Sponsored by KPMG

The e-Crime Report 2011

Managing risk in a changing business and technology environment

e-crime CONGRESS

www.e-crimecongress.org/global

AKJ Associates

The e-Crime Report 2011 is edited and published by AKJ Associates, a business information company that owns the global e-Crime Congress and PCI Series brands. Our initiatives are specifically designed to deliver practical frameworks, innovative solutions and technical guidance to senior stakeholders and decision makers who work for global enterprises and public sector organisations. Delegates who attend AKJ Associates' events represent departments that include security, IT, risk, compliance, audit, investigations, fraud, forensics, HR and legal. Industry sectors typically represented include banking and finance, insurance, telecommunications, legal services, media and entertainment, military and defence, pharmaceuticals, retail and transport and travel. Over the past 10 years, AKJ Associates has hosted events in major centres of commerce such as Amsterdam, Abu Dhabi, Brussels, Cairo, Dubai, Frankfurt, Johannesburg, London, Madrid, Milan, Moscow and Paris. For more information please visit www.e-crimecongress.org, www.pci-portal.com, or www.akjassociates.com.

About KPMG

KPMG Risk Consulting brings together specialists with skills focused on the Information and Technology Risk agenda. We have a team of over 3,500 professionals advising clients across all markets and geographies of the technology and data risks they face. We are part of KPMG's global network of over 140,000 professionals in 150 countries.

We help our clients to prevent, identify and remediate Information and Technology failures and ensure systems are fit for the future. Our independent advice and advanced technology capabilities help our clients manage their technology risks and use their data to its full potential.

Our award winning Information Protection team helps organisations assess risk and design, test, and implement the controls required to protect them from security breaches, including accidents and cyber attack.

Why KPMG

- Award winning – KPMG was awarded 'Information Security Consultancy of the Year' at the SC Magazine Europe Awards 2011. We received this award in recognition of our ability to assist businesses with understanding and implementing information security management processes. We have also received an Management Consulting Association (MCA) Management Award for Business Strategy for our work with a leading bank on a major third-party security assurance programme.
- Commitment – KPMG's client relationships are built on mutual trust and long-term commitment to providing effective and efficient solutions. We are dedicated to providing a service that is second to none.
- Industry knowledge – Through I-4 (the International Information Integrity institute) we help the world's leading organisations to work together to solve today's and tomorrow's biggest security challenges.

Executive Summary

By Malcolm Marshall, Partner, KPMG

Recent reports of cyber attacks launched against large companies demonstrate that protecting and securing data is more important now than ever before. Cyber attacks can have a negative impact on brand value, reputation and the ability to generate revenue. Identifying how a data compromise could occur and ensuring adequate incident response procedures are in place are key to reducing the risk of suffering from a data breach.

As sponsors of the e-Crime Report 2011, KPMG in association with the e-Crime Congress surveyed over 200 senior security decision makers globally across all industry sectors to explore three key areas. Firstly, their views of the threat landscape today. Secondly, the impact of new emerging technologies and business models on the level of e-crime risk and finally, how organisations can structure a response to the threat of e-crime.

Managing information and technology risk is now vital to maximising commercial potential

Ensuring the continuity of business operations and protecting sensitive data is not just about how much you spend, but whether you understand your risk profile and spend effectively.

Over the past few years, big changes have occurred in the cyber threat landscape. Recent incidents demonstrate that the emergence of 'hactivism' and the increased prominence of state sponsored cyber attacks have serious implications for all industry sectors.

In the recent e-Crime Survey, only 6% of respondents indicated that the overall level of e-crime risk their organisation faces has decreased over the past year. In addition, over 80% of respondents identified that, in the next 12 months, the use of smart phones, social networking, and consumer devices use are set to increase e-crime risk for their organisations.

Managing technology and information risk is now vital to protecting your brand and reputation.

Security, governance and compliance frameworks must evolve to meet the demands of changing business models

Despite having to deal with a constantly evolving risk landscape, information security strategies should still be based around a common framework that delivers the following core pillars of capability: prevent, detect and respond. However, strategies must be structured so that they are sufficiently flexible and agile to adapt as circumstances change.

Threat modelling, risk assessment techniques and an understanding of the threat landscape should be incorporated to provide intelligence that can ensure available resources are targeted to the right areas. It is increasingly difficult to predict the nature and severity of attacks. Testing and updating incident response capability to make sure it is fit for purpose is therefore vital. There is no point in putting your seatbelt on after the crash has happened.

Major changes in the threat landscape make cyber defence a board issue for every organisation

Cyber security is now on almost all board agendas and frequently at the top. Many CEOs at large companies have been briefed by intelligence agencies and have a better understanding of the severity of the threat landscape.

It is important that cyber defence is not just thought of as a security issue or a technology issue. It is at the very heart of how a business builds trust with customers, as well as how it builds and protects brand value. The issues at stake are sufficiently important that the definition of strategy and investment needs to sit with the board. The level of investment needs to reflect business appetite for risk and support business goals. This is still very rare. Heads of Security and CIOs often second-guess the Board's risk appetite and willingness to spend.

Reducing risk, protecting data and securing technology requires a strategic, business led approach

Effective risk and security management frameworks need to be corporate wide, proactive, forward looking, closely integrated with other risk disciplines and have board-level engagement. Approaches that attempt to measure and manage risk in silos will fail.

A successful strategy requires risk, security and technology teams to work alongside colleagues in sales, legal, fraud prevention and crisis management functions, as well as those in charge of procurement, marketing and press relations.

Contents

For any questions or queries please contact jon.hawes@akjassociates.com

Managing information and technology risk is now vital to maximising commercial potential

Information security frameworks are being challenged to evolve. Technological innovations are enlarging the attack surface and placing IT departments at odds with regulatory requirements. The expanding cross-border influence of regional data protection and privacy legislation is increasing the burden of compliance. The range of actors that pose a credible threat to the confidentiality, integrity and even availability of sensitive data has grown to include state sponsored attackers and self-styled hacktivists. In this changing environment, the ability of an enterprise to safeguard electronic assets and IT systems without limiting operational flexibility or increasing complexity will be determined by how risk is managed.

"Meaningful risk assessments on cyber threats can only be achieved by filtering threats through a checkpoint to separate from what is possible that which is realistic, distil what is credible to that which is probable and present that which will cause pain in a relevant context to the business."
Financial Services

"A business does not travel in a straight line; its course will zigzag constantly and once every three to four years as a new CEO is appointed it may change course completely. Security risk management has to account for changing dynamics internally as well as externally."
IT Service Provider

"Too often security in an organisation is like a game of blackjack: there are those that calculate the odds and those that trust to luck. The question is whether those who calculate the odds have influence at the right level of the organisation."
Oil and Gas

A diversifying threat landscape changes the rules of cyber defence

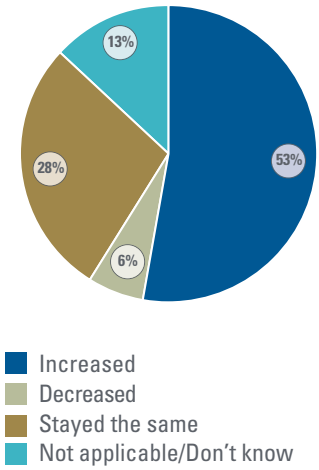
Recent cyber attacks reported in the media demonstrate that organisations need to reconsider their risk profile, reassess how they measure the effectiveness of their information security posture and update their incident response plans.

Tactics and technical tools developed by financially motivated, well organised and well financed crime syndicates are now sold or freely shared and distributed on the internet. As a result, the average level of attack sophistication is increasing. It is becoming easier for groups or individuals with adequate expertise but low levels of resources to bypass IT security defences, gain a foothold within a network and launch an attack.

An organisation's cyber risk profile is no longer determined by the potential monetary value of information to attackers. The threat landscape is made up of many malicious players with different motivations and aims. These players range from governments, intelligence agencies and organised crime syndicates through to geographically dispersed 'hacktivists' who share common social, political or ideological beliefs. Targets may be attacked for actions that are perceived as unethical or undemocratic, (for example in the case of attacks launched by hacktivists), or because of a political desire to gain economic and military advantage, (for example in the case of state sponsored attacks).

Attackers who are not motivated by personal financial gain are likely to be far more persistent in pursuit of a goal. As attackers with this profile become more active in the cyber threat landscape, organisations must firstly reassess their potential as a target based on factors such as the public or strategic sensitivity of information they have access to and who their clients or partners are. Secondly they must improve their ability to defend against attacks that aim to disrupt operations or reduce the ability to generate revenue. Finally they must ensure they can respond to a broad range of malitious activities that include altering database records to compromise data integrity, making changes to the configuration of IT systems or source code, disrupting critical IT processes to halt business operations and extracting specific data such as emails, contracts, or design blueprints.

In relation to the threats your department focuses on mitigating, has the overall level of e-crime risk your organisation faces increased decreased or remained the same over the last 12 months?



"Cyber attacks from organised crime were more predictable because they ran a P&L and basically operated like a business. That is not the case with state sponsored attackers."
Telecommunications

"It's not about just about sophisticated cyber criminals any more. The capability to cut through IT defences like butter is now the domain of teenagers using their parents' broadband connection."
Financial Services

The prioritisation of risk management focuses attention on the 'Crown Jewels'

'Worst case scenarios' are currently rare. However, attacks such as Aurora,[1] Stuxnet,[2] and Night Dragon – not to mention Wikileaks emerging as a wholesale channel for whistle-blowers to disclose politically and commercially sensitive information – demonstrate that there is no cause for complacency.[3]

In a climate of financial uncertainty and instability, security leaders will continue to deploy their resources – whether human or financial – to those areas where they will have most visible and valuable effect. A corollary of this is that protective efforts may be focused on the 'Crown Jewels', those assets that have a high level of confidentiality and competitive or intellectual value.

This brings with it a fresh set of challenges: identifying and agreeing what those assets comprise; finding out where they are located, (there will almost certainly be multiple instances of the same piece of valuable information); and understanding the lifecycle of the assets from creation or receipt through to destruction. It is then necessary to ascertain what processes and functions use the assets, verify who has access to them, establish who should have access to them and work out how changes to business processes may affect all of the above.

The implication of focusing on the 'Crown Jewels' with the aim of directing resources to best effect is that risk management becomes king. Once risks have been identified the options are to mitigate and prevent, or make a conscious decision to accept, a given risk. The quality of the decision that is made will be highly dependent on how well that given risk is understood in relation to the particular operating model, or models, of the business.

Any security plan needs to involve all the elements of protect, detect, contain, recover and, perhaps most importantly, learn. Where low probability, high impact risks are tolerated, response plans should be drawn up to ensure that crisis management involves the right decision makers and that escalation paths are clearly defined.

"Information sharing, a mobile workforce, the use of third-parties, or the awareness and capability of employees 'to do the right thing': the challenges that today's CISO must grapple with are as much driven or dependent on people as they are on technology."

Mark Waghorne
mark.waghorne@kpmg.co.uk
+44 (0)20 7311 5220

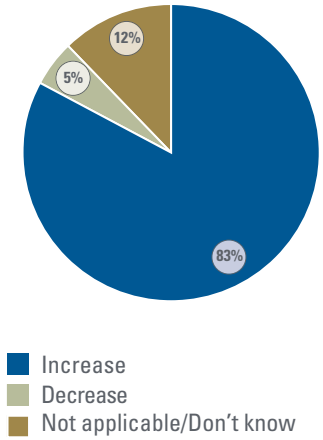
[1] http://www.wired.com/threatlevel/2010/01/operation-aurora/
[2] http://www.schneier.com/blog/archives/2010/10/stuxnet.html
[3] http://www.mcafee.com/us/about/night-dragon.aspx

Forget necessity, technology is the new mother of invention

The success of strategic commercial aims, the extent of operational efficiency and the limits of revenue generation are becoming more dependent on technological factors. In the past, the ability to profit from a growing level of digital interconnectivity was restricted by the market saturation of available technology, its functionality and its scalability. The recent convergence of four key trends, (the mobile workforce, cloud computing, the consumerisation of IT and an array of on-demand, web enabled services), has effectively removed these barriers.

The security, governance and compliance issues that are thrown into sharp relief by these trends are, in their detail, unique for every organisation. In common, they demonstrate two requirements. Firstly, all of an organisation's risk related functions, including information security, must cooperate to provide meaningful management information and risk metrics that can inform business decisions. This will allow executives to effectively weigh up the benefits and pitfalls of emerging opportunities.[4] Secondly, information security stakeholders must help their organisation to take advantage of innovations that enable cost savings and improvements in productivity by charting a course that mitigates technology and information risks without obstructing identified business goals.

Do you believe that mobile employees and home-workers using the same IT hardware for business and personal use will contribute to an increase or decrease in e-crime risk for your organisation?



"The complexity of security challenges created by technology is only increasing. We are still dealing with the problems of five years ago – how are we realistically going to get ahead of the curve to a point where we can deal proactively with things like with cloud?"
Legal Services

"We live in an era of low predictability and changes happen very fast. IT security has had to evolve at the speed of the internet."
Oil and Gas

[4] http://www-935.ibm.com/services/us/ceo/ceostudy2010/images.html

Security policy must be aligned and integrated with business strategy

As business operations evolve and IT delivery mechanisms change, the traditional model of monitoring compliance against policy is struggling to keep pace. The automation of compliance processes through the adoption of governance, risk and compliance (GRC) platforms may go some way to redressing the balance. However, layers of technical complexity designed to enforce policy requirements are of little help if they hinder workforce efficiency.

A more proactive approach that aims to 'build security in' to everyday activities is only sustainable if policy meets the realities of organisational demands. The custodians of IT-based security governance mechanisms must deliver policy that is better aligned to operational needs, identify where the business' direction of travel is at odds with current security practice, help find workable solutions and improve information security posture where it matters most.

Operationalising security
Building security into normal operational capability must become a priority for CIOs as companies will have to drive down its associated costs. Where that means outsourcing parts of security operations to lower total cost of ownership, it also means ensuring the competence of service suppliers.

Building from secure components, rather than "inspecting security in"
A move towards secure architecture can reap benefits by reducing the need for inspection, testing and assurance. This can be applied not just to networks and operating systems, but to the entire application development process.

More efficient management of third parties
Whether through shared compliance assessments or new assurance standards, the importance of getting Service Level Agreements and Master Service Agreements right first time will only increase.

Smarter use of information security management standards
Where compliance with security standards becomes a legally defensible position, managing security is no longer an optional extra for companies looking to protect themselves from liability arising from negligence. Standards such as ISO/IEC 27001:2005 provide a foundation for subsequent fine-tuning and adaptability of risk mitigation, to enable better response to new threats.

"Advances in the consumer IT marketplace are having a revolutionary effect on the corporate landscape. Technical solutions alone cannot solve the security and legal issues that surround cloud computing and the consumerisation of IT. A different approach to policy and IT governance is required."

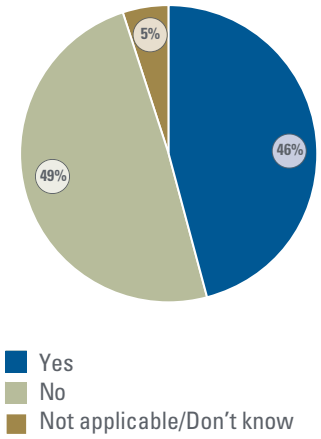
Denis Verdon
denis.verdon@kpmg.co.uk
+44 (0)20 7694 4136

Compliance must do more than 'tick a box' for the auditors

As industry and government bodies introduce further IT and data security regulations,[5] organisations will need to find more cost-effective and less time consuming ways of meeting multi-jurisdictional compliance requirements. In view of the rising costs related to a data breach,[6] it is important that investments in compliance do more than 'tick a box' from an audit perspective. By striking the right balance between effecting business change, redesigning IT processes and implementing technical controls, enterprises can create value from compliance spending and reap the dual rewards of increased efficiency as well as increased security.

To deliver an improved information security and risk management posture from compliance investment, internal stakeholders must join the dots between business strategy, the threat landscape and security priorities. For example, organisations are reducing the time it takes to launch new products due to competitive and financial pressures. As a result, development life cycles for feature rich, web-facing applications are being shortened. This means less time is available for security testing and assurance. Cyber criminals are taking advantage of this, focusing attacks on web applications in order to compromise sensitive data.[7]

Do you believe that the risks associated with cloud computing are fundamentally the same as those associated with outsourcing?



"What is the business appetite for being proactive in terms of security? When times are hard, a refined approach goes by the board. You look at what can reasonably be dispensed with and start asking questions like; 'How could we get the regulators to agree that a solution path, which is the bare minimum, represents a proportional response to their requirements?'"
IT Service Provider

"The CIO has no global vision of regulation. You have to have someone outside of IT to tell IT what they are doing and assess the bigger picture in terms of risk."
Legal Services

"A disconnect between the speed at which controls have been implemented and the competitive necessity of rapid change has created a dynamic whereby security exists primarily to solve an immediate requirement or resolve an incident, rather than to provide a stable basis for growth."
Financial Services

[5] http://www.ft.com/cms/s/0/b09059e4-9b8f-11e0-98f2-00144feabdc0.html#axzz1QTyzz7Qv
[6] http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20110321_11
[7] http://dvlabs.tippingpoint.com/img/FullYear2010%20Risk%20Report.pdf

Is your controls environment in control?

Historically, security policies have been documented and controls implemented in a reactive manner, either in response to incidents or, more likely, adverse audits. As a result they often only serve an immediate and narrow purpose: they tick a box; they provide a compliance green light. But does this mean they have solved the underlying problem? How much consideration was given to the projected lifespan of the controls implemented? What measures have been put in place to measure their effectiveness? What intelligence was used in the decision-making process to ensure and the agility to prevent, detect and respond against future threats? In many cases the answer to these questions is 'little' or 'none at all'.

The implementation of a set of controls is only the beginning. All controls should be given a lifespan. The threat landscape and how it impacts risk profile should be continually revisited and revised. The output from available tools should be used to help shape and define the actions and processes that need to be triggered when things do go wrong. As we conduct more of our everyday business than ever before in digital surroundings and as companies and industries rely on technology in many guises as a critical enabler, regularly measuring businesses risk profile in the cyber domain is essential to establish that the appropriate level of trust is imparted to service providers.

Stay current with developments that may change the level of trust that is acceptable. Use threat modelling and impact assessments as tools in a robust and agile strategy. Focus on implementing the right controls in the right places to counter internal and external threats. External intelligence sources should also be identified and used to inform your decision making. Bear in mind that damage to reputation may outweigh direct financial impact. Media response plans should form a part of any damage limitation strategy.

"Many companies are finding it challenging to monitor and track compliance with existing policies. The federated nature of many IT functions conspires against adopting a process-driven approach. In addition, as platforms and data repositories are replicated, the same protection schemes are not always applied."

Ben Potts
ben.potts@kpmg.co.uk
+44 (0)20 7694 2905

Security, governance and compliance frameworks must evolve to meet the demands of changing business models

To reduce costs, improve collaboration and raise productivity, businesses have a mobile workforce who access data using the internet. Meeting the need for "any user, any content, any location, any time" has led to information being shared between individuals as well as organisations and the interlinking of systems to improve accessibility. These developments expand the attack surface and make it increasingly difficult to comply with internal governance or external regulatory requirements.

"Security is being squeezed in the middle - between the threat environment and the internal environment. We need to evolve constantly just to stand still."
Financial Services

"Off shoring and outsourcing, more and more being pushed to third parties. The disconnect is whether the board see the same risk landscape as those at the operational front line."
Telecommunications

"Most risk management is based on guesswork. You work out what you can afford and you drop the controls you can't. It's amazing how much risk the board and business lines will tolerate when they find out what it will cost to mitigate."
Legal Services

Social media: friends and foes

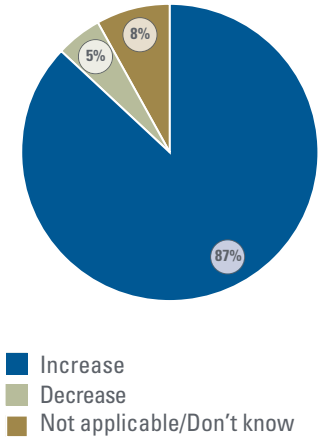
Disclosing the details of recent transactions and purchases using Blippy. Taking advantage of Foursquare's reward culture that offers exclusive deals when users 'check in' to businesses that range from hotels to cafes. Tweeting on just about anything. Professional and personal identities are blurring as individuals publish more and more information online.

Social media applications have entered the mainstream.
The average age of users is increasing and so is their wealth and earning potential. This makes them an attractive attack vector for fraudsters. The future of targeted malware delivery is also inextricably linked to social networking.
As profiles amalgamate information from compatible third party applications, cyber criminals are able to rely on an exploding volume of sources that supply actionable intelligence which can be used in spear-phishing attacks.

Although methods of authentication and authorisation on social networking sites are currently very weak, user levels of virtual trust are disproportionately strong. Executives or their family members are publishing details of current activities and interests.[8] Relationship or project managers are 'linking in' with clients to reveal who they are working with, (potentially breaking non-disclosure agreements). Spear-phishing is likely to become more refined as data mining of social networking sites is automated.

Interest in mining social networks is not restricted to cyber criminals.[9]
The question of whether we are close to 'the end of privacy' will continue to be hotly debated as the volume of personally relevant data held online continues to grow.[10]
The real issue perhaps, is not that users are making decisions in a vacuum of information, but that they are willing to sacrifice confidentiality for convenience.

Do you believe the availability of multi-functional internet-hosted software. (e.g. social networking, webex, webmail, etc), in the workplace that has more advanced or user-friendly capabilities than in-house IT products will contribute to an increase or decrease in e-crime risk for your organisation?



"Just as social engineering makes email a more effective attack vector, the fact that people find using social networks so attractive means that if phishing was bad, this is going to make things a lot worse."
Security Service Provider

[8] http://technology.timesonline.co.uk/tol/news/tech_and_web/article6644199.ece
[9] http://www.newscientist.com/article/mg19025556.200-pentagon-sets-its-sights-on-social-networking-websites.html
[10] http://news.cnet.com/8301-1009_3-10310446-83.html

The mobile workforce…

Mobilisation is achieved by running applications, virtualised or otherwise, on handheld devices. By developing an application that mobilised just one department, a company in the financial services sector built a revenue stream worth over half a million dollars per year. Its success was so significant that after the initial trial period of thirty days the application was classified as business critical.

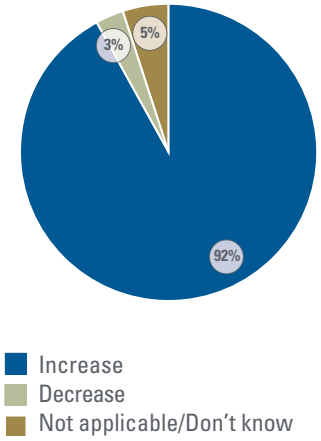
The aim of workforce mobilisation is to maximise both productivity and operational output. To make mobilisation effective, 'usability' must be considered the top priority. With smart phones connecting to the internet as well as interacting with business systems, security policy must be designed to take the following into consideration; as the number of controls increases, the level of usability plummets.

With sensitive information flowing through wirelessly enabled portable devices, they are an attractive target for cyber criminals. Data that can be compromised ranges from calendar and meeting entries through to confidential documents. Technical defences, such as anti-virus, that consume high volumes of processing power or memory are unsuited to devices such as smart phones and tablet computers. Performance reduction from utilising restricted memory also affects the user experience and hence productivity levels. This means risk judgements must be made regarding the pragmatic deployment of personal consumer devices without over-burdening technical security measures.

A number of smart phone operating systems exist in the marketplace. With no likelihood of imminent convergence the advantage of this is that it removes a single target base for attackers to exploit. Nonetheless cyber criminals will likely transfer the knowledge and optimise the techniques that they have acquired while crafting desktop-based endpoint attacks to suit the mobile landscape. The development of custom code to target the most widely used operating systems is a certainty.

As the third party marketplace for mobile applications gathers momentum, it is likely that cyber criminals will create applications that appear legitimate but are in fact malicious.[11] 'Time delay' Trojans are one potential threat in which an initial application download is harmless, with subsequent updates installing malicious code. With devices often running a mixture of third party and corporate applications, a key focus for securing the mobile workforce must be whether applications are trusted, and how security is certified.

Do you believe the use of consumer oriented IT hardware with internet connectivity, such as smart phones and tablet computers, for business related purposes will contribute to an increase or decrease in e-crime risk for your organisation?



"Employees now want to interact with software on multiple platforms, smart phones are one example; we are seeing a trend towards a complex endpoint environment with fewer security mechanisms."
Software Manufacturer

[11] http://www.csoonline.com/article/680919/ca-discovers-fake-antivirus-smartphone-app?source=CSONLE_nlt_salted_hash_2011-04-29

…meets the consumerisation of IT

Configuration management and application policy must not interfere with the user experience. Technology is available to consumers that surpasses the functionalities of that which is available in the workplace. 'Lock down' (the creation of a highly restricted environment) will not encourage employees to make full use of business-issue mobile devices. If anything, it is likely to drive consumers to use their own devices for business purposes – a trend widely referred to as 'consumerisation' or 'bring your own device', (BYOD).

The BYOD trend creates a number of risks, but one company's research suggests it also offers an opportunity to enhance security. A poll of 10,000 employees revealed far more corporate devices were lost each year than personal devices. It also found that the upper age limit of personal devices averaged eighteen months. This therefore represented the worst-case scenario in terms of a failure to apply security patches.

The results also demonstrated that employees wanted to keep company data on personal devices and did not want the company to control them. The ability to use personal devices for work purposes meant many employees were prepared to add security functionality to their devices, which they would not have done otherwise. Users wanted the IT department to help them to do this. Also, they were happy to provide IT support themselves via a forum with corporate IT as a partner rather than a single port of call. This meant employees could be moved away from the IT helpdesk and assigned more productive tasks.

Any BYOD programme needs to involve stakeholders such as HR and Legal. It should also cover regulatory issues such as e-discovery requirements. While data synching between corporate and personal machines can be controlled with existing technology, an 'end user licence agreement' should clearly define employee responsibility for backing up data in case a device has to be taken from them for any reason, as well as the parameters of who is liable for replacing the device. Actively engaging employees on the subject of using their own devices for work purposes can provide security departments with invaluable information on usage patterns. The potential benefits of adding log management on employees' personal devices may, in time, also allow security departments to assess whether particular areas of a business are being targeted by electronic attacks.

"What is your acceptable use policy? Do you have the right to forensically analyse the device. Who owns the data? The legal questions are the hardest and internal legal teams may not know the answers."
IT Hardware Manufacturer

"It's virtually impossible to ensure a fleet of iPhones are kept up to date; you can't control patch management short of bringing in every device. You have to change your perspective. We shouldn't be afraid of taking risks just because there is no security solution out there that we can apply."
Food and Drink Manufacturer

Cloud: eating from the forbidden fruit?

The nature of a 'true' cloud suggests the concept of dynamic data transit, storage and processing[12], in which information is transfered and replicated between virtualised, geographically dispersed data centers. Processes may also move as computing resources are allocated on the basis of available capacity. This enables workloads to be scaled up and down on demand. While there are a wide range of issues that should be carefully thought through by any company moving data or processes out into the public cloud, sometimes referred to as 'Outsourcing 3.0', the potential regulatory implications are likely to be a key area of concern for large, global organisations and particularly those in the banking and finance industry.

Where regulated data moves from one location to another in a public cloud, it would cross a number of jurisdictions and be subject to a range of potentially conflicting laws, making compliance complex at best and at worst impossible. Some laws, (for example the European Data Privacy Directive), place restrictions on the movement of personal data. Moreover, legal definitions of what constitutes personal data vary widely on a global basis. Encryption is widely used as a solution for complying with requirements to protect customer data, and some cloud providers are already investigating ways to use encryption in order to satisfy privacy or data protection regulatory bodies.[13]

In view of the locations in which data may be processed, transferred, or stored – either in the cloud itself or on backup tapes – laws that govern encryption and decryption should be carefully considered. These include restrictions on key strength, requirements that cover 'removable media', (including back-up tapes), and key protection requirements that exist to safeguard against disclosure of personally identifiable information. For example, Indian law requires that encryption keys for data held in the country are provided to the telecommunications ministry; the RIPA Act in UK law states that if data is transferred into the country, the encryption keys must be handed over if demanded; Russia has restrictive controls on which encryption solutions can be used, as technology cannot be legally deployed if it is not available for purchase in the country.

For those that operate in a highly regulated environment, the ability to secure information may not be enough to satisfy compliance requirements. The concepts of the public cloud imply the reuse of storage space by multiple parties. Banking regulations regarding information security generally require systems that hold sensitive data to be cleansed to a level that in some cases requires storage devices to be destroyed. Questions as to how this might be achieved by on-demand service providers serving thousands of customers lead to further questions about how auditors, internal or external, might verify that all instances of data – including data remnants that may remain in slack space - have been wiped, not just deleted.

"Currently about 80% of what we do is bespoke, 20% is standardised. We and other cloud providers I speak with, are trying to change that."
IT Service Provider

"When reporting to regulators, log files may have to be provided in a specific format. European regulators have been known to demand logs in Central European Time for servers based in the UK. Whether cloud providers themselves could, or would be prepared to action this, if regulators demanded it is an unknown quantity, but in multi-tenanted environments the answer if clients asked the question would almost certainly be 'no'."
Financial Services

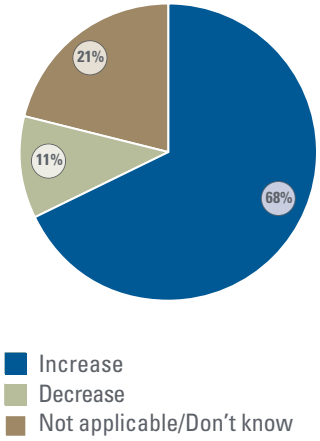
[12] http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
[13] http://www.nytimes.com/2010/09/20/technology/20cloud.html?pagewanted=1&_r=2&th&emc=th

Cloud: eating from the forbidden fruit?

For some organisations, the costs of governance may outweigh any decrease in capital expenditure that cloud provides from a pure IT perspective. Internal and external audits may require evidence of system integrity, an impossible task if cloud suppliers are not willing to let customers access their systems. Some organisations in the investment banking industry are subject to strict regulation that requires them to list very specific data inventories. This necessitates a deep understanding of data flows that must then be explained to auditors. However, data flow is radically different in cloud environments and data lineage is not possible to audit. The movement of certain information may even attract financial penalties when archiving data across Europe and globally. If data relating to a transaction crosses a regulatory border, it could attract an additional tax.

While financial regulations in the area of outsourcing focus on 'material' fiscal process, requiring that some use dedicated systems, there are currently no such specific guidelines on cloud computing. The extent to which end users can tie a cloud provider to their governance requirements will be a deciding factor when evaluating which processes may or may not be moved from the corporate data center to the public cloud. For example, the risk of a system blackout on sensitive dates caused by large updates or changes to operating software means many organisations tightly restrict these activities through change control procedures before the end of a financial quarter or at year end. Similarly, in a 24/7 global finance business, markets typically have to close in US before IT updates are executed or maintenance is carried out. Cloud providers with multiple customers are unlikely to be able to meet competing demands from clients with different financial and operational cycles.

Do you believe that the opportunity to transfer data or layers of IT infrastructure to outsourcing or 'cloud' providers whose services are accessed by the internet will contribute to an increase or decrease in e-crime risk for your organisation?



"When considering that one cloud provider currently has 500,000 servers, while hygiene is an issue it is also a reality that some data will be exposed. With buyouts and acquisitions in the cloud space it is not only the size of existing server farms that may prove challenging; one company inherited 10,000 servers from the original 500 that they managed."
Audit and Accounting

"We have thousands of customers. Can you imagine letting each one audit us? We would have multiple audit parties in our facilities and systems every day. That in itself is a security risk."
IT Service Provider

Major changes in the threat landscape make cyber defence a board level issue for every organisation

The ability of attacks to pass under the radar of defence mechanisms indicates a tipping point is approaching in the battle to secure data and maintain continuity of operations. Evolutions in the cyber threat ecosystem, both in terms of the actors involved and the technical sophistication of attacks, have amplified the limitations of traditional IT security control frameworks. There is growing recognition that in the case of targeted attacks it is neither possible to defend against every eventuality, nor realistic to eradicate all those vulnerabilities that may lead to an incident.

"Corporate endpoints are now in the line of fire as well as those belonging to end users, although with mobilisation and consumerisation those may be one and the same. We are seeing malware normally thought of as password stealing going after intellectual property. Attacks wait for users to browse before exfiltrating traffic to escape detection. Things are getting a lot worse, but then again we tend to see the bleeding edge of what is coming down the line because of who is targeting us."
Oil and Gas

"Investment priorities are shifting to bolster the capabilities to 'detect' and 'respond' with the aim of minimising the impact of an event when it does occur, rather than fighting a losing battle to completely negate the risk of compromise."
Oil and Gas

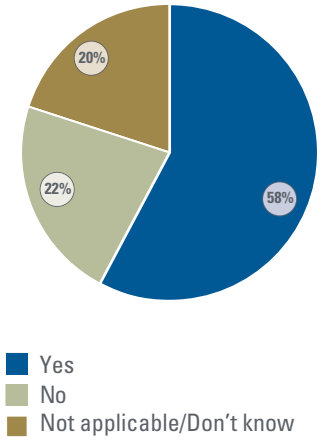
High rollers are raising the stakes in attack sophistication

Organised crime syndicates are motivated to develop commoditised, mass-market attacks that are repeatable, automated and deliver a regular financial return on investment with low risk of capture. Governments do not work to the same model. State sponsored attacks, (also referred to as Advanced Persistent Threats or APTs), are developed so that they cannot be conclusively traced. They are designed for micro-distribution and are only deployed against a narrow range of targets, thereby minimizing the chance they will be detected. Return on investment is measured in strategic rather than purely financial terms. They also have access to significantly greater levels of financing for research and development.

As nations continue to compete for economic and military advantage in cyber space, major changes will occur in the cyber threat ecosystem. Organisations that are regularly targeted by APTs will respond to attempted or successful intrusions by constantly improving their defences. The ability of APTs to infiltrate IT systems and remain undetected while an attack is executed will therefore require continuous and escalating investment. The result of this is that malware developed with government funding will be capable of bypassing all but the most advanced security technology. If such malware becomes available to less sophisticated players, they will capitalise on its capabilities by integrating them into mass-market attacks used by financially or ideologically motivated attackers. Reportedly, some governments already interact and pool resources with experts in the cyber criminal underground.

Stuxnet is the only example in the public domain of malware that is specifically designed to disrupt a narrow range of operational processes within SCADA systems. SCADA systems are complex and are used extensively by critical national infrastructure to monitor and control industrial processes. Stuxnet's development would have required a significant degree of planning and access to experts with specialised technical knowledge. Estimates cited in the press suggest it cost between $5 to $10 million.[14] This may not be unrealistic. Stuxnet's design demonstrated an unprecedented level of technical complexity. It combined four zero day exploits, (vulnerabilities in computer code for which a patch is not available). It was also designed to spread and remain undetected within well-defended targets that were not connected to the internet.[15]

Do you believe that prioritisation challenges exist within your organisation between the need to maintain service levels and the practicalities of detecting e-crime incidents that your department is responsible for mitigating?



Attacks such as Stuxnet currently represent examples of extreme outliers rather than the norm. However, the prioritisation of cyber defence at national and supranational level acknowledges a significant change in the levels of investment that attackers will be able to rely on and consequently their capabilities to compromise the security and integrity of critical systems and data.

"If cyber criminals get hold of Stuxnet they will try to reverse engineer it, so extrapolate the capabilities of Stuxnet forward and think 'Just how bad could it get if something this sophisticated was in the hands of your average bad guy?'"
Transport and Logistics

"Compared with DIY online fraud kits that retail for $200 - $400 the cost of Stuxnet demonstrates a huge differential in the resources that may now be directed at compromising electronic targets."
Security Service Provider

[14] http://www.newsweek.com/2010/10/04/stuxnet-worm-latest-attack-in-growing-cyberwar.html
[15] http://abterra.ca/papers/How-Stuxnet-Spreads.pdf

Predictably unpredictable

Coined recently by Nicholas Taleb in his 2007 book,[16] the 'black swan' event is the occurrence that while considered highly unlikely or even impossible based on our current knowledge nevertheless does occur. These events, caused by 'the unknown unknown', come by surprise but are rationalised with hindsight. It's common to find that given their perceived improbability, such risks are simply accepted or ignored. Despite the fact it is without precedent, Stuxnet underlines the importance of spotting trends and creating frameworks to manage them.

Governments continue to develop offensive cyber capabilities that aim to infiltrate, exfiltrate and disrupt. The development of highly sophisticated malware code by state-sponsored organisations has the potential to radically affect the speed at which the wider threat landscape evolves. Reportedly malicious software designed by one APT for espionage has been through four development cycles, with testing at national level.

Politically or ideologically motivated attackers may not in the past have had access to high levels of expertise, resources or investment. However, that status quo is likely to change as advanced malware designed for targeted attacks filters down into the wild, reaching a wider community of cyber criminals and hackers. As the number of potential targets in terms of people, assets and operations consequently expands, the rules that have previously defined how organisations assess where risk resides will no longer be adequate.

Failure to consider a threat vector will inevitably translate into an inability to respond effectively. The problem is how to quantify the impact of the highly unlikely. To establish a basis for accepting, transferring, or mitigating a risk, the level of threat must be understood, analysed and evaluated. But how can organisations prepare for the highly unpredictable?

Standard corporate risk management processes are simply not designed to deal with black swan events. Security professionals need to learn from past proof of concept events that have demonstrated an approach is ineffective. They must be prepared to change course. Balancing the mitigation of threats with operational business needs necessitates a dynamic approach to managing risk. Recognition must exist at the highest level of the requirement to provide a mechanism for dealing with the unexpected.

"What would a black swan event look like in the security world? Disruption of critical national infrastructure or even the Internet would certainly rank high in business impact terms, especially for those invested in cloud services. It's not easy to expect the unexpected but we can be prepared."

Jamie Travis
jamie.travis@kpmg.co.uk
+44 (0)20 7311 1779

[16] N.N. Taleb, The Black Swan, Second Edition, Penguin, 2010

Targeted attacks poised to enter the mainstream

Previous evolutions in the threat landscape demonstrate that cyber attacks which rely on a broad range of compromise create the conditions for those that follow to be stealthier, increasingly automated and more targeted. As malware becomes more sophisticated, malicious players who control large networks of infected computers (botnets) may be able to harvest intelligence on the systems that are connected to infected devices, narrow down who those systems belong to and profile the defences that are in place. The segmentation of infected devices based on such criteria would pave the way for the automation of attacks designed to target highly specific information in a narrow range of organisations, such as those launched by ATPs.

In the early days of the internet, hackers discovered that by installing malicious software on large numbers of computers with connections to the internet, it was possible to control those machines remotely and launch DDoS attacks that could disrupt websites and other web-facing business applications. When anti-virus software (AV) was made available to protect computers from infection, new techniques were developed to ensure that malware could be installed, evade detection and remain active even when users regularly updated AV.

As online banking and retail services attracted more customers, attackers created new types of malware that allowed them to carry out a wider range of remotely controlled malicious activity once a computer was infected. For example, as fraudsters migrated to the online environment, 'man-in-the-middle' and 'man-in-the-browser' (MITB) attacks were developed to target individuals using specific services delivered by specific organisations. MITB attacks automated the theft of funds from bank accounts accessed over the internet by identifying when a user visited the website of a specific bank and hijacking money transfers.

'Drive-by downloads' automated the process of infecting computers and botnets grew in size to include desktops, laptops and servers that were used by businesses and government departments. Attackers programmed malware so that it could be updated with new functionalities, allowing them to repurpose a single point of compromise. This meant they could extract value from a device, regardless of whether malware had infected a virtual server or a laptop. Depending on the type of device that was compromised, a single malware infection could then be used to record and transmit keystrokes, infect other systems or devices, or search for, encrypt and then extract specific types of data or documents containing key words or phrases.

"Looking beyond the challenges that Web 2.0 has posed for the security industry the advent of Web 3.0, or the semantic web, is likely to bring with it more content, more content types and more chances of infection."
Security Service Provider

"You have the 'mass market' threats and then the highly specialised jewel thief of the cyber underground. The two are linked. For example, within a botnet of thousands of computers, some devices will give access to organisations in a particular industry sector, a few of those will belong to people with the right level of influence and a few of those will have access to data being targeted. As cyber criminals harvest intelligence on the infected devices they control, what we current see as micro-distribution attacks will become far more common."
Oil and Gas

Fortune favours the well prepared

With threats from hacktivists, state sponsored attackers and organised crime syndicates the outlook may seem challenging, but should not be viewed with gloom. There are many things, often basic and inexpensive, that organisations can do to protect themselves and make sure they react effectively in the event of an incident.

1. Implement a well-documented, well-understood and embedded incident management plan in advance. Creating one 'on the fly' during a time of crisis is a sure-fire recipe for disaster. The plan must highlight paths of escalation and detail the circumstances in which they need to be activated.
2. Undertake a refreshed risk assessment at predetermined intervals. This should help identify and keep track of the information, systems, infrastructure and processes that are critical to your business.
3. Ensure that you deploy patching procedures, especially on key or 'at risk' systems. Staying up-to-date lessens your vulnerability to known exploits.
4. Consider the implementation of software version control. This is relatively easy to do for important systems where executable code is static and may be important when trying to identify the presence of malware.
5. Maintain up-to-date, multi-layered anti-malware defences. Have a response plan for what to do when infections are detected beyond closing the single door that allowed a compromise to occur.
6. Thinking beyond technical platforms. Consider the use of open source intelligence to identify whether the business is indeed a potential target. This could provide an early warning of possible attacks and their likely source of origin.
7. Don't forget about people. Protecting information assets should be as much a standard, embedded process for all employees as any other fundamental business process. Investing in awareness and changing employee behaviours can bring a great return.
8. Identify key third-party suppliers, verify that they are protecting information adequately and make sure robust processes are in place to verify that suitable controls exist.
9. Develop a security roadmap that accounts for business technology. Think about consumerisation and whether partitioning a 'work' module and a 'personal' module on a single device may be a starting point. Think about the cloud. Making data architectures and applications 'cloud ready' now may avoid a nasty surprise or reengineering in the future if, or more probably when, data and applications end up there.
10. Last but not least, don't try and go it alone. Legal, HR, Risk and Public Relations can provide great support and advice about what to do in the event of an incident. Make sure a plan is in place for when and when not to; go public; disclose to regulators; involve law enforcement.

"In addition to working with colleagues in fraud prevention, legal and crisis management, the age of new media means that information security stakeholders must also engage proactively with PR and corporate communications."

Mark Waghorne
mark.waghorne@kpmg.co.uk
+44 (0)20 7311 5220

Managing risk, protecting data and securing technology requires a strategic, business led approach

Companies compete in a highly interconnected world and must balance an increasing number of priorities. As technology drives an unprecedented rate of change, the speed at which opportunities and risks are being created is accelerating. To maintain competitive advantage, organisations must question the extent to which they are resilient to the impact of the unexpected and improve their ability to adapt in the face of a horizon that is shortening internally and externally.

"As security evolves into a business discipline the less it becomes about technology and the more it becomes about identifying trade offs in risk, which is only possible with visibility into risk. This requires 'security' to be integrated into decision making processes from the start."
Gambling

"You can't go to the board and talk about a 'rare but expensive' event and hope to get budget. Because they will ask you 'how expensive?' If you can't quantify that in money then you are not speaking the language of business. If it's less than 10 million, it's a rounding error. That makes you rethink risk."
Insurance

"Avoid fire fighting. If you have fire-fighters in your security organisation then beware – you are breeding arsonists."
Media

"You can spend a lot of time thinking about unknown unknowns, I'm interested in the known knowns and why they are not fixed. Getting the basics right is essential before you start to think outside the box, so show me the problems that are high probability, high risk. When it comes to high risk, low probability black swan events it's about how you respond to them, not how you prepare for them."
Financial Services

On an effective risk management framework…

"A single common risk management structure should be in place covering the entire organisation, with clearly defined roles and responsibilities including; a risk assessment process, which is both consistent across all risk areas and the organisation; policies, standards and procedures developed and implemented to ensure that all identified risks are managed within the organisation's risk appetite; a process for the regular monitoring of risk management processes; a process for regular risk reporting to executives and to the board, with facilities to enable the assimilation of feedback into the risk processes; and a process to communicate risk information to the organisation's stakeholders."

Telecommunications

…and charting the journey to success

"Once you know where you are, you can work out how to get to where you want to be and you can prioritise. Mapping and documenting the relationship between assets, business processes and technology to understand what comprises sensitive enterprise assets and business critical operations on a holistic scale is a good place to start. That helps with working out what is at risk and what the impact of an incident would be. You can then start a planning cycle to achieve change. Focus on key cost areas to identify where and how you should be spending. Don't start off on a course that does not account for the global ripples of innovation – security can't say no anymore, it has to provide a workable solution that won't slow things down. If you are seen as a department that slows things down, people won't come to you and ask for your help."

Financial Services

The primary goal of most businesses has always been to identify opportunities that enable them to maximise profit and shareholder value. Inevitably this means decision makers are willing to accept risks in order to extract the maximum reward. In some industries the levels of risk that a business is willing to accept are significant.

Historically the primary goal of a security strategy has been to implement programmes of work that 'maximise' the security of an organisation, with decisions often made in isolation of business direction. Unsurprisingly, this caused conflict with business lines who felt security was an inhibiting factor to 'getting things done'.

Modern CISOs will not be thanked for enforcing controls that limit the ability of the business rapidly to expand services or provide new functionality. Closer alignment with the business enables a greater understanding of opportunity risk. In turn this leads to solutions that are built with greater agility, flexibility and scalability such that investment in a specific control or set of controls does not prevent the business missing out on revenue generating opportunities.

Richard Meal

On risk management metrics…

"Enterprise governance functions must evolve the frameworks they use so that they are suitable for monitoring a vast range of business impacts caused by regulation, globalised business models and so on, some of which are tied to factors outside the traditional scope of the corporate environment. They also need to measure the effectiveness of controls and often that is done not by looking at what you can measure – statements about the number of hits on a firewall are pointless - but asking what you want to prove. Start off with a range of questions and then prove or disprove them by interrogating stakeholders."
Legal Services

…and the value of audits

"You get a lot of people doing security who aren't really doing security, they are auditors. How does an auditor know your risk? You can use standards to help, but remember that their maturity is at a very, very early stage. Accountancy has been around for decades and the audit standards there are still being tested. Compliance needs to be tied together to ask what it means for your business. Otherwise you can fall into an activity trap of doing things for the sake of it, or to appease the regulators. Being highly compliant but useless at risk is hardly the ideal outcome. Neither is compliance at the expense of the user experience – internal or external. That won't wash with business process owners. Resolve risk rather than ticking a box for the auditors – although audit should dovetail with your strategy. Look at how compliance can be used to improve business efficiency. The key question is whether what you are doing is effective, otherwise it is the activity trap."
IT Service Provider

The modern world is moving faster and changing direction more frequently than before. Businesses need to build strategies that are more agile, responsive and flexible in order to maximise revenue generating opportunities. Security strategies need to keep pace with those changes to support emerging technologies, be able quickly to adapt to changes in the threat landscape and clearly identify how those changes impact the risk exposure of the business.

In the past, security was a difficult sell internally and getting airtime with board members was nigh on impossible. The increase in cyber criminal activity over the past twelve to eighteen months, coupled with the global media frenzy surrounding data breaches, means the visibility of these incidents and the associated consequences have better visibility in the boardroom and at executive level today than ever before.

Senior security professionals must take advantage of this to make their strategy more visible, gain the right support and work with the business to document risk assessments, detail the impact of a breach, then present the findings to executives.

Paul Hanley

On challenges and hurdles

"Security has to be in the line of business traffic in order to be effective. It has to be embedded. Inclusion in the change control and change management (CM) template is one of the 'holy grails' for security. If there is no security box to be checked in the CM template, then security will always be a reactive force. If this is the way things are, it could be that a business has too high a risk appetite, or maybe does not fully understand its technology risks. The issue security has to deal with is that in the mind of a business the threat landscape is to an extent academic. Boards look at risk in general. Technology risk is somewhat esoteric to them and it takes a skilled risk manager to translate technology risk into something the board can relate to and understand. Sure, a company can have audits in place but who has the incentive to care about the results? You can do risk assessments, but most IT risk assessments fail to be meaningful because either a) there is no simple way of reporting, then the guy who communicates with the board oversimplifies or b) you have a risk manager who can talk to the board but knows little about technology and if that is the case information on technology risk tends to live in a lower level of the enterprise. Ultimately, everything is a choice about risk apart from regulation. Regulation is an incentive for the board to care about security. You have to comply in order to do business and so the business has no choice. Certain provisions included in regulation that touch on technology risk and security can be seen as necessary best practice and a lowest common denominator for security measures."

Gambling

'Security as an enabler' is an over-used term. However a successful security strategy must now be clearly aligned with – and traceable back to - the goals and strategies set out by the business. It must also be informed by regulation and the rapidly changing threat landscape. It must be based around embedding controls that minimise risk exposure to the business, maintaining that exposure at an acceptable level in line with the business risk appetite and be supplemented with robust controls and processes that can be invoked should incidents occur.

It is essential that security has a strong alignment with and affinity to, the lines of business as well as IT functions. Risk assessment methodologies need to be aligned in such a way that the identification and measurement of risk is consistently applied and the subsequent articulation of that risk is easily translated to business and technology managers.

A well-governed and understood risk acceptance process is essential to underpin and support any decisions made by the business. This risk identification and acceptance process must take into consideration the value of the opportunity in terms of revenue generation, the capex and opex cost of introducing controls to mitigate a risk and the cost to the company in the event that a breach occurs, (including direct and indirect financial losses).

The manner in which residual risks are articulated should be modified depending on the audience and the role of the individual who has responsibility for accepting and signing off risk on behalf of the business. For example a Finance Director may not understand the implications of SQL injection if the risk and impact is written purely for a technical audience.

Ben Potts

On an effective philosophy…

"Focus on understanding values and mission-critical processes. Fuzzy terms like 'reputational risk' are only real once you've experienced customers leaving you or no one wanting to do business with you. Until then they are unquantifiable. Look at recent breaches and ask some critical questions through the eyes of the business. What was the financial impact on sales and share price? What was the level of customer churn? What was the impact on sales for the next quarter? You can talk to the board about trust and 'the terrible impact' of a breach, but there are organisations out there who lost massive volumes of data and had their names on the front page of the news whose share price is higher today than it was before they were attacked. The real cost to businesses due to an incident is the downtime; having to shut down systems and servers; taking time to do the investigation; pulling IT off projects that make money; the call centers dealing with complaints. For the leaders of global business, profit is the mile stick by which the relevance of change is measured and change is nothing new. Shift your frame of reference and look at what slows profit – not whether an incident is going to cost you less than your CEOs bonus – and then ask yourself some searching questions about how you contribute to the bottom line."
Financial Services

…and navigating change

"Proactive horizon scanning, yes, sure, but also because of the pace of change and the unknown, you need to build in an adaptive capacity. You can't plan for every variable. A strategy of 'prevent, detect, respond' is too simplistic. Consider a wider range of mitigation strategies as part of broader risk management process – this will help better plan investment options."
Financial Services

Measuring the success of a security strategy is not always simple to achieve. Many controls are implemented as an 'insurance policy' and assigning measurement criteria to the effectiveness of controls is not straightforward.

A successful approach is to understand what elements within a reporting dashboard really answer the "so what?" question at board level. Base-lining current state really helps to bring a problem to life for stakeholders and makes it easier to then track and evidence improvement through the implementation of a strategy.

To prove beyond doubt that a problem is not just theoretical, run a series of pilots that capture and analyse data in live environments. Not only does this approach prove the existence of a problem, it indicates the scale of the problem and provides a clear baseline against which to measure improvement when industrialising these controls across the enterprise.

Other areas that are easy to evidence include items such as cost savings introduced through the simplification and automation of complex and manually intensive processes or the reduction in online fraud through the introduction of fraud and transaction monitoring controls to risk assess each high risk transaction.

Whatever decision is taken, it must answer the "so what?" question and be presented in a manner that means something to senior business executives as well as technology executives.

Ben Potts

On threat assessments…

"Threat forecasts must be built on frameworks that can anticipate the direction of tomorrow's world and with so many things being uncertain it is inexcusable not to know what you can be certain of – which means really getting to understand the business. Then you need to understand what threats exist, which ones are relevant, how relevance changes depending on decisions you make and what impact they may have. This can only be achieved with a solid understanding of what is valuable and where vulnerabilities lie. The value of the 'what could happen' risk assessment needs to be built on likelihood and impact – not your gut feeling as a security professional. Support operational goals by understanding plausible threats and harm caused. Matching a single control to many threats is not feasible. You need to look beyond tools and think about people and skills."

Financial Services

…and why context trumps technology

"When it comes to security, companies tend to under-invest in people and over-invest in tools. Sure, you need to have tools and some are better than others, but tools don't usually make decisions, or at least not totally unassisted by human judgement. Despite advances in tools, putting pieces of the security puzzle together requires people. A tool can take a lot of time just to configure, six months to a year maybe, and its output still won't make a decision for you. The most important thing you need is people with knowledge of the business, because you can't worry about everything all the time. For example, a vulnerability in isolation does not mean much, although it is good to know of its existence. For example, a software patch that, say, Microsoft calls 'critical' in a technology context may not be critical to your business if all your sensitive applications run on Linux. Context changes the way you judge the severity or level to which your environment is susceptible to a vulnerability. Just taking 'the IT view' is likely to lead to over-reaction or under-reaction; you have to establish business context to drive efficiency. This is much more challenging if a business operates in silos, which are harder to coordinate and increase complexity. De-siloing also means you can make better decisions about how technology adds value and whether products that you evaluate are compatible with others you are using."

Gambling

Despite having to deal with a constantly evolving risk landscape, information security strategies should still be based around a common framework that delivers the following core pillars of capability: prevent; detect; respond (to include contain and recover); and learn (to include analyse and adapt). They must be structured so that strategy is sufficiently flexible and agile to adapt as circumstances change.

Threat modeling, risk assessment techniques and an understanding of the threat landscape should be incorporated to provide intelligence that can drive and shape the split of investment across the core pillars of strategy. The level of investment must be commensurate with the business appetite for risk and support business goals.

Whatever the accepted split across these pillars, they must be underpinned by appropriate investment in people, process and technology. The level of investment must be commensurate with the business appetite for risk and support business goals.

Finally, by ensuring that you work with the business to define a strategy, implement an adequate set of controls and processes across the enterprise and have those supported by a robust risk acceptance process, you will find yourself in a defensible position with key stakeholders and executives when an incident or compromise occurs.

Paul Hanley

Glossary

Botnet
A network of computers controlled remotely by malicious software that is installed on the computers

Cloud computing
Processing power, storage, software or other computing services delivered over the internet as a commoditised service

Data Mining
The automated identification or collection of data based on key words or phrases

DDoS
An attack launched using a botnet that makes a system or application that is connected to the internet unavailable to users

Drive-by download
A process of installing malware on a computer that does not require any action on behalf of the user and takes place without their knowledge

Encryption
A data security solution that converts information into a string of numbers and requires a user to have access to 'keys' that can reverse those numbers to display the original information, a process called decryption

E-discovery
A process that requires specific electronically stored information to be identified, collected and presented, usually in response to litigation, a regulatory enquiry, or internal investigation

Malware
Software that is written and designed to achieve a malicious goal

Man-in-the-middle attack
An attack in which internet communications between one computer and another are intercepted by an unknown third party who is able to see communications that are sent between those computers

Man-in-the-browser attack
An attack in which internet communications between one computer and another are intercepted by an unknown third party who is able to change the communications that are sent and received by the browsers used by those computers

Patch
An update to existing application code that fixes an error in the original code

Phishing
The mass sending of emails with fraudulent or criminal intent to an list of recipients unknown to the attacker

Public cloud
Computing services that are dynamically scalable, typically delivered on a shared platform used by other individuals, and billed on a 'pay-per-use' model

Slack space
Space within a file system used to store data that does not have data stored on it

Spear-phishing
The sending of emails containing content that is created for specific recipients known to the attacker in an effort to infect a machine with malware or gain access to information

SQL injection
An attack that sends malicious commands to a web application in an attempt to access information held in databases that are connected to that application

Trojan
Software that appears to perform a legitimate function but is in fact malicious

KPMG key contacts

Paul Hanley
paul.hanley@kpmg.co.uk
+44 (0)20 7694 5122

Malcolm Marshall
malcolm.marshall@kpmg.co.uk
+44 (0)20 7311 5456

Richard Meal
richard.meal@kpmg.co.uk
+44 (0)20 7896 4220

Ben Potts
ben.potts@kpmg.co.uk
+44 (0)20 7694 2905

Jamie Travis
jamie.travis@kpmg.co.uk
+44 (0)20 7311 1779

Denis Verdon
denis.verdon@kpmg.co.uk
+44 (0)20 7694 4136

Mark Waghorne
mark.waghorne@kpmg.co.uk
+44 (0)20 7311 5220

Methodology

The content of this report, sponsored by KPMG, is based on the results of a survey that was conducted online and at the e-Crime Congress 2011 as well as a series of interviews conducted with senior security professionals working for global businesses.

The e-Crime 2011 Survey was completed by over 200 professionals, including a select group of KPMG's clients. The results reflect the views of a cross-section of information security stakeholders working for departments that include IT, risk, audit, security, fraud, investigations and compliance. Their responsibilities include the design and coordination of strategy, ensuring data is protected from internal and external threats, meeting regulatory compliance requirements and running investigations. Survey data is presented in aggregate.

In addition to the e-Crime 2011 Survey, a series of interviews were conducted with senior security professionals working for global businesses. The interviews were conducted under Chatham House Rules. Quotes from those interviews appear throughout the report and are attributed by industry sector only. They provide a range of insights, views and opinions on the findings of the e-Crime 2011 Survey and the issues raised by respondents.

KPMG and the e-Crime Congress would like to express their thanks to all those that contributed and assisted in the writing of this report.