "information society enablers" – from social media platforms to search engines – must now "ensure a secure and trustworthy digital environment throughout the EU". Critics worry that a lot has been left open to interpretation, with many now debating which companies fall into the net. All are heavily dependent on each other for their networks and security, so there will be an imperative for greater collaboration among companies than is currently the case.

The fact that these issues have been debated and that these debates are shaping our laws is good, whatever the opinion of the outcome. Our digital age is delivering an impact akin to that of the Industrial Age, and the regulatory framework in which we do business must reflect this.

Until now, companies and organisations have developed in a regulatory vacuum, creating their own advantage in a new frontier. The forces of the free market have not been adequate. It is time to establish an understanding of rules and conventions around how we should behave. The ultimate aim for the EU is to remove barriers and create opportunity by making it easier and more secure to do business in the region. As a professional, I embrace this aim. As a professional community, (ISC)²® understands that we must do the same so that we can provide the reality check around how this legislative landscape is working, and inform how it will need to develop as the digital era continues to shape our future.

For more information visit: www.isc2.org

Who can you trust?

Ian Glover, president of CREST, explains why penetration testing is a vital weapon in the battle against cyber crime and why you wouldn't want just anyone trying to break into your company

With more sophisticated cyberattacks expected from hacktivist groups, organised criminal gangs and state-sponsored cyber terrorists, it is more important than ever that companies discover where their security weaknesses are and fix them before someone else finds and exploits them.

The best way to discover where vulnerabilities lie is to simulate a malicious attack, from inside or outside of the organisation, in order to see how easy it is to break into a network or computer system and steal valuable data or deny access to critical assets. This is called penetration testing, and the demand for this skilled, technical and clearly sensitive investigation and analysis has risen rapidly.

While penetration testing has traditionally been associated with government organisations and large financial institutions and corporations, it is now commonplace among medium-sized companies, NGOs and the wider public sector.

But this is sensitive work and companies need to be very clear who they are dealing with and have confidence in professionally qualified and skilled individuals with the appropriate processes and methodologies to protect data and integrity. It is a common misconception that the security industry is simply made up of ex-hackers – who, let's face it, most organisations would be reluctant to trust.

This is where CREST comes in. CREST was established in 2006 by the technical security industry with the support of the UK government and is the not-for-profit accreditation and certification body representing the technical information security industry. It provides internationally recognised accreditation for organisations and certification of individuals providing penetration testing, cyber incident response and threat intelligence services. All CREST member companies undergo stringent assessment every year and sign up to a strict and enforceable code of conduct; and CREST-qualified individuals have to pass the most challenging and rigorous examinations in the industry worldwide, to demonstrate knowledge, skill and competence.

For example, CREST practitioner entry-level examinations are aimed at individuals with typically 2,500 hours of relevant and frequent experience, while candidates for CREST Registered Tester examinations should have at least 6,000 hours – three years or more and, at a certified level, 10,000-plus. All these individuals have to resit the examinations every three years, which reflects the fast-moving nature of the industry.

This means that organisations wishing to buy penetration testing services have the confidence that the work will be carried out by trusted companies with the appropriate policies, processes and procedures for the protection of client information, using qualified individuals with up-to-date experience and understanding of the latest vulnerabilities and techniques used by real attackers.

CREST members work very closely with the UK's critical national infrastructure providers where cyberattacks could do the most damage – from energy and utilities companies to major financial institutions. Working with the Bank of England, government and industry, CREST developed a new framework to deliver controlled, bespoke, intelligence-led cyber security tests for the UK's most important financial institutions. The CBEST scheme is the first initiative of its type in the world to be led by a central bank.

However, recent reports show that companies of all sizes are under threat from cyberattacks, so CREST also helped to develop the technical assessment and certification framework for the UK government's cyber security standards, Cyber Essentials and Cyber Essentials Plus. These set down baseline requirements for cyber hygiene and are now mandated for some government contracts dealing with sensitive data.

The penetration testing activities are also supported by similar accreditations and certifications for cyber security incident response. This helps organisations assess how prepared they are to manage a cyberattack and CREST is working with the law-enforcement agencies to provide a register, where companies can look for help in recovery following a successful attack.

As we have seen, the results of a successful cyberattack can be devastating for businesses and individuals, so UK companies and the government need a professional cyber security industry they can trust and rely on. ●

For more information, visit: www.crest-approved.org

Stuart J. Green
digital engineering

Return of the bulldog spirit

It's not that long since our last cyber security supplement, but a lot has changed since then, writes **Stuart J Green**

So, here we are, writing for another supplement on cyber security and, in such a short space of time since the last one, so much has changed.

TalkTalk is now declaring that its "incident" (maybe that should be in the plural) last year cost the company £80m and approximately 100,000 customers, Safe Harbor has been declared useless, and there's a new scheme rising out of those particular ashes which appears to be on shaky ground (depending on whose opinion you want to take). And to top it all off, EU data protection legislation is about to come into force which will mean vast changes for many organisations throughout the UK.

All things "cyber", that long-standing realm of the geek, are now hitting the mainstream media with startling regularity, with increasing severity and with greater aplomb.

Yet, for some, it is business as usual.

Take the business that had £40,000 taken from its bank account because its telephone system was compromised.

In this case, the "clever" criminal managed to get into the telephone system, create a divert to their mobile phone and take calls as though they were the owner of that business.

A few conversations with their friendly bank manager, and £40,000 was there, in the branch, ready for collection, in person, by the criminal themselves.

Or there's the consultant that dealt with a number of businesses that did not realise one of its laptops was compromised; that their email was being deleted and diverted through rules added to their own email program.

As a result, some of the consultant's clients paid over £30,000 each to a bogus company through invoices that looked like the real thing.

Bearing in mind the financial impact that both of these examples have suffered, what do you suppose has been done? A full review of their internal security? Extensive remediation? Overhaul of policy and procedure?

Well, I'll tell you. Nothing. Not a jot. Zip. Diddly squat. Nada. That's what has happened post-incident in these cases.

In both cases, the role of "victim" has been adopted and worn proudly as a badge of honour.

Whatever happened to that Bulldog Spirit? That plucky Britishness that we call on when the chips are down and we have to stand up and be counted?

We are at war with an unseen enemy and it is waging a war of attrition against our businesses, against our communities and against our people. And we are letting them win.

In this technologically advanced society in which we work and play, we have the equipment and systems to prevent these types of attack. We can prevent spam email. We can stop Drive-By Downloads. We can wipe out Ransomware. We can even protect against DDoS.

As a nation, we don't have to suffer this seemingly unstoppable onslaught of cyberattacks that grab the headlines.

If objects kept getting thrown through our windows, we would take action to stop those, wouldn't we? It's difficult to purchase a new car or a new house without an alarm or locks, isn't it? Why can't we apply this thinking to our workplace?

Yes, we might have to spend a bit of cash, we might have to invest in (shiny) new things and we might have to work a little bit differently sometimes, but we've done this before in tackling physical crime so we can do it again to tackle virtual crime.

Business leaders: *stand up and be counted*. Fly a new flag. Fly the flag of resilience. "Deal With Us Because You're Safe With Us" needs to be the new mantra that wins business. As consumers and businesses, we want to be safe.

It's time for the Return of the British Bulldog Spirit.

It's time to fight back.

For more information visit: www.sjgdigital.com

irm
information risk management

What's your data worth to a hacker?

Building a case for cyber security is difficult if you can't put a price on your data. **Charles White** of IRM reveals what personal and corporate information can fetch on the dark web

For the past ten years or so, companies have been embracing a whole new world. The internet has brought massive change – with new and lucrative markets opening up, and costs falling while improving the customer's experience.

Trading hours are a thing of the past. As consumers, we expect to serve ourselves 24 hours a day, seven days a week: no more waiting for airline tickets in the post, or choosing from a limited TV schedule – we print at home, and watch our favourite programmes on demand.

All of this is made possible by connecting companies to the internet, and it's great. But hidden among the exciting new world is an inherent threat – one that we often hear about, but too many companies still haven't taken seriously enough. The hacker.

Who wants your data?

Today, data is the lifeblood of most organisations. Marketing mines it for profiles and trends; sales teams use it for targeting; finance processes it; management needs it for reporting. For some companies it's a product, too – to be sold, or shared with commercial partners.

Your data can be manufacturing formulas or customer credit-card details; internal strategy documents or human resources records. In today's world, all business information is stored digitally somewhere – online, in the cloud, hosted or local.

It's valuable stuff, and not only to you. Stealing data has become big business – and serious and organised crime groups are profiting.

Forget the movie stereotype of a hacker: a young loner, tapping away in a messy bedroom while his parents watch *Coronation Street* downstairs.

The reality is professional organisations that are geared up to monetise your data, whether by selling it or through extortion and blackmail.

Black-market value

To find out what your data is worth to a criminal, we took to the dark web. Here, anything from passports to credit-card data, bank account details to personal identities and passwords, can be bought and sold, anonymously.

Currently, one customer's personal details are worth £33. If you also hold card and bank account information, that rises to £81 per record. And where companies keep employees' passport details – say, as evidence of their right to work in the UK – those are worth £2,000 each.

It can be hard to build a business case for cyber security; but multiply those figures by your customers and staff, and you quickly arrive at the black-market value of the asset you need to protect.

Unfortunately, company executive boards often don't know just what a lucrative target their data is.

Multiple risks

The monetary value of your data is not the only risk. Yes, a consumer can challenge a suspicious purchase made on their credit card, but their broken confidence is much harder to repair.

In a competitive market, where customers can choose easily, a major data breach can cause a company pain in many areas at once:

- Direct remediation costs
- Falling customer retention and confidence
- Dip in share price
- Loss of market share

Risk and opportunity

No executive board is going to welcome limitations to opportunity and growth. Understandably, they'll want to make the most of all the rich data and technology available – and to enable that, you first need to make it safe.

To build a proportional cyber security response, corporate leaders need to understand data's value, both to them and to the black market. The more it's worth, the more there is to protect.

For more information visit: www.irmsecurity.com

Take back control

Fight cyber security on a battleground where you can win

Innovative, inspiring companies don't leave cyber security to chance. They face it head on...

The government recommends a layered approach to cyber security which goes beyond perimeter defences. The key is deciding which layers your business needs.

To find out, we ask questions such as:

- What is your most important data? Where is it held? What extra layers do you have in place to make sure it's protected if someone gets through your perimeter defences like anti-virus?
- How do you make sure your most valuable, sensitive or potentially embarrassing information is protected inside - and outside - your organisation? How can you pull the plug remotely if something goes wrong?
- How do you deal with a problem like email? How can you strip away all the potentially risky bits and leave only the parts you KNOW are safe?
- Are you SURE that you've never been breached and nothing is already sitting on your systems? If a threat has already bypassed perimeter defences, on average it's not found for over 200 days. And the longer it remains, the more damage it can do.
- How are you protecting yourself from your friends, as well as your enemies? How are you compensating for human frailties and insider threats where data gets maliciously or mistakenly shared?
- How do you stop getting bombarded with false positives and only deal with real threats?

If you're an innovative and inspiring company, and you'd like help answering these questions, please get in touch on **01296 621121** email **cybersecurity@avatu.co.uk**

New Statesman reader offer

Is somebody already inside your network?

Ignorance is not bliss for cyber security.

Find out if anyone has already breached your defences with a special 30-day systems review.

Contact our cybersecurity advisors
on 01296 621121
email: cybersecurity@avatu.co.uk

Avatu - information security advisors for inspiring companies

avatu

www.avatu.co.uk