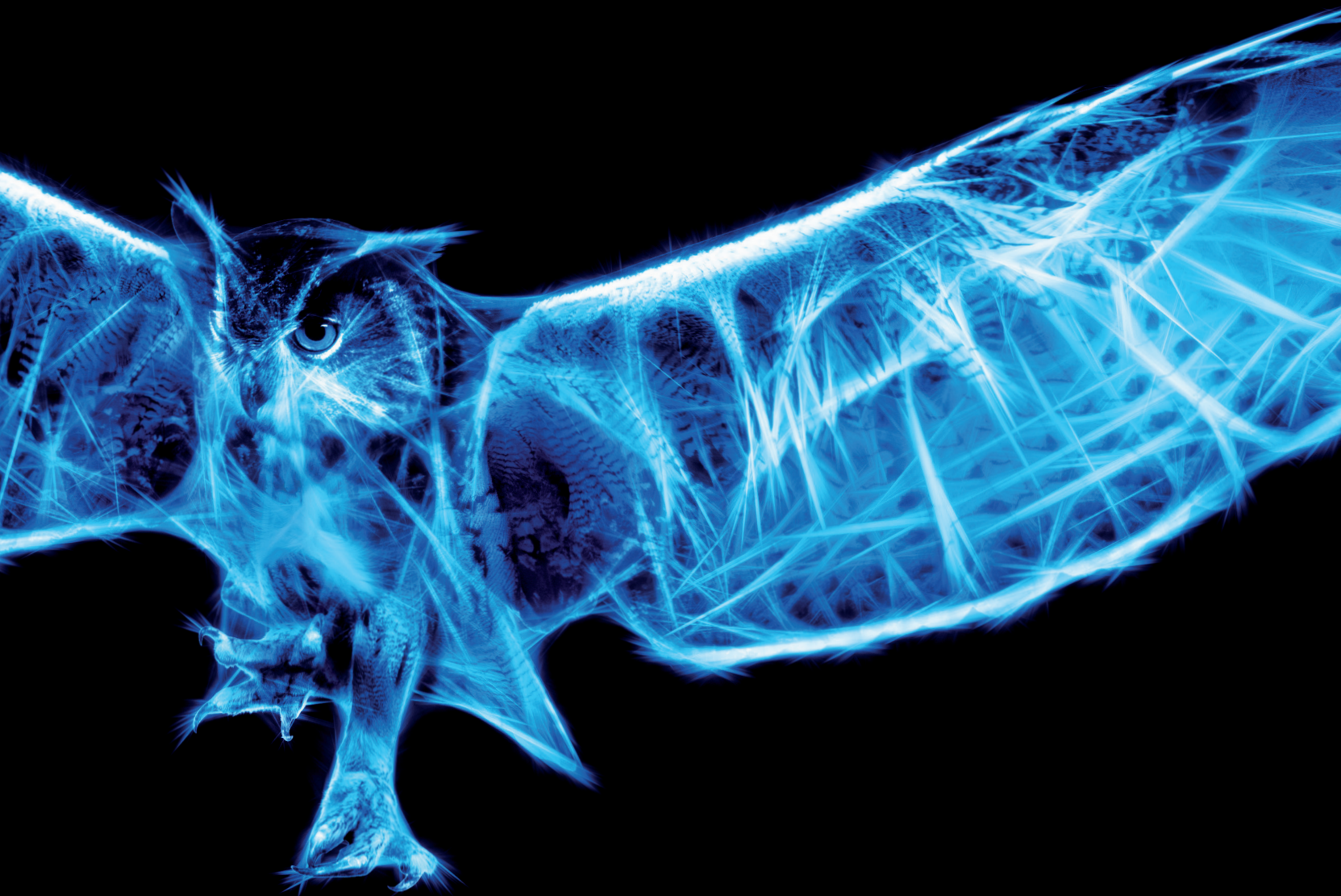




cutting through complexity

FTSE 350 CYBER GOVERNANCE HEALTH CHECK

An insight into the
issues of today
and tomorrow



FOREWORD

Cyber security continues to rise up the board agenda with major incidents becoming increasingly commonplace across a range of industries. This risk is not about to fade away, but will likely intensify in the years ahead as companies continue to digitise more of their operations. The reality is that cyber security is an internet-age issue that society as a whole has a responsibility to confront, and leading businesses must play their part.

The 2014 Cyber Governance Health Check (The Tracker) assesses and reports levels of cyber security awareness and preparedness across many of the FTSE 350, from a governance perspective. Under the Government's National Cyber Security Programme and Strategy, the Department for Business, Innovation and Skills is working in collaboration with business advisory firms to develop and manage the Tracker process.

In this report, you'll find detailed analysis of this year's assessments, highlighting areas where a number of large companies are succeeding in their response to the cyber security threat – and areas where more work is required. You'll also find a series of viewpoints from KPMG's cyber security experts – our perspectives on the challenges we see facing companies as they plan their cyber security response and what the future holds.

These viewpoints draw on our experience of working closely with leading businesses as they attempt to manage cyber risk in the context of their strategic objectives. For many businesses, this is an issue that is now rising to the top of the corporate agenda very quickly; as we explain in this report, our role is to help businesses manage cyber risk in a way that delivers potential competitive advantage rather than impeding growth.



Simon Collins
Chairman
KPMG in the UK

A stylized, handwritten signature in blue ink, consisting of a large 'S' followed by a cursive 'C'.

CONTENTS

Executive summary	1
The trends analysed	2
The deafening silence: How to get cyber risk on the board agenda	3
Third party control: Working for the common good	5
Best of friends: A security strategy that balances risk and reward	7
Top 10 findings	9
The CISO of the future: Geeks need not apply	11
Cyber comes of age: Why security must professionalise	13
Future trends	15
Why choose KPMG's cyber security team?	17
HMG cyber security initiatives	19

EXECUTIVE SUMMARY



Tony Cates
Partner
Audit



Malcolm Marshall
Partner
Cyber Security

Cyber risk is moving up the risk agenda

The majority of this year's FTSE350 Cyber Governance Health Check participants (88%) include cyber risk in their "Risk Register", with most giving it at least biannual consideration. More than a quarter rank cyber threats amongst their top risks, with 89% regarding cyber risks as moderately or extremely important. Over 58% expect risk to increase over the next year, an optimistic 8% expect a decrease, while the rest expect status quo.

Boards are demanding more informed debates

Management information is beginning to improve. One in five respondents (21%) say their boards get comprehensive information, while a further 55% say boards get some. Almost a third (30%) of boards now regularly receive intelligence on cyber threats.

Focus on third parties

A third of participants (33%) now audit third parties and suppliers on cyber risk, while 44% subject them to pre-contract due diligence. Just under half (48%) include cyber risk clauses in contracts. Companies are working to reassure customers of their robust approach to cyber security, with 45% of responding companies describing their risk management approach on their website or in their annual report.

Board members realise they face personal risks too

92% of interviewed board members say their directors have at least some understanding of the risk of being targeted by an electronic attack, though just 1 in 6 (17%) regard themselves as having a full understanding of this risk. Many (48%) have undertaken cyber risk training over the previous 12 months.

Government guidance is gaining traction

The Government's "10 Steps" guidance has become an integral part of the security process at an increasing number of companies. A majority of firms (58%) have assessed their risk management processes against this guidance.*

As the statistics from this year's Cyber Governance Health Check show, there is much for our leading FTSE companies to think about when it comes to cyber security. Risk management, controls, board expertise, budgets, management information: these are the here-and-now concerns which demand immediate consideration.

*For all data, please see the UK Government's 2014 FTSE 350 Cyber Governance Health Check.

CURRENT TRENDS



**Alejandro
Rivas-Vásquez**
Principal
Cyber Security

Boardroom engagement

Boards are getting to grips with the risks that cyber threats pose to their business, both operationally and strategically. Now that almost all respondents include cyber risk in their “Risk Register”, with most of these companies discussing risk at least biannually, this awareness should cascade down through their organisations.

However, there is more to be done. While board members are aware of the personal cyber risks they face alongside the corporate threat, too few have a full understanding of the dangers. Directors who have received no cyber risk training over the past 12 months should be encouraged to sign up for support in the year ahead.

Understanding what is important

Most respondents have a clear, or at least acceptable, understanding of what constitutes their companies’ key information and data assets – the crown jewels. But the frequency with which boards review such assets is still too low: most do so rarely or not at all.

In today’s fast-moving marketplace, an organisation’s precious assets may change quickly, as the business develops new products or services, say, or engages in M&A. Boards need to know what their crown jewels are, where they are, and how they are protected.

Mitigating risks at third parties

More companies are paying attention to the cyber risks stemming from their engagement with suppliers and other third parties. However, whilst there is an increase in the percentage of respondents that perform pre-contract due diligence and post-contract security audits, we also noticed a significant increase in the percentage of respondents that include a cyber-related clause in third-party contracts. This trend could lead to complacency in the future, with companies relying on contracts rather than active compliance or audit activities.

Who leads cyber?

Making it clear who is accountable for any type of risk is a crucial element of good governance, but respondents are divided on who is their “most senior cyber risk owner”. While 31% identify the CFO, 16% look to the CEO, and 15% pick out the CIO. This year’s survey also highlights a trend for accountability, moving away from the main board and towards the audit committee.

But what of the bigger picture; the issues which, while more long-term in nature, nevertheless merit careful thought? Over the following pages, KPMG experts opine on those points. These topics may well be the focus of future Health Check reports. As such, we would be well advised to start thinking about them now.

ISSUE 1



Phillip Hodgins
Principal
Cyber Security

THE DEAFENING SILENCE: HOW TO GET CYBER RISK ON THE BOARD AGENDA

I believe cyber security is relevant to every decision a company's board takes and that a targeted strategy can give a business a clear edge over its rivals. So why is this issue so rarely on the board's agenda? My experience is that not enough organisations consider that they may already have a problem or that effectively managing cyber risk extends beyond just the IT department.

I think the single most important reason for this hesitation is that organisations find it challenging to quantify cyber risks they face. I don't meet enough companies that think about cyber security in the context of the corporate objectives they're working to achieve. They may have a general awareness of cyber security issues, but that doesn't mean they have grasped the most serious and relevant threats to their specific organisations.

Size of the prize versus scale of the threat

For me, the fundamental principle is that each organisation's cyber risk profile is unique to it. So, first of all, you need to understand the value of what you have – and what could be lost in the event of a cyber attack. That will be easier for some organisations than others – for example, a retail bank could, to some extent, determine the financial value of stolen data on


the black market but it may be less obvious for, say, an aerospace company to determine what the value of its intellectual property on a new design project might be. The bigger question, though, is the long term impact of a cyber incident on the company's performance and reputation were that data to be lost or that design to be stolen?

This is why I say cyber risk is relevant in every decision the board makes. Just as boards assess financial risks before embarking on a particular course of action, so too should they have the data available in order to be able to take cyber risk into account.

A good example might be the business opportunity presented by a move into a new market. I think the board should be asking questions such as: what additional cyber risk does taking this opportunity expose us to?; to what extent can we mitigate the risk?; and does the scale of the opportunity justify the risk we will have to accept?

Securing competitive advantage

I think boards that ask such questions will find themselves having more constructive conversations about cyber risk. If the risk is considered in this proactive and forward-looking manner, you will have an opportunity to secure a competitive advantage over rivals still

An abstract graphic consisting of numerous thin, overlapping blue lines that fan out from the right side of the page, creating a sense of motion and depth.

operating reactively to a generalised threat. Your board will make better informed decisions about both existing operations and new opportunities – including whether or not to embrace these opportunities – while developing much more specific responses to each new threat as it emerges.

The spate of cyber security failures that have hit the headlines are not isolated incidents and every company is exposed to risks of its own. I believe organisations can learn from these high-profile cases, but only if they draw out the lessons relevant to them rather than talking about a general, non-specific threat.

Once boards understand the potential impact of cyber risk on their own companies' future performance in much more specific terms, I expect conversations about appropriate management of that risk to be more commonplace and far richer.

**“CYBER SECURITY
IS RELEVANT TO
EVERY DECISION
A COMPANY’S BOARD
TAKES”**

ISSUE 2



Matthew Martindale
Director
Cyber Security

THIRD PARTY CONTROL: WORKING FOR THE COMMON GOOD

I believe that while an organisation is legally accountable for any breach of its data security, even where the breach happens at a third party, many businesses have not assessed the risks to which they're exposed via these relationships. Often, businesses don't even know who all their suppliers are, or what data they process or store, let alone understand the cyber security threats posed by these third parties.

I don't think this complacency is acceptable. The damage caused to an organisation by a data breach will be no less because it happened at a third party. And cyber criminals increasingly see third parties as the perfect way to launch attacks on the business.

No respecter of size

Both large and small organisations have work to do on this issue. Smaller businesses are often focused on cost-efficiency; when they outsource work, for example, they prioritise savings rather than asking difficult questions about cyber security and data protection. Often, when they outsource their IT they think they have outsourced the cyber security problem. Larger companies, meanwhile, are working with hundreds or even thousands of suppliers – they may not even have


a complete list of these third parties. Some of these suppliers are small organisations that provide a specific service but don't have the level of control maturity large companies expect.

The complexity of the supply chain is also an issue. You may have thoroughly assessed the cyber security risks posed by a third party supplier, but what about the dangers associated with its third parties? I don't think too many businesses are focused on fourth- or fifth- or even sixth-party risk.

Then there is the growing sophistication of cyber attackers who see service suppliers as rich pickings. A provider of payroll, IT, legal or cleaning services, say, may have links with hundreds of clients – any vulnerability in their systems provides attackers with a potential route into all of those companies, often preying on the supplier's trusted relationships.

Shutting the door on attacks

I believe companies need to be more strategic as they seek to mitigate third-party risk. Too often, I see security rushing in, imposing unrealistic controls on relationships with suppliers in their anxiety to shut down all risk. Nor do



companies think about risk holistically – cyber security is just one question for a business thinking about how to get best value from a supplier and operating in a silo is inefficient and counter-productive.

My immediate recommendation to clients is often that their organisations need to build a clearer picture of who their suppliers are, what services they provide, what data they host and process, and how they engage with them. Once you have the bigger picture and can work collectively, security will be just one component of the risk assessment. And in putting the basic relationships in better order and ensuring you have the right to work with suppliers to assess their security controls, you will be able to engage more constructively with them.

However, I believe that while this risk assessment and assurance process is important, the real opportunity in future is to build more of a risk eco-system. Businesses that take a leading role in educating and supporting their supply chain will be in a much better position to get these third parties on board with the right controls and protections.

That might be something as simple as offering your own company's cyber security awareness training to the employees of your suppliers. Or it might be sharing information about

the latest virus or system vulnerability. I believe that if companies learn how to collaborate more effectively, the supply chain as a whole will be more secure and each individual company will be better protected as a result.

This collaboration should be a constant theme for cyber security professionals. We should be working together to align the demands businesses make on their suppliers so that these firms – many of which are smaller enterprises – aren't expected to comply with a multiplicity of differing requirements. There may even be a role for government intervention – either as a catalyst for this collaboration or as a medium through which we agree common standards.

**BUSINESSES THAT
TAKE A LEADING
ROLE IN EDUCATING
AND SUPPORTING
THEIR SUPPLY
CHAIN WILL BE
IN A MUCH
BETTER POSITION**

ISSUE 3



Tom Burton
Director
Cyber Security

BEST OF FRIENDS: A SECURITY STRATEGY THAT BALANCES RISK AND REWARD

Although companies are increasingly taking cyber security seriously, too often their efforts are incoherent with their overall business strategy. Many companies fail to ask themselves: 'What are we trying to achieve as a business, and what are the cyber threats to those objectives that we need to counter?'.

Holding back the business

I meet too many companies where there is a direct conflict between their cyber security policy and what the wider business hopes to achieve. A strategic objective might be to break into an emerging market but a rigid security policy devised for stable developed markets gets in the way.

Risk isn't binary: it's not something that you either have or you don't. Effective treatment of risk balances the cost and impact of mitigation on the business, and the appetite and preparation for the residual risk that remains. It demands dialogue: the enterprise can then decide whether the risks it faces are acceptable given the returns expected in a particular opportunity.

Mind the gaps

Security's budgets are finite. Those that fail to prioritise will inevitably leave key areas exposed to undue risk while protecting the less important. There is a better approach. A clear linkage between business objectives, the threats to those objectives, and the enabling security capabilities to counter the threats, makes the investment decision easier and it becomes a straightforward balance between ROI and residual risk.

Without a clear strategy and roadmap, people look for the latest, greatest thing being promoted in the market. Companies end up focusing disproportionate resource into the implementation of expensive technology solutions – viewing them as some kind of universal panacea for any security fears – rather than emphasising skills and awareness, or focusing on targeted security investments to enable business change.

Even when technology forms part of a capability, the essential components such as process, organisational structure, training, business and cultural change, and compliance monitoring can be left unaddressed. Alignment drives a more strategic approach to security, and

also encourages security to focus on how it can help the business to help itself.

In an ideal world

When the strategy director spots an opportunity and considers what operational enablers are required to exploit it, working with security to develop the most effective cyber risk management should be second nature. Risk should shape strategy, and strategy should drive security requirements.

This requires change. It demands a cultural recognition by the business that security matters, but is able to help. The security function has to meet the business halfway; security doesn't know best, but needs to communicate in terms the business understands. Information security must be accessible and relevant, and not exist as a silo within IT, marking its parent's homework and simply adding cost.

There should be clear end-to-end traceability in security strategy and plans. It will start with the business objectives and initiatives; from these, the threats that could disrupt the objectives should be identified; these threats require a variety of capabilities to bring the risk to within the business's appetite; and these capabilities will be realised through the implementation of business

change covering all aspects of people, process and technology. When the strategy or threat changes it will be easier to assess the impact that it will have on the security posture, the risk profile and the investment required.

I believe security can become a key competitive advantage. A business that is proud of its security will gain the trust of its stakeholders. A business that takes control of all the levers relevant to the execution of its strategy is going to be stronger and more agile; cyber security is one of those levers as it enables the exploitation of capabilities that interact with cyberspace. The antithesis is a business without confidence in its ability to seize opportunities when they arise, or worse, one that pursues opportunities blind to the consequential risks with potentially fatal results.

**“ STRONG ALIGNMENT
BETWEEN THE
BUSINESS AND
CYBER SECURITY
TEAMS CAN HELP
ORGANISATIONS PURSUE
NEW OPPORTUNITIES
MORE EFFECTIVELY ”**

TOP 10 FINDINGS



HOW ARE CYBER RISKS PERCEIVED IN YOUR BUSINESS?

58% of respondents expect cyber risk to increase

29% of chairmen are anxious about cyber risk

48%

have a **basic understanding** of information assets shared with third parties

...but Chairs

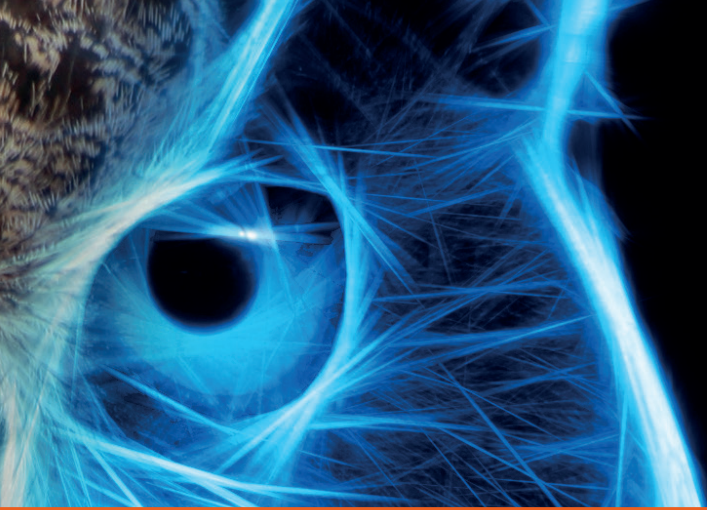
did **not** have a strong **understanding** of how they dealt with third-party risk

WHAT ABOUT THIRD PARTIES?

ARE YOU DOING ENOUGH?

74% think their board colleagues take cyber very seriously

48% of chairs had IT security/cyber **training** in the last 12 months



WHO IS IN CHARGE?

89%

see **responsibility** for cyber threats sitting with the **board, executive or audit committee**

15%

see the **CIO** as the senior cyber risk owner; nearly half say it is the **CEO** or **CFO**

25%

of respondents have **never received intelligence** from their **CIO** on cyber threats

30%

of respondents **regularly receive cyber intelligence**

WHAT DO YOU BASE YOUR DISCUSSIONS ON?

ISSUE 4



Del Heppenstall
Director
Cyber Security

THE CISO OF THE FUTURE: GEEKS NEED NOT APPLY

I believe that in five years' time, the role of the CISO will not exist – at least not in its current form. Companies will still have CISOs but I expect them to be very different to the people inhabiting those roles today. They'll be less technically minded and more focused on the whole business and its strategy; they'll also be much more senior and influential.

I have already begun to see that shift, with some businesses no longer requiring a CISO who is an absolute technical expert; rather, they are looking for someone who can articulate a cyber security strategy in the context of the company's business strategy – and someone who sees the cyber threat as just one of a number of risks to be managed and mitigated.

Leaving IT behind

I don't see how the CISO of the future can meet those needs while remaining within the IT function. There will no doubt be IT people with day-to-day security roles but they will report to a CISO who is much closer to the CIO, and whose role is wider, encompassing strategy, policy and crisis management within the broader business context.

The CISO may not even come from an IT background. The CISO of the future


will need to be able to communicate effectively with the board about cyber risk and its relevance to the business in succinct terms; these are people who will switch off very quickly if you speak in technical jargon.

I also think CISOs with an IT background will find it tough to accept they have to take risks. In future, they'll need to be enablers – people who can work with the business to help it achieve its objectives, even if that sometimes means accepting that it isn't possible to mitigate all risk. I worry that too many people who have come up through traditional IT roles have a solutions-driven view of the world and in some cases a 'computer says no' mentality.

The agent of change

I'm not dismissing everyone with an IT background and there will be IT professionals who have what it takes to succeed in what is going to be an enhanced role. I see the CISO of the future as a transformational leader who can bring the security agenda to life while enabling business change in a far more risk-balanced way.

These CISOs will be strategic thinkers who are much more proactive in their efforts to help the business move



forward while still managing its regulatory responsibilities, especially in areas such as data privacy, where the compliance burden continues to increase.

I also think companies will focus on the cyber agenda as they collapse risk management – even including the traditional corporate security function – into a single role. And they’re going to be much more externally focussed, managing relationships with third parties and suppliers, for example, in the broadest sense, rather than just monitoring the cyber security risks that these links may pose.

For those who step up to the plate, this is an amazing opportunity. I believe CISOs are ideally placed to ensure their companies are finding the right balance between risk and innovation – and, in doing so, to deliver strategic advantage over their competitors.

**“ CISOs ARE IDEALLY
PLACED TO ENSURE THEIR
COMPANIES ARE FINDING
THE RIGHT BALANCE
BETWEEN RISK AND
INNOVATION ”**

ISSUE 5



Bia Bedri
Director
Cyber Security

CYBER COMES OF AGE: WHY SECURITY MUST PROFESSIONALISE

There's a worrying truth at the heart of cyber security work. Despite mankind's growing dependence on the internet, we have only recently begun to professionalise the response to those who seek to prey on the vulnerabilities this dependence creates.

I believe that until relatively recently, those on the frontline of the cyber security battle were either security purists or people who fell into their roles. They weren't cyber security professionals appointed by their organisations as part of a strategic risk management process; they were technical security specialists or they had stumbled across this work and discovered a passion for it.

From passion to profession

Given the seriousness of the threat posed by cyber attackers, themselves becoming more professional by the day, we need to up our game. Fortunately, well-managed organisations increasingly share that view: we are now seeing cyber security develop as a profession in its own right. A better mix of people are coming into the role, including cyber specialists, risk managers, business leaders and former military personnel, and career paths are emerging for those

who want to stay in cyber security for the long term.

However, there is more work to be done in professionalising this crucial function. The divide between those for whom security is a passion and those for whom it is a career has certain advantages – each brings different types of skill. But fragmentation can cause problems too, especially as cyber risk has to be seen in the wider context of the organisation's strategic business objectives. Not enough has been done to ensure our profession is mature enough to cope with the massive responsibility it bears in the internet age. And there aren't enough of the right people to go round: KPMG's own skills survey found that more than 70% of firms experience difficulty recruiting cyber experts who are business savvy.

I want to see businesses developing their cyber security response and recruiting for it so as to ensure that this trend continues. They should be hiring and developing professional risk managers who are capable of reconciling the business's strategic objectives with the cyber dangers – and other risks – it faces.

Building a community of expertise

Part of the challenge will be to foster closer collaboration between business, academia, government and professional bodies. We should be working together in order to ensure cyber security professionals have all the skills and knowledge needed to head off the threat posed by the criminals.

What's really needed is a community of cyber professionals – universities need to be prioritising research in this area, businesses need to be funding that work and our professional bodies need to help pull all these strands together. There will be a role for government too, which has begun to recognise the economic threat posed by cyber attacks – for example from other countries stealing our intellectual property.

The good news is that we have come a long way already. When my own career in cyber security began, I was constantly told by chief information security officers that they didn't have the budgets or the access to senior management they needed; today, by contrast, many boards do recognise cyber risk as a fundamental issue they must confront and the cyber security profession is getting the recognition it deserves.

As for cyber security specialists themselves, the challenge now is to embed awareness of risk in the collective consciousness to such an extent that people change their behaviour – in business but also in wider society. If your community is educated on the basic controls it can put in place and if your management is constantly considering risks and threats, your cyber security team will be free to concentrate on the bigger picture: the sort of strategic response to risk management we should all have the right to expect from a mature and sophisticated profession.

THE CRUCIAL CHALLENGE FOR CYBER SECURITY SPECIALISTS NOW IS TO EMBED AWARENESS OF RISK IN THE COLLECTIVE CONSCIOUSNESS TO SUCH AN EXTENT THAT PEOPLE CHANGE THEIR BEHAVIOUR – IN BUSINESS BUT ALSO IN WIDER SOCIETY

FUTURE TRENDS



Malcolm Marshall
Partner
Cyber Security

CYBER SECURITY IS AT THE HEART OF YOUR BUSINESS

In a world in which cyber criminals are smart, resourceful and well-motivated, businesses will need to make cyber security a priority. This cannot be left to the technical specialists in IT and cannot be addressed in isolation. Cyber security, if not already a board level issue, is destined to become one that the C-suite will need to grip in the context of its wider digital business strategy. Getting it right will create strategic advantage whilst failure to adequately address the challenge may threaten the sustainability of the business.

Cyber space is becoming our world

The internet now stands at the heart of the global economy, powering innovation and growth. Analysts estimate that the internet contributes more than 8% of UK GDP, while more than 25% of our retail activity will be online by 2016.¹

Social media is transforming the way we communicate, as well as changing our views on privacy. We increasingly spend our time immersed in online activities and have become ever-more dependent on those connections in our daily lives.

The internet of things promises to network every aspect of our lives: smart

cities, smart buildings, smart grids, smart homes and wearable technologies. Cisco estimates that over the next ten years, the potential value created or shifted by the adoption of the internet of things will be \$14.4 trillion globally.²

The enormous business potential of this revolution is rightly recognised, but cyber security is often ignored. Innovative cyber criminals and determined governments will exploit this omission.

There can be no absolute security and walls will keep falling

Today, anyone who guarantees 100% protection from cyber attack is either complacent or deluded. We should not cling on to the illusion that it is possible to keep sophisticated attackers out.

A new approach to cyber security is needed. Focussing on protecting our perimeter – on keeping cyber attackers out – is no longer sufficient.

The boundaries of modern enterprises are rapidly disappearing as businesses work closely with suppliers and customers, or in joint ventures with other partners. Staff are mobile too, often working flexibly using their own devices.

[1] <https://www.bcg.com/documents/file100409.pdf>

[2] http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf

Security is only as good as the weakest link into your network – attackers routinely look for the easiest way in and are happy to exploit weaknesses in the security of customers, suppliers, staff or anyone else who can provide the access they need.

Scaremongering is easy and many boards are alarmed by the frequency with which companies are compromised. Major news stories which follow add reputational damage to the direct costs of the breach. Bold businesses look beyond the fear and uncertainty of this troubled environment to a more reasoned approach based on strategic defence.

Companies will learn to get smarter about what they protect and how

Businesses need a much better understanding of what they really want to protect. Where is the risk greatest, what are the company's "crown jewels" in information terms, and who really needs access? This should not be a debate about cyber security, but a business-led discussion about protecting corporate value.

Security systems will no longer admit some people and deny others – instead, they will be more dynamic, using the information the company holds on those looking for access and their typical behaviours in order to make judgements about whether their requests are acceptable risks.

Big data and analytics tools will offer new insights into what is suspect.

Companies will have to make hard choices about risk management and cyber security teams will be held to account on the return-on-investment they deliver. We will make choices on the extent to manage risk, whether to in-house or outsource the task and the extent of risk transfer through the growing cyber insurance market or by expecting suppliers and other partners to shoulder some of the burden of risk.

We will work together to defeat the cyber threat

Cyber criminals work in concert. A black economy has sprung up in which, for a price, criminals trade information about businesses' vulnerabilities and swap the attack tools required to exploit them. These attacks take place at scale – compromising hundreds of thousands of systems, stealing millions of payment card details and tens of millions of passwords.

A single criminal campaign can attack hundreds of different organisations, while one weak system compromises the security of an entire community. Our cyber security effort needs to be collective, sharing intelligence and tactics and working in real time to repel threats. Only by working together will it be possible to defeat such attackers.

In an increasingly inter-dependent world, this co-operative and proactive approach to cyber security is imperative.

If the collective approach fails, we risk falling apart

In the face of such an unprecedented threat to security, it would be easy to lose sight of the transformational benefits that the internet offers – including freedom of speech, expression and enterprise.

However, just as the internet will fuel innovation and growth so too will it act as an enabler for crime and terrorism. It provides a medium through which uncomfortable, libellous and even seditious ideas can move freely.

Given these anxieties, it is inevitable that individual nations will seek to regulate the digital economy. They will try to tax enterprise, to protect privacy, to limit sedition, to investigate crime and to defend critical infrastructure.

The risk is that nations will act autonomously and differently – a 'Balkanisation' in which governments force a break-up of the internet into a tapestry of separately regulated national networks, while simultaneously claiming extra-territorial jurisdiction over the information held on their citizens.

For all the difficulties of managing cyber security in the connected age, we must continue to promote the benefits of the global digital economy and to stand firm against over-regulation from the State, wherever it may originate.

A communal and strategic approach to cyber security can help us all achieve the economic promise of the internet.

WHY CHOOSE KPMG'S CYBER SECURITY TEAM?

AWARD WINNING

Whether it's SC Magazine or the MCA Awards, KPMG shines in independent recognition. Forrester also recognises KPMG as a leader in Information Security Consulting, highlighting our strong focus and ability to take on challenging engagements.

GLOBAL, LOCAL

We have over 2,000 security practitioners working in KPMG's network of firms, giving member firms the ability to orchestrate and deliver to consistently high standards globally. KPMG member firms can service your local needs from information security strategy and change programmes, to technical assessments, forensic investigations, incident response, training, and even ISO 27001 certification.

COLLABORATIVE

KPMG member firms facilitate and work with collaborative forums to bring together the best minds in the industry to collectively solve shared challenges. KPMG's I-4 forum brings together over 50 of the world's biggest organisations to discuss emerging issues and solutions.

TRUSTED

KPMG in the UK have a long list of certifications and permits to work on engagements for many of the world's leading organisations.

THE PRINCIPLES OF OUR APPROACH

We believe cyber security should be about what you can do – not what you can't.

DRIVEN BY BUSINESS ASPIRATIONS

We work with you to move your business forward. Positively managing cyber risk not only helps you take control of uncertainty across your business; you can turn it into a genuine strategic advantage.

RAZOR SHARP INSIGHTS

In a fast-moving digital world of constantly evolving threats and opportunities, you need both agility and assurance. Our people are experts in both cyber security and your market, which means we give you leading edge insight, ideas and proven solutions to act with confidence.

SHOULDER TO SHOULDER

We work with you as long term partners, giving you the advice and challenge you need to make decisions with confidence. We understand that this area is often clouded by feelings of doubt and vulnerability so we work hand-in-hand with you to turn that into a real sense of security and opportunity.

HMG CYBER SECURITY INITIATIVES

National cyber security programme

Cyber attacks are one of the top four threats to UK national security alongside international terrorism (National Security Strategy 2010). The UK Cyber Security Strategy, published in November 2011, sets out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment. Government has put in place a National Cyber Security Programme backed up by £860 million of Government investment to 2016 to help meet the objectives of the strategy.

<https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace>

Cyber essentials

Cyber Essentials is a Government-backed and industry supported scheme to guide businesses in protecting themselves against the most common cyber threats. Cyber Essentials is free to download and any organisation can use the guidance to implement essential technical security controls. Companies can also apply to be certified against two levels of badge, Cyber Essentials and Cyber Essentials PLUS and if successful, advertise the fact that the company adheres to a government-endorsed standard.

<https://www.cyberstreetwise.com/cyberessentials>

10 steps to cyber security

The 10 Steps to Cyber Security guidance demonstrates how to safeguard a company's most valuable assets, such as personal data, online services and intellectual property. It is designed to reinforce the idea that cyber security is a strategic business risk that needs to be managed at board level.

<https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility>

CERT-UK

CERT UK is the national computer emergency response team in the UK and works closely with industry, government and academia to enhance UK cyber resilience. It provides national cyber security incident management, and support to Critical National Infrastructure companies to handle cyber security incidents. CERT-UK also promotes cyber security situational awareness, and provides the single international point of contact for co-ordination and collaboration between national CERTs.

<https://www.cert.gov.uk/>

Cyber security information sharing partnership (CISP)

Part of CERT-UK, The Cyber Security Information Sharing Partnership (CISP) is a joint initiative between industry and Government to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and reduce the impact upon UK business. Any UK registered company with an electronic communications network in the UK can apply for membership of the CISP.

<https://www.cisp.org.uk/>

Cyber security incident response scheme

The Cyber Security Incident Response scheme provides access to industry expertise to enable businesses to respond effectively to the consequences of cyber security attacks. The scheme is led by the Council of Registered Ethical Security Testers (CREST) and endorsed by GCHQ and the Centre for the Protection of National Infrastructure (CPNI).

https://www.cesg.gov.uk/ServiceCatalogue/service_assurance/CIR/Pages/Cyber-Incident-Response.aspx

Cyber security skills: a guide for business

This guidance sets out Government and industry-supported cyber security skills activities and initiatives.

<https://www.gov.uk/government/publications/cyber-security-skills-a-guide-for-business>

CONTACT US

Simon Collins

Chairman

KPMG in the UK

T: 020 7311 8959

E: simon.collins@kpmg.co.uk

Malcolm Marshall

UK and Global Head

Information Protection & Business Resilience

KPMG in the UK

T: 020 7311 5456

E: malcolm.marshall@kpmg.co.uk

Tony Cates

Head of Audit

KPMG in the UK

T: 020 73118791

E: antony.cates@kpmg.co.uk

www.kpmg.co.uk/cyberftse350

© 2015 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.

OLIVER for KPMG | OM025060A | January 2015