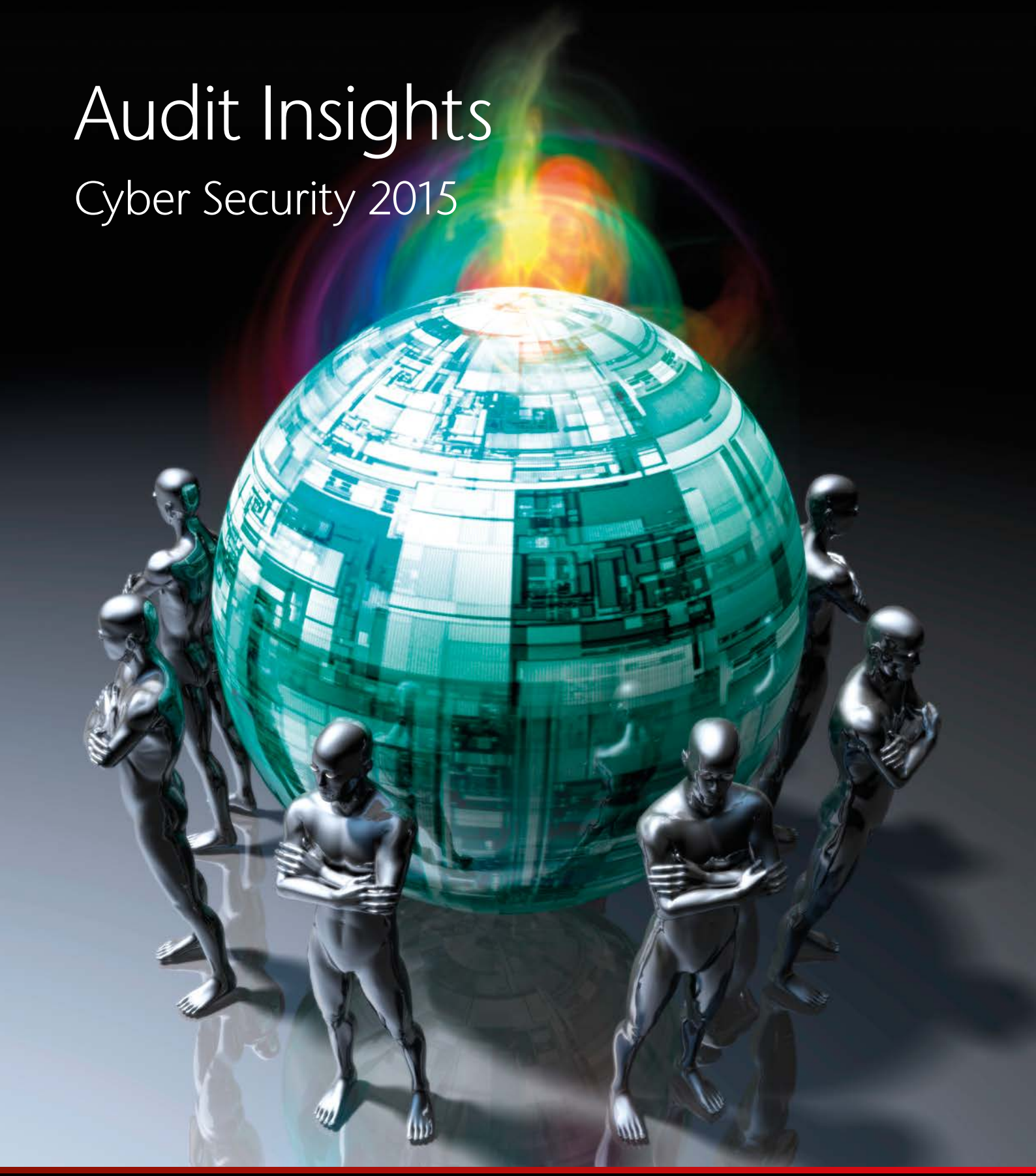
ICAEW

INFORMATION TECHNOLOGY FACULTY

Audit Insights

Cyber Security 2015



About the ICAEW IT Faculty

The ICAEW IT Faculty provides products and services to help its members make the best possible use of IT. It represents chartered accountants' IT-related interests and contributes to IT-related public affairs. It also helps those in business to keep up to date with IT issues and developments. As an independent body, the IT Faculty is able to take an objective view and get past the hype which often surrounds IT, leading and shaping debate, challenging common assumptions and clarifying arguments.

The faculty's thought leadership programme, *Making Information Systems Work*, looks at how technology is transforming the way we do business and interact with each other. Our work brings together leading thinkers from business and research through panel discussions, reports, and lectures on the basis of three themes which are essential to the success of IT – value, trust and standards. Our report *Building Trust in the Digital Age: Rethinking Privacy, Property and Security* considers the actions that individual businesses can take to address concerns about the security and use of digital information, as well as the wider social and legal implications of digital technology.

The IT Faculty leads the work on *Audit Insights: Cyber Security* and has a wide-ranging programme of activities around cyber security including roundtable discussions, conference panels and member guidance. All related material is available at icaew.com/cyber

For more information on the IT Faculty and how to get involved, please visit icaew.com/itfac or contact Richard Anning at richard.anning@icaew.com, or on +44 (0)20 7920 8635.

About the ICAEW Audit and Assurance Faculty

The ICAEW Audit and Assurance Faculty is a leading authority on external audit and other assurance services. It is recognised internationally by members, professional bodies and others as a source of expertise on issues related to audit and assurance. *Audit Insights* is one of several initiatives launched by the faculty.

Through *AuditFutures*, the faculty is asking big questions about the future of the external audit profession. It convenes stakeholders who normally do not talk to one another and aims to create opportunities for dialogue and for collaborative and creative solutions to emerge. In partnership with the Finance Innovation Lab, we are building a movement for wider behavioural change and we are developing innovation projects for systemic effect.

Through the *re:Assurance* initiative, the faculty is finding out where assurance services over business information, such as key performance indicators, could strengthen markets and enhance confidence. *Re:Assurance* also asks how the International Framework for Assurance Engagements can be applied and developed. The faculty responds to demands for practical guidance with publications such as *The Assurance Sourcebook*.

The faculty's Audit Quality Forum (AQF) brings together external auditors, investors, business and regulatory bodies, encouraging stakeholders to work together by promoting open and constructive dialogue about transparency, accountability, reporting and confidence in external audit.

For more information on the Audit and Assurance Faculty, the current work programmes and how to get involved, please visit icaew.com/audit. To learn more about *Audit Insights* please contact Henry Irving at henry.irving@icaew.com, or on +44 (0)20 7920 8450.

ISBN 978-1-78363-170-4

Audit Insights

Cyber Security 2015

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 2015 report provides an update to the four flags highlighted in the first *Audit Insights: Cyber Security* report, published in November 2013.

Executive summary

The importance of cyber security continues to grow as businesses increasingly use digital technology to transform their business operations and customer engagement. This update to the 2013 *Audit Insights: Cyber Security* report raises specific issues and concerns that auditors are aware of in the cyber-security environment.

MANY BUSINESSES HAVE TAKEN MEASURES TO IMPROVE THEIR CYBER SECURITY

Board awareness of cyber risks is higher than ever before. This awareness is resulting in greater management focus and more resources being directed towards cyber security. It is also encouraging to see greater confidence in board conversations, with boards more willing to challenge CIOs and less willing to take technical responses at face value.

Businesses are increasingly recognising the importance of cyber-security training. However, in many cases training has not received enough input from subject-matter experts. Therefore, while this is a welcome step for many organisations, further investment and action may be required to achieve sustainable improvements.

There is growing acceptance of the need to categorise and prioritise different types of data. However, the focus on critical data has often been driven by concerns about compliance with data protection regulation.

THE THREATS CONTINUE TO GROW

There has been no let up in attacks, as evidenced by a range of industry surveys, high-profile breaches and continuing concern in government. These trends reflect the experience of auditors, who have continued to see an increase in the number and scale of cyber attacks on businesses.

Economic growth is leading to new business activity, which in turn creates new cyber risks. Businesses may be acquiring other businesses to support their growth. They may be expanding into new markets or developing new products. In particular they may be looking to exploit digital channels more extensively. All of these activities may expose businesses to new risks in the supply chain, increase the challenges of getting security measures right and heighten the impact of security breaches.

The growing reach of social media is also exposing businesses with poor response capabilities. Increasingly, news of data breaches or compromises is spreading incredibly quickly across platforms such as Twitter. However, businesses are often slow to respond and only provide limited information to customers, which can amplify the impact of the breach.

Executive summary

Continued

THERE IS A GROWING GAP BETWEEN BUSINESS AND CYBER ATTACKER CAPABILITIES

We welcome the improvements to the cyber-security practices in many businesses. However, the threat environment continues to change at a rapid pace and few businesses are managing to close the gap between their security capabilities and those of attackers. Many businesses are falling further behind and the risks are growing.

To prevent the gap from growing further, businesses need to focus their finite resources in the right places. In particular they need to balance investment in existing preventative controls with investment in new skills and solutions in monitoring, detection and response.

Viewing security as a cost or compliance issue is likely to be a significant barrier in this context, and emphasising the positive case for security can lead to greater business commitment.

GOOD INTENTIONS MUST BE MATCHED BY ACTION

Many businesses have good intentions to improve their cyber-security capabilities but are still in the early stages of change. While auditors are seeing a lot of planning, all too often that has not yet been translated into tangible actions and improved performance.

Difficulty in quantifying benefits and tracking progress hinders good management. Many businesses struggle to build effective management information about their security activities.

Few businesses are also tracking progress against clear goals, which makes it harder to drive change and ensure that good intentions are being translated into effective action.

There are questions about whether there is a commitment to deliver real change. While most businesses are concerned about cyber security, it remains to be seen whether it is a high enough priority in most businesses in the absence of stronger commercial or regulatory pressures.

The changing landscape for security

Audit Insights: Cyber Security **highlighted the changing landscape for cyber security.** Business data is increasingly spread across supply chain partners, cloud providers and mobile devices. Attacks come from around the world for a variety of reasons and the impact of security breaches is growing.

To respond to these threats, businesses need to change their actions, mindset and behaviour around security.

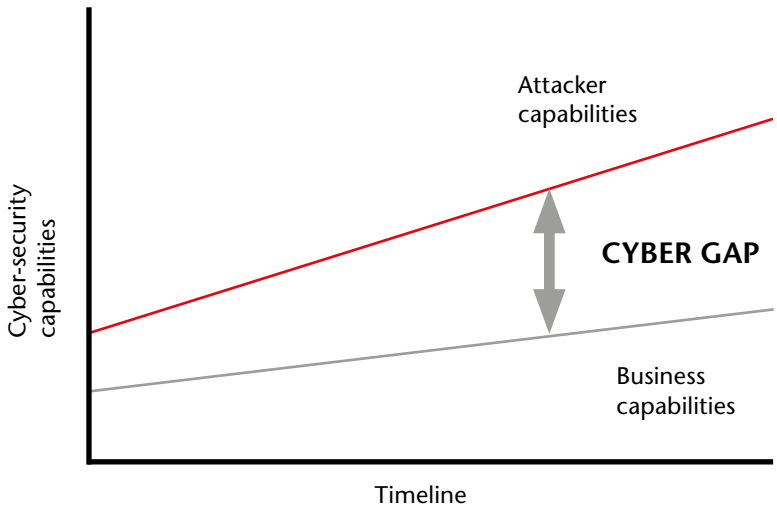
The 2013 report raised the following four flags for businesses, policymakers and other stakeholders.

- Businesses should consider 'cyber' in all their activities.
- Businesses need to accept that their security will be compromised.
- Businesses should focus on their critical information assets.
- Most businesses don't get the basics right.

Since the 2013 report there have been improvements across all of these flags. This updated report highlights specific examples, such as an emphasis on training to improve basic security behaviour, growing acceptance of the assumed state of compromise, and greater board engagement on identifying critical data. In the appendix we map specific updates to each of the four flags.

However, businesses need to do much more. As a framework for this review, we compare the extent to which businesses are improving their cyber-security capabilities with the capabilities of attackers, and assess whether the gap between the two is growing.

IS THE CYBER GAP GROWING?



Many businesses have taken measures to improve their cyber security

Board awareness of cyber risks is higher than ever before. Personal experiences of cyber attacks, high-profile media stories and UK Government initiatives, such as the FTSE 350 tracker, have all helped to raise cyber security up the board agenda. Audit committees are asking auditors more questions about the way that cyber risks are being managed. This awareness is resulting in greater management focus and more resources being directed towards cyber security.

It is also encouraging to see greater confidence in board conversations, with boards more willing to challenge CIOs and less willing to take technical responses at face value. As a result, they are starting to dig deeper on the issues and ask more questions about risk mitigation and response plans.

Businesses are increasingly recognising the importance of cyber-security training. This is a welcome development, as training focuses on the people aspects of security, which were highlighted in the 2013 report as frequently the weakest link in security. Surveys consistently show a clear connection between training and improved security and therefore this focus should provide significant benefits to businesses in the future.

In some cases we have seen a shift in security training from a responsibility of the IT department to a broader business task which sits in areas such as HR and internal communications. This may enable security awareness and good practice to become more embedded into wider business operations and strategy.

However, in many cases training has not received enough input from subject-matter experts. Good training should focus on a small number of simple messages and drive changes in behaviour, as well as inform staff about basic policies and procedures in place. There needs to be a balance between technical instruction and exploring broader culture change, with a focus on the outcomes from the training. Subject-matter experts can bring a broad understanding about the real-life application of good practices and thereby improve the quality of the training.

Therefore, while greater emphasis on training is a welcome step for many organisations, further investment and action may be required to achieve sustainable improvements.

BOX 1: CYBER INSURANCE

One of the elements of risk mitigation which has gone up board agendas has been cyber insurance. Like other areas of insurance, it transfers the risk of cyber-security breaches to the insurance company and covers at least some of the costs related to data breaches. General policies may provide some protection in the event of business disruption. However, there is a growing market for specialist polices, especially around breaches of security for personal data.

The development of the cyber-insurance market has been hindered by two main factors:

- a lack of information about the frequency and impact of breaches, which has made it impossible to calculate risk and price policies appropriately; and
- a lack of clear standards about cyber-security practices, which has made it difficult to specify required behaviours from the policy holder.

The cyber-insurance market is well developed in the US, and this has been heavily driven by the data generated by breach notification laws in personal data. The market in the UK is still in early stages and the proposed EU breach notification laws could spur market growth. It is also hoped that the UK government's Cyber Essentials scheme, which sets out core cyber hygiene measures, may spur the market by creating a clear standard.

However, concerns remain about the value of coverage. If a business is not following basic security standards, for example, the policy may not be as effective as expected. Although cyber insurance can play a useful role in a business's risk management strategy, it is not a replacement for following core cyber hygiene measures.

There is growing acceptance of the need to categorise and prioritise different types of data.

The 2013 report emphasised that businesses need to operate on the basis of an 'assumed state of compromise' and focus their resources on their critical data. Auditors have seen a widespread acceptance of this new business reality, alongside a growing number of conversations about the identification and prioritisation of key data assets.

The focus on critical data has often been driven by concerns about compliance with data protection regulation. The increase in fines and reputational damage from breaches of personal data has led to a demand to bring privacy and cyber-security discussions closer together. This trend is likely to increase, especially given the proposed European Regulation on Data Protection, which further increases fines and creates a new requirement to report any breaches of personal data to appropriate authorities.

Recommendations

- Boards should continue to build their knowledge and confidence on cyber risks, and challenge IT functions to explain their security strategy and risk mitigation plans.
- All boards should ensure that they can identify their critical data and its associated risks, even where regulatory pressure does not exist.

The threats continue to grow

Businesses are experiencing record numbers of cyber attacks. There has been no let up in attacks, as evidenced by a range of industry surveys, high-profile breaches and continuing concern in government. The Department for Business, Innovation and Skills (BIS) *Information Security Breaches Survey 2014* reported a substantial increase in the impact of breaches. These trends reflect the experience of auditors, who have continued to see an increase in the number and scale of cyber attacks on businesses. Box 2 describes some of the high-profile breaches since the publication of the 2013 report and box 3 outlines the Heartbleed bug, a major vulnerability discovered in 2014.

BOX 2: HIGH-PROFILE BREACHES

- **Target** – this breach resulted in the theft of 40m credit card details and 70m customer details. The timing of the breach (in the run-up to the 2013 holiday season) meant that the impact was particularly significant – there was a 46% drop in net profit over that quarter, $61m in costs related to the breach, reduced customer satisfaction and a drop of 11% in the share price. The breach was a key factor in the departure of the CEO and the CIO and the positions of some non-executive directors and members of the audit committee have also been threatened based on their poor level of oversight. It is notable that attackers accessed Target's data through the compromised systems of a heating, air conditioning and refrigeration supplier, illustrating the risks of integrated supply chains. Another weakness exploited by attackers was the point-of-sale system, which had been customised to provide enhanced marketing opportunities without full consideration of the security risks.
- **Morrisons** – this breach of payroll systems resulted in the theft of the details of 100,000 employees. The data was then posted on a website, although subsequently removed. This was the result of the actions of an employee, rather than an external hacker, highlighting the continuing threat from insiders and the need to focus on processes and people as much as technology.
- **eBay** – this breach led to 145m customer records being accessed by hackers. eBay has been particularly criticised for the way that it responded to the breach and handled customer communications. It took almost three months for eBay to admit the breach to customers and little explanation was provided for what caused the breach. Inconsistent advice was given, for example eBay claimed passwords were encrypted and therefore couldn't be accessed by the attackers but then advised customers to change passwords. The password resetting process was also poor, with users experiencing long delays. This contrasted with the actions of shoe retailer **Office**, which responded quickly to a security breach and provided helpful information to customers very early in the process.

The UK Information Commissioner also publishes information about breaches of data protection regulation and the fines imposed. For example, in July 2014 online travel agency **Think W3** was fined £150,000 after hackers stole data related to more than 1m credit and debit cards.

BOX 3: HEARTBLEED BUG

The Heartbleed bug, discovered in April 2014, refers to weaknesses in software code that is found throughout the Internet. This bug, found on software used in many websites, made them vulnerable to attacks and enabled hackers to steal encryption keys and user information such as passwords. Although it received widespread publicity, security specialists estimated that the majority of affected websites had still not been fully fixed by the summer of 2014.

But there have been encouraging developments in law enforcement against attackers, especially with cross-country operations. For example, a massive network of computers used for illegal purposes (a botnet) was taken down. This stopped the spread of Cryptolocker ransomware, a virus that encrypts a computer and will only unlock it on payment of a fee. This was a coordinated effort across many countries, although it was only expected to stop the spread of the malware for a short period of time.

Economic growth is leading to new business activity, which in turn creates new cyber risks.
While economic growth is very welcome, it underlines the need for businesses to integrate cyber considerations into their strategy and operations.

For example, activities around transactions can lead to specific cyber risks. Businesses may be acquiring other businesses to support their growth. In the process, various third parties will gain access to sensitive commercial information. Acquired companies may have poor levels of security, and integrating IT systems may create new exposures. Businesses may be preparing themselves for new financing, sale or an IPO, which may require a clean bill of health regarding cyber risks.

Businesses may be expanding into new markets or developing new products. Staff numbers may be increasing to deliver new work. Businesses may be investing in the development of new intellectual property or making greater use of social or mobile technology to reach new customers or improve operations.

In particular they may be looking to exploit digital channels more extensively. Retail businesses, for example, increasingly need to operate as omnichannel businesses, with digital channels operating alongside traditional bricks and mortar models. Mobile technology is also critical to developing new customer service models and engaging with customers.

All of these activities may expose businesses to new risks in the supply chain, increase the challenges of getting security measures right and heighten the impact of security breaches.

The growing reach of social media is exposing businesses with poor response capabilities.
Increasingly, news of data breaches or compromises is spreading incredibly quickly across platforms such as Twitter. This is leading to greater emphasis on two areas. First, there is a trend to more proactive monitoring, enabling businesses to detect any breaches quickly. Second, businesses need to be prepared to respond effectively to breaches or face the wrath of unhappy users.

We have seen examples of both good and poor responses in 2014. A good response is typically characterised by speed and openness. A business, for example, can contact customers early, keep them updated on developments and provide clear guidance on any steps that the customer should take, such as change passwords. However, businesses are often slow to respond and only provide limited information to customers, which can amplify the impact of the breach. As a result, greater emphasis needs to be placed on building strong detection and response capabilities.

Recommendations

- Boards need to ensure that security is designed into their strategy and operations, especially for new activities, rather than considered as an afterthought.
- Boards should focus their attention on their monitoring, detection and response capabilities, and not just consider preventative actions.

There is a growing gap between business and cyber attacker capabilities

As a result of the growing threat, few businesses are managing to close the gap between their security capabilities and those of attackers. In many cases businesses are falling further behind and the risks are growing.

In part this reflects the need to build broad cyber awareness and good practices across businesses. While this may require some investment in technology solutions, improving basic security behaviour remains a critical part of building good cyber-security capabilities.

It also reflects the need to invest in greater specialist skills in cyber security, both at the level of individual businesses and across the economy more broadly. Companies with a large global footprint outside the UK and the major developed economies may particularly struggle to find appropriate technical skills around the world.

To prevent the gap from growing further, businesses need to focus their finite resources in the right places. In particular they need to balance investment in ongoing preventative controls with investment in new skills and solutions in monitoring, detection and response.

Getting this balance right is a real challenge and businesses often focus on the easier or less costly measures rather than the most important measures. For example, effective monitoring systems and processes are essential but often difficult and costly to implement.

Viewing security as a cost or compliance issue is likely to be a significant barrier in this context, and emphasising the positive case for security can lead to greater business commitment.

BOX 4: THE POSITIVE CASE FOR CYBER SECURITY

Cyber security is typically approached as a matter of risk or compliance and the aim is to avoid negative outcomes eg, data breaches or business disruption. It is possible, though, to develop a more positive business case for security, and ultimately view it as an opportunity for competitive advantage.

It is important to be a trusted partner as digitisation of the economy continues, and auditors are seeing growing demand for assurance in this area across supply chains in particular. A trustworthy reputation may also breed greater customer loyalty. As a result, by building strong security capabilities, businesses may benefit from more efficient operations, supply chain and customer service, as well as a stronger brand in the market.

Deploying new digital technologies effectively is also underpinned by solid security and risk management. Good practices will enable businesses to be more agile and responsive to new technologies, deploying them quickly and safely. Security concerns may delay the roll-out of new products and services, and poor implementation may create new risks.

However, the positive case for security relies on customers, suppliers and other stakeholders recognising the importance of good security and rewarding those who do follow good practices. It also relies on transparency and clarity around what constitutes good practice, so the lack of clear standards in this area adds to the practical difficulties.

Businesses can't build capabilities alone and governments can play a useful role. The skills gap is causing particular concern at government level. The UK Government has recognised the need to grow the technical skills base, with investment in universities, and the development of new academic centres of excellence, research institutes and centres for doctoral training. A new master's degree in cyber security was announced in July 2014 and the 'Cyber Security Challenge UK' initiative has aimed to get talented young people to enter the cyber-security profession.

There have also been initiatives to improve more general awareness of cyber security. For example, the 'Cyber Streetwise' campaign has been led by the Home Office, working closely with BIS and the Cabinet Office. It targets consumers and small businesses with the aim of improving basic cyber savviness. Training has also been developed by BIS, together with ICAEW, the Law Society and the Solicitors Regulation Authority, which targets professional advisers such as lawyers and accountants.

Furthermore, regulators are showing more interest in the cyber-security capabilities of businesses, with some examples outlined in box 5. Breach notification laws are well established in the US. The EU has also proposed mandatory breach notification for specific critical industries in its draft Cyber Security Directive and for breaches of personal data in its draft Data Protection Regulation.

BOX 5: EMERGING REGULATORY RESPONSES

In June 2014 the Bank of England announced a new framework for cyber-security testing in the financial services sector: CBEST. This outlines an approach to testing the resilience of financial service firms in the light of highly sophisticated and targeted attacks. It is based on intelligence on current threats and will replicate the expected behaviours of attackers. While participation in the tests is voluntary, the Bank hopes that take up will be high, as institutions will be able to improve their security substantially through better understanding of their own capabilities and greater intelligence about cyber threats.

The US Securities and Exchange Commission has also started to consider cyber security in its activities. In April 2014, it announced that it would be examining certain broker-dealers and investment advisers with a particular focus on their cyber-security preparedness.

While these initiatives are still in early stages, they may indicate the start of a broader trend towards regulator interest in cyber security. However, this also raises fresh challenges. Some businesses, for example, have expressed concerns about sharing sensitive information about security with regulators based on concerns about the regulators' own security capabilities or the potential interplay with security agencies.

Industry bodies can act as useful intermediaries in this context, providing industry-wide support while avoiding some of the concerns about regulatory involvement. Examples of industry cooperation are outlined in the final section of this report.

Recommendations

- Boards should focus on making a positive case for security, based around being a trusted partner in the digital economy.
- Policymakers should increase their support for businesses in building strong cyber-security capabilities, especially in training for smaller businesses.

Good intentions must be matched by action

Many businesses have good intentions to improve their cyber-security capabilities but are still in the early stages of change. While auditors are seeing a lot of planning, all too often that has not yet been translated into tangible actions and improved performance.

The 2013 report highlighted a variety of underlying factors which make it difficult to get basic security right. Often these are not quick or easy to solve. The scale and complexity of IT environments in large businesses, for example, makes it very challenging to roll out upgrades and fixes quickly, inevitably leaving them vulnerable to attack for a period of time. This continues to be a major problem and is likely to be aggravated by new business activities such as acquisitions.

Difficulty in quantifying benefits and tracking progress hinders good management. Many businesses struggle to build effective management information about their security activities. It is difficult to build strong business cases for many security measures, as the benefits primarily relate to the reduction of risks and the avoidance of breaches. Some of the government initiatives on data sharing may help to provide a stronger evidence base around the benefits of good security and the impact of breaches. However, quantification of the benefits is likely to remain problematic.

In addition, few businesses are tracking progress against clear goals, which makes it harder to drive change and ensure that good intentions are being translated into effective action. For the most part, management information continues to focus on technical measures and preventative controls. Better management information with greater business focus can enable more effective board intervention and leadership.

There are questions about whether there is a commitment to deliver real change. While most businesses are concerned about cyber security, it remains to be seen whether it is a high enough priority in most businesses in the absence of stronger commercial or regulatory pressures.

It is possible that having good cyber hygiene will become a standard part of doing business and it will become impossible to be part of supply chains without being able to demonstrate that basic measures are in place. The UK Government is hoping that its 'Cyber Essentials' scheme will be adopted across supply chains and become an integral part of doing business. To drive initial take up of the scheme, it is now mandatory for businesses to comply with 'Cyber Essentials' when bidding for certain government contracts.

Customer attitudes can also drive changes in business behaviour. The kind of breaches highlighted in this report can lead to substantial bad publicity and damaged reputation. It is difficult, though, to point to long-term losses as a result of breaches. Although the Target data breach has had a major impact on board awareness in the US, Target's profits and share prices have rebounded. Poor response and customer communication may have the greatest impact in this context, as a bad customer experience is less likely to be forgotten than the simple fact of the breach.

There is also a need for greater coordination and system-wide actions. The inter-connectedness of the environment means that individual businesses are not in full control of the risks; they rely on others to implement good security and can be impacted where third parties, such as trading partners or service providers, fail to do this.

This is clearly the case in supply chains, where integrating systems with suppliers can lead to new weaknesses. Many large companies incorporate security requirements into supply chain contracts and invest resources in reviewing the compliance of suppliers. There is also greater consideration going into models such as joint ventures around what information should be shared in the relationship.

Government intervention in cyber security is difficult, as the environment changes quickly and risks vary depending on the nature of the business. As a result, industry bodies and supply chains can play an important role in coordinating and improving security in ways that are appropriate to their specific business risks.

BOX 6: SECTOR-BASED RESPONSES

The defence industry is one of the most advanced industries in this context, given the extent to which it relies on intellectual property and has been the victim of cyber attacks. The UK Defence Cyber Protection Partnership builds cooperation across public and private sector organisations with the aim of improving security. It focuses particularly on sharing information about threats, raising awareness around cyber security and pushing standards down the supply chain.

The corporate finance community also collaborated on a guide, *Cyber-Security in Corporate Finance*, which sets out good practice in the context of corporate finance activity, such as raising finance, and mergers and acquisitions. Led by ICAEW and supported by the UK Government, the guide was developed by a working group which included a number of trade bodies, regulators and leading firms.

But the risks are not confined to supply chains; they can go across the whole system and economy. For example, poor security in one business may enable hackers to use their computers to attack other businesses. This diffusion of responsibility through the system potentially acts as a disincentive to improving individual security. It leads to broader questions around market failures and the role of governments (and others) in encouraging collective action. It also links to the alignment of economic incentives, and the extent to which the market rewards the right behaviour.

Recommendations

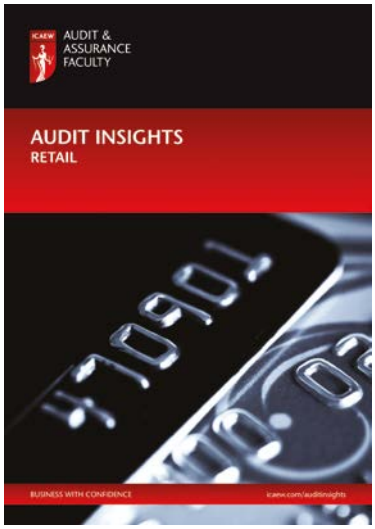
- Boards should consider their information needs regarding cyber risks and ensure that they can track the progress of security activities appropriately.
- Boards should encourage working with supply chain partners and industry bodies to share information on threats and attacks, and drive the adoption of appropriate standards across supply chains.

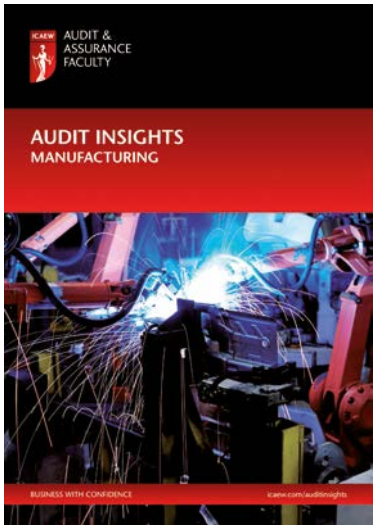
Appendix: updates to the 2013 report

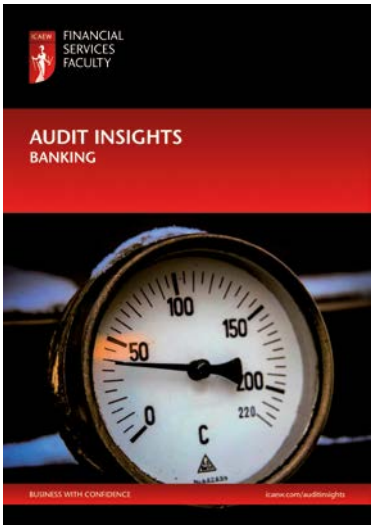
2013 FLAGS AND RECOMMENDATIONS	UPDATE
Flag 1: businesses should consider 'cyber' in all their activities	
• While cyber security has gone up the board agenda, in many businesses it remains a technical risk which is under the responsibility of the IT department and CIO. • The pigeon-holing of cyber risks 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 has been little evidence of a shift from technical to business risk and most businesses are still struggling to translate general awareness of cyber security into specific business risks. Some regulators are starting to look at these issues in more detail, such as the Bank of England and the SEC in the US.
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.	There is now widespread acceptance of this business reality. The need for a strong response capability has increased, especially given the impact of social media. However, most businesses still need to work on this. There has been little evidence to date of the impact of information-sharing mechanisms.

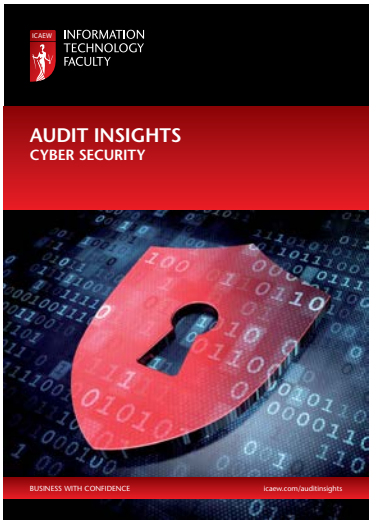
2013 FLAGS AND RECOMMENDATIONS	UPDATE
Flag 3: businesses should focus on their critical information assets	
• Given that businesses will increasingly experience data compromises, they need to focus on their key data. It is no longer possible to protect all data all of the time and therefore businesses 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.	Auditors have seen improvements in this area, although many businesses are still planning rather than acting. The next 12 months will show the extent to which businesses are making real changes.
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.	This has been the area of greatest improvement, with more resource and management focus. Training in particular has been a key priority, which should lead to better individual behaviour. However, key challenges remain, such as complexity and having the necessary skills.

Other reports in the *Audit Insights* series









For more information please visit
icaew.com/auditinsights

Faculties Online

Easy access to the information you need to succeed.

How do you stay on top of the latest trends and updates while still doing your day-to-day job to the highest quality?

ICAEW's seven faculties and three supporting communities offer specialist technical information and thought leadership in their respective fields.

You can now subscribe to Faculties Online, the online resources of all the faculties and their communities for a single fee.

Faculties Online subscribers will get access to resources covering:

- Audit and assurance
- Business performance management
- Corporate finance
- Excel
- Finance and management
- Financial reporting
- Financial services
- Information technology
- Private clients
- Tax

ICAEW

BUSINESS WITH CONFIDENCE

icaew.com/facultiesonline

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 142,000 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

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

T +44 (0)20 7920 8681
E itfac@icaew.com
icaew.com/auditinsights

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