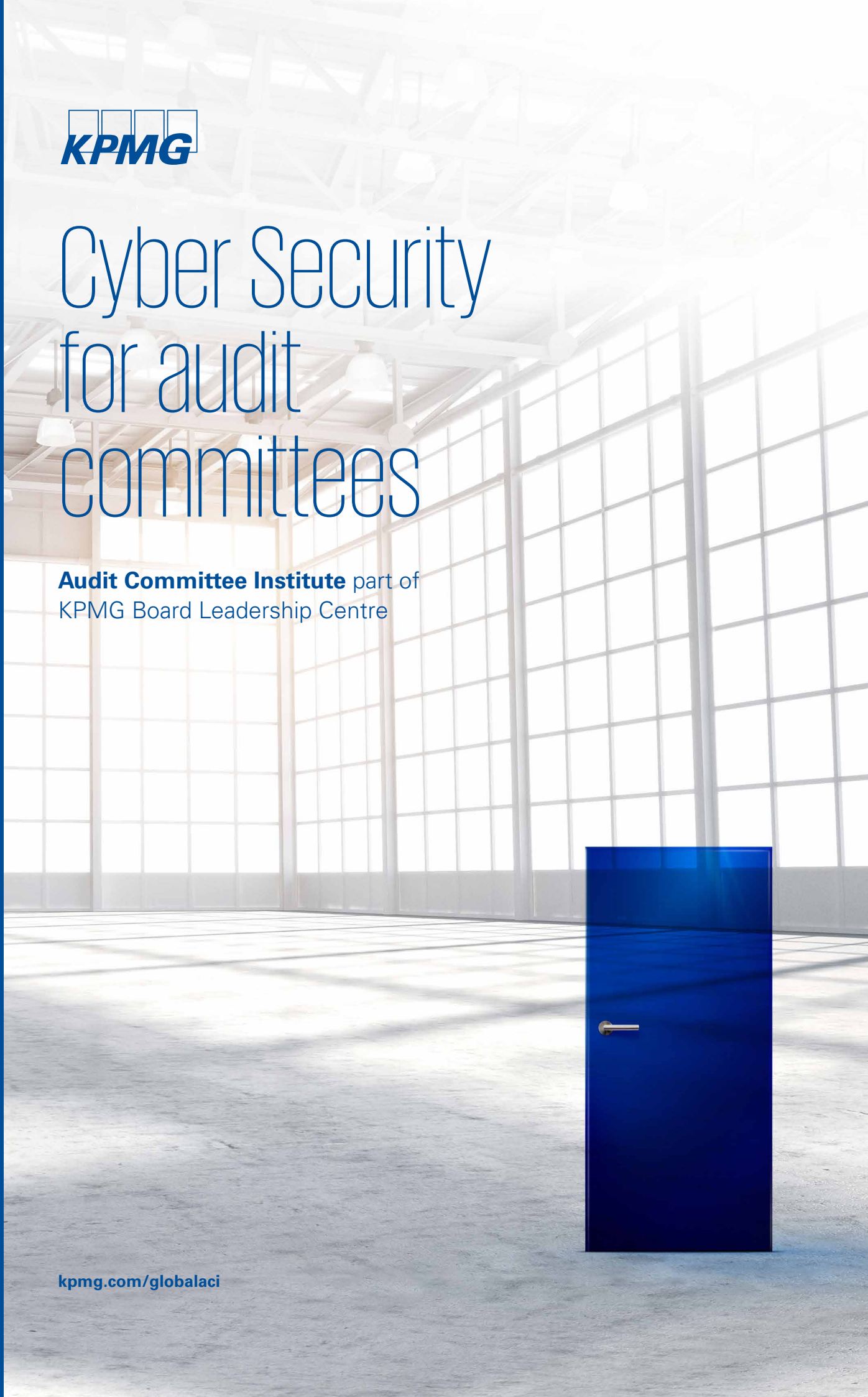

Cyber Security for audit committees

Audit Committee Institute part of KPMG Board Leadership Centre

kpmg.com/globalaci

An introduction to cyber security for audit committes

Audit committees have a critical role to play in ensuring that their organisations have robust cyber security defences – not in understanding the minutiae of the technology involved, but in leading governance and policy. UK Government Communications Headquarters director Sir Iain Lobban has been quoted[1] as saying that business secrets are being stolen on an 'industrial scale' with 70 sophisticated cyber espionage operations a month against government and industry networks. Clearly, this is not an issue where a 'wait-and-see' approach is viable.

This means being able to answer questions such as:

What are the key assets requiring protection?

How are they being protected?

Who is responsible for protecting them?

What level of cyber security risk is considered acceptable?

How would the organisation respond to a major cyber security incident?

If the answers to these questions are not at your fingertips, you are not alone. However, the expectations of audit committees in terms of cyber security are growing.

1 BBC interview July 2013 on cyber attacks at UK firms

What is the threat?

Organised crime has found cyberspace to be a lucrative opportunity. Exploiting vulnerabilities in computer systems allows criminals to compromise and remotely control computers; recording key strokes, monitoring screen displays and manipulating the computer user into divulging sensitive data. Cyberspace allows the attacker to be anywhere in the world, routing their attacks through multiple countries and jurisdictions, complicating investigation and law enforcement.

Malicious employees can also collect large amounts of sensitive company information and remove it easily from company premises; they can also introduce malicious software which can corrupt company databases or sabotage network operations.

Corporate espionage by firms is commonplace in cyberspace. Attacks often target sensitive intellectual property, and there have been instances of major firms having being compromised over many months with large amounts of sensitive data being stolen.

Activism is also commonplace in cyberspace. Sabotage and denial of service attacks are becoming increasingly frequent. In the past they would have been attributed to 'hacktivist' groups such as Anonymous; but increasingly attacks appear to politically motivated.

The potential impact of a cyber security breach

A cyber security breach can impact:

- Financial systems and assets – through fraud, theft and extortion.
- Intellectual property and trade secrets – through espionage.
- Brand and online presence – through public censure, defamation, liability and embarrassment.
- Business continuity – through sabotage or disruption of operations.

What is the role of the audit committee?

Most corporate governance codes around the globe set out that audit committees be responsible for the review of a company's internal control and risk management systems, unless such issues are expressly addressed by a separate board risk committee or by the board itself.

Findings from KPMG's 2014 Global Audit Committee Survey suggest that globally only 38 percent of audit committees currently have primary oversight responsibility for cyber security risks and 45 percent believe the audit committee (or board) doesn't devote sufficient time to cyber security. When asked, to rate the "quality of the information you receive about cyber security," 25 percent of respondents considered it to be good, 43 percent noted that it was generally good but that issues arose periodically and 32 percent said it needs improvement – the highest degree of dissatisfaction of any of the 11 risk areas tested in the survey.

It's not just banks which are targeted by hackers

Cyber security and the increasing focus on audit committees

Governments around the world are aware of the growing importance of cyber security, not only to public sector institutions, the military and organisations which are part of the critical national infrastructure, but also to private sector businesses.

As an example, the UK government has invited all FTSE 350 companies in July 2013 to take part in a 'cyber governance health check'. The health check involves both the company chairman and the chair of the audit committee completing a questionnaire intended to assess how well issues such as protecting intellectual property and safeguarding customer data are managed. This approach is designed to ensure that cyber awareness is an agenda item for the board, not just the chief information officer.

In the US, the Securities and Exchange Commission (SEC) have issued guidance on disclosures of cyber security issues in annual reports. Inviting firms to "disclose the risk of cyber incidents if these issues are amongst the most significant factors that make an investment in the company speculative or risky". Firms are asked to consider the probability of cyber incidents and the magnitude of the risk, including the adequacy of their security controls in the context of their industry sector. The risk statement may also include outsourcing risks, material cyber incidents, risks of incidents being undetected for extended periods, and cyber insurance coverage.

A risk to somebody else

The risk remains that organisations consider themselves a low-value target for cyber criminals and under-invest in protective measures as a result. The September 2013 Norton Cyber Crime survey estimated global cyber crime as costing over US$113 billion over the last 12 months. It's not just banks which are targeted by hackers attempting to steal money, such as the global network of hackers which stole US$45m from ATMs in over 20 countries. The reality is that all companies are an attractive proposition for cyber criminals with a wide range of motivations.

Personal data breaches have become common place. In 2011, a firm announced that personal data of millions of customers had been stolen by hackers – an example of a high profile incident with significant financial and reputational consequences.

Espionage has traditionally been seen as the stuff of James Bond films, but it is now a fact of life for many firms, whether the source of the threat is competitors or state sponsored. Intellectual property is being systematically targeted and stolen through cyber attacks, and not just in the aerospace and defence sector. In February this year, a cyber security firm (Mandiant) published a detailed expose of a seven-year campaign

of cyber espionage targeting over 150 firms worldwide. This is one of many cyber espionage campaigns exposed by the security community over the last two-three years.

There have also been instances of data being stolen on such a scale and damaging IT infrastructure to such an extent that businesses have been close to being shut down. A single destructive attack in August 2012 disrupted over 30,000 desktop computers at a Middle-eastern Oil company.

Companies which are part of the critical UK national infrastructure are potential targets for hostile nations or terrorists. Cyber attacks are becoming commonplace during periods of international tension, with examples of politically motivated attacks against the US, Israel, Pakistan, India and South Korea over the last two years.

'Hactivists', those using hacking for politically or socially motivated purposes, also target businesses, although their aim is typically to cause reputational damage and promote a change in corporate strategy rather than to access financially valuable data or disrupt production.

Organised crime syndicates can also use cyber attacks as a means to hold organisations to ransom. The likes of stock exchanges, betting exchanges, and online trading platforms – and anything else which lives or dies by being available online to customers – are all vulnerable to attack.

Cyber attacks can be mounted against any part of the organisation's business; not just its core operations, but also supporting functions, such as human resources, finance and business development. High levels of automation now mean that computers not only provide our office information technology, but also have an unseen role controlling industrial processes, buildings and infrastructure.

An attacker may also gain access to an organisation's systems through the IT infrastructure of a customer or supplier, or through the home computer or mobile phone of an employee. Organisations going through a phase of restructuring (such as acquisition or merger) may be at particular risk due to market sensitivity, staff morale issues, network reconfigurations and the engagement of external advisers.

Cyber security is not just a technical issue; it is an integrated approach to preparing, protecting, detecting and responding to cyber incidents.

Striking the right balance between security and cost

There is no such thing as absolute security. A well resourced and determined adversary is likely to eventually find a way to defeat even the best security measures, whether the weak point is information security, physical security or people. Each organisation needs to strike a risk balance between defending its key assets against cyber attack and the cost of cyber security measures.

Cyber threats should be considered as part of the organisations risk management and governance framework, with risk registers reflecting the potential risk of cyber attacks on key corporate assets or business processes.

Many organisations develop attack scenarios to test the ability of the organisation to handle a cyber attack. Such scenarios include a description of the motives and intent of a potential attacker, the circumstances in which the attack is carried out, and the techniques used by the attacker.

Boards should be encouraged to think broadly about possible scenarios, and be prepared to use multiple scenarios to test different aspects of an organisation's cyber security.

What does good cyber security look like?

Getting the basics right is important - from technical security measures, such as running anti-virus software or setting up firewalls to protect company networks, to the establishment of a cyber incident management policy, and a broad user education and awareness campaign. These steps won't stop every attack, but could block many.

At the heart of this advice is information risk management – understanding the organisation's key information assets and managing the risks to those assets – a board level responsibility.

Programmes to improve cyber security must take a holistic view of security which includes people, culture, business processes and technical security measures. Cyber security is not just a technical issue; it is an integrated approach to preparing, protecting, detecting and responding to cyber incidents.

Staff can unintentionally represent the greatest source of vulnerability, so education and awareness training is important to reinforce the necessary behaviours. A governance structure to monitor the effectiveness of the cyber security system and an intelligence system tracking cyber threats and helping inform risk decisions are also part of a leading practice approach.

Our insight: today's outlook – and tomorrow's

We are seeing a significant growth in the number of sophisticated organised crime syndicates targeting individuals within organisations to gain access to valuable corporate data. Also, ever-more 'Trojan' websites are being set up and genuine websites compromised. This is done to lure users into inadvertently downloading malicious software, ultimately giving hackers access to corporate networks.

The other big trend is currently state espionage, with long-term intrusions leading to a range of challenges including significant quantities of intellectual property being stolen. The scale of this issue is far larger than many organisations appreciate, due to a combination of a reluctance to directly attribute attacks to nation states and to report security breaches when and if they are identified.

Tomorrow's big challenge, regardless of any new threats emerging, is protecting the ever-greater range of technology, such as mobile devices. How best to secure cloud computing services is also a concern which is likely to grow. Finally, the increasing militarisation of cyber space is a potential issue, and one which could disrupt, and possibly erode value, for other users such as businesses and their customers."

The focus should be on creating greater agility.

Protecting value

There are many ways of providing independent assurance of a firm's cyber security capabilities. A cyber maturity assessment, for example, takes a systematic approach to reviewing a firm's cyber security, from its technical security measures to the overall information risk management and governance framework within which cyber security sits.

Individual security processes and control measures can also be independently assessed, tested and certified. While all of these steps can build confidence in an organisation's approach to cyber security, it is ultimately for the board to discuss and reach a judgement on the acceptable level of risk to their business.

The fast-changing nature of cyber threats means that businesses need to invest, strategically and financially, in order to stay ahead of the criminals. Achieving better cyber security doesn't necessarily mean erecting more and more barriers; the focus should be on creating greater agility, providing the capabilities needed to counter threats as they evolve. It is also important to have the ability to notice when defences are breached, so that damage is limited.

Some companies are taking this issue very seriously and are investing in understanding cyber security risks and adopting a pragmatic approach to mitigating risks. However, others are not, and in doing so are taking a significant risk with the value of their businesses in the widest sense, including the loss of intellectual property to competitors, reputational damage in the eyes of loyal customers and straight forward financial loss.

Cyber security considerations for audit committees

Cyber threats should be considered as part of the company's risk management process, and the audit committee should test whether the company has:

- Identified the critical information assets which it wishes to protect against cyber attack – the crown jewels of the firm – whether financial data, operational data, employee data, customer data or intellectual property.
- Intelligence processes in place to understand the threat to the company's assets, including their overseas operations.
- A way of identifying and agreeing the level of risk of cyber attack that the company is prepared to tolerate for a given information asset.
- Controls in place to prepare, protect, detect and respond to a cyber attack – including the management of the consequences of a cyber security incident.
- A means of monitoring the effectiveness of their cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls.
- A programme of continuous improvement, or where needed, transformation, to match the changing cyber threat – with appropriate performance indicators.

Contact us

Stephen Bonner
Partner
KPMG UK's Information Protection and Business Resilience team

Tel: +44 20 7694 1644
e-Mail: stephen.bonner@kpmg.co.uk

About the Audit Committee Institute

Sponsored by more than 30 member firms around the world, KPMG's Audit Committee Institutes (ACIs) provide audit committee and board members with practical insights, resources and peer exchange opportunities focused on strengthening oversight of financial reporting and audit quality, and the array of challenges facing boards and businesses today – from risk management and emerging technologies to strategy and global compliance.

For more information on the work of the ACI please click on our web site www.kpmg.com/globalaci

www.kpmg.com/globalaci

CREATE | CRT089155 | December 2017