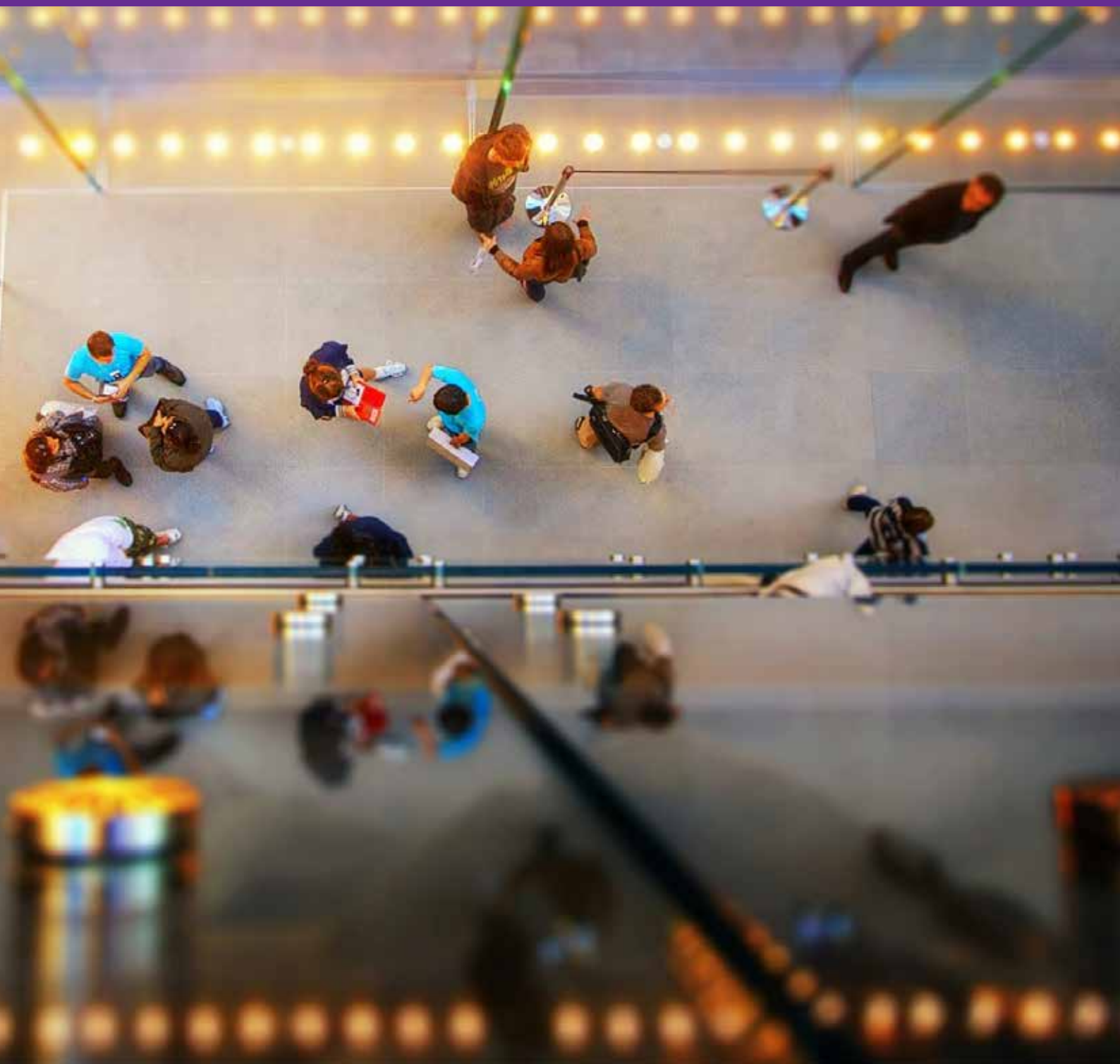
Securing the digital enterprise

The cyber security journey – from denial to opportunity



Foreword

Businesses have every reason to be concerned about the rising threat level facing organisations today; rarely a week goes by without security hitting the headlines around the world.

Most recently WannaCry and Petya renewed our focus on cyber security. Threats do not necessarily require technologically advanced tools, but may be very damaging by simply exploiting known weaknesses.

Organisations who will be able to defend themselves more successfully during a significant attack will be those that treat cyber security as a journey and not a destination – it cannot be 'fixed'. By focusing on innovation, they can maintain a sustainable risk position against the evolving threat landscape.

With cyber security being the cornerstone for most businesses' digital innovation, the role of the Chief Information Security Officer (CISO) is central to all this. But their role is changing from being technology-led to business-led.

Which begs the question: can the CISO lead the way in terms of changing an organisation's culture to embed security? Is their role to enable a digital business?

Together, BT and KPMG have developed this paper based on their experience with organisations they work with. It will hopefully provide a practical guide to those organisations that are on their journey to use security as a business enabler as well as a useful checklist for those who are already on their journey.

Brian T Geffert, Global Chief Information Security Officer, KPMG and Mark Hughes, President, BT Security

Executive summary

Cyber crime is big business, and it's becoming more of a threat every day, as more and more people and devices connect to the internet. The chances of a business or an individual becoming a victim have never been greater. Cyber security dominates the media. State-sponsored attacks. Multi-billion dollar organised crime. And the occasional over-enthusiastic teenager.

In our first whitepaper last year[1], BT and KPMG focused on how cyber crime is changing, who these ruthless criminal gangs and individuals are, and how to fight back.

This year, we're taking a different approach. We look at the practical steps businesses go through on their journey towards managing the risks.

This is a real risk

In July 2016, the UK's National Crime Unit found cyber crime had overtaken 'traditional' crime for the first time, with over two million incidents of computer misuse that year.

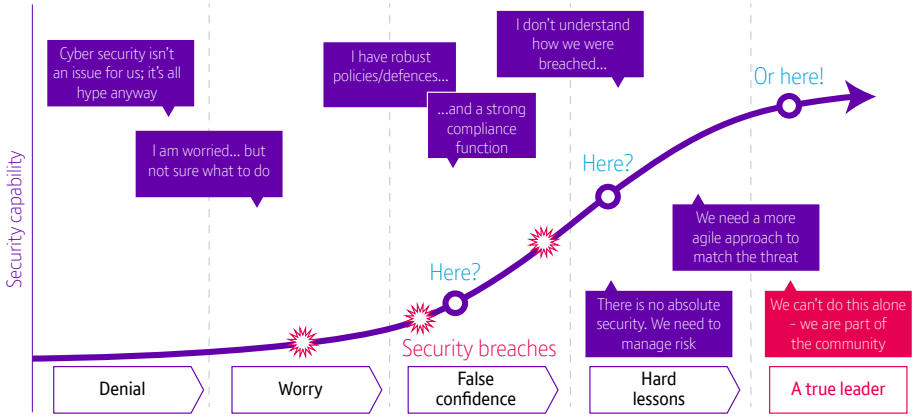
There are those who criticise cyber security companies for scaremongering and exaggerating the threat to drum up business. But boards struggle to set the issue in a business context, and demystify a world of complexity.

So, it's time to look differently at cyber security. Move beyond the jargon and understand the real risks of the digital world.

Make sure you know where you are on your journey

Trying to run before you can walk wastes energy and resources, and it makes you a target not just for cyber criminals but for over-zealous cyber security salespeople. There are five stages to the maturity journey: denial, worry, false confidence, hard lessons, and true leadership.

At each stage, you'll wrestle with different problems.



Denial – 'It won't happen to me'

Cyber crime is only hype, right? It only affects large companies – banks, the defence industry, major retailers, perhaps oil and gas. But not us. Even if it is real, if large firms can't get it right, what chance do I have?

The hard reality is that all firms face cyber attacks. Any business is a potential target.

But the basics help. Teaching your staff, and being aware of how criminals work, is just as important as the technology you use.

The National Cyber Security Centre (NCSC) believes that getting the essentials right will block a significant number of attacks, and help make criminals look elsewhere for their quick profit. Things like keeping software up to date, using decent passwords, and having simple backups.

Worry – 'Get as much security as possible'

You know there's a risk, but now you're a target for the salespeople of security firms. You buy new software, and invest in a vast array of malware detection and containment systems. But while some see technology as the cure-all, others see the answer as policies, governance and standards.

Either way, during this phase firms begin to gain confidence in their defences. They've got the basics in place, and their systems are secure. They'll be fine. After all, they've put in place people, processes and technology. The job is done, right?

> "Many people look at the technical issues but not the business holistically."
>
> Paul Wood, Chief Risk & Compliance Officer, Bloomberg

Security 101

Have a contingency plan	Keep security software updated	Make sure passwords are strong
Have up-to-date security policies in place	Educate staff and refresh training regularly	Make sure data is regularly backed up

False confidence – 'We're ready'

But more sophisticated attacks do happen. Criminals stop hitting companies indiscriminately, and begin to target individuals. Insiders steal data and defraud employers. You'll be shocked by what can happen, and the damage to your reputation it can cause.

So, you relook at your policies, question your assumptions and investments, and start to translate the jargon to actually understand the risks and issues your company faces.

Hard lessons – 'There's no absolute security'

It's not until you've been attacked that you realise: it's part of business in a digital world. No system is perfect. And so, that's when firms think more about cyber insurance – as they try and soften the blow from a more extreme attack. Talk turns to cyber scenarios. Cyber exercises. Planning for major incidents. Senior management begins to understand just what it could feel like.

From this point, cyber defences become more responsive. They're less about process and compliance, and more about responding to an ever-changing and adaptive threat.

True leadership – 'We must work together'

True leaders think differently about security. They see cyber security as an opportunity – a business unit, not a cost centre. They assess the risk and understand how to apply scarce resources to what matters most, realising they cannot secure everything. They are involved in building new services, and tracking and monitoring their security, to continuously adapt their defences to deal with the changing threat.

But most importantly, they realise that people are at the heart of security. It's not just about teaching them, but about understanding people and their behaviour, so that you can spot the unusual and the different.

Leaders realise they're part of a community. The whole community faces cyber risks. Criminals, state attackers and casual hackers don't respect our boundaries, our stovepipes or our professional groupings, so true leaders build communities of defenders, consider the mindset of the attackers, and see value in making their lives more difficult And, ultimately, to choosing the right path.

> "Security is not a project, it is a journey."
>
> Christine Maxwell, Governance, Risk & Compliance Director, BP

Chapter 1 – Denial

Despite the hype and media coverage of large scale attacks, the reality is that all firms face low-level cyber attacks every day. The majority of these are unsophisticated, but depressingly effective nevertheless.

Ransomware has become endemic – just look at WannaCry, which hit over 200,000 systems across organisations in 150 countries. Attacks like these encrypt your data and the criminals demand a ransom of a few bitcoins to free it.

But WannaCry was avoidable. Had companies updated their computers, they would have been fine. But, because they didn't, it became a real crisis for those with outdated, unsupported operating systems. Or for those who hadn't set up their firewalls as tightly as they should have.

Businesses also see confidence tricks. Criminals will try and persuade gullible employees to make fraudulent transfers. The latest FBI statistics included over $5.3 billion[2] of reported CEO frauds and business email compromises.

It's easy for firms to abandon their cyber security journey, in the belief that if large firms can't get it right, what chance do they have?

'This is all media hype anyway…'

As more and more people and devices connect to the internet, the opportunities for criminals just get greater. In the UK, for example, the Office for National Statistics reported in July 2016 that cyber crime and fraud had overtaken 'traditional' crime[3]. And in its yearly crime survey, it recorded two million computer misuse offences to the year ending September 2016.

Sophisticated, highly organised cyber crime gangs are running global networks. They cost the global economy hundreds of billions of dollars. Some of the world's top banks, retailers, airlines and government sites find that 90 per cent of their traffic are from 'botnets'[4].

So why do some firms not think cyber crime is a threat, when all the statistics show that it's increasing?

'Nobody's interested in hacking my firm…'

A lot of firms succumb to 'it will never happen to us' syndrome – that somehow their company is different and that cyber crime happens to other people, not them.

Many companies, especially small and medium enterprises (SMEs), believe they're immune. Yet half of SMEs suffered at least one cyber attack in the last year[5]. William Dixon, Director of Intelligence at Barclays, sees the criminals looking at softer targets: "We're seeing criminals increasingly targeting SMEs and high value account holders."

While not always the prime target, hackers can also use SMEs as a backdoor to another firm's system – one further along the supply chain. Take the US discount retailer, Target. One weak link in their supply chain cost them an estimated $260 million to their bottom line.

There are several reasons for this denial. But for many, it's just that cyber crime is abstract. It's not always obvious, or visible, so we don't pay attention to it.

Cyber crime can also be disconcerting and uncomfortable, especially when people don't understand the technology behind it. Even the term 'cyber' carries a mystique and can obscure rather than clarify the nature of the threat.

Attitude plays a role. Millennials, for example, are far more adept at using technology than their parents – bravely running into new trends. Yet this fearlessness means they can also be foolhardy. Many young people are simply unaware of the seriousness of online crime and its implications[6], preferring to just click and get what they want. We also increasingly see this behaviour in business.

Cyber crime has no boundaries. There's no absolute immunity. No region, industry or organisation is bulletproof.

Recommendation one: get the basics right

Start with good housekeeping, it will address the majority of issues. Get the basics right – firewalls, anti-virus, patching, password security and backups.

Make sure everyone has a responsibility for cyber security, not just the IT people. Basic common sense for all employees (especially the leadership) is essential.

Inventory your assets and focus on investing in protecting your most sensitive information.

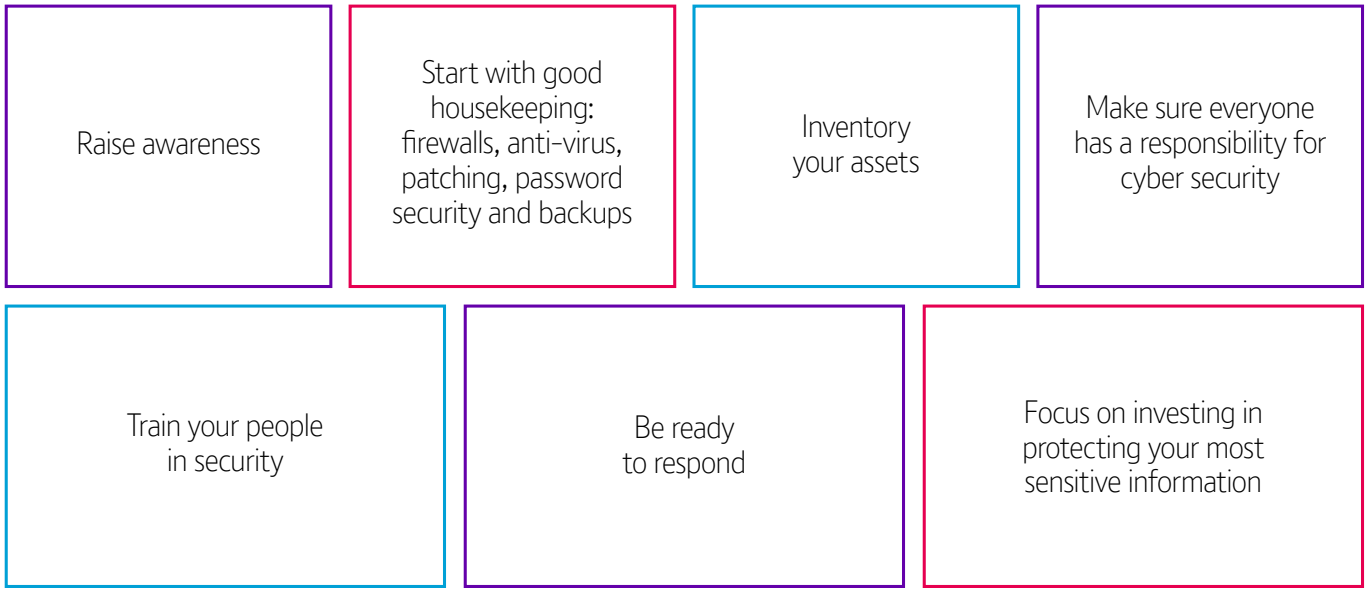
Be ready to respond if you do have a security breach. Cyber insurance can offer real benefits by giving you specialist support if the worst happens.

Changing how people behave can be a difficult task. The most common password is still password123. Train your people in security. Raise awareness. Run campaigns to get key messages across. You should make the training mandatory for all new joiners, and run regular refresher courses.

But also think about more tailored training and regular updates to keep it fresh.

Getting the essentials right will help to deter criminals and make them look elsewhere.

Cyber security:
get the basics right



What questions should you be asking yourselves to get to the next stage?

- How do our existing security controls stack up against government cyber guidance, for example the UK Government's 'cyber essentials' guidance?
- What steps have we taken to educate and inform our employees?

And then ask yourself whether you, as a leader, are doing your part.

Chapter 2 – Worry

Once the significance of good cyber security has finally sunk in and you fully appreciate the potential damage of an attack, the next step in your journey begins: worry.

Boards start to fret about how best to protect themselves. How much should they spend? And on what? Some see technology as a cure-all, while others see the answer in policies, governance and standards.

Either way, suddenly you're a target for the salespeople in security firms. Companies buy new software, flashy hardware arrives in the data centre, and a growing array of malware detection and containment systems appear.

When you're not a specialist in the industry, how do you filter the good information from the bad? How can you choose what to buy? Who do you trust in the face of media hype?

So, you hire new people to join the team. A Chief Information Security Officer (CISO): the 'IT security nerd'. But in the worst case, they just become a scapegoat when there's an attack.

> "The organisation was growing in terms of the problems we were dealing with rather than the direction we needed to travel in."
>
> Colleen McMahon,
> Deputy CISO, GSK

'I can buy my way out of the problem'

The first thought is often to invest - heavily. Firewalls, anti-virus, malware detection, DDoS protection, and every other kind of technology to prevent a potential breach. In fact, 60 per cent of IT decision-makers say they intend to spend more on security[7]. IDC predicts that by 2020 organisations will spend $101 billion on cyber security software, services and hardware[8].

Investing in IT security is important. But how do you decide what to budget for?

Perhaps there's more to consider here. Have we really got the balance right? Should we not just be funding technology, but investing in people? In training them? Educating them? Raising awareness? And creating processes, which change how people behave?

But it's just as dangerous to depend on process as it is to depend on technology. You can create an environment where policy and compliance becomes king. And security becomes just a tick-box exercise.

> "Compliance is not a signal to sit back and say we've cracked it."
>
> Craig Rice, Director of Security, Payments UK

'Security is not my problem – the IT department sorts it out'

People can be the weakest link in the security chain. But with a little work they can be your greatest asset. Indeed, our recent CEO research found the top three most important factors in cutting your security risks. These are: security governance processes, security technology, and sharing tools and knowledge with peers and partners.

Take phishing, for example. This attack method has been growing in sophistication over the last few years. In the past, it's had a very low success rate because the lack of personalisation, and poor spelling or grammar became well-known red flags.

Criminals are now targeting more specifically to improve the success rate.

> "How rigorously do you deal with employees who don't take security seriously? There must be real consequences."
>
> Paul Wood, Chief Risk & Compliance Officer, Bloomberg

"Policy should be combined with education and training as an ongoing process, not a one-off."

Paul Wood, Chief Risk & Compliance Officer, Bloomberg

Think of phishing as casting out a rod and hoping something bites. Well, now it's turned into 'spear-phishing'. They see a fish and they target them specifically. The criminal business model has changed. They spend more time researching their target. And then use that information to personalise their approach. Criminals are after information, so they can use it to get to your corporate data, or to help them commit fraud.

'Whaling' or CEO fraud goes a step further. The 'big phish' in an organisation: the CFO or other senior executives, are the target here. If a criminal steals the CEO's email, they can impersonate them, and abuse their authority, like making fraudulent money transfers. Sometimes these phishing emails come from third parties you might trust: legal firms or accountants who have been hacked themselves.

Everyone at every level in an organisation is vulnerable to this type of attack. When a phish gets through your technology, your employees need to be able to recognise the danger. This is where education and awareness come in. You have to put in programmes to change your people's behaviour and culture towards information and business security.

"Education of staff is of significant benefit, we routinely see companies investing in technical solutions while neglecting the human aspects. There is a significant benefit obtainable where investing in staff education is undertaken but explaining it as a benefit to their home life and that of their families and children. People buy into this free personal education much more readily than another compulsory work policy."

Steven Wilson, Head of Business, European Cybercrime Centre, Europol

The top three most important factors in cutting your security risks

Security governance processes

Security technology

Sharing tools and knowledge with peers and partners

‘It’s impossible to stop this anyway, so why bother worrying?’

Automated security defences are getting better. They’ve evolved. And despite high-profile media coverage, modern IT systems are far harder to break into than they were five years ago. The latest operating systems have far more effective countermeasures to attacks.

But, of course, criminals adapt too. Security researchers found five new malware variants every second in 2016[9].

Whatever we create, criminals look to find a way around.

Fingerprint, eye scans and other biometric ID checks have helped. As has looking into how people behave, and the methods and techniques they use. Combining all of these will help us check whether people are who they say they are. Biometrics in particular could finally solve the problem of weak and reused passwords.

But technology alone will only win battles. It won’t win the war. We must combine technology, people and processes to stand a chance.

Recommendation two: don't start with technology

Buying technology shouldn't be your first priority. Assess your current controls against best practices, and take the time to understand how they may protect the assets you have against threats you're actually seeing. Once you understand the gaps, you can refine your controls, and make sure you're getting the full benefit from them.

It's important that you don't just concentrate on one aspect of security – even if you do it really well. You could have the most robust policies and governance, but they'll only work so far.

But also, don't take it all on at once. You'll never succeed with a scatter-gun approach. Prioritise. Decide what matters most. Use your new CISO and business strategy to help guide you and spend the money wisely. Demand that your CISO talks with the broader business, and challenge him or her to come up with usable security solutions rather than just saying no.

Consider that, from a return on investment perspective, you may be better off getting the basics right and then focussing on your highest value assets. As you do that remember to invest in preparing for your response to a cyber incident.

Remember there's no absolute protection against cyber attack. Accept that you won't be able to defend against highly targeted attacks every time. You'll get breaches. What matters is how you respond to common scenarios, when they do occur. Plan and run exercises for these scenarios. Teach your team, and streamline your responses.

1. Prioritise
2. Decide what matters most
3. Use your CISO and business strategy to guide you
4. Demand your CISO talks with the wider business
5. Demand usable security solutions.

What questions should you be asking yourselves to get to the next stage?

- Have you got the balance right between people, process and technology?
- Are you clear what the business really needs to protect, and who has decided that?
- Have you planned, prepared and exercised for potential attacks?

Chapter 3 – False confidence

The next step in the journey is for organisations to move beyond worry to a certain level of confidence in their security defences. After all, they've invested in the software, people and processes. The job's done, right? You've framed your ISO 27001 certificates and you've got compliance functions on track – particularly if you're in a heavily regulated industry.

But more sophisticated attacks do happen. Criminals stop hitting companies indiscriminately, and begin to target specific individuals. Insiders steal data and defraud employers.

'My new CISO will deal with all the problems for me...'

It's easy to overlook the importance of people in these circumstances, especially in teaching your employees about the risks. But if firms are thinking about the people, it's usually the new CISO – and handing the responsibility over to them.

But how qualified are these people? Have you considered whether they even need to have cyber security experience? Are they more guard dog than guide dog? Someone focused on technology is more likely to create an environment of 'no', not 'how?', which could delay your strategy and lose you opportunities.

There are many reports that explain how there's a skill gap in cyber security, from network engineers to the board. Demand for skills is high, while supply is low. But many firms often use the role as a scapegoat when things go wrong – if they suffer a data breach, the CISO is the first to go.

> Many so called 'experts' are a bit too full of actual bluster and bluff about management and risk, they focus on the IT aspect – with an 'I've got a better tool than you' type attitude. We have approached security to enable the business to do good business, focus on delivery which is a mixture of people, processes and tech, rather than an over reliance on a single domain and a focus on the use case rather than the function.

"We are re-writing our security strategy now because we think things have fundamentally changed."

Christine Maxwell, Governance, Risk & Compliance Director, BP

'I've invested in security, so nothing will happen'

Our CEO research found 68 per cent of CEOs are entirely (or mostly) confident about how they can transform their business without compromising on security.

Your cyber dashboard is green, so what can go wrong?

But when did you put in your policy? When did you last refresh it? Who have you shared it with? When did you last test it? Has it really stood the test of time?

A one-page security policy that they wrote several years ago, perhaps to resolve an audit finding isn't going to stand that test. Perhaps it was filed somewhere, but hasn't been shared with the people who need to use it. Or it's very high level, with few or no processes underneath to show how people can use it, and doesn't match the business' strategy anymore.

Policies should let people 'do the right thing' and stay secure and agile when they're working.

"Security is not an afterthought, not a bolt on after the event."

Paul Wood, Chief Risk & Compliance Officer, Bloomberg

When they've figured out the size of the problem, put the right processes, governance and people in place and installed the right software, companies often rest on their laurels. They get lazy.

But cyber security isn't something you do once and then forget about. Criminals are evolving, so you have to, too. Attacks can and do happen. You'll be shocked by what can happen, and the inevitable media coverage which follows.

So, you relook at your policies, question your assumptions and investments, and start to translate the jargon to actually understand the risks and issues your company faces.

There's no absolute security, and you need to make hard judgements.

Case study company Z

An organisation who implicitly trust their 20 administrators don't audit or log anything on those privileged accounts. They never imagined someone else may gain the credentials and do harm.

"The rapidly changing threat landscape calls for new cybersecurity tactics in the enterprise to meet the ever evolving cybersecurity challenges."

Tracey Pretorius, Director Cybersecurity & Cloud Strategy, Issues Management at Microsoft Corporation

> "Drive security down in contracts with your suppliers."
>
> Security advisor at a national Computer Emergency Response Team

workers – to gather information. How many conversations or meetings are in the canteen? How much confidential information thrown away in regular waste, which the cleaners collect? How many ID badges do people (apparently) lose? And, of course, the wide range of outsourced firms who support every aspect of a modern business.

'I've got the right security culture in my organisation'

You can't completely protect against an attack. A determined attacker will find a way.

Criminals now realise that the people, processes and tech inside many of the large corporations have become more difficult to breach (not impossible, just not cost effective).

So where do they turn their attention? To the supply chain.

Those companies with people who have physical access – like cleaners, baristas, canteen staff or agency

> "From individuals to enterprise businesses, vendors must be committed to helping customers get secure – and stay secure – especially in a new world of persistent cyberthreats."
>
> Tracey Pretorius, Director Cybersecurity & Cloud Strategy, Issues Management at Microsoft Corporation

'I'm prepared'

What would you do if you had to pay bitcoins after 2,000 computers were locked?

You might have a process for dealing with a hack, but the first question you need to answer is: 'Do you pay the ransom?' Unfortunately, a typical answer is usually: 'Uh, I don't know, who makes that decision?'

Well, what's the impact on the business? If you pay them are you opening yourself up as a target? What's the public perception? Who makes the decision? How do you handle media? Or if you don't pay, how much time will your business be able to keep running? What's the cost going to be to recover, versus the cost of paying a few hundred pounds?

If you pay them (and we know people do), you need to have or buy bitcoins. Not as easy with anti-money laundering regulations in force.

Or is there a half-way house? Do you negotiate for more time to fix it, or more time to get a better price?

These are just one set of typical discussions around a ransomware scenario. Other scenarios include data breaches, distributed denial of service attacks, sabotage and cyber fraud. Perhaps a combination of these.

> "We are battle-ready, but not battle-tested."
>
> Scott Mcelney, Head of Threat Intelligence & Consultancy, Clydesdale Bank

Recommendation three: check your assumptions

Make sure you've thought of all the likely scenarios, and know what you're going to do. Make sure you have a process that regularly reviews your security strategy and the policy that underpins it. Make sure the board and CEO champion and lead by example. Leaders must walk the talk.

Next, ask yourself the big questions. Is the policy still appropriate for your needs? Have you had any changes that would affect your policies?

You need to give your processes a bit of flex, so they can change quickly when you need them to, for example if you acquire a new company, or a new type of attack appears.

You're only as strong as your weakest link, so make sure all your policies flow to your suppliers too. If you can, think about how their business is changing too. Consider asking them to show you how they follow your policies. Get them to audit themselves, for example with the cyber essentials or ISO 27000, but also be ready to probe and test whether they really 'get cyber security' and just how they would respond to a real cyber attack. Are you confident in their response, and how would it impact you as a consumer of their services?

Think about rolling training out to suppliers and sub-contractors too. You can use it to cover the physical threat, like tailgating and social engineering, as well as cyber risks, like spotting phishing emails.

Make sure your business recovery strategy has cyber scenarios. And that you have the right response tools in place to help you work through major cyber incidents and more rapidly recover from loss or disruption.

Checking your assumptions

Think of likely scenarios and responses	Have a regular security review process	Allow flexibility in case the threat changes
Make sure all suppliers are adequately prepared and follow your policies	Assess policy changes and suitability	Make sure the board and CEO champion and lead by example

What questions should you be asking yourselves to get to the next stage?

- Is the board and executive really taking ownership of the cyber strategy and how it works day-to-day?
- Do our employees really understand their role in protecting the organisation?
- Have we made cyber security part of our incident response and business recovery plans? And tested those plans?
- How are we dealing with our supply chain's cyber security?

Chapter 4 – Hard lessons

> "Unfortunately, your risk appetite the day before the incident is very different to your risk appetite the next morning."
>
> Glen Attridge, Head of Cyber Defence and Security Response, Royal Bank of Scotland

Even the best prepared organisations often learn hard lessons after a major cyber attack. Suddenly, the media spotlight turns on senior executives, and it's tempting to play the blame game, trying to find the guilty party, which can cost jobs.

But these incidents are a time for level-headed responses. And the confidence to look at why it happened, and sensible steps to avoid it happening again.

Cyber attacks drive companies to focus more on the particular risks, which they're forced to live with and can insure against. Talk turns to cyber scenarios, to cyber exercises and to planning for responses to a major attack. From this point, firms get more responsive. It's less about process and compliance, and more about being agile and changing.

So just what are the real lessons from these surprising incidents? And why do firms who have invested millions in cyber security still get caught out?

> "WannaCry was good in helping drive awareness. It gives us an opportunity to drive home the message on good cyber security."
>
> Security Advisor at a national Computer Emergency Response Team

'We bought everything, so how did this happen?'

Few firms really set up their tech well, and many don't have the skills to manage it all. Understanding your security architecture matters: how do all these devices work together? How do they counter common attacks, and where are the overlaps or – worse – gaps?

When your tools are complex, you'll have trouble getting them to work well together, or you'll have tools only one person can use properly – which will take the focus off of hunting.

So, you need to invest in the 'glue' – the small marginal investments in people and integration – which help you to get the most from your technology. The more you can link the controls to an understanding of the threats you face day-to-day, the better.

Another danger lies in the time it takes you to roll out everything you've bought. All too often, we see that the tech is 'old' before it's ready to roll.

Case study company M

"No, we don't do network inventory management – we don't see it as a security control. We have however just bought a great high tech solution because we had some security budget left over. We haven't got it operational yet but that's the plan for next year."

'Should we outsource the problem?'

Faced with such a daunting problem, some companies may feel cyber security is too difficult, and that outsourcing is the answer. Sometimes this can be a great solution – reputable managed security service providers now offer a very high level of security. They're well administered and supported by teams who are used to dealing with cyber attacks and the consequences.

> "If you bring something in you need to implement it, not just leave it on the shelf."
>
> Scott Mcelney, Head of Threat Intelligence & Consultancy, Clydesdale Bank

But you can never really outsource all of your cyber security – only the technology. Ultimately, only you can decide about the risks and how to deal with an attack. Only you carry the ultimate reputational and legal risks of getting it wrong. Two-thirds of IT decision makers say they want their security to become more flexible and customised to fit the specific needs of their organisation[10].

The reality is, it's a partnership. All too often people outsource functions without thinking about how they will stay an intelligent customer, and without helping their provider to be an intelligent supplier.

The challenge is then one of building a genuine partnership with the most important suppliers. Companies and suppliers are co-dependent. If a supplier gets breached, so does the company – and both take the reputational hit. The goal is to move the relationship between a company and its suppliers beyond the usual contractual discussions into a 'cyber ecosystem'. To involve suppliers in planning scenarios and running exercises, and working together to understand how best to manage those cyber risks.

‘How do we insure ourselves against this in the future?’

Everything is becoming cyber – our world is now digital – and so is business. Traditional insurance has started to think about how it would address cyber security. An organisation’s data has become an asset which needs to be protected. Access to that asset needs to be protected from interruption, or it can’t generate revenue - which could be costly in terms of money, customer trust and customer loyalty.

Understanding how your organisation’s digital business generates revenue will be the key to knowing what you need to insure, and how long that data can be inaccessible before you start to lose money.

Cyber insurance provides your organisation with a means to mitigate risk through transferring it, but it needs to be used in conjunction with an active information security program. It will provide you with access to a panel of specialists that can help with communications, brand and reputational risk management, legal advice or forensic capabilities; which you may not keep readily to hand, through an event. Finally, it can provide you with resources to supplement your team in maintaining the potentially upbeat tempo over a long period of time to recover from an event.

Insurers too have started this journey and may not necessarily have all of the actuarial data and experience that they have with other areas they insure. That means it will be important to understand their experience and comfort level with underwriting in the cyber area as you look to make them a part of your security program.

Recommendation four: your business is unique, it'll need a unique approach

"Don't have a one size fits all approach – what may be relevant for one area of your business may not be okay for another. You have to align your approach to your business strategy."

Paul Wood, Chief Risk & Compliance Officer, Bloomberg

Overly complex tech can make security gaps worse. If your team can't understand the technology, they'll be distracted. Only once you're comfortable that your tools and processes are working should you look to close any gaps with technology or new processes.

When picking new technology, think about whether your people know how to use it. It might be better to get a tool that's an 80 per cent fit, but everyone knows how to use it, or it works well with what you have, or it's easy to automate. Better that than the most technically brilliant tool that's harder to drive and doesn't integrate.

Don't be afraid to outsource areas that aren't linked to your core business, or ask others for help. If you do need to fully outsource your security, treat your outsourcer as a partner. Work with them. Make sure you have someone who has overall accountability, and is focused on getting the right service and results.

Over time, your company will change. Make sure you don't set your service level agreements and metrics too high. But make sure providers hit them. Ideally, you need to make the contract flexible enough to cope with the fact that the kinds of attack you face could change.

Make sure you document the scope, the capacity and responsibilities. Review them often to make sure the service always meets your needs; but don't under-estimate how much it costs to fix things after an attack.

If you need to divert your people for a month to deal with the aftermath of an incident, it'll ripple out and delay everything else – which could cost you in various ways. Insurance and having the right relationships in place to get help can soften this blow. And people often overlook this.

What questions should you be asking yourselves to get to the next stage?

- Have we really integrated our security controls correctly, and have we been willing to test and probe those controls?
- Can we be agile enough in updating and refreshing our controls to match a changing cyber threat?
- Do we understand the role of cyber insurance in helping us deal with the more extreme scenarios?
- How long could we maintain a major IT remediation crisis before it impacted daily business and strategic projects, and do we need to stretch that time?
- Do we have the relationships that could support us through an incident if needed – both for fixing the incident and running business as usual?

Chapter 5 – True leadership

Attackers don't play by the same set of rules we do – they don't have to deal with regulators and data protection authorities.

True leaders think differently about security. They see cyber security as an opportunity – a business unit, not a cost centre. They help implement new services, tracking and monitoring their security, continuously adapting their defences to deal with the changing threat. They develop metrics of security which resonate with the business, and give senior leaders appropriate confidence in the organisation's security stance.

Most importantly, they realise that people are at the heart of security. It's not just about teaching them, but about understanding them and their behaviour, so you can spot the unusual and the different.

Leaders realise they are part of a community. The whole community faces cyber risks. Criminals, state attackers and casual hackers are against all of us. True leaders build communities of defenders, consider the mindset of the attackers, and see value in making their lives more difficult. They focus on public-private partnerships for help and data exchange.

Thinking about cyber risk

There are three 'zones' you can end up in here. The zone of routine, the zone of surprises and the zone of catastrophe. To start, it can be hard to get to grips with cyber risk. Most firms get used to the routine cyber attacks after a while – their controls deal with the attacks, their Security Operations Centre manages the incidents, and the executive finds out how often and how drastic the attacks are. Everyone starts to get comfortable – you're in the zone of routine.

"Cyber attacks will continue to evolve, which is why the public and private sectors must continue to work at pace to deliver real-world outcomes and ground-breaking innovation to reduce the threat to critical services and to deter would-be attackers. No single organisation can defend against the threat on its own and it is vital that we work together to understand the challenges we face. We can only properly protect UK cyberspace by working with others, particularly with business and wider society."

Ciaran Martin, CEO,
National Cyber Security Centre

But the most cyber-savvy firms think about the more unusual events – the potential surprises. These are the scenarios that are possible. They've happened to other firms. Maybe not in the same sector, but close enough that you could imagine how criminals could develop a similar attack for your industry. Savvy firms play these scenarios out, sometimes testing the board and executive, other times letting ethical hacking teams loose in their systems.

And so, attacks are less surprising.

Leaders have got the plans to deal with unseen but proximate events, so they can buy cyber insurance that's realistic and linked to what's actually likely. They're dealing with the zone of surprises.

Now comes the real challenge: the zone of catastrophes. This is where you haven't seen these kinds of cyber attacks before, or perhaps the community thinks they're a one-off. They scare people, but people simultaneously think they won't happen.

There isn't an answer to these events, but there is a response. Sometimes it's worth thinking differently. Ask yourself, what would really disrupt your business if it happened? Imagine the worst case, and then ask what can you do? What should you do? The answer might not actually be security. It might be choosing to structure your business differently. Or accepting that, in these worst cases, parts of your business will fail.

These are big business choices, you shouldn't take them lightly. The trigger which causes catastrophe could just as easily be an IT outage or a supplier's business failing, just as it could be a deliberate cyber attack.

"We have really benefited in the area of cyber security because banks have collaborated. We work hard to be part of that community. We can't do it on our own."

Scott Mcelney,
Head of Threat Intelligence & Consultancy, Clydesdale Bank

'We're in this alone'

Security is quite a secretive business. Worse still, when handling a major incident, it's human nature to keep tight-lipped, not sharing anything until you've dealt with the issue.

But most attacks don't target a single organisation. Organised crime groups carry out campaigns of attacks. They target hundreds or thousands of firms. More indiscriminate attacks can hit millions of people. State espionage campaigns aim to collect intelligence on particular topics, but will target any company with that information or which helps the attacker get closer to the source.

In short, if you're being attacked – so is someone else. You're both sitting in your windowless incident room, wrestling with the consequences, blissfully unaware of each other; but you both probably have a vital piece of the jigsaw, and so might the police and government.

You can't build trust between companies half-way through an attack. You have to nurture these relationships beforehand.

Taking the bold step of sharing what's happening also matters. Many advise against it: cautious legal advisers, embarrassed executives, secretive security experts.

Be brave and reach out. You'll be surprised at the results.

"Cybercrime is increasingly a global issue, it needs a global response to tackle it effectively. The sharing of information allows industry to develop a collective exterior shield that slows down or disrupts attacks before they hit corporate defences. The concept of continuing to defend only against attacks is outdated and there needs to be a partnership with law enforcement to disrupt and arrest key actors who to date have acted with impunity, confident that their technical skills could hide them from the authorities."

Steven Wilson,
Head of Business, European Cybercrime Centre, Europol

'Twice a year is fine, or is it?'

How often should the board and executives think about cyber security? It's always a major topic of debate – particularly for regulators. Most boards, executives, risk and audit committees now have a regular slot on their agenda for cyber security; perhaps twice a year.

The problem with these sessions is that they often treat cyber security as a separate and disconnected issue from the broader operational risk, or even business strategy discussions, and they come with scary war stories, attack statistics and a few incidents. They might include a sweep up of what improvements the firm has made, and maybe some research to compare yourself to your peers – just to give you that feeling of being 'in the pack'.

We need to stop this. We need to stop treating cyber security as something special.

Make it a main concern. Make it part of all your other discussions. When you're talking about risk, think about what happens in a cyber attack, rather than having a single 'blob' on the risk map called cyber.

You can only do this if you separate out the impact of very different types of cyber attacks: the major data breach, the ransomware attack, the denial of service attack, the cyber fraud, the confidence tricks (like phishing).

Calling everything cyber doesn't help.

And when you release a new digital service, you need to think about the cyber security. Balance the risk and reward: these are business judgements. How much business could you lose if customers can't use the service because your security was lax?

How much are you exposed to fraud? Would people think you negligent if a hacker got into this service? And where would the liability lie? These are all hard business questions.

"A top management issue continues to be driving business innovation and growth while simultaneously providing the right protection against an ever evolving cybersecurity threat landscape."

Tracey Pretorius,
Director Cybersecurity & Cloud Strategy, Issues Management at Microsoft Corporation

"A clear cyber strategy, that the leadership team has bought into, means that we're all on the same page."

Christine Maxwell, Governance, Risk & Compliance Director, BP

Be ready for some big shifts

According to our research, only 26 per cent of CEOs see security as a differentiator in their digital transformation programmes. Cyber security is in for some big changes. The shift to cloud holds bigger surprises. Companies with no IT have arrived. Businesses who work entirely in the cloud. They don't have the traditional infrastructure we would expect.

And that means the defences we'd see at the perimeter have disappeared.

Meanwhile, employees are bringing their own devices. This can be scary, not just for the business and the CISO, but for regulators. Suddenly they're finding that how people should secure their network doesn't work anymore.

And suddenly the CISO has no IT security role: it's all in the cloud, but they definitely still have to think about how to secure their information, while playing a vital part in linking the business to the technology services.

Cloud providers have started to ask themselves hard questions. How much risk are they prepared to take on? Where might the liability lie for breaches? And, how do they charge for it?

"Security used to be one of the reasons organisations were slightly hesitant to move to the cloud – now security is the very reason why they are wanting to move to the cloud."

Tracey Pretorius,
Director Cybersecurity & Cloud Strategy, Issues Management at Microsoft Corporation

New challenges, new opportunities

Now you can have a much deeper relationship with your customers. Suddenly you can give them custom services.

On the other hand, you're much more likely to get attacked.

So you need to balance giving a good customer experience, and making your service secure. Perhaps there are some win-win scenarios here. When you're more secure, you can be more confident that a customer is who they claim to be – and can do a lot more for them.

Passwords seem old fashioned. We're much more likely to see biometrics, like fingerprints, combined with analysing people's behaviours, to recognise who they are. Firms can then score individual purchases for risk. We can keep monitoring fraud, and tweak the alert levels to keep fraud to acceptable levels. These are business judgements.

Look for opportunities to embed security as your business changes. Value flexibility, embed accountability and build resilience.

The future has great potential. But we need to look at cyber security differently.

We need to change.

Recommendation five: be part of the community, and share your experiences

Build a network of peers and trusted information sources in your sector and further afield. Be prepared to share what your organisation is seeing and seek to get involved with the community through things like the UK NCSC's Cyber Information Sharing Portal, but remember: sharing is a two-way street; you have to give something back to the community.

Think about a blend of building relationships with your peers, formal sharing platforms and maybe even commercial threat feeds.

If you're going to share – make it timely. The quicker you can tell others about an attack, the quicker the community can do something about it: together.

Make cyber security something you always consider. Talk about it like you would any other business concern. If you can think of it as an everyday part of doing business, you can manage the fear and uncertainty much better.

And be open to thinking very differently about cyber security. It's about helping your business succeed. It's not about saying no. Challenge old ways of thinking: they won't help you succeed in a digital world.

What questions should you be asking yourselves to get to the next stage?

- Are we really prepared to play our part in the community as leaders? To share intelligence, good practice and hard-won lessons?
- Have we really considered the full range of cyber scenarios and risks? And what we need to do to improve?
- Do we really see cyber security as a major part of our business strategy? Have we got the balance right between using new digital channels and managing the risks?
- Has cyber security become mainstream in our business, and are we really thinking about how to help the business succeed and take advantage of new opportunities?

Conclusion – Where are you on your journey?

We can all learn lessons from those who are further ahead on their journey to becoming a true security leader.

The hard reality is that all firms face cyber attacks. Any business is a potential target.

As you move from worrying to false confidence, you'll get the people, processes and technology to protect yourself; but it's often not until you're attacked that you truly understand what the risks of working in digital are like, let alone how to start thinking differently about security.

From the board down, we must change how we see cyber security. The mindset and models will just keep us saying the same things. It's not sustainable. These myths will become traps, unless we make security another thing we always think about.

Technology is changing. The threats are changing. We have to cut through the jargon, and think about our roles differently. If we want to understand the risks we need to communicate better. The role of the CISO is shifting: from guard dog to guide dog. They're moving into roles which mean they need to start thinking about how security affects bigger business decisions.

By starting to ask ourselves some hard questions, we can change our approach and help our businesses succeed.

References

1.Taking the offensive – Working together to disrupt digital crime, http://www.globalservices.bt.com/uk/en/point-of-view/disrupting-cyber-crime

2. FBI, Public Service Announcement, I-0540417-PSA, Business Email Compromise https://www.ic3.gov/media/2017/170504.aspx#fn1

3. Office of National Statistics, Crime in England and Wales, year ending September 2016

4. https://www.threatmetrix.com/digital-identity-blog/cyber-security/fcc-hit-botnet-attack/

5. https://securityintelligence.com/20-eye-opening-cyber crime-statistics/ (Accessed 23/03/17)

6. https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Britain-Thinks-Cifas-Young-People-Report-Young-People's-Attitudes-to-Commiting-Fraud.pdf (Accessed 23/03/17)

7. Ovum Security Intelligence Market Research commissioned by BT, April 2017

8. http://fortune.com/2016/10/12/cyber security-global-spending/ (Accessed 06/04/17)

9. http://www.silicon.co.uk/workspace/five-malware-variants-second-201602 (Accessed 31/03/17)

10. Ovum Security Intelligence Market Research commissioned by BT, April 2017

Find out more at: www.bt.com/security