ICAEW

INFORMATION TECHNOLOGY FACULTY

AUDIT INSIGHTS
CYBER SECURITY

BUSINESS WITH CONFIDENCE

icaew.com/auditinsights

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.

The IT Faculty has led 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.

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 and also asking how the International Framework for Assurance Engagements can be applied and developed. The faculty answers demands for practical guidance with publications such as *The Assurance Sourcebook*.

The faculty also hosts the *Audit Quality Forum* (AQF) to bring 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 978-0-85760-943-4

AUDIT INSIGHTS
CYBER SECURITY

FOREWORD

Audit is a public interest activity. Reports from external auditors build confidence in financial statements and give credibility to companies and comfort to their stakeholders. External auditors see many issues during their work in auditing the financial statements of a company including issues related to its assets, people and markets.

Audit Insights is an opportunity for external auditors to bring some of their knowledge of a market sector or specialist field to the public, capturing more of the audit value for the public benefit. Shared insights and observations have been brought together, in an environment that protects client confidentiality, to produce this document.

Audit Insights: Cyber Security is the work of a group of external audit experts from large and medium-sized audit firms with many years' combined experience of auditing companies. Representatives of the following firms formed the working group of external audit experts: BDO, Deloitte, EY, Grant Thornton, KPMG and PwC.

The shift from 'information security' to 'cyber security' represents a change.

Traditional approaches to information security have focused on internal controls to achieve the confidentiality, integrity and availability of data. While these controls remain important, cyber security incorporates a wider range of internal and external factors:

- Potential threats now come from around the world and can involve organised criminals, corporate spies and hacktivists, as well as disaffected or careless employees.
- Security weaknesses can be found throughout a supply chain, not just within a single business.
- The impact of security failures can extend across every aspect of a business, including disruption of operations and customer service, interference with production control systems, damage to brand and reputation, theft of intellectual property or commercially sensitive information and regulatory fines.

Managing cyber-based risks to individual businesses, as well as the wider economy, requires many different stakeholders to work together. By sharing the insights in this report, we want to support informed public debate and help businesses to understand the changing nature of the threats that they face.

EXECUTIVE SUMMARY: FOUR FLAGS FOR CYBER SECURITY

The importance of cyber security has grown in recent years as reliance on information technology and the internet has increased. Cyber security issues affect businesses of all sizes and across all sectors. This report highlights four areas that external auditors believe are of most interest and relevance to senior management, non-executive directors, investors, policy-makers and other stakeholders.

FLAG 1: BUSINESSES SHOULD CONSIDER 'CYBER' IN ALL THEIR ACTIVITIES

Digital technology and the internet provide many opportunities to improve business performance. The ability of businesses to make use of new information about customers, competitors and others will increasingly influence business success. Alongside these opportunities, though, are risks around the security of important information and the digital infrastructure. A business needs to manage these cyber risks to ensure that it exploits opportunities in a secure and sustainable way.

Boards have become increasingly aware of cyber risks. However, cyber risks are frequently pigeon-holed as technical risks which are under the province of the Chief Information Officer (CIO). This makes it difficult to reach decisions which balance the opportunities and risks of digital technology and recognise the significant business impact that cyber security failures could have. In order to manage these risks effectively, businesses need to approach cyber risks as an integral part of business strategy and operations, not as a specialist technical topic.

FLAG 2: BUSINESSES NEED TO ACCEPT THAT THEIR SECURITY WILL BE COMPROMISED

While businesses still need to apply appropriate preventative controls to protect their information, they increasingly need to operate in a way which assumes that some of their information will inevitably be accessed by others.

An assumed state of compromise calls for a new mindset around security. For example, some degree of security breach has to be tolerated as an unavoidable part of doing business in a digital world. Businesses increasingly need to promote operational resilience and prioritise activities which deal with

EXECUTIVE SUMMARY: FOUR FLAGS FOR CYBER SECURITY

breaches, such as intelligence and monitoring, detection and response. There also needs to be a change in security culture to emphasise collaboration and information sharing ahead of secrecy and working in isolation.

FLAG 3: BUSINESSES SHOULD FOCUS ON THEIR CRITICAL INFORMATION ASSETS

Businesses cannot sustain an approach of protecting all their information at all times. Instead, businesses increasingly need to prioritise their information assets and focus their resources on their 'crown jewels'. This enables a more sophisticated risk-based approach to security which balances the benefits and costs of security measures, and identifies where security breaches would have a substantial impact on the competitiveness and sustainability of the business.

Most organisations, however, struggle to identify their critical information assets. In order to prioritise and protect their key information assets appropriately, businesses will need to develop far greater discipline and rigour.

FLAG 4: MOST BUSINESSES DON'T GET THE BASICS RIGHT

It is estimated that up to 80% of security breaches could be prevented by implementing basic good practices in cyber security. However, businesses of all sizes and across all industries still struggle to get the basics right.

There are a variety of reasons for this struggle, including complex IT environments and lack of expertise. However, people continue to be the weakest link in implementing effective security and human failings are increasingly being exploited by attackers to gain access to confidential information. Businesses will need to build greater personal accountability into their security policies and procedures in order to change behaviour and improve the implementation of security measures.

A CHANGING LANDSCAPE FOR SECURITY

Businesses need to expand the focus of their security activities in response to the changing environment. Traditionally, a business built defences around its boundaries and aimed to become a secure fortress. However, changes in technology and business models in recent years have made the organisational perimeter increasingly porous. Mobile devices, cloud computing, social media, outsourcing of services – all of these trends have led to large amounts of data being stored or accessed outside the boundaries of a business and its direct control. As a result, many businesses have valuable or confidential information held by suppliers or professional advisers, in IT outsourcing or cloud service providers or on the personal devices of employees.

This means that a business may need to extend its view of security. As well as protecting information which remains under its direct control, it may also need to consider the protection of information which is outside its immediate boundaries, or which is accessed by third parties.

Governments are increasingly interested in the ability of businesses to protect themselves and their wider supply chains against cyber-attacks. Given the importance of the growing digital economy, the impact of continuing security failures on individual businesses may be significant. Conversely, there is an opportunity to develop competitive advantage for national economies as secure places to do digital business. Furthermore, governments need to work closely with the private sector to ensure that cyber risks are managed appropriately because much of the critical national infrastructure is owned or operated by the private sector and so many private businesses are within the supply chain of the critical national infrastructure.

As a result, we are seeing increased government interest in this area. Effective regulation is challenging, given the speed of technological and business change, and there are inherent risks of unintended consequences around greater regulatory activity. However, government interest in this area is likely to grow, especially if breaches and losses continue to increase.

High levels of uncertainty about cyber threats will continue to hamper good decision making around security and pragmatic approaches are needed to cope with this. There is little reliable information about the scale of attacks and breaches and their real impact on consumers, businesses and the wider economy. IT security industry surveys may be perceived as self-serving and exaggerating the threat. Yet, national intelligence services may be unwilling to share information about the attacks they see for reasons of national security and most businesses continue to be reluctant to admit attacks or failures.

While there are initiatives to encourage greater information sharing, lack of transparency and good information is likely to remain a significant challenge. This will continue to hamper both business decision making and government policy-making. We therefore need to develop different, pragmatic approaches to cope with this high degree of uncertainty. For example, it may be helpful to break down specific types of cyber risk and build an evidence base where this is possible.

FLAG 1: BUSINESSES SHOULD CONSIDER 'CYBER' IN ALL THEIR ACTIVITIES

As businesses become increasingly reliant on digital technology to conduct all their operations, they need to understand both the opportunities and the associated risks. Digitisation is seen as a way of increasing efficiency, reducing costs and engaging more effectively with customers. It can enable businesses to reach new markets and find new ways of working within the organisation and with partners and suppliers. The ability to make use of information about customers, suppliers and competitors and others will increasingly influence business success. All of these trends are likely to accelerate as new waves of technology or managed technology services become increasingly affordable.

Exploiting new opportunities raises new risks around the resilience and reliability of the digital infrastructure and the security of valuable and important business information. Cyber security failures can cause significant damage to a business, including business disruption, reputational damage or loss of competitive advantage. Conversely, demonstrating good security in operations and customer-facing activities could increasingly become a point of competitive differentiation and advantage. As a result, the ability to exploit digital technology in a secure and resilient way will become increasingly central to business success.

While cyber risks have gone up the agenda of many boards, they often remain pigeon-holed as technical risks, reported on by the CIO. It is a welcome development that boards are more engaged on the subject of cyber risk, and this interest is reflected in growing numbers of cyber-related questions being put to auditors by non-executive directors in particular. However, many businesses are struggling to translate a general awareness of cyber risk into an understanding of the specific risks to their business, as well as the key steps they should take.

Central to this problem is the presentation of cyber risk as a discrete, and usually technical, topic, which misses the essential point that cyber risks are fundamentally business risks which underpin most operational and strategic activities. This approach makes it difficult to reach decisions which balance

the opportunities and risks of digital technology and recognise the significant business impact that cyber security failures could have. In order to manage cyber risks effectively, businesses need to approach them as an integral part of business strategy and operations, not as a technical or specialist topic.

Investors, regulators and other stakeholders need to consider how to incorporate cyber risks into existing governance frameworks. While boards should have growing interest and responsibility over cyber risks, stakeholders such as investors and regulators also need to consider how they will gain comfort over the ability of an individual business to protect the information that is critical to its future success and withstand attacks on its digital infrastructure.

Controls around the security of financial information have been part of the financial statement audit for many years. However, wider cyber security issues do not come within the financial statement audit; rather, they fall under the broader governance, compliance and risk management responsibilities of the board. Auditors can play an important role in both challenging and providing assurance over the management of cyber risks. External stakeholders also need to consider how businesses can meaningfully report these risks and provide appropriate levels of confidence.

Growing digitisation creates systemic risks to the economy which justify government attention. To date, governments have typically focused their attention on protecting critical national infrastructure from cyber risks. While this focus has been appropriate, governments may need to take a broader interest in cyber risks across the economy. The impact, for example, of a major incident in a large company or across a supply chain could have a significant impact on the economy, regardless of whether it is classified as critical national infrastructure. Given the interconnectedness of the economy, incidents can also spread across supply chains quickly, meaning that poor practices in one business can put others at risk.

BOX 1: THE RESPONSE OF GOVERNMENTS

The UK government published a cyber-security strategy in November 2011 and has taken a keen interest in promoting good cyber security. This focus reflects the importance of the digital economy to UK GDP, as well as the opportunities for UK security firms in building their businesses.

SOME OF THE KEY ACTIONS INCLUDE:

- **Awareness raising and good practices** – the UK intelligence agency GCHQ and the Department for Business, Innovation and Skills have published a variety of guidance on good practices, centred on the *Ten Steps to Cyber Security*.[1]
- **Information sharing** – the Cyber Information Sharing Partnership has been established to support business in sharing information about cyber-attacks and incidents.
- **Building skills** – the government is working with industry and universities to build PhD programmes, encourage apprenticeships and run competitions in cyber security.
- **Encouraging market incentives** – by endorsing a single organisational standard in cyber security, for example, it is hoped that businesses will be encouraged to demonstrate their capabilities to supply chain partners, insurance companies and customers. The FTSE 350 Cyber Security Tracker[2] aims to help larger companies benchmark themselves against peers in this area.

Many of these components are mirrored in initiatives by governments around the world. The US government, for example, has a Comprehensive National Cyber Security Initiative, which incorporates many elements similar to the UK government's strategy. The EU also has a cyber-security strategy which aims to improve security standards and responses across the EU, coordinate actions and share information.

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf.
2 A survey of FTSE 350 boards about their cyber governance processes, which has been carried out in the autumn of 2013 by the audit firms on behalf of the government.

FLAG 1: BUSINESSES SHOULD CONSIDER 'CYBER' IN ALL THEIR ACTIVITIES CONTINUED

Furthermore, it is essential to build business and consumer trust in digital technology if we are to maximise its benefits and grow digitally-based economic activity. Security has to be at the centre of this trust, and continuing security failures risk eroding public trust. Consequently, governments have a legitimate interest in ensuring that businesses of all sizes and across all industries respond effectively to the challenges highlighted in this report. This is reflected in the growing interest of governments around the world in promoting good security practices in businesses.

Nevertheless, effective government action is difficult to achieve because of the pace of change in technology and business models and the inherent international dimensions of cyber risks. Regulatory frameworks are therefore problematic in practice and if this points to the need for government advice instead, then the highly individual nature of the risks to each business means that it is hard to get beyond high-level generalisations. Furthermore, in the light of the Snowden revelations in particular, work may be required to build business trust in the actions of governments and how they may use sensitive information about threats, vulnerabilities and breaches.

Recommendations

- 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.
- Non-executive directors should challenge executive management to present a coherent approach to cyber risks across the business.

FLAG 2: BUSINESSES NEED TO ACCEPT THAT THEIR SECURITY WILL BE COMPROMISED

Although cyber threats remain highly uncertain, media reports, industry surveys and anecdotal evidence all suggest a growth in possible sources of threat and volumes of breaches. Organised cyber-criminal gangs, state-sponsored industrial espionage, hacktivists and lone hackers are all potential threats to businesses. Internal threats also remain strong, through the actions of disaffected or careless employees or contractors.

Business information is increasingly being spread across a supply chain of service providers. Many businesses have transformed the way they operate in recent years through the use of outsourcing and sub-contractors. As a result, a large business will typically transact, directly and indirectly, with thousands of suppliers, service providers and sub-contractors, often stretching across the world. Some of these suppliers may have access to valuable or confidential business information in order to do their jobs. Engineering sub-contractors, for example, may be given access to intellectual property; lawyers may have access to models being prepared to bid for companies or contracts; and accountants will have access to financial information.

While there may be significant benefits to operating in this way, in terms of efficiency, flexibility and access to specialist services, this 'extended enterprise' is creating serious challenges to information control and security. Procurement processes should address issues of information security, with the contract specifying control requirements and any assurance processes which are to be carried out. However, there is often a tacit assumption that suppliers will follow good practices and few contracts have adequate explicit provision in this area. This problem is likely to get worse with trends such as cloud computing, as businesses frequently have to rely on suppliers' terms and conditions and may have little opportunity to specify their own requirements or obtain assurance about suppliers' controls and processes.

There is a growth in end-user devices that are bolted onto corporate networks and often designed with functionality rather than security in mind. The pervasive use of tablets and smartphones is well established and employees are increasingly demanding the ability to access corporate systems on a mobile basis. The trend of Bring Your Own Device (BYOD), where employees

FLAG 2: BUSINESSES NEED TO ACCEPT THAT THEIR SECURITY WILL BE COMPROMISED CONTINUED

use their own computers, smartphones and tablets, rather than corporate devices, to access business systems and data, has mushroomed in recent years. This has led to a loss of control over devices and a mix of personal and business data on many devices. There is also a growing variety of internet-enabled devices, from intelligent household devices to engine management systems, which may connect to corporate networks to send or receive data.

In many cases, these devices are designed to be cheap, disposable and easy-to-use. Building in high levels of security is not always a key priority for designers and manufacturers, and developments in this area may therefore increase the vulnerability of organisations.

Businesses need to be agile and able to respond quickly to many types of cyber threats. Adversaries, whether from internal or external sources, can be highly targeted, sophisticated and persistent in their actions. Furthermore, many incidents can be traced to careless behaviour by employees. Businesses need to build a culture of learning around incidents and maintain the trust of all their stakeholders where significant breaches occur. This is especially important given the speed at which breaches, and the impact on customers, can be communicated around the world through social media such as Twitter.

Recent IT trends mean that businesses need to accept that their information security will inevitably be compromised and this calls for a new mindset around security. While businesses need to continue to apply appropriate preventative controls, they cannot expect to be able to secure information in all the places that it may be held

BOX 2: INTELLIGENCE AND MONITORING, DETECTION AND RESPONSE

A new approach to security increasingly emphasises resilience, and may mean prioritising security resources on activities such as intelligence and monitoring, detection and response. Possible actions to consider include:

- **Intelligence and monitoring**: intelligence on potential threats can be gathered from a variety of sources. Businesses or security service providers can, for example, monitor open sources of data and social media to identify where data has been leaked into the public domain. They can tap into the communications of potential attackers through the darknet or deep web[3] or hacktivist lockers[4]. They can also participate in information sharing schemes with trusted partners or the government and its security agencies, whereby they can understand attacks experienced by others and prepare for similar attacks in future.
- **Detection**: attackers can breach systems for months before being detected, stealing large amounts of sensitive data in the process. Therefore early detection is imperative in order to close down the breach and limit the damage caused. Having a clear baseline which represents normal activity is an important part of the detection process, as it enables abnormal activity (eg, high levels of data downloading, systems activity at unusual times of the day or access from unexpected places) to be quickly identified and investigated.
- **Response**: as well as implementing technical remedies to breaches, a business may need to manage a variety of stakeholder relationships in order to limit the overall impact of breaches on the business. This could include responding to customer concerns, ensuring compliance with any regulatory requirements and keeping investors informed. Learning lessons and continually improving resilience are also important, and simulations of major cyber incidents which test the ability of the business to respond and recover are typically very valuable.

3 Parts of the internet that are not accessible through conventional search engines. Specialist knowledge or software may be required to access resources, or resources may be shared through trusted networks of connected computers (often known as peer-to-peer file-sharing).

4 A private space, not accessible from search engines, where hacktivists can share information about their activities.

and against all possible threats. Instead, they need to operate in a mode which assumes security has been compromised and some information has been accessed by others. We term this 'an assumed state of compromise'.

A significant culture shift is needed to accept that some security breaches, and the rectification and other costs they involve, will be an inherent part of doing business in a digital environment, just as shrinkage costs are a feature of retail business. While a business can work to reduce these costs, they will not be eliminated entirely.

The assumed state of compromise also moves businesses towards a culture of collaboration and sharing information about common threats with trusted partners. This contrasts with traditional approaches, which have emphasised the need to keep information about systems and security confidential for reasons of competitive advantage or for fear of reputational damage. However, adversaries often work together and share information to mount sophisticated attacks. Consequently, there is a need to move from a defensive and secretive culture of 'need to know' to a more collaborative culture based on 'need to share'.

Recommendations

- 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.
- 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.

FLAG 3: BUSINESSES SHOULD FOCUS ON THEIR CRITICAL INFORMATION ASSETS

Businesses cannot protect all their information assets in all cases – they need to focus attention on their 'crown jewels'. Businesses often take a default position of retaining and protecting all information because filtering and prioritising information assets is difficult and time-consuming. However, this approach is becoming increasingly unsustainable given the enormous growth in data that most businesses are experiencing, as well as the great variety of security threats and weaknesses that exist.

Instead, businesses will have to prioritise their information assets and focus their resources on the information that is most critical to the competitiveness and sustainability of the business, and its ultimate success.

This shift will require significant improvement in understanding of information assets, as few businesses today are easily able to identify their most critical pieces of information, where they are stored and who has access to them. Businesses will therefore need to develop a higher level of discipline and rigour around the prioritisation of different types of information and make hard decisions on what is really critical.

By prioritising information assets, businesses can move from a technology or compliance-based approach to security to one which is based on risk. Many businesses approach security as a technology or compliance issue and try to lock down all information, frequently on a tick-box basis. Prioritising information assets leads to an approach which is based on risk and enables more sophisticated decision making on the justification of specific controls.

BOX 3: PRIORITISING INFORMATION ASSETS

Many businesses struggle to identify their critical information assets and undertaking a full prioritisation exercise can be a time-consuming and resource-intensive task. However, businesses can start by categorising data and systems to help them to identify their critical assets. They can then consider:

- Why do we care about it?
- Where is it?
- How well protected is it?

When looking at these questions, most organisations focus on what information is valuable to them:

- What would cause significant disruption if unavailable or corrupted?
- What would cause financial or competitive loss or reputational damage to the business if it were acquired by others or made public?

When looking at cyber risks, it is also helpful to consider the motives of potential adversaries and identify what information might be targeted by others, whether criminals, corporate spies, hacktivists or disaffected employees:

- What information would be advantageous for criminals or other businesses to acquire?
- Does the business engage in behaviour or take positions on any issues that might make it a target for a hacktivist group?

This exercise will be different for every business as it is closely related to risk appetite, competitive strategy and regulatory context. However, there are likely to be common themes within specific industries, for example:

- Intellectual property may be a key concern for R&D intensive businesses, although this can diminish once inventions are patented and put in the public domain.
- Consumer businesses may focus on protecting customer data and ensuring that customer services are not disrupted.
- Manufacturing businesses may concentrate on the reliability and efficiency of production and supply chain systems, as well as ensuring the quality and safety of products.
- Professional services firms may be most concerned with sensitive commercial information contained in contracts, tenders and financial models.

For example, it is important to recognise that all controls have costs attached to them, both in terms of direct costs of operating the control and the opportunity cost of slowing down or even preventing other business activities. A risk-based approach enables decision making which balances the costs and benefits of security controls. Where businesses have achieved this shift and approach controls as a matter of operational risk, they might choose to loosen controls if it can help them to be more responsive and innovative.

However, managing security as part of wider operational and business risk creates a demand for clear quantification of the costs and benefits of security measures. Such measurement has been a long-standing problem in the security field and capabilities here will need to improve to support more sophisticated decision making around specific controls.

The prioritisation of information assets needs to be supported by effective arrangements for information ownership, responsibility and accountability. This ensures that specific individuals are motivated to act and make evidence-based decisions on the use and protection of information, as well as dealing with broader questions of information quality. Strong governance therefore underpins a risk-based approach to security.

It is important to define information ownership clearly and properly. The difference between responsibility and accountability can be helpful here to ensure that accountability stays at a senior level, while responsibility for detailed tasks is delegated to the appropriate levels.

Responsibility for specific information also needs to sit with appropriate individuals who understand the role of that information in the business and have the authority to make decisions about its protection and use. While this role sometimes falls to senior executives, they often have neither the detailed knowledge nor the time needed to make good decisions about information. Alternatively,

in many organisations, the CIO is seen as the owner of information. However, as with cyber risk more broadly, such an approach can place undue emphasis on technical aspects and ownership of information should lie primarily with individuals in business functions.

Recommendations

- 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.
- 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.

FLAG 4: MOST BUSINESSES DON'T GET THE BASICS RIGHT

It is estimated that up to 80% of security breaches could be prevented by implementing basic good practices[5]. Such steps have been highlighted in many publications including the 2012 advice published by the UK government, *Ten Steps to Cyber Security*, and include up-to-date malware protection, controlled access to systems and regular system back-ups.

However, it is clear that businesses find it extremely difficult to get the basics right in practice. Furthermore, auditors frequently highlight the same problems every year, with little progress in between. While management usually have good intentions to make improvements, this is rarely translated into effective action.

Difficulty in getting the basics right can be attributed to a variety of factors. Experience shows that organisations of all sizes and across all industry sectors still struggle to achieve basic hygiene measures, albeit for different reasons. The speed of technology and business change also means that the key elements of basic hygiene need to be reviewed on a regular basis as circumstances may change.

The size and complexity of the IT environment in large companies typically make even basic security steps extremely challenging in practice. As businesses grow, they bolt together large numbers of devices, pieces of hardware and software applications. Systems may have been extensively customised over the years to meet changing business requirements. Complex systems environments can be further complicated by a patchwork of IT suppliers and just keeping malware protection and other software up to date can be costly, time-consuming and difficult to manage. The particular issues facing large companies are also highlighted in ICAEW's *Audit Insights: Banking* report.

By contrast, difficulties in getting the basics right in small and medium-sized enterprises (SMEs) can usually be attributed to a lack of skills, resources and prioritisation. Few smaller businesses have dedicated or specialist security staff and general management may struggle to understand the technical language prevalent in information security. Furthermore, in many SMEs, day-to-day operational matters take priority over security measures, resulting in poor levels of security.

5 As outlined by GCHQ in the *Ten Steps to Cyber Security*.

People continue to be the weakest link in implementing basic security measures. High-profile breaches can often ultimately be linked to human error or carelessness. For example, clicking on infected links and bringing viruses or other malware into the organisation, for example, is common. Connecting infected external devices, using mobile devices without appropriate security or sharing work-related information over social media are also widespread.

Far from getting easier, the challenge of implementing basic security measures is getting harder for many businesses, especially those with a high staff turnover or numerous contractors. A transient workforce makes it difficult to maintain a consistent security-conscious culture. Ensuring that staff has sufficient training, without investing large amounts of time and other resources, is particularly demanding.

Furthermore, modern workers' attitudes towards technology differ from earlier generations. They may be far more comfortable with using new technology and sharing information and can bring new skills and opportunities to organisations. However, enthusiasm for new technology is not always matched by an awareness of the risks involved.

In order for people to change their behaviour, businesses will need to build greater personal accountability into security policies and procedures. A key challenge in getting people to follow good practices is that there is often little personal benefit in doing so. Indeed, security measures frequently slow down work or hinder the employee from doing what they want to do. Psychological research shows us that people are generally poor at making decisions around risk and trading off short-term benefits against long-term costs and uncertainties. As a result, businesses need to ensure that the consequences of careless or non-compliant behaviour are clear.

BOX 4: THE HUMAN FACTOR

The UK Information Commissioner's Office publishes many examples of breaches of data protection laws which have been caused by careless behaviour, including personal information being repeatedly sent to the wrong recipients, personal data being uploaded onto public websites and the loss of computers containing large amounts of unencrypted personal information.

Modern techniques of attack exploit careless or malicious activities of employees. Many targeted espionage attacks on companies start with a sophisticated 'phishing' email, where an employee, often a senior executive, receives an email which purports to come from a fellow employee. Instead, the email contains a link with malware, which gives the attackers access to the employee's computer. Social media are often used to find information to personalise emails and make them more convincing.

For example, the 2012 attack on Saudi Aramco, whereby a virus infected 30,000 computers and destroyed their hard drives, is reported to have started with a phishing email sent to an employee. Companies can run fake phishing exercises to test and educate staff, and one such example showed that over 25% of staff clicked on the malicious link.

Getting employees to connect infected USB sticks into corporate networks, whether maliciously or innocently, is another common means of attack. For example, it is reported that the 2010 Stuxnet attack on the control systems of Iranian nuclear power plants involved an infected external device such as a USB stick. It remains unclear whether the employee was aware of the infection.

FLAG 4: MOST BUSINESSES DON'T GET THE BASICS RIGHT CONTINUED

It is possible to approach accountability in different ways. Businesses can 'make it personal' and use the trend of BYOD to improve behaviour. When using their own devices, employees may be more directly incentivised to look after them properly. Alternatively, businesses can bring in stricter penalties where employees fail to look after assets properly. When this is done effectively, there can be a significant drop in the number of devices lost.

New skills are needed in order to bridge the gap between security and the wider business. In many businesses, there is a large gap between boards, in particular, and the security function, hindering effective communication and common understanding of risks. In these circumstances, it is difficult for businesses to make good decisions about security and achieve high levels of senior commitment to good security.

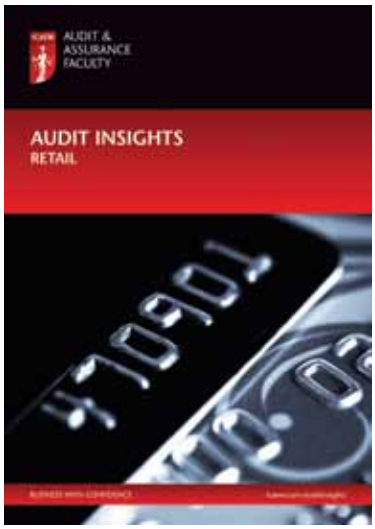
Information security leaders increasingly need to focus on communicating with other business leaders, bridging the gap between the board and the security function. A Chief Information Security Officer with substantive business skills can perform this role. In practice, though, most businesses establish fairly technical posts more akin to a head of IT security.

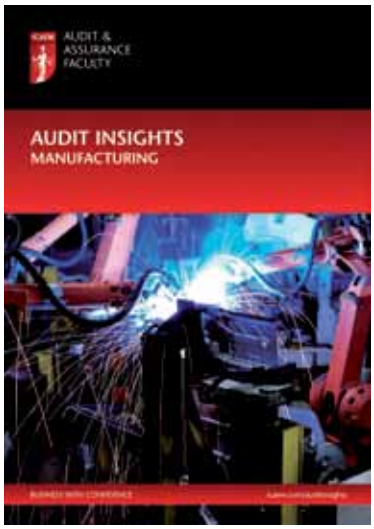
Likewise, greater awareness and skills around cyber security are also needed in business roles. If cyber is to become part of a business's DNA, rather than being left to IT and security experts, a wide variety of employees will need to understand and engage in discussions about security issues.

Recommendations

- 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 identify the right questions to ask.
- Boards should demonstrate commitment to a strong security culture and show leadership to encourage behavioural change where needed.

OTHER REPORTS IN THE AUDIT INSIGHTS SERIES





For more information please visit
icaew.com/auditinsights

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 140,000 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