http://www.pwc.co.uk/cybersavvyceo

Delusions of safety?

The Cyber Savvy CEO: Getting to grips with today's growing cyber-threats

Secure Information is Power

pwc

Contents

It’s time for CEOs to gain a clear understanding of the threats on the Internet

In June 2011, Nintendo joined fellow online games company Sony and US-based defence contractor Lockheed Martin in confirming that it was among the latest targets of cyber-attacks. The announcement came just days after the UK’s Chancellor of the Exchequer, George Osborne, told an international conference that British government computers are now on the receiving end of over 20,000 malicious email attacks every month[1]. The message is clear: no organisation in any sector is safe – and the threat is growing.

Nobody can say the world had not been warned. In January 2011 the World Economic Forum named cyber attacks as one of the top five threats facing the world—alongside planetary risks posed by demographics, scarcity of resources, concerns over globalisation, and weapons of mass destruction. Far from suggesting that fears over cyber threats may be over-hyped, the WEF highlighted the danger that they were actually being underestimated.

A few days later, UK Foreign Secretary William Hague proposed that Britain host an international summit on cyber security. Addressing the Munich Security Conference, he said: “The Internet, with its incredible connective power, has created opportunity on a vast and growing scale…but there is a darker side to cyberspace that arises from our dependence on it.”

As Mr Hague spoke, police across the world were continuing their efforts to track down the members of the hacktivist collective who unleashed disruptive attacks against a number of companies that had withdrawn services from WikiLeaks, including Mastercard, PayPal and Visa.

Against this backdrop, this paper examines why entering the cyber environment represents a seismic shift in the security landscape for all organisations. We will also highlight some of the structures, actions and capabilities that organisations can apply to achieve sustainable success in the cyber age.

Security is a key enabler in the cyber world

Operating securely in the cyber environment is among the most urgent issues facing business and government leaders today. Achieving this requires two assets. The first is an understanding of online operating and business models: how many people know how Google makes money? The second is an ability to protect and support those models.

Far from being a barrier to participating in the cyber world, effective security is a critical enabler for any organisation seeking to realise the benefits of taking activities online.

[1] http://nakedsecurity.sophos.com/2011/05/16/uk-government-under-cyber-attack-says-chancellor-george-osborne/

Unprecedented opportunities

The growing threat reflects the explosion of online services in all sectors. Across the world, more and more private and public sector organisations are capitalising on web, mobile and social media platforms to improve their performance and serve customers more effectively. Online interactions bring a blend of four key benefits: lower costs to serve, higher speed to market, greater customer loyalty, and—in the case of the private sector—the potential for higher revenue growth.

These benefits are seeing the cyber revolution gain momentum at breathtaking speed. Some 10% of consumer spending in the UK is now transacted via the Internet[2], and 115 million Europeans will be using mobile banking services by 2015[3]. The public sector around the world is also reaping massive benefits. In 2009, 65% of enterprises in the EU obtained information or downloaded official forms from public authorities' websites[4]. More than half of these businesses returned the completed forms, saving time and money on both sides. And in 2010, nearly 100 million US taxpayers submitted their tax returns online[5].

> "The cyber world continues to represent a powerful and effective way for HMRC to engage with and support its customers. It does however also present a series of new challenges and risks which need to be fully understood."
>
> — Jeff Brooker, Director — Security and Information, HMRC, the UK government's main tax-collecting authority

The darker side

As usage of online services increases, so do the scale and sophistication of cyber attacks, directed against targets ranging from countries' critical national infrastructure (CNI) and the global financial system, to less obvious targets such as mining companies.

One of the most alarming attacks was the Stuxnet computer virus that emerged in mid-2010. This malicious software (malware) program was created with the aim of sabotaging Iran's nuclear programme, by increasing the speed of uranium centrifuges to breaking-point and simultaneously shutting off safety monitoring systems. Commercial cybercriminals are mounting equally sophisticated attacks.

Such examples underline how opportunities and risks in the cyber world have risen to a new level. We will now look at the characteristics of the cyber domain that make it such a break with the past, and examine where the threats are at their greatest.

Our PwC / ISF QuickPoll: the view from the front line

PwC worked with the Information Security Forum (ISF)—the world's leading independent authority on information security—to conduct an online QuickPoll with PwC's clients and ISF's Members. We refer to the findings at relevant points throughout this paper.

All the respondents are senior decision-makers in information security, representing a blend of public and private sector organisations. The findings provide a snapshot of current concerns and perceptions among the professionals charged with leading the fight against cyber attacks.

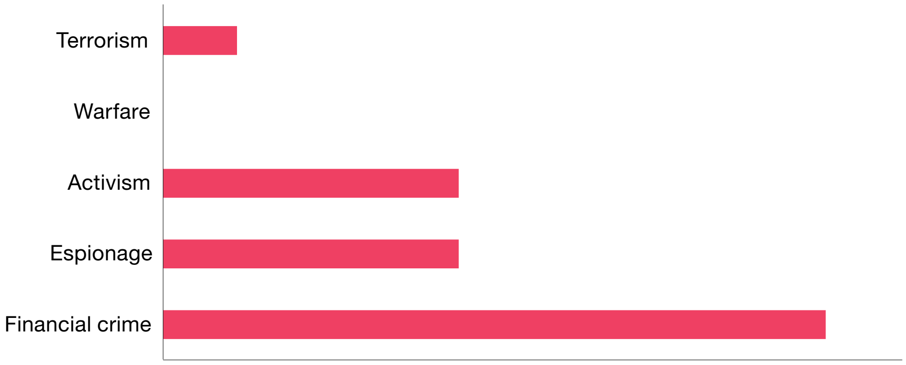
[2] http://press.kelkoo.co.uk/uk-online-shoppers-are-the-biggest-spenders-in-europe.html
[3] http://www.pwc.co.uk/eng/services/digitaltransformation.html
[4] http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/E-government_statistics
[5] http://www.irs.gov/efile/index.html

Where is the pain today?

Our PwC / ISF QuickPoll: Financial cyber-crime leads the way

Of the PwC clients and ISF Members we interviewed in our online survey, 85% said their organisation had suffered a cyber-attack of some sort in the past six months. Half of these attacks were financial in nature, while activism and espionage were also relatively common.

Has your organisation suffered from any of the following cyber incidents in the last 6 months (tick all that apply)?



There are two main reasons why operating in the cyber domain represents such a radical departure from operating in the traditional physical world.

First, cyber has ***no boundaries***. Indeed, it has the effect of destroying or dissolving any boundaries that were there before. And second, its opportunities and risks are ***asymmetric***. The cost and effort involved in developing a piece of malware are far below what would be required to develop a physical weapon with the same scale and scope of impact.

In combination, the low barriers to entry and absence of boundaries make cyber attacks hugely unpredictable, since they can come from virtually everywhere—including from thousands of computers worldwide in a coordinated attack on one target. As our QuickPoll global illustrates, these factors mean most organisations are now subject to attack.

Cyber security: looking outwards…

Similarly, cyber security represents a break with the past. Traditional IT security developed from technical origins in the 1980s to become information security in the 2000s. But all too often, information security has remained an inward-looking set of processes and behaviours, seeking to reinforce and protect the external boundaries that used to make up the perimeter of an organisation.

In the cyber domain there are no boundaries. When they participate in the cyber world, organisations plug their internal systems, information and processes into the cyber domain. Although the perimeter is still protected by measures such as firewalls, the boundary has become porous. So cyber security needs to be outward-looking, crossing boundaries of all kinds—organisational, national, physical, technological—while still protecting the data that represents the valuable assets of the organisation.

...and collaborating

This outward-looking stance demands greater collaboration between organisations across both the public and private sectors. In our view, it is no coincidence that PwC's 14th Annual Global CEO Survey, published in January 2010, reveals an intensifying focus on collaboration via technology. Of the 1,201 business leaders we interviewed worldwide, some 54% are putting technology investment into growth initiatives that will support collaboration, including mobile devices and social media. And 77% expect to change their business strategies over the next three years in response to consumers' growing use of these means of communication.

The shared nature of cyber threats means cyber security is a particular focus for collaboration, not least between business and government. Public-private organisations, industry bodies, regulators and third-party suppliers all have useful roles to play in sharing information and experiences. Threat horizon workshops can be conducted at an organisational, industry, supply chain or public-private level. And cyber crisis simulation exercises—often conducted jointly with other organisations—are useful ways to sharpen people's awareness, decision-making skills, and understanding of their roles.

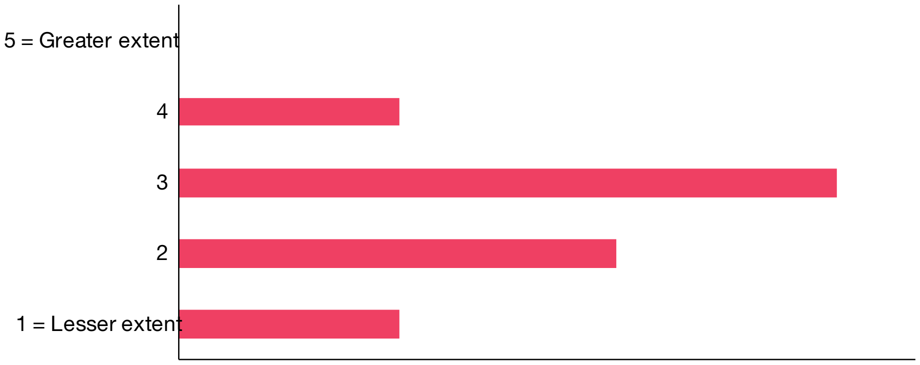
Experience shows that collaboration on cyber risks within the private sector and between the private and public sectors can face challenges around competitive confidentiality, and raise concerns that too much information is flowing one way. As the graphic below shows, information security professionals feel that public-private collaboration in this area is not yet working effectively. But there is no doubt that collaboration to address these shared threats should ultimately benefit organisations in all sectors.

> "Business in the cyber world means a disruption of traditional perimeter thinking. Users go mobile with new technology while attribution to a geographical location disappears. At the same time collaboration, communication and cooperation across logical company borders increases. The task of cyber security is to enable users doing their business securely, everywhere, on every device, with everyone."
>
> — Dr. Gunter Bitz, MBA, CISSP, CPSSE Head of Product Security Governance at SAP AG, a global leader in business management software.

Our PwC / ISF QuickPoll: Collaboration between public and private sectors to address cyber threats is not yet effective

When we asked our sample of PwC clients and ISF Members how effectively business and public sector organisations are working together in their local market to address cyber threats, their responses showed there is still a long way to go. Only one respondent rated the effectiveness of public-private collaboration at four out of five, and none gave it five out of five.

In your local market, how effectively are business and public sector organisations working together to address cyber threats?



Who are the attackers – and what's motivating them?

Different organisations often have their own specific way of categorising cyber threats. In PwC's view, there are five main types of cyber attack, each with its own distinct – though sometimes overlapping – methods and objectives. They are:

Financial crime and fraud – This involves criminals – often highly organised and well-funded – using technology as a tool to steal money and other assets. The stolen information may sometimes be used to extort a ransom from the target organisation.

Espionage – Today, an organisation's valuable intellectual property includes corporate electronic communications and files as well as traditional IP such as R&D outputs. Theft of IP is a persistent threat, and the victims may not even know it has happened – until knock off products suddenly appear on the market, or a patent based on their R&D is registered by another company. These crimes may be carried out by commercial competitors or state intelligence services seeking to use the IP to advance their R&D or gain business intelligence.

Warfare – This can take place between states, or may involve states attacking private sectors organisations, especially critical national infrastructure (CNI) such as power, telecoms and financial systems. The Stuxnet attack on Iran's nuclear programme was a particularly dramatic example. In May 2010, the US appointed its first senior general specifically in charge of cyber warfare.

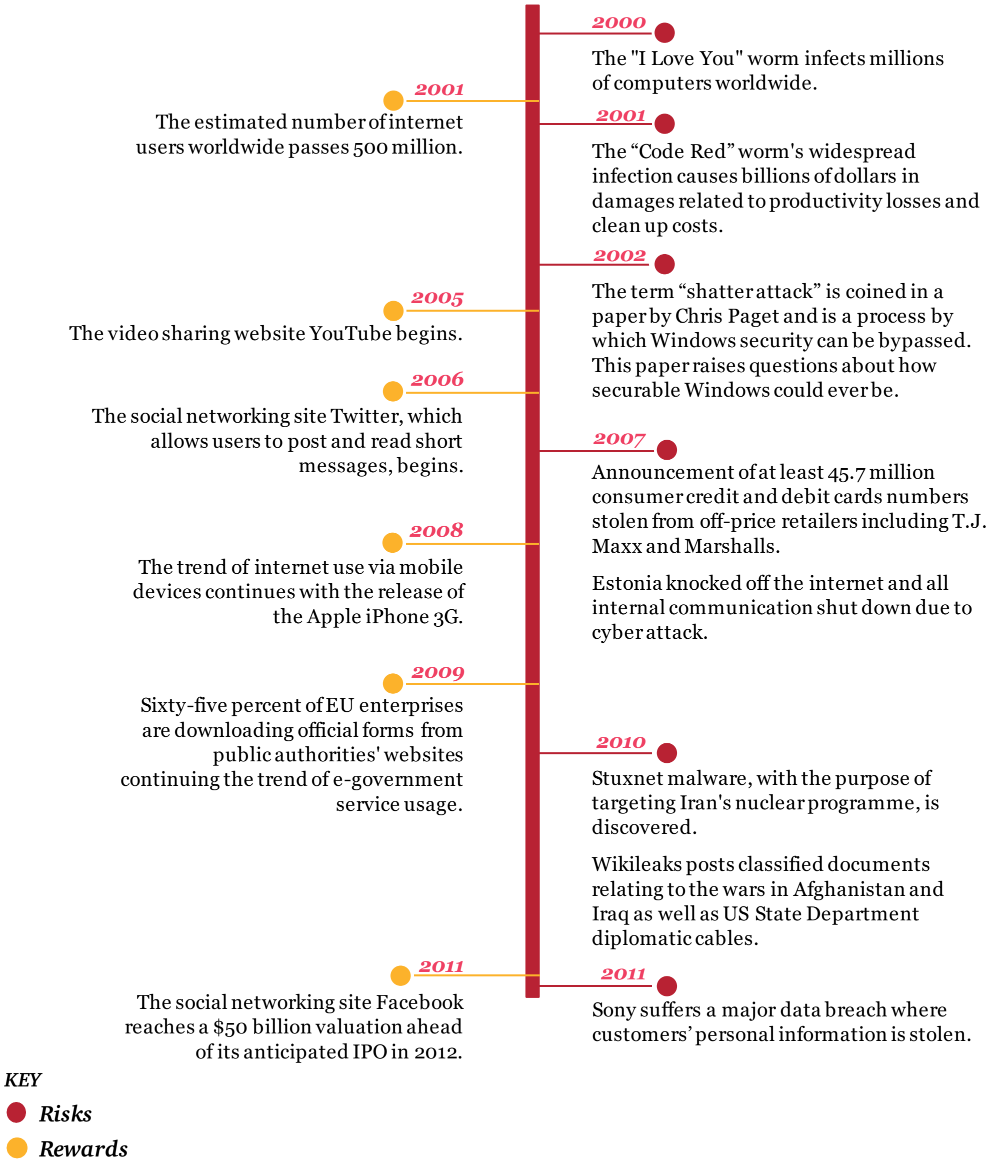
Terrorism – This threat overlaps with warfare. Attacks are undertaken by (possibly state-backed) terrorist groups, again targeting either state or private assets, often CNI.

Activism – Again this may overlap with some other categories, but the attacks are undertaken by supporters of an idealistic cause – most recently the supporters of WikiLeaks. Organisations need to anticipate these threats by thinking through how activists might view particular actions they take.

Secure information is power

Against this background, the axiom "information is power" has gained even deeper resonance. With so much more data to store, access and analyse to create valuable insights and intelligence, companies know that information is now a greater source of power than ever before—but only if it is secure. The ongoing escalation in the security threats to information is illustrated in the timeline of advances and attacks in Figure 2, highlighting that the business and political communities are effectively engaged in an ongoing arms race with cyber attackers.

Figure 2: A timeline of cyber risks and rewards



2000 ●
The "I Love You" worm infects millions of computers worldwide.

2001 ●
The estimated number of internet users worldwide passes 500 million.

2001 ●
The “Code Red” worm's widespread infection causes billions of dollars in damages related to productivity losses and clean up costs.

2002 ●
The term “shatter attack” is coined in a paper by Chris Paget and is a process by which Windows security can be bypassed. This paper raises questions about how securable Windows could ever be.

2005 ●
The video sharing website YouTube begins.

2006 ●
The social networking site Twitter, which allows users to post and read short messages, begins.

2007 ●
Announcement of at least 45.7 million consumer credit and debit cards numbers stolen from off-price retailers including T.J. Maxx and Marshalls.

Estonia knocked off the internet and all internal communication shut down due to cyber attack.

2008 ●
The trend of internet use via mobile devices continues with the release of the Apple iPhone 3G.

2009 ●
Sixty-five percent of EU enterprises are downloading official forms from public authorities' websites continuing the trend of e-government service usage.

2010 ●
Stuxnet malware, with the purpose of targeting Iran's nuclear programme, is discovered.

Wikileaks posts classified documents relating to the wars in Afghanistan and Iraq as well as US State Department diplomatic cables.

2011 ●
The social networking site Facebook reaches a $50 billion valuation ahead of its anticipated IPO in 2012.

2011 ●
Sony suffers a major data breach where customers’ personal information is stolen.

KEY

● *Risks*

● *Rewards*

Source: PwC Analysis

This escalation has made cyber security a key board-level risk issue and its importance is also increasingly recognised by investors and regulators. In February 2010, the semiconductor manufacturer Intel became the first company to disclose a “sophisticated incident” of computer hacking in its 10-K filing to the US Securities and Exchange Commission.

As governments and companies face up to the threats to their data, they know they are now up against a global, sophisticated and well funded cybercrime industry. A few years ago, many incidents consisted of hackers sending out a mass attack and seeing where it stuck. Today, many attacks are managed against a solid business case and specific objectives, tailored to a specific organisation, and developed using a network of third-party specialists including R&D specialists, cryptographers, programmers and list suppliers.

Key barriers to effective cyber security

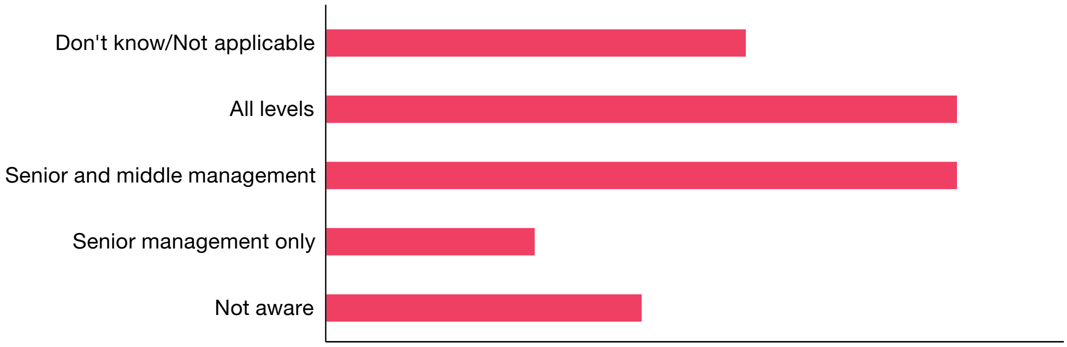
To defend themselves effectively against increasingly sophisticated attacks, many organisations need to overcome a number of entrenched barriers. Four are especially prevalent:

- ***A need for new skills and insights:*** To use a military analogy, the migration to cyber is as disruptive as moving from horses to tanks. In today's world, a 15 year-old hacker might have a better understanding of security risks than a seasoned leader. The people engaged in securing cyberspace face a need to keep raising their game faster than the attackers.
- ***Integrating security into the business:*** Cyber security used to be pigeon-holed as an IT issue, creating a communications gap between business managers and security professionals. Awareness is now growing that cyber security is not only a technical issue, but a core business imperative. PwC's Global State of Information Security Survey 2011 confirms that executive recognition of security's strategic value is now more closely aligned with the business than with IT, with the single most common reporting channel for chief information security officers (CISOs) now being to the CEO rather than the chief information officer (CIO). Since 2007, the proportion of CISOs reporting to the CIO rather than CEO has fallen by 39 per cent.

Our PwC / ISF QuickPoll: There is little awareness of cyber risks below middle management levels

Our research suggests that the challenges of creating and embedding a cyber risk-aware culture, and of ensuring aligned responses at all levels, are increased by a relative lack of awareness of cyber-risks lower down the organisation. Of PwC clients and ISF Members we surveyed, only 29% said people at all levels of their organisations were aware of cyber risks. Even more worryingly, 14% of respondents said nobody at any level was aware of these risks.

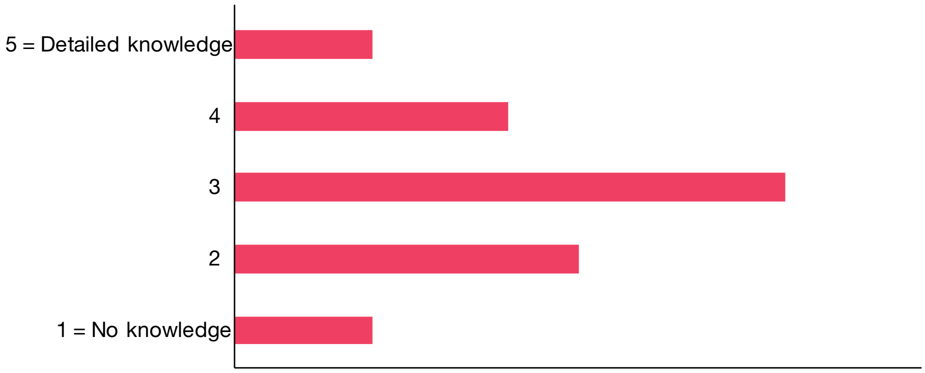
How aware are your people at all levels of cyber risks?



Our PwC / ISF QuickPoll: Organisations are unclear about what is being said about them online—and their employees are unclear about what they are allowed to say

When we asked PwC clients and ISF Members whether their organisations knew what their customers and employees are saying about them on social networking sites, their responses were spread evenly across a range from a lack of awareness to full awareness. This same lack of clarity applies to employees' knowledge of what they are allowed to say online. Only 9.5% of our respondents are confident that their employees have a detailed knowledge of this — the same proportion as say they have no knowledge.

Do your employees know what they are allowed and what they are not allowed to say when they are on-line?



- ***Consistent, aligned and connected responses at every level of the organisation:*** Traditional organisational structures tend to be too slow and rigid to enable the speed and flexibility of response needed in the cyber world. Faced with attackers who move quickly and unpredictably, organisations need to be able to move information and decisions up, down and across their structures fast and flexibly. Unless it is applied in a way that acknowledges and factors in new and emerging threats, even the the ISO/IEC 27001 information security standard may not help to support the necessary degree of agility and responsiveness.

- ***Creating a cyber risk-aware culture:*** A cyber attack can gain entry via any node on an organisation's network—including a third-party supplier, customer or business partner. This means everyone involved in the organisation's cyber-linked activities shares direct responsibility for security, and that awareness of cyber risks needs to be an integral part of every decision and action. Yet we are in an era when many younger employees access social networks in the workplace, and when organisational cultures can change rapidly. Significantly, our QuickPoll of PwC clients and ISF Members reveals a worrying lack of knowledge of what customers and employees are saying about their organisations on social networking sites, and of what employees are actually allowed to say online. These findings underline the need for a security-aware culture, greater risk awareness and clear policies continually reinforced by the tone from the top.

Six steps to the cyber-ready organisation

To address the threats we have described, many public and private sector organisations will need to transform their mindset towards cyber as well as their capabilities. There are six steps that organisations can take to reshape themselves for the cyber world.

> "Making your firm cyber-ready is not easy, and requires an organisation-wide initiative which only comes with a shift in top management attitude. Introducing the role of 'Cyber Savvy CEO' is a signal to that effect. That, however, is only the beginning not the end of a synchronized firm-wide initiative to position it better in a fast changing market."
>
> — Ajay Bhalla, Professor of Global Innovation Management, Cass Business School, London

1. Clarify roles and responsibilities from the top down

As we have already highlighted, the CEO needs to come to grips with the threats from the Internet—that's why we have introduced the concept of the cyber savvy CEO. In the future, we believe that leadership by a CEO who truly understands the risks and opportunities of the cyber world will be a defining characteristic of those organisations—whether public or private sector—that realise the benefits and manage the risks most effectively.

While many organisations have historically pursued cyber security in response to regulatory pressures, the real benefit lies in enabling the business to seize the opportunities—whether these involve driving growth by selling through new channels, or delivering public services at higher quality and lower cost. Leadership by a cyber savvy CEO will enable the organisation to understand these opportunities and realise them securely and sustainably through effective security.

Our PwC / ISF QuickPoll: Cyber responsibilities are split between 'risks' (CRO) and 'opportunities' (CIO)—with neither area owned by the CEO

According to our survey, organisations are continuing to divide ownership and accountability for cyber risks and opportunities at board level.

Cyber opportunities are overseen by a wide variety of C-level executives in different organisations, with the CIO being the single most common owner (in six out of the 21 respondent organisations), In contrast, cyber risks are usually owned either by the Chief Risk Officer (CRO) or Chief Information Security Officer (CISO).

Significantly, the CEO is still relatively uninvolved in either area, owning cyber opportunities in two of the 21 organisations, and cyber risks in only one.

2. Reassess the security function's fitness and readiness for the cyber world

Organisations already have IT security functions that may be doing a good job in protecting against traditional threats. As new risks emerge, the focus needs to be upgrading or transforming the existing capabilities to deal with them. Rather than creating something new from scratch, this means building on the existing base to ensure that the organisation's responses to its security needs fully encompass cyber security.

3. Achieve 360-degree situational awareness

To align its security function and priorities as closely as possible with the realities of the cyber world, the organisation also needs a clear understanding of its current and emerging cyber environment. This demands situational awareness (see information panel), which is a prerequisite for well-informed and prioritised decisions on cyber security actions and processes.

Achieving situational awareness can be a particular challenge for large public sector organisations, which may have to scan an economy-wide landscape, and for multinationals with global opportunities and exposures. Our research among PwC clients and ISF Members indicates that situational awareness is currently being undermined by a lack of measurements and KPIs to support effective management of cyber threats and opportunities.

Situational awareness: know the landscape—and the behaviours

Situational awareness—a term drawn from military strategy—means knowing the landscape surrounding your own position, including actual and potential threats.

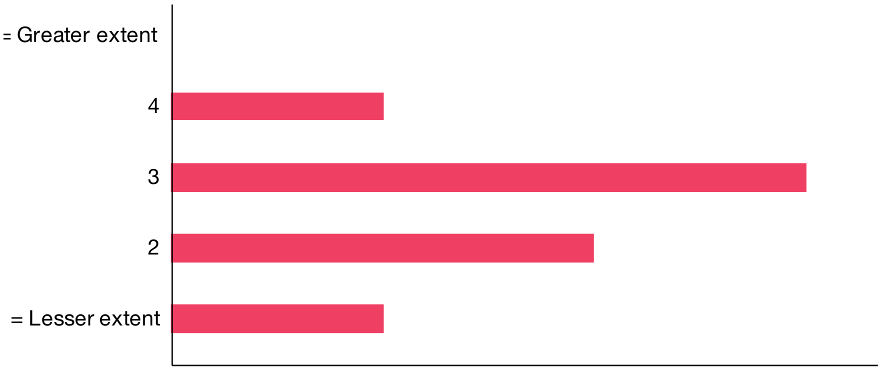
Detailed investigations of cyber incidents can also help organisations develop situational awareness. Knowing exactly what happened, when and how, helps organisations identify root causes and remedies, and provides valuable intelligence about the motivations, psychology and behaviour of attackers. Perhaps the organisation is contemplating an acquisition or project that might attract the attention of activists with cyber-attack capabilities. Situational awareness should flag such risks.

Our PwC / ISF QuickPoll: KPIs to manage cyber risks and rewards are not yet in place

None of the PwC clients or ISF Members participating in our poll rated their organisation's measurements and KPIs on cyber risks and rewards as meriting a score of five out of five. Most felt the current status of these measure to be middling at best.

Ask yourself to what extent your organisation has measurements and key performance indicators that enable you to properly manage the balance of risks and rewards in the cyber world?

In our QuickPoll, we asked: to what extent does your organisation have measurements and key performance indicators that enable you to properly manage the balance of risks and rewards in the cyber world?



4. Create a cyber incident response team

As we noted earlier, traditional organisational structures may have the unintended effect of hampering the quick and decisive responses needed in the cyber environment. Many organisations will already have an incident response team but the speed and unpredictability of cyber threats mean this may need to be adapted and streamlined, in order to enable information, intelligence and decisions to flow more quickly up, down and across the business, from board level to IT and business operations, and sometimes to and from other organisations.

A well-functioning cyber incident response team means an incident spotted anywhere in the business will be tracked, risk-assessed and escalated. Decisions and actions can then be made quickly, and forensic cyber investigations and/or external specialists brought in as necessary. Rather than leaving senior management wondering whether an incident is actually a threat —'Do we really have a problem?'— the team will channel the right technical, business and insight quickly to the relevant decision-makers.

5. Nurture and share skills

To make the most of its situational awareness and information stack, an organisation will also need to invest in cyber skills. However, as we noted earlier, these are in short supply. A recent survey by the SANS institute found that 90 per cent of companies had experienced difficulty recruiting people with the cyber security skills they needed and yet amongst the same employers, nearly 60 per cent said they planned to create more jobs in cyber security in the next few years.

Given the restricted supply line of new cyber-savvy talent, it is up to employers to find new ways of inspiring those with the skills and desire to keep our businesses safe. For example, the most valuable technical expertise and insight may well be found among younger employees at the lower levels of the organisation. Some organisations may even want to consider more radical approaches, such as putting younger employees on a board committee focused on cyber security.

6. Take a more active and transparent stance towards threats

The unpredictable and high-profile nature of cyber threats tends to engender a defensive mindset. But a number of cyber-savvy organisations are now getting onto the front foot by adopting a more active stance towards attackers, pursuing them more actively through legal means, and communicating more publicly about their cyber threats, incidents and responses.

Clearly, these responses must stay within the law—so it is important to ensure that well-meaning employees do not take things too far by hacking back. The CEO and board should also be clear about the organisation's stance on prosecuting or suing attackers, and must be sure the business has the necessary evidence to support any legal action. By taking a more active stance against attacks on its commercial or national interests, the organisation can show that it takes attacks seriously and will strive to bring offenders to justice.

Rising to the challenge: an agenda for business and government

The threats from the Internet represent a massive challenge shared by the public and private sectors worldwide. It is also a challenge that neither can tackle effectively on its own.

In today's interconnected world, the government's ability to deliver efficient, reliable and secure services is a critical factor in business confidence. And governments want a robust and vibrant public sector to generate growth and employment. Neither sector's objectives can be achieved without using the cyber environment—which demands cyber security.

To meet the imperatives of the cyber era, we believe that most public and private sector organisations will need to adopt new structures, roles and governance, while also engaging in close and continuing collaboration around the cyber agenda with other organisations.

Having the courage to let go…

This in turn demands a new mindset focused not on protecting the organisational entity itself but its wider ecosystem, while still ensuring the organisation's critical information assets are secure. Embracing the cyber world means opening up systems and processes to external suppliers, customers, partners and employees, and accepting culturally and psychologically that the old boundaries are being swept away.

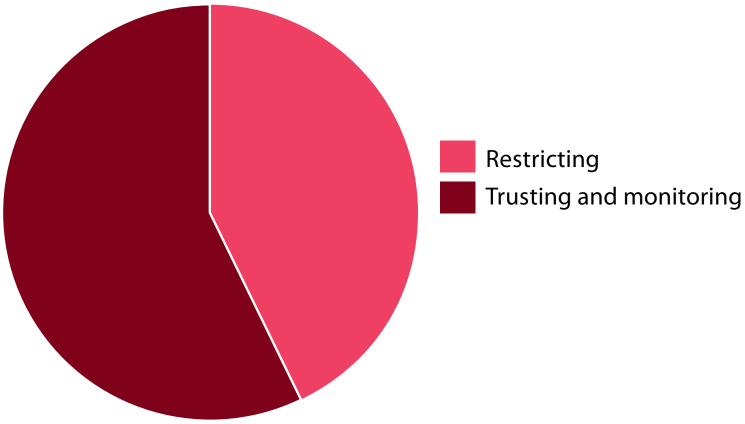
This is a major change. Traditionally, organisations have exercised control within their perimeters by prohibiting some behaviours and monopolising power at the centre. These approaches worked in the old world of physical supply chains. But they have the effect of inhibiting the speed and flexibility needed in the cyber world.

> "We are promoting an initiative for an organisation-wide cultural shift towards greater cyber security awareness. We have identified a step up in dispersed attacks and are preparing ourselves accordingly. It is anticipated that this threat will become more severe and impact more industries, and we certainly put much importance on an organisation approach to cyber security."
>
> —Itzik Kochav, Chief of Data Protection at Clalit Healthcare, one of Israel's leading health service organisations.

Our PwC / ISF QuickPoll: Organisations are moving from restrict-and-control to monitored trust

According to our research, most organisations have moved away from managing people by restricting what they do, and are instead managing them on the basis of trust and monitoring. This appears to be a sensible response to the advent of the cyber world. Yet other findings – notably on the relative lack of awareness of cyber risks at the lower kevels of organisations – cast into doubt whether organisations' workforces are really ready for such an approach.

Do you manage your people by restricting what they do, or by trusting and monitoring them?



...and move from proscriptive rules to monitored trust

This means companies need to let go of the old levers of power. Their security against cyber threats is critically dependent on their interconnected supply chains, and on the people working in them understanding the threats and behaving the right way. So organisations must move away from rules-based prohibition and control, and towards monitored empowerment and trust, at all levels from the individual employee to the supply chain to the collaborative business partner or government.

Governments: achieving win-wins through collaboration

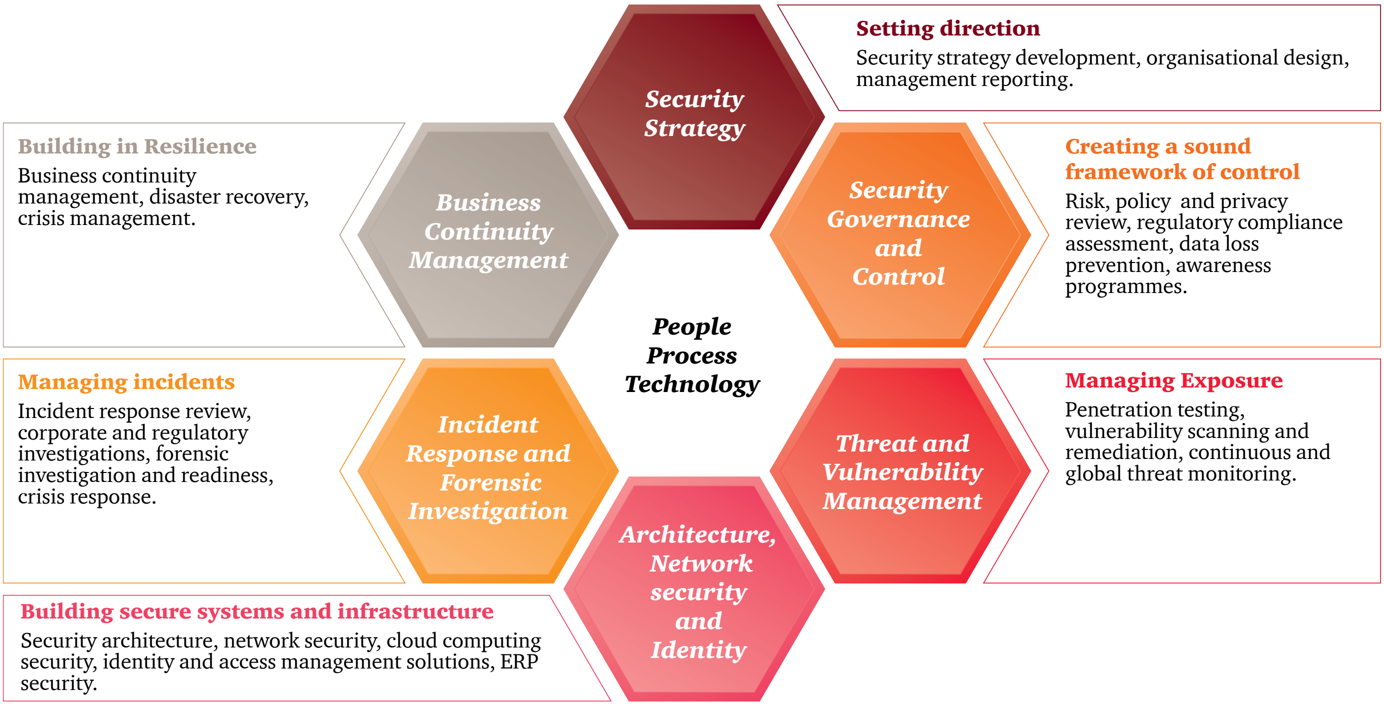
For their part, governments themselves can play a further critical role in strengthening cyber security, by bringing different stakeholders together to achieve win-wins through greater collaboration across sectoral and national boundaries. The most efficient and effective way to tackle a shared threat is through shared information, which can both heighten awareness and avoid the need for organisations to reinvent the wheel. Governments are ideally placed to foster this collaboration.

Time for the cyber savvy CEO to step up

Today, more and more organisations in all sectors are seizing the opportunities created by the Internet. In PwC's view, the only way to do this securely and sustainably is by ensuring that cyber awareness and responsiveness are infused into every employee, every decision and every interaction. It's time for CEOs to make this happen.

About PwC's Information and Cyber Security Team

The PwC Information and Cyber Security team has over 30 years' experience in all aspects of security, from espionage to governance risks. Our globally based team understands and speaks business language, we know when and how best to involve experts in legal, IT, business continuity, disaster recovery, crisis management, fraud, forensic and human resources. This wide range of know-how means we can help your organisation to devise a dynamic and forward-thinking security strategy that identifies the security risks you face, and offers practical and effective ways of ensuring they are addressed. PwC were recognised by Forrester in 2010 as a leader in Information Security and Risk.


Security Strategy
Security Governance and Control
Threat and Vulnerability Management
Architecture, Network security and Identity
Incident Response and Forensic Investigation
Business Continuity Management
People
Process
Technology

Setting direction
Security strategy development, organisational design, management reporting.

Creating a sound framework of control
Risk, policy and privacy review, regulatory compliance assessment, data loss prevention, awareness programmes.

Managing Exposure
Penetration testing, vulnerability scanning and remediation, continuous and global threat monitoring.

Building secure systems and infrastructure
Security architecture, network security, cloud computing security, identity and access management solutions, ERP security.

Managing incidents
Incident response review, corporate and regulatory investigations, forensic investigation and readiness, crisis response.

Building in Resilience
Business continuity management, disaster recovery, crisis management.

If you would like to discuss any of the issues raised in this report, please speak to your PricewaterhouseCoopers contact listed below

Grant Waterfall
United Kingdom
grant.waterfall@uk.pwc.com
+44 (0)20 780 42040

William Beer
United Kingdom
william.m.beer@uk.pwc.com
+44 7841 563 890

Otto Vermeulen
Netherlands
otto.vermeulen@nl.pwc.com
+31 88 792 63 74

Ed Gibson
USA
ed.gibson@us.pwc.com
+1 (703) 918 3550

Contributors

The following individuals in PwC contributed to the production of this report.

Nick C Jones
PwC Public Sector Research Centre United Kingdom

David Moloney
PwC United Kingdom

Clare Geldart
PwC United Kingdom

Sarah Nolton
PwC United Kingdom

Andrew D Miller
PwC United Kingdom

Ariel Litvin
PwC Israel

A special thank you to Fox-IT in the Netherlands, who made a significant contribution to the content of this paper.

Join the debate: www.psrc.pwc.com

The Public Sector Research Centre is PricewaterhouseCoopers' online community for insight and research into the most pressing issues and challenges facing government and public sector organizations, today and in the future.
PRSC enables the collaborative exchange of ideas between policy makers, opinion formers, market experts, academics and practitioners internationally.

To register for this free resource please visit www.psrc.pwc.com

HB-2011-08-18-1531-CG

www.pwc.co.uk