ICAEW INFORMATION TECHNOLOGY FACULTY

Audit insights: cyber security

Closing the cyber gap

BUSINESS WITH CONFIDENCE

icaew.com/auditinsights

Foreword

Audit is a public interest activity. Audit reports build confidence in financial statements and give credibility to companies and comfort to their stakeholders. Companies also benefit from the insight that auditors have into business processes and the wider market environment. *Audit insights* is an opportunity for auditors to bring their knowledge of a market sector or specialist field to the public, capturing more of the audit value for the public benefit.

Audit insights: cyber security is the work of a group of audit experts from the six largest audit firms based on their many years of experience in IT audit and assurance in the UK and internationally, and based on their current involvement in planning and delivering IT audit and assurance engagements. This report provides a further update to the four flags highlighted in the *Audit insights: cyber security* report, published in November 2013 and updated in October 2014.

Executive summary

The importance of cyber security continues to grow as businesses increasingly transform their operations and engage with stakeholders on the basis of digital technology. This update to *Audit insights: cyber security* raises specific issues and concerns that auditors are aware of in the 2015 cyber security environment.

BOARDS ARE STRUGGLING TO HAVE MEANINGFUL CONVERSATIONS ABOUT CYBER SECURITY

Most companies still struggle to join up IT and information risks with wider understanding and management of business risks. This increases the challenge of good decision making about cyber security and undermines meaningful board accountability for it.

The need for clearer accountability is brought into greater relief by the growing emphasis on response and resilience. Businesses need to be able to manage the reputational impacts of major breaches and present clear, senior-level spokespeople who can represent both the technology and business dimensions of the incident.

In addition many businesses have been investing more and more resources in cyber security. At the same time they may be experiencing more breaches than ever before. Therefore, it is right for boards to be asking fresh questions about the value of spending on security, and the benefits that they are getting from it. Security professionals need to be able to articulate the answers more clearly.

BUSINESSES NEED TO TRANSFORM THEIR APPROACH TO CYBER SECURITY

Communication difficulties are symptomatic of the need for businesses to make deeper changes in their approach to cyber security. As cyber security has gone up the agenda, most businesses have added cyber into existing risk management frameworks and tools. However, there are limits to what this can achieve. Many of the steps taken are exposing a much deeper gap in understanding about how cyber security fits into a business. In order to close this 'cyber gap', businesses need to put cyber security at the heart of their business model and focus on becoming a trusted partner in a digital environment.

The need for this shift is made all the more urgent by the growing influence of disruptive technology and the pressure on organisations to innovate and respond quickly to new technology trends, business models and ways of working. However, businesses must manage this in a considered way to ensure that they respond in a proportionate, pragmatic and timely manner which manages the associated risks.

Executive summary

Continued

SUPPLY CHAIN CYBER RISK MANAGEMENT IS A SIGNIFICANT OPPORTUNITY FOR CHANGE

Pressures to transform approaches to cyber security are being particularly felt in supply chain risk management. Many high-profile security breaches have occurred as a result of vulnerabilities in suppliers. As a result, businesses are increasingly looking to gain assurance about the cyber security practices of their supply chain partners. This covers a wide variety of partner organisations, including IT service providers, suppliers of non-IT goods and services and subcontractors.

Getting assurance over the cyber security practices of all suppliers is unrealistic and management needs to prioritise and target its efforts. This means moving beyond the traditional focus on highest-value suppliers to understand where the biggest cyber risks lie. It also requires businesses to build appropriate ongoing assurance processes through the life cycle of the contract, and not rely entirely on the procurement process to manage the risks.

There is no consistent method to supply chain assurance in cyber as there is no clear and single standard to underpin it. As a result, large businesses frequently send questionnaires to suppliers to assess their practices and gain assurance over the risks. But this is leading to significant gaps in meaningful assurance down supply chains. There is a lot of paperwork and obfuscation but it is not necessarily changing behaviour or improving security practices.

Introduction

The gap between the cyber capabilities of businesses and attackers continues to exist. In spite of significant efforts from businesses to improve their cyber security practices, most of them are still struggling to close the 'cyber gap' which was highlighted in the *Audit insights: cyber security 2015* report. In some cases auditors are even seeing businesses going backwards in their practices, as management considers the business has achieved compliance with basic security measures and sees no value in further investment.

The past 12 months have seen many high-profile data breaches. The 2015 Information Security Breaches survey by the UK Department for Business, Innovation & Skills shows significant increases in breaches for all sizes of organisation. These results are supported by many other surveys and anecdotal evidence suggesting continuing high levels of attacks and breaches.

Boards are under pressure to provide greater transparency over cyber risks. As a result of this challenging environment, there is growing pressure for boards to articulate their management of cyber risks better, provide greater transparency over mitigating actions and strengthen lines of accountability. This is aligned with broader moves to improve non-financial reporting in annual reports and other areas of corporate governance.

Improving cyber risk reporting and board accountability is seen by some as a good way of achieving real changes in behaviour and increasing standards of cyber security. It is reflected in a number of ideas and initiatives, such as the evolving Senior Manager Regime in financial services, which will introduce a higher level of accountability for those involved in the management of financial institutions.

In addition, businesses are seeing growing and continually shifting regulatory demands, particularly around personal data. There is evolving EU legislation on data protection and broader network security, which will require the notification of security breaches, among other things. Financial services companies are also particularly targeted, with, for example, the Bank of England incorporating security breaches into general requirements about the notification of significant incidents.

A year of high-profile breaches

Since the publication of the *Audit insights: cyber security 2015* report, there have been many high-profile breaches reported in the media. These include the following cases.

TalkTalk – the company suffered two major breaches in 2015. In October the personal details of a significant number of customers were stolen, with TalkTalk unable to provide a clear description of the extent of the breach. Meanwhile in February, account details of some customers were stolen by hackers and customers were subsequently contacted by scammers with the intention of getting their bank details. The breach was discovered because of a spike in customer complaints about scam calls.

Ashley Madison – in August 2015 hackers published the names, email addresses and other sensitive information related to more than 30m individuals registered with the online dating site. This led to the resignation of the CEO and class suit actions against the company.

Carphone Warehouse – personal details of up to 2.4m customers were accessed by hackers.

Earlier high-profile breaches at the end of 2014 concerned **Apple's iCloud**, resulting in the publication of private photos of celebrities, and **Sony**, resulting in the publication of staff emails.

The impact of these breaches has therefore been wide-ranging, including financial loss, reputational damage and loss of board jobs, as well as the breach of users' and employees' privacy and exposure of customers to potential scams.

Boards are struggling to have meaningful conversations about cyber security

Understanding of cyber risks is disjointed between technical and business functions. All the evidence suggests that cyber security has gone up board agendas significantly in recent years. But, while the technical aspects of security may be known and well understood by specialists, most companies still struggle to join up IT and information risks with wider understanding and management of business risks. This increases the challenge of good decision making in cyber security and undermines meaningful board accountability for it.

Communication is a key barrier to better common understanding and discussion. The language that surrounds cyber security is highly technical and largely impenetrable for the layperson. An important requirement of the chief information security officer (CISO) role is to translate the technicalities into a more business-orientated language, and businesses should ensure that their CISO can meet this need. But such roles are limited to the largest companies. In addition it remains difficult to find the individuals with the right mix of technical and business skills, with training and development in the sector still largely focused on the technical aspects of security.

More work is needed to define organisational structures which support appropriate responsibility and accountability for cyber security. Information security functions have grown in recent years and the biggest issue facing most large security departments is a lack of specialist skills. This is leading to fresh thinking about the most effective organisational structures, mixing outsourcing with in-house expertise to enable access to the required specialist skills, while maintaining sufficient knowledge to manage relationships.

However, in many businesses it remains unclear who is accountable for cyber risks at board level. There are a number of board members who could be accountable, including the CEO, the chief risk officer and the CIO. HR directors have a significant role to play, given the strong cultural and behavioural change aspects of security, as do senior operational personnel. Many businesses are still working these issues out and there is not yet a clear consensus on the best organisation structure.

Non-executive directors and audit committees also have important responsibilities. Broadly speaking, they have improved their ability to ask good, challenging questions of executive management in this area. However, in many cases their ability to understand answers and thereby hold management to account in a meaningful way is limited.

The need for clearer accountability is brought into greater relief by the growing emphasis on response and resilience. Coping with breaches requires organisation-wide capabilities which go far beyond technology and IT departments. Businesses need to be able to manage the reputational impacts of major breaches and present clear, senior-level spokespeople who can cover both the technology and business dimensions of an incident.

This may require the involvement of a CIO as well as more business-focused board members, and it is unclear how many board members today would be comfortable in taking on such a role.

Boards are asking different questions about the economics of security. Many businesses have been investing more and more resources in cyber security every year. At the same time, they may be experiencing more breaches than ever before. Therefore, it is right for boards to be asking fresh questions about the value of spending on security and the benefits that they are getting from it.

Security spending has been traditionally based on identifying the costs of measures versus the benefits of avoiding losses caused by security breaches. Analysis focuses on specific preventative actions. However, organisations are increasingly widening their focus to include intelligence, monitoring, detection and response activities. The profile of security spending is therefore changing to reflect this broader range of operational activities, resulting in different discussions about the value and return on spending. Security professionals need to be able to articulate the answers more clearly.

There are also opportunities for businesses to shift their approach onto the top-line opportunities from good security. This could mean an enhanced brand, based on a strong security culture. It could be the ability to join a particular supply chain and benefit from the opportunity to bid for additional contracts.

There can also be tangible economic incentives for improving cyber security practices, for example:

- financial services companies can use good cyber security practices to demonstrate effective operational risk management and thereby reduce capital requirement; and
- businesses can lower cyber insurance premiums by demonstrating good practices and adherence to industry standards.

New thinking may be required which reflects how cyber risks are different from other operational risks. Many aspects of cyber risks are similar to other operational risks. The impact of sabotaging systems to cause business disruption can be clearly quantified, although the likelihood of it occurring may be harder to predict. The actions required to manage the impact of the theft of personal data are similar to any major PR disaster suffered by an organisation.

But there are other aspects of cyber risks which may make traditional approaches to risk more difficult to transfer directly. The ‘black swan’ nature of some cyber incidents, where they are very rare but catastrophic when they do happen, makes them very hard to mitigate and manage. The potential contagion aspects of some incidents, where one set of infected systems could quickly spread viruses along an entire supply chain, complicates management and prediction.

Boards are struggling to have meaningful conversations about cyber security

Continued

Can cyber risks be insured?

Insurance has been heavily promoted as a way of improving security practices and managing the risks. This is reflected in a lot of interest from boards about the coverage available and the extent to which it is appropriate for their business.

But there continues to be significant levels of hesitation in buying coverage because of a lack of confidence in what to buy, what it covers and whether the policy would pay out in the event of a breach. The economics of insurance remain difficult because of the lack of data to price polices. There are also deeper discussions, though, about the extent to which cyber risks are insurable. For example, there is a proposal, Cyber Re, for the UK Government to reinsure some aspects of the cyber risk market, similar to the initiative concerning buildings insurance against terrorist attacks in the 1990s. Without such guarantees, it is argued, the market in certain areas of cyber security will never grow because the risks are simply too unpredictable and potentially too large to insure.

The acceptance that some compromises are inevitable also requires new thinking. Traditional thinking about security has had the core objective of stopping all breaches. But our *Audit insights* series has highlighted that security compromises are becoming an inevitable part of the business environment. Businesses will never be able to stop all breaches, even if they had unlimited resources.

This raises questions about risk tolerance, for example – what level of breach is acceptable? What about the value of spending time and money on security – how much security is enough? And what is the value of any assurance over cyber security if breaches will still occur?

Recommendations for boards

- Define clear lines of responsibility and accountability for cyber security so that it is embedded in day-to-day operational responsibilities and subject to appropriate board oversight.
- Work with security professionals to build better communication about the articulation and management of cyber risks and the value of security spending.
- Ensure that non-executive directors and audit committees have sufficient knowledge and confidence to hold management to account in a meaningful way.
- Explore new questions in cyber security such as risk tolerance and risk appetite of the business.

Businesses need to transform their approach to cyber security

Communication difficulties are symptomatic of the need for businesses to make deeper changes in their approach to cyber security. As cyber security has gone up the agenda, most businesses have added cyber into existing risk management frameworks and tools. This is seen in steps such as:

- cyber risks being added to internal risk registers;
- auditors being asked about cyber risks by audit committees;
- enterprise risk management systems being adapted to include cyber risks; and
- regular reporting and discussion of cyber risks being incorporated into board meetings.

This can lead to significant improvements in cyber security practices and it is welcome that many boards see these steps as important. However, there are limits to what this can achieve. Many of the steps described are exposing a much deeper gap in understanding about how cyber security fits into a business.

To some extent this gap will narrow as the cyber security field matures and boards increase their experience, knowledge and confidence around cyber risks. However, in order to close this 'cyber gap' more, businesses need to put cyber security at the heart of their business model and focus on becoming a trusted partner in a digital environment.

Transformation requires significant commitment from both security specialists and boards. This presents a major challenge to the security community to engage more meaningfully with boards and translate cyber risks into the context of the specific organisation. Many security professionals lack the skills to do this and, while progress is being made, the gap between business and technology remains too large in many cases.

Boards need to reflect on how to make cyber security more central to their business model. They also need to encourage a major change in culture so that security is seen as an enabler and a way of operating and engaging with the world, rather than a matter of compliance with processes and procedures.

What does a more cyber-secure business look like?

Few, if any, boards would claim to have conquered the challenges of good management and oversight of cyber security. The unique nature of the risks to each business, and the speed of change in technology, makes it difficult to identify good practices which would be appropriate to all businesses. But organisations which have started to transform their approach to cyber security tend to exhibit common features, such as:

- clear responsibility for cyber security in IT and operational functions;
- improved understanding between boards and technical specialists;
- security issues being raised early in key projects and innovations to ensure security is designed into services, processes or systems;
- a road map which identifies critical business data and associated risks; and
- participation in networks to share intelligence about attacks and attackers, typically organised across industry lines.

Businesses need to transform their approach to cyber security

Continued

Disruptive technologies are making this shift more urgent. The need for this shift is made all the more pressing by the growing influence of disruptive technology and the need for businesses to innovate and react quickly to technology trends. These trends will only accelerate as more and more areas of business operations move online and rely on technology to deliver services to customers, as shown by the following examples.

- The Internet of Things will link all kinds of physical objects together, enabling more data to flow across value chains and supporting greater automation and smart operations.
- The FinTech community is developing many innovative financial services, payment systems, virtual currencies and other initiatives which will increasingly change how financial transactions are undertaken.
- There are more opportunities for virtual business and operational models, based on networks and platforms, with less formal boundaries and where there may be less clarity around the identity and location of people.

Businesses must manage this in a considered way to ensure that they respond in a proportionate, pragmatic and timely manner which manages the associated risks. This requires cyber security, and privacy, to be considered at the earliest possible stage of innovations. Processes and systems should be designed with security and privacy in mind, and the costs of security should be factored into margins and the economics of products or services. But many businesses are failing to do this.

To keep up with such trends and innovation, there is widespread growth of shadow IT systems in operational, marketing and product-development functions, which are outside the formal control of IT functions. In these cases, businesses can be opening themselves up to risks which could lead to potentially serious data breaches.

There are also practical limitations in being able to achieve security or privacy by design when buying in products and services from third parties. In these cases, processes will already be designed, and contracts may have standard terms and conditions. Businesses therefore need to balance the opportunities from new technologies with the need for secure systems and identify and mitigate any risks which are created from products and services.

Transformation also needs to be based on greater cooperation and collaboration. Cyber security will not be most effective when organisations work in isolation. It may be the case that businesses see competitive advantage and brand value in building a strong security culture. Furthermore, cyberattacks often focus on highly sensitive company data, increasing the desire for secrecy around the issue. Nonetheless, it is essential to cooperate and collaborate.

Trusted communities and networks play a vital role in sharing intelligence and good practices. There is a need, though, to extend these beyond major industries such as financial services, and into smaller and medium-sized businesses. To date, few smaller businesses have joined such networks and greater consideration should be given to how peer learning can be encouraged in this context.

Larger organisations are benefitting from the move of CISOs between businesses and across industries. There is a growing tendency to recruit senior security professionals from other industries to enable learning across the community and share knowledge about what different sectors are doing.

But nation states have also always played a role in protecting trade and key business interests, and cyberattacks raise many questions about the legitimate role of states in providing intelligence and other practical support to businesses based on their greater resources and power.

This requires effort from both businesses and governments in building engagement and communication channels. It also requires clarity from governments on where their priorities lie to ensure appropriate expectation setting. To date in the UK, meaningful intelligence sharing and action has focused on the critical national infrastructure. There has been limited practical support for other business sectors, despite government ambitions to ensure the UK is a safe place to do digital business.

Recommendations for boards

- Develop a clearer understanding of how cyber security fits in with the business model of the organisation.
- Build in security and privacy by design to innovation and business projects. Where this is not possible, through the use of third-party products and services, understand and mitigate any risks.
- Lead the shift to a culture and mindset where security is seen as an enabler of digitally based businesses rather than compliance with processes and procedures.
- Encourage participation in networks to share information and intelligence with peers.

Supply chain cyber risk management is a significant opportunity for change

Pressures to transform approaches to cyber security are being particularly felt in supply chain risk management. Many high-profile security breaches have occurred as a result of vulnerabilities in suppliers, opening up access into the systems of larger businesses. One of the causes of the major data breach at the US retailer Target, for example, was the compromised systems of an air-conditioning supplier, which enabled access into Target's billing systems by hackers.

As a result, businesses are increasingly looking to gain assurance about the cyber security practices of their supply chain partners. This is also an approach which is encouraged by the UK Government. It would prefer to see supply chain pressures improve security rather than creating regulation, and it has taken a lead by mandating compliance with the Cyber Essentials standard as part of the bidding process for some government contracts.

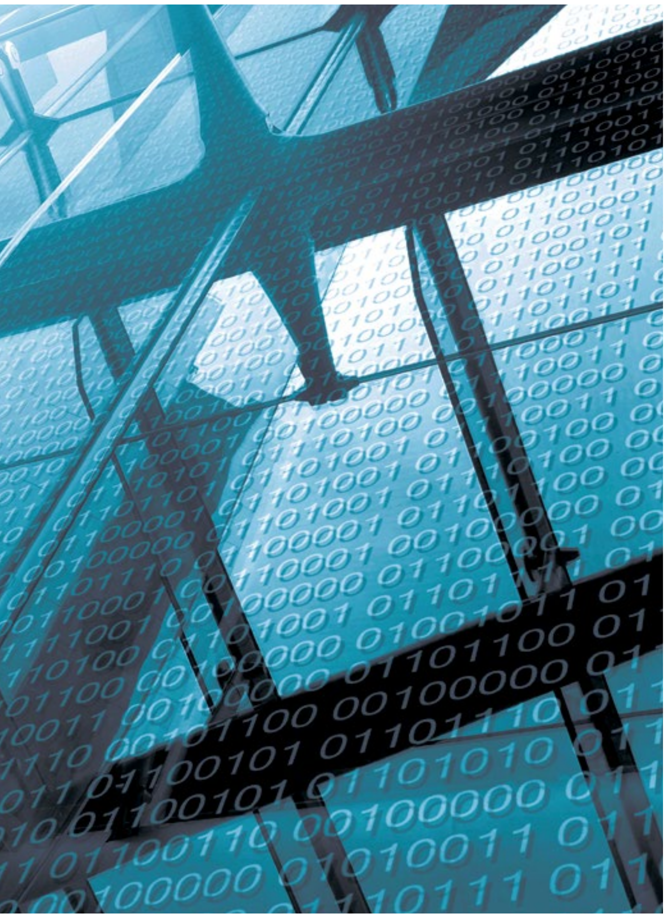
However, businesses need to think beyond IT suppliers. This covers a wide variety of partner organisations, including IT service providers, suppliers of non-IT goods and services and subcontractors. It is therefore important to consider the whole value chain of the organisation. In the process, businesses need to recognise they cannot outsource cyber risks, although they can transfer elements of the risk through contractual measures.

Businesses need to prioritise and target supply chain assurance activities around the areas of greatest risk. A typical large business will have thousands of suppliers. Getting assurance over the cyber security practices of all of these suppliers is unrealistic and management needs to prioritise and target its efforts. However, many businesses focus on the wrong things.

Traditional approaches to supply chain risk, for example, prioritise the suppliers associated with the highest value spend. While this may be appropriate for many types of risk management, it is unsuitable for cyber risk management. Instead the key selection criteria should relate to access to critical data or systems. A company dealing with records management, for example, might have a relatively small spend associated with it but expose the business to high levels of cyber risk.

Efforts also typically focus on procurement processes, for example requiring compliance with specific standards in order to tender for work, or requiring bidders to complete questionnaires about their practices as part of the bidding process. Less attention is paid to ongoing assurance processes. However, it is crucial for businesses to gain assurance through the life cycle of contacts. Otherwise there will be no way to check that suppliers are doing as they promised through the bidding process or to review the risks if the environment changes.

There is no consistent method to supply chain assurance around cyber security practices, as there is no clear and single standard to underpin it. This is a recognised problem and the UK Government has tried to mitigate it through the development of Cyber Essentials. However, adoption remains low and increasing take-up, especially among smaller businesses, is a major task.



As a result, larger businesses often send questionnaires to suppliers to assess their practices and gain assurance over the risks. But this is leading to significant gaps in meaningful assurance down supply chains. There is a lot of paperwork and obfuscation but it is not necessarily changing behaviour or improving risk management. Consequently, it may be adding a burden to procurement and bidding processes rather than leading to stronger security.

Summary of security standards

ISO 27001 is the best established standard in information security but many feel it may be unsatisfactory as the business itself defines the scope and controls. Therefore, detailed understanding of what has been included in the certification process is required to assess whether it is sufficient in the circumstances.

Cyber Essentials was launched in 2014 and aims to stop low-level indiscriminate attacks. It focuses on 'cyber hygiene', specifying the five most important technical controls, based on evidence from GCHQ. Therefore, it is a starting point for improving cyber security, especially for small businesses, but will not be sufficient for more complex or risky businesses.

Other common standards or frameworks include the following.

- PCI-DSS, which is an information security standard specific to payment cards, so that any organisation that wants to take card payments must be compliant.
- IASME, which is aligned to ISO 27001 but designed specifically for smaller organisations.
- COBIT, which is a framework for IT controls and governance used by many audit and assurance professionals.
- NIST, which is a US framework for information security controls. It is risk based, so that different templates of required controls can be developed for different businesses, based on industry, size etc.
- ISF Standard of Good Practice, which is developed by the Information Security Forum, an organisation of technical specialists.

The International Standard on Assurance Engagements (ISAE) 3402, which reports on controls in service organisations, is also relevant in this context.

Supply chain cyber risk management is a significant opportunity for change

Continued

While the proliferation of standards is a significant problem, there is no one-size-fits all solution due to diversity in businesses and operating models. This creates different levels of risk, which has to be reflected in any approach that is adopted.

It is also possible that this strategy will increasingly exclude smaller businesses from supply chains, as they do not have the resources to provide high levels of assurance in this area. They may conclude that they do not have the resources to comply and will refocus their efforts into other customers in the future. In this context, large businesses may have a responsibility to help smaller businesses down their supply chain comply with their requirements.

Improving the management of supply chain cyber risk presents an opportunity for rethinking organisational responsibilities. As part of the management of supply chain cyber risks, a business needs to define where responsibility lies. With IT suppliers, it sits naturally in the IT or security department. However, with operational suppliers, responsibility may be less clear. Security specialists may not have the knowledge or influence to challenge operational departments, and the responsibility for gaining assurance over cyber risks should lie in those operational departments.

This, therefore, presents a great opportunity to transfer responsibility into operational departments more generally and gain broader business buy-in to cyber security requirements.

Recommendations for boards

- Prioritise the cyber risk attached to suppliers across the business, based on access to sensitive systems and data rather than size of associated spend.
- Ensure that assurance is gained throughout the life cycle of the contract as well as at the time of purchase.
- Consider who in the organisation is responsible for gaining this assurance.
- Be prepared to answer questions about cyber security from potential customers or clients as part of their assurance processes.

Appendix

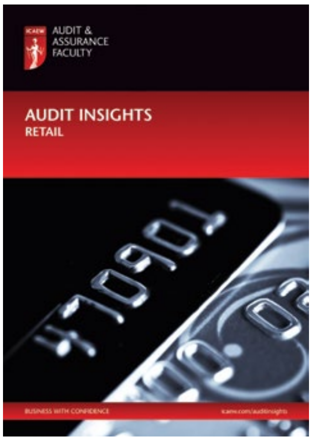
2013 FLAGS AND RECOMMENDATIONS	UPDATE
Flag 1: businesses should consider 'cyber' in all their activities	
• While cyber security has gone up the board agenda, in many cases it remains a technical risk which is under the responsibility of the IT department and CIO. • The pigeon-holing of cyber risks makes it difficult to recognise the full business impact of security breaches, such as loss of intellectual property, reputational damage or business disruption. It also makes it difficult to balance the opportunities from new technologies, such as mobile, with the risks. • This creates new systemic risks to the economy, as well as challenges to investors and regulators about cyber risk reporting and assurance. • Recommendation 1: boards should increasingly look for evidence from all parts of the business that managers are aware of the risks that digital technology brings to strategy and operations, and are taking appropriate actions to manage those risks. • Recommendation 2: non-executive directors should challenge executive management to present a coherent approach to cyber risks across the business.	There are high levels of awareness, and boards recognise the potential impact of a serious cyber security incident. However, most businesses continue to struggle with accountability for security, and the need to shift it from IT functions into wider operational functions.
Flag 2: businesses need to accept that their security will be compromised	
• Cyber risks are growing due to the changing security landscape. Data is spread across an array of suppliers, service providers and devices. Attacks from all sources are increasing. As a result, businesses need to operate on the basis of an 'assumed state of compromise.' • This means investing in new capabilities such as intelligence, monitoring, detection and response. While preventative controls remain important, greater attention needs to be given to resilience and quick response. • There also needs to be a change of mindset, which emphasis collaboration and information sharing rather than secrecy. • Recommendation 1: boards need to accept that security will be breached. To reflect this, board reporting should increasingly focus on learning from specific incidents and near-misses as well as understanding what level of breach an individual business is prepared to tolerate. This represents a significant change in security culture. • Recommendation 2: boards should also encourage and participate in regular and ad hoc cyber simulations. These can sharpen decision-making processes at all levels of the business and identify potential weaknesses in response capabilities.	This has become an accepted state of affairs and the level of breaches is generally viewed to be under-reported. Some improvements are evident This is especially true in the case of sharing information and the building of communities. These are of growing value, although limited in practice to the largest players in specific industries where there is mutual benefit and trust between parties. There are also improvements in areas such as threat analysis and coordination of activities between different geographies.

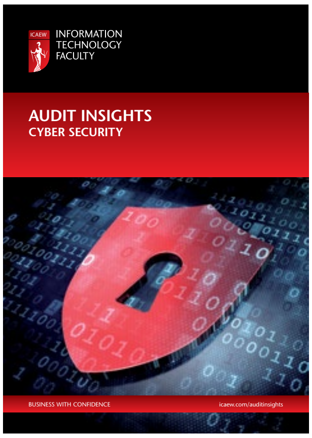
Appendix

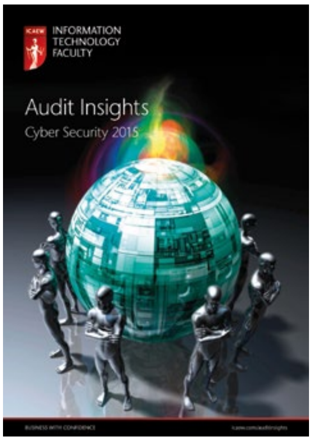
Continued

2013 FLAGS AND RECOMMENDATIONS	UPDATE
Flag 3: businesses should focus on their critical information assets • Given that businesses will increasingly experience data compromises, they need to focus on their key data. It is no longer possible to protect all data all of the time and therefore businesses need to prioritise resources accordingly. • Most businesses are not very good at doing this and greater discipline and understanding of organisational data will be required. • Recommendation 1: boards should ask themselves whether they can identify their critical information assets and whether they know where they are stored and who has access to them. If this is not clear, they should work with senior management to build understanding of critical information assets and the specific risks surrounding them. • Recommendation 2: boards should ensure that appropriate levels of responsibility and accountability are in place to support the effective prioritisation of information assets and good decision making about the use and protection of information.	Some organisations are making progress in this area by building roadmaps and classifications of data assets. In many cases this is leading to better understanding of what organisations don't know about their data, as well as what they do know.
Flag 4: most businesses don't get the basics right • Up to 80% of security breaches could be prevented by having basic cyber hygiene in place, such as anti-malware software. • However, most businesses still fail to get these basics right. For large businesses, the complexity of the environment makes it difficult to keep up with threats. For smaller businesses, they may lack the skills and resources needed. • For all businesses, people are still the weakest link in security and most breaches can be attributed in some way to human failings. Therefore greater personal accountability is needed to drive behavioural change. • Recommendation 1: boards should ask the business's IT and security practitioners about the extent to which they are getting the basics right. Government advice and third-party advisers can help boards to identify the right questions to ask. • Recommendation 2: boards should demonstrate commitment to a strong security culture and show leadership to encourage behavioural change where needed.	Skills remain a key challenge in improving basic security. There is also a need for organisations increasingly to think in terms of a cultural shift rather than simply driving compliance with formal policies and procedures. This is particularly the case as workplaces become more dominated by 'millennials', who may have different attitudes to security and be more open with their data. Some organisations are going backwards as they believe they have achieved basic security and have stopped investing in further measures.

Other reports in the *Audit insights* series







For more information please visit
icaew.com/auditinsights

ISBN 978-1-78363-385-2

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 144,000 chartered accountants worldwide. We provide qualifications and professional development, share our knowledge, insight and technical expertise, and protect the quality and integrity of the accountancy and finance profession.

As leaders in accountancy, finance and business our members have the knowledge, skills and commitment to maintain the highest professional standards and integrity. Together we contribute to the success of individuals, organisations, communities and economies around the world.

Because of us, people can do business with confidence.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com

Chartered Accountants Worldwide

GAA Global Accounting Alliance

ICAEW
Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK

T +44 (0)20 7920 8635
E itfac@icaew.com
icaew.com/auditinsights

linkedin.com – find ICAEW
twitter.com/icaew
facebook.com/icaew