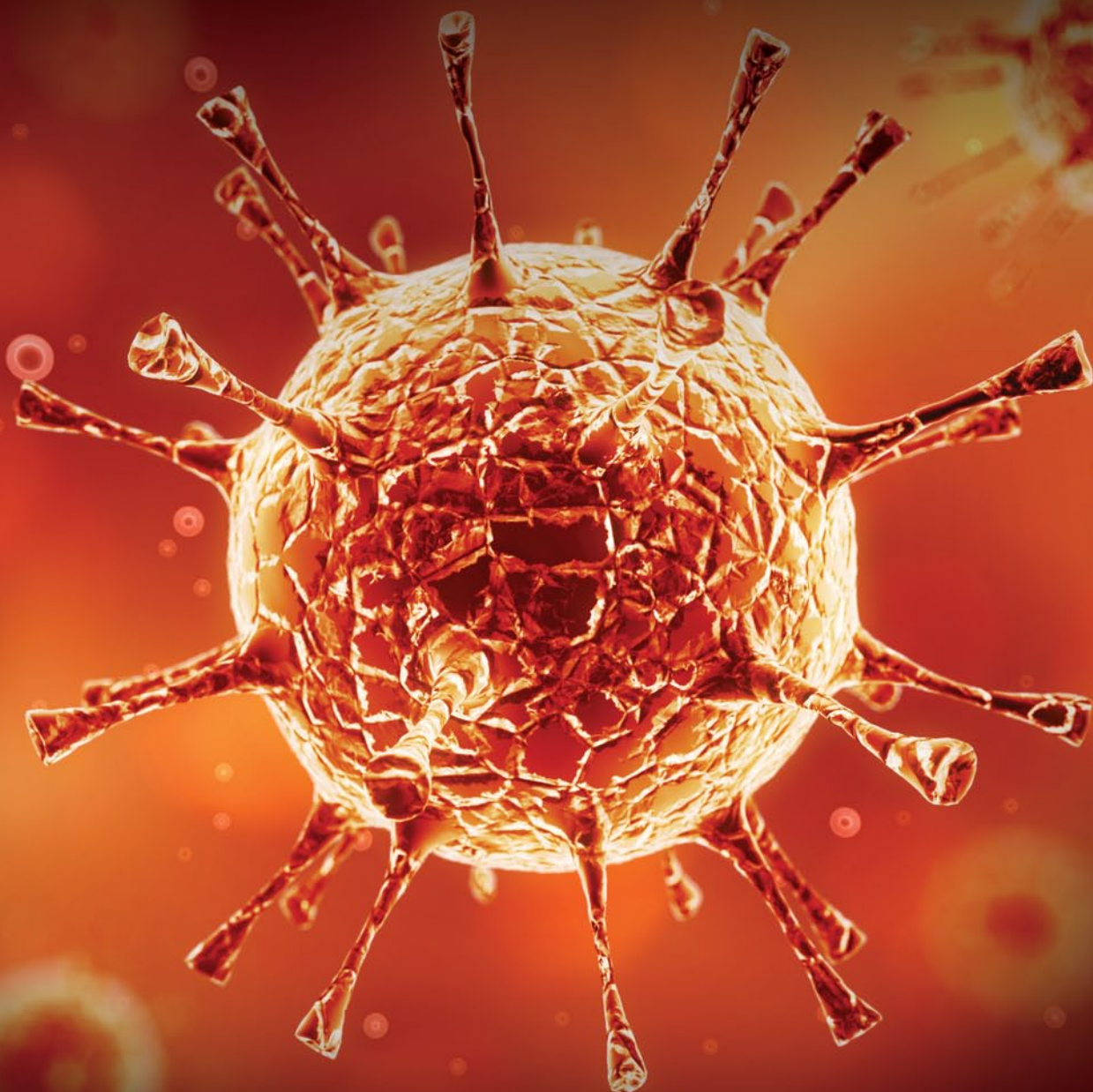




INFORMATION
TECHNOLOGY
FACULTY

Audit insights: cyber security

Taking control of the agenda



Contents

Foreword	4
Executive summary	5
Introduction	7
See cyber risks as real and dynamic	9
Take behavioural change seriously	12
Recognise security as a precondition for operating	15
Appendix	18

Foreword

Reports from external auditors aim to 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.

External auditors see many issues during their work in auditing financial statements that have a broader application and are of wider interest than the financial statements alone. This includes issues related to an organisation's assets and liabilities, people, processes and the market in which it operates.

Audit insights is an opportunity for external auditors to share some of their knowledge of specific sectors with the public, capturing more value for a wider audience. Shared insights and observations have been brought together in an environment which protects client confidentiality to produce this document.

Audit insights: cyber security is the work of a group of audit experts from the six largest audit firms, with an independent chair, based on their many years of experience in IT audit and assurance in the UK and internationally, and on their current involvement in planning and delivering IT audit and assurance engagements. This report provides a further update to the four findings highlighted in the *Audit insights: cyber security* report, published in November 2013 and updated in 2014 and 2015.

Executive summary

The impact of cybercrime is growing across the economy and cyber risk continues to be high on board agendas. However, businesses are struggling to turn general awareness and concern into effective action. This slow pace of change is increasingly frustrating governments and regulators, and businesses need to show more urgency and take control of their cyber agenda.

See cyber risks as real and dynamic

Many organisational risks are fairly static and predictable. By contrast, cyber risks are constantly evolving at a high pace and in an unexpected manner. The broad and connected nature of cyber risks make them particularly hard to manage. Cyber risks also remain largely abstract and high level rather than real and operational. To improve their management of cyber risks, boards need to adopt an approach and mindset that is more fundamentally agile and business-centric.

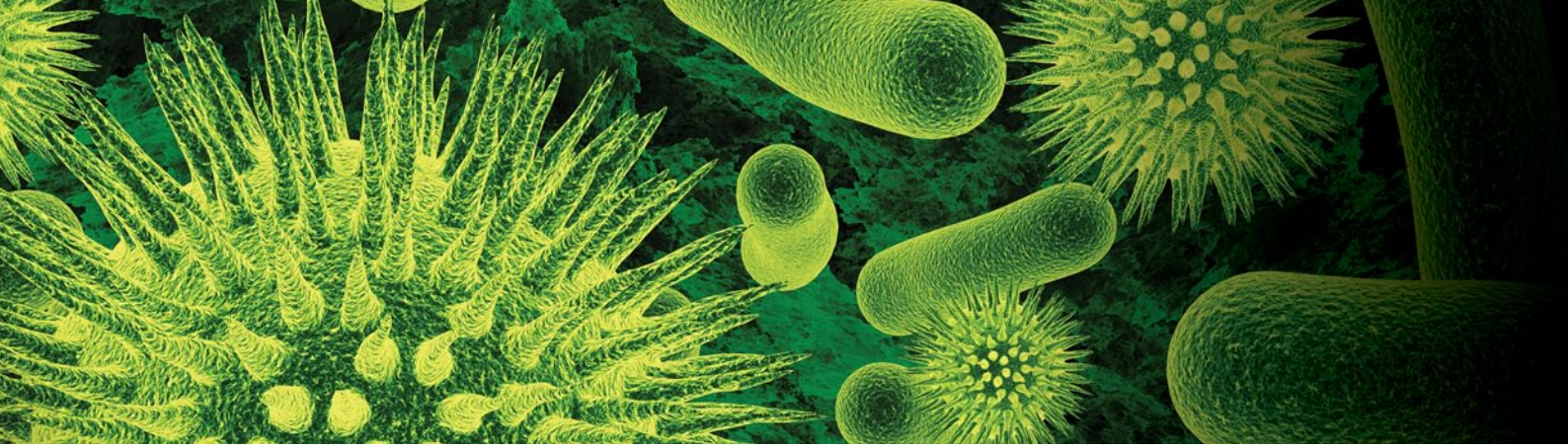
Knowledge about cyber security has improved on many boards. However, there is still scope to improve the quality of many boards' cyber security discussions, which can often exhibit lack of confidence, limited challenge to specialists and poor articulation of why cyber security matters to the organisation.

Take behavioural change seriously

It has been said for many years that people are the weakest link in cyber security. To mitigate this, most businesses undertake security training and awareness campaigns for employees. Yet it is proving difficult to embed the behavioural changes needed to support effective cyber processes within an organisation.

In response, some businesses are attaching more significant consequences where staff fail to comply with policies and expected behaviours. Organisations also need to rethink their approach to cyber security training more radically to improve their results. Training is often generic and does not connect good practices with the specific business imperative for following them. Until businesses get better at linking cyber risks with business objectives, and attaching real consequences to non-compliance with expected behaviours, cyber security training and campaigns are unlikely to have the desired impact.

While training and awareness-raising activities are important, they are only part of the picture. Leading businesses recognise that good cyber security behaviour is a matter of organisational culture, meaning that security is integral to the values and goals of the organisation, with strong leadership at the heart of this cyber security culture. A good culture is also reflected in responsibility for an ownership of cyber risks. This should be spread across the organisation and not limited to IT or specialist functions.



Recognise cyber security as a precondition for operating

If companies cannot keep their goods and customers safe, their ability to trade successfully will ultimately be diminished. It seems strange, therefore, that many businesses continue to view cyber security as a bolt-on activity rather than as a precondition to operating. While a digital infrastructure underpins the activities of most businesses today, many organisations only consider cyber risks as an afterthought.

By designing everything with security in mind, good practices simply become part of the job. In contrast, retrofitting security into solutions late in the process means that it typically becomes a 'blocker', and cyber security requirements add time, complexity and effort into tasks. This substantially increases the challenge of changing behaviour to be more security-conscious.

Because of the changing nature of cyber risks, businesses need to build in flexibility and resilience as far as possible. The principle of cyber-by-design has to be accompanied with an approach of regular review and re-evaluation of the risks. To prioritise cyber security requirements, businesses also need to be prepared to make difficult decisions. Adopting a 'sticking plaster' approach to security may be pragmatic but a business may need to recognise that at some point, more fundamental change is needed.

Introduction

Businesses are struggling to turn general awareness and concern about cybercrime into effective action. There are various reasons for this, including lack of knowledge, insufficient economic incentives and specific challenges around the nature of cyber risks. However, businesses need to exhibit greater determination to take control of their cyber agenda.

The 2016 UK crime statistics highlight the extent of cybercrime and fraud, showing nearly 6 million computer-related fraud and other incidents, and **1 in 10 adults as victims**. Businesses continue to suffer high-profile breaches and show poor response capabilities, demonstrated in September 2016 when Yahoo took two years to discover and admit that 500m of its user records had been breached. This is leading to growing frustration within governments and regulators at the current slow pace of change in business practices needed to deal with cyber risks. More radical regulatory action is possible in order to drive quicker improvements.

Increasing regulation around the world

Regulators around the world are strengthening rules concerning the protection of personal data and the management of cyber risks, especially for businesses in financial services and other areas of critical national infrastructure.

New or forthcoming legislation in the EU includes:

- the General Data Protection Regulation (GDPR), which updates and replaces the existing regulatory framework around the protection and use of personal data; and
- the Network Information Security (NIS) directive, which specifies obligations regarding cyber security in certain industry sectors, largely associated with the critical national infrastructure and major information processing activities.

In the UK, the Information Commissioner is becoming more proactive in examining the privacy policies of major technology companies such as Facebook.

In the US, the SEC has become more interested in the cyber agenda, auditing brokers and advisers on their cyber security practices. It is increasingly proactive in challenging filers about whether they are reporting their cyber risks appropriately. In addition, there is a trend towards civil litigation, with growing numbers of customers and shareholders suing companies and directors after a breach has occurred.

Asia is also experiencing this regulatory trend, as many countries look to strengthen their data protection regimes in particular. Australia, for example, has proposed a breach reporting requirement in this context. Singapore is planning to implement a new cyber security law in 2017.



Businesses today need to recognise good cyber security as a business imperative and shape their management of cyber risk to maximise the benefits. They can build a positive case for cyber security based on business trust, brand, culture, organisational agility and long-term competitive advantage. This means taking control of the agenda, and approaching it from a mindset that emphasises being proactive, agile, focused on behavioural change, and building cyber into the DNA of the organisation.

Otherwise, their approach will increasingly be driven by the requirements of regulators. While this may provide clearer incentives for action, relying on regulation to shape an approach to cyber risk will leave a business behind the curve given the pace of change in technology, business models, ways of operating, and cyber-attacks. It will also potentially lead to a tick-box mentality rather than the behavioural change required to embed good practices in the organisation and provide the flexibility needed to respond to new and evolving cyber threats.

See cyber risks as real and dynamic

The nature of cyber risks

Many organisational risks are fairly static and predictable. By contrast, cyber risks are constantly evolving at a high pace and in an unexpected manner, as follows.

- Threats change as attackers get more sophisticated and find new ways of breaking into systems. New attackers also emerge, as easy-to-use tools reduce the level of skill required to carry out attacks.
- Vulnerabilities change as businesses digitally transform their business models and ways of working, potentially creating new weaknesses in business processes, eg, mobile ways of working, or adoption of the internet of things.
- Existing controls and assurance models are superseded by new approaches. For example, moving to cloud-based systems has made traditional assurance models around IT controls more difficult to apply.
- The impact of failures increases as businesses capture more data and rely more heavily on digitally-based services. A slow or poor response to a major breach is very quickly and publically shared over social media, increasing at least short-term reputational damage.

The broad and connected nature of cyber risks also make them particularly hard to manage, as detailed here.

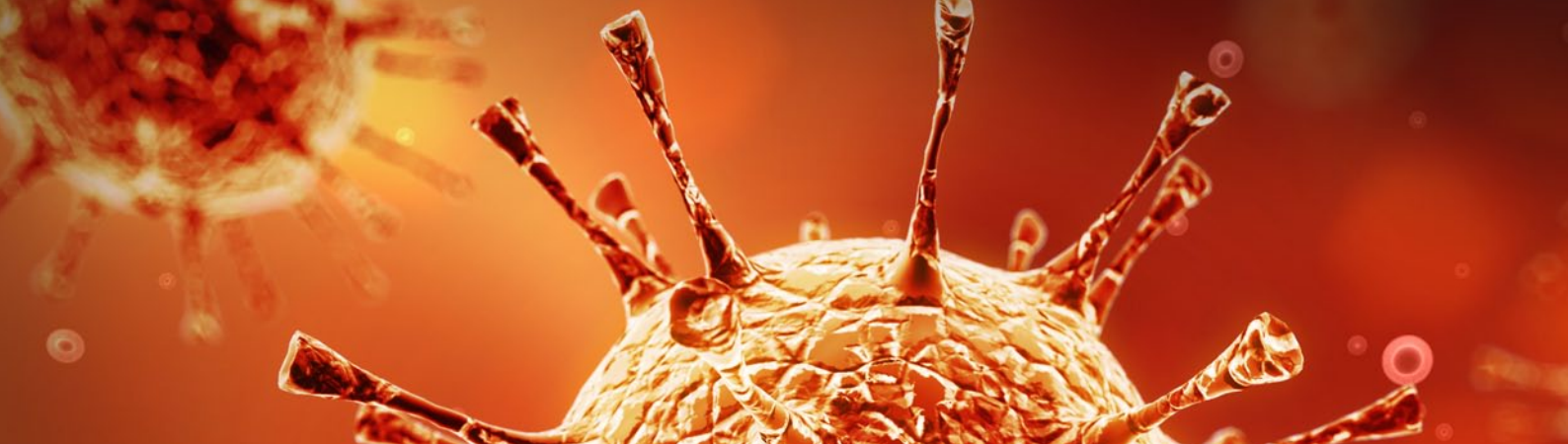
- They are multifaceted in nature and require a variety of different measures across the entire organisation.
- The impact of failures cannot necessarily be isolated or contained within single systems, networks or organisations, creating potential systemic risks.
- Integrated and connected supply chains mean that businesses are not in direct control of many areas of risk and are therefore reliant on the control delivered by others.

This dynamic and multidimensional nature requires a different way of thinking. There is still a need for good controls, and the *Audit insights: cyber security* series has emphasised the importance of getting good basic security right. Highlighting 'cyber' as a specific risk can help to get attention in the first instance. Integrating cyber risks into general governance and risk processes can then provide discipline and a structured way of approaching the topic.

However, businesses need to go further. Many businesses, for example, enter 'cyber risk' onto a risk register. They may review the risk and their response once or twice a year. But this will not enable them to cope with the pace of change and the complexity of cyber risks. It also means that cyber risks remain largely abstract and high level rather than real and operational.

Instead, boards need to adopt an approach that is more fundamentally agile and business-centric, including the following.

- Being proactive in identifying and coping with fast-changing threats and weaknesses.
- Regularly reviewing data assets and prioritising their 'crown jewels' of data.



- Disaggregating 'cyber risk' on risk registers and embedding more specific cyber risks into business operations.
- Building response and resilience capabilities in the event of attacks and breaches.

Improving board discussions

Knowledge about cyber security has improved in many boards. Non-Executive Directors in particular have been able to share knowledge and experience between and across sectors. There is still scope to improve the quality of many boards' cyber security discussions, though, as they can exhibit the following.


- A lack of confidence, leading to over-reliance on specialists and limited meaningful challenge to actions, frameworks and recommendations.
- Lower quality information to support decision making compared to more established risk areas, such as lack of historical or comparative data, or a lack of business context for technical information.
- Weak articulation of why cyber security matters to the business, the magnitude of risks and the proportionality of response.

There are a number of approaches and tools that can help boards improve the structure and confidence in discussions. The [US NIST framework](#) provides an industry-based approach to understand risks, mitigating actions and resilience. Reviewing cyber risks on a more regular basis than other types of risk can build up experience, knowledge and confidence. External advisors can support boards in asking the right questions and engaging in meaningful debate. The three lines of defence model is also a common approach deployed in many areas of organisational risk and assurance and is increasingly popular in the cyber risk area.

The three lines of defence

This model applies controls, assurance and oversight at three different levels in the organisation.

- The first line is at an operational level, with controls built into processes and local management responsible for their operation in practice ie, identifying and managing risks on a day-to-day basis.
- The second line is at functional specialism level, for example the role of cyber-security specialists and a chief information security officer ie, providing oversight and expertise.
- The third line is at the level of internal audit functions or independent assurance providers ie, providing assurance and challenge concerning the overall management of the risks.



Boards can find it helpful to map out responsibilities, oversight and assurance across these three different levels. This can provide comfort as well as a way of ensuring sufficient challenge throughout the organisation.

Internal audit functions play a crucial role here. Few internal audit functions in practice, however, have sufficient experience and expertise in cyber risks. In many cases, they are struggling to transition from a focus on technical IT and operational controls to a wider view of the governance and strategy around cyber risks.

Making discussions real and personal is another common theme. Ways of doing this include the following.

- Focusing on the specific business context around attacks and vulnerabilities, and the potential impact on business critical assets.
- Using tools such as incident simulations, scenario planning and cyber war games.

Linking cyber risks into strategic discussions can also help boards who are more focused at that level. For example, digitally transforming business models, expanding into new markets and M&A activity all have significant cyber risks that should inform broader strategic discussions.

Finally, it is helpful to have a more external focus and learn from events elsewhere. This could include intelligence on threats and attacks on others, cyber security activities of peers, experiences in other industries and the perspective of regulators. Drawing on the circumstances and impacts of recent high-profile breaches can also energise board discussions.

Checklists for boards

- **Be ready to respond.** Consider the most serious possible breach and ask whether the organisation, and board, are ready to cope. What do you do if competitors access your IP? How do you reassure customers if their data is stolen?
- **Build intelligence.** What do you know about specific threats, the actors and their possible methods? How have other major breaches happened, and how do your defences compare? What are your peers doing to manage their risks? How can you get ahead of the regulators?
- **Be specific and real.** How can critical data actually be accessed, and by whom? What controls are in place, and how do you know whether they are working? How will you detect any breaches?
- **Link to strategic change.** How are major strategic initiatives changing the risks? What is the impact of any M&A activity? What are the risks attached to new products or market expansion?

Take behavioural change seriously

Attaching consequences

It has been said for many years that people are the weakest link in cyber security. Poor password discipline, clicking on infected links, inserting infected USBs into systems – all are very common ways that attackers can exploit human weaknesses to get access to systems and data. Indeed, as businesses generally get better at technical controls against external attacks, criminals are increasingly targeting staff to provide unauthorised ways into networks and data. Furthermore, accidental data loss as a result of staff actions is still very common.

To mitigate this, most businesses undertake security training for employees, with the best ones doing it on an ongoing basis, not simply at the point of joining. Some organisations also test employees, for example sending fake phishing emails, or do physical checks to identify passwords written down and left unhidden or screens that are unlocked. Employees are often obliged to read and accept security policies on an annual basis.

Yet, it is proving difficult to embed behavioural changes, despite years of investment in such activities. In response, some businesses are attaching more significant consequences where staff fail to comply with security policies, for example incorporating training and testing activities into performance objectives.

Tailoring training

Organisations also need to rethink their approach to cyber security training more radically to improve their results. Training is often generic and does not connect good practices with the specific business imperative for following them. Typically, all employees go through the same training, although specific roles are likely to require very different levels of cyber risk awareness and training, for example the following.

- Those handling customer data or sensitive commercial data will need high levels of awareness and care in their day-to-day jobs and therefore detailed training may be needed.
- Those in finance functions may be subject to specific attempts of social engineering and fraud on which training could particularly focus.
- Others in the organisation may just need general awareness of good security practices.

Furthermore, psychological and behavioural economics research shows that people often have difficulty in understanding risks and typically prioritise short-term benefits, such as ease of use, ahead of longer-term risks. Building a strong and personal message around the value and benefits of good security is critical to success.

Unfortunately, this highlights a key weakness of many businesses that has featured throughout the *Audit insights cyber security* reports – the difficulty in articulating the specific benefits and risks from cyber security. Until businesses get better at linking cyber risks with business objectives and operations, and attaching real consequences to non-compliance with expected behaviours, cyber security training and campaigns are unlikely to have the desired impact.



Making change stick

The Driver and Vehicle Licensing Agency (DVLA) is an executive agency of the UK Department of Transport. It holds over 45 million driver records, over 39 million vehicle records and collects around £6 billion a year in Vehicle Excise Duty. Effective information governance and cyber security are critical to its digital transformation and maintaining public confidence in its services. Embedding good information security behaviours across its 5,500 employees is also vital. Some of the Agency-wide factors that support this include the following.

- Proactive leadership on all aspects of information security through a senior data governance board reporting directly to the executive team.
- A willingness to learn and share, for example the Agency recently took part in a consensual audit carried out by the Information Commissioner's Office, which assessed the security of its personal data and its data sharing controls and received a high assurance rating.
- A comprehensive assurance programme for third parties receiving DVLA's data to help ensure they meet their contractual obligations to protect it.
- A tailored annual information security training programme for all staff which is fresh and engaging.

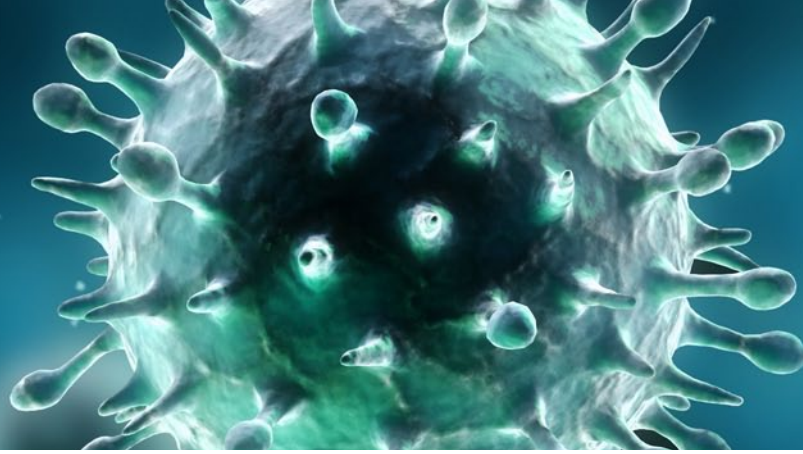
Cultural transformation

While training and awareness-raising activities are important, they are only part of the picture. Leading businesses recognise that good cyber security behaviour is a matter of organisational culture. This means security is integral to the values and goals of the organisation. Security-conscious behaviour is expected by peers, not driven by checklists or performance-related incentives.

Strong leadership is at the heart of a cyber security culture. Boards in leading organisations just 'get' the importance of security and role model the right behaviours. This contrasts with leaders in less security-conscious organisations, who are often prone to bypassing controls themselves or see security purely as an IT or compliance matter.

A good culture is also reflected in responsibility for and ownership of cyber risks. This should spread across the organisation and not be limited to IT or specialist functions. It needs to spring from grassroots activities and not be imposed from the top. Features like cyber security champions can play a useful role in embedding it into local cultures.

Underpinning change is a strong emphasis on communication that removes the technical jargon and translates cyber security into language that is understandable and meaningful for employees. The UK Government survey on Cyber Security Breaches 2016, for example, highlights the way that the health and care sector can effectively link security into an existing culture focused on patient confidentiality. Financial services businesses usually have cultures that are strongly based around risk and regulation and cyber security can be aligned to this.



Insider attacks

Insiders present a major threat in cyber security. Although media stories often focus on external attackers, or careless behaviour by staff, many high-profile breaches have been enabled by the deliberate actions of insiders. This could be for criminal aims, stealing data to use for their own benefit, or to sell to others. A recent example was the [data breach reported by Sage software](#) in August 2016, when a member of staff was arrested shortly after the incident. Insiders can provide access into systems for third parties. Whistleblowing, from Wikileaks to the Panama Papers, frequently relies on the actions of insiders to pass data over to journalists and others.

Therefore, when considering people-related issues, businesses also need to think about the actions of those who may be motivated to act against the interests of the organisation, and put in place controls to identify suspicious activity or potential threats. Data analytics, for example, presents good opportunities to monitor employee activities and flag behaviours or patterns that need further investigation.

Checklists for boards

- **Attach consequences.** What behaviour is unacceptable because of cyber risks? How do you know if non-compliance is occurring? What happens to employees who do not follow the rules?
- **Tailor activities.** How relevant is cyber security training to specific roles and responsibilities? Do higher-risk jobs have higher levels of training and awareness-raising activities? Are staff clear about the purpose of good cyber behaviour?
- **Hold boards to the same levels of accountability.** Are boards expected to follow the same rules as staff? Are you clear as to the purpose and consequences of non-compliance? Do you see yourselves as role models for good cyber behaviour? Do you act as role models?
- **Remember insider risks.** What is in place to detect suspicious behaviour or patterns? How are disgruntled or disaffected staff identified? Do you know how much system access potentially disaffected staff have?

Recognise security as a precondition for operating

Cyber-by-design

If companies cannot keep their goods and customers safe, their ability to trade successfully will ultimately be diminished. Looking back through history, a secure infrastructure has always underpinned the development of successful companies and industries, from trading companies to railroads. It builds the trust of customers and investors and supports the expansion of markets. In contrast, lack of security and trust slows growth and discourages trading.

It seems strange, therefore, that many businesses continue to view cyber security as a bolt-on activity rather than as a precondition to operating. A digital infrastructure underpins the activities of most businesses today. Given the widespread impact of cybercrime across the economy, as highlighted earlier by the UK crime statistics, it might be expected that businesses would want to demonstrate their security and trustworthiness in this context. Yet, many organisations only consider cyber risks as an afterthought.

Recognising cyber security as a precondition for operating means designing all activities based on consideration of cyber risks. It is easy to envisage cyber-by-design principles at the heart of IT systems development to ensure the right technical controls and a resilient architecture. But to be meaningful, the principle needs to be all-encompassing and included in the design of, for example:

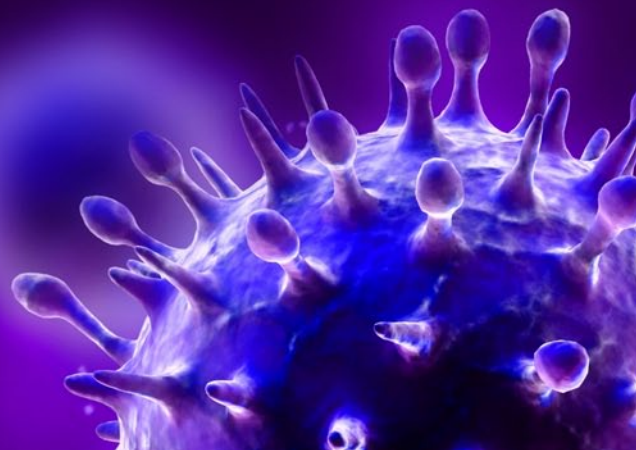
- business processes and organisational change;
- governance and oversight models;
- innovation and new product development; and
- mergers and acquisition activity.

Retrofitting security

There is always a tension between locking down systems and data and providing easy access to enable efficient working. By designing everything with security in mind, and proactively assessing this balance, security features can be added in a way that employees may not notice or do not add further work. As a result, good practices simply become part of the job.

In contrast, retrofitting security into solutions late in the process means that it typically becomes a 'blocker' and cyber security requirements add time, complexity and effort into tasks. This substantially increases the challenge of changing behaviour to be more security-conscious. Furthermore, it raises significant risks of shadow IT, which operates outside the control of the IT function. A typical example here is the use of personal emails by employees as a way of bypassing stringent controls. The result is far lower levels of security in practice than intended.

The emphasis on design-led security is mandated in the new EU data protection regulation. This common approach may help businesses to adopt new approaches and innovate in the cyber area.



GDPR leads the way

The General Data Protection Regulation (GDPR), due to come into force across the EU in 2018, will significantly strengthen business obligations around the protection of personal data. While it focuses on a sub-set of organisational data, it will have implications for how businesses think about its security and use of data more broadly.

It has been negotiated over many years and balances a number of competing interests, but it can be seen as leading in some of the obligations it will impose on businesses, including the following.

- Incorporating principles of privacy-by-design and privacy-by-default into business change projects, for example minimising the amount of personal data held and creating default settings which maximise privacy.
- Undertaking privacy impact assessments when projects have a major impact on the collection or use of personal data.

Complying with these principles will take a significant amount of change in many organisations and could lead to a different way of thinking about data across businesses that emphasises earlier thinking about security in business change projects.

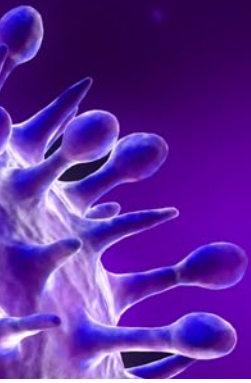
It should be noted that it is expected that **the UK is still likely to comply with the new regulation**, or something similar to it, regardless of the long-term relationship that is developed with the EU.⁴

Review and re-evaluate

Given the importance of designing a business based on cyber security, start-ups have an inherent advantage as they can build their systems and processes from scratch to be more secure. They do not have to grapple with the challenges presented by a mix of old legacy systems and the difficult job of process and cultural change. Given the technology-base of many start-ups, it might be expected that they, in particular, would 'get' cyber risks and adopt this approach.

But the picture in reality is more mixed. Start-ups tend not to have a mature risk culture and are driven more by the entrepreneurial instincts of the founders. The economic incentives around technology business models mean that early priorities are likely to be growth and building user numbers, which emphasise speed to market and functionality rather than security. Most start-ups will use cloud-based technology, so may see cyber risks as a matter for the cloud provider rather than for themselves. Even though they may be very digital-savvy, that does not necessarily translate into high levels of awareness or understanding around cyber risks.

Furthermore, businesses have to cope with constant change in cyber threats and the business environment. As a result, businesses need to be forward-looking in their design and build in flexibility and resilience as far as possible. The principle of cyber-by-design has



to be accompanied with an approach of regular review and re-evaluation of the risks. It needs a mindset of continual improvement and minimising of risks and impacts.

To prioritise cyber security requirements, businesses also need to be prepared to make difficult decisions. Product launches may need to be delayed if the design is not sufficiently secure, for example. Furthermore, adopting a 'sticking plaster' approach to security may be pragmatic but a business may need to recognise that at some point, more fundamental change is needed.

Checklists for boards

- **Implement cyber-by-design.** Are new products and services designed with cyber risks in mind? Do business change projects consider cyber risk early on? What are the risks of poor design? Where does shadow IT mean that security is lower in practice than expected?
- **Continually review and re-evaluate.** Are designs building in flexibility and resilience to cope with changing cyber risks? How often do you review cyber risks? How do you incorporate changing risks into existing processes?
- **Take difficult decisions.** Are you ready to delay major change or strategic projects if the security is not good enough? Is your business using a 'sticking plaster' approach to an old infrastructure? Is this sustainable?
- **Embed cyber into start-ups.** If investing in new businesses, are you considering the cyber risks? Are they designing themselves to be cyber secure and resilient?

Appendix

2013 findings ▼

1	Businesses should consider cyber risk in all their activities	UPDATE ▼
	<p>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.</p>	<p>Businesses are committing significant amounts of money to managing cyber risks. They are also willing to invest in hiring senior cyber security staff.</p> <p>Greater challenge is needed from boards, however, to ensure that money is being spent wisely and that appropriate mitigations activities are being undertaken.</p>
	<p>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.</p>	
	<p>This creates new systemic risks to the economy, as well as challenges to investors and regulators about cyber risk reporting and assurance.</p>	
	<p>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.</p>	
	<p>Recommendation 2: non-executive directors should challenge executive management to present a coherent approach to cyber risks across the business.</p>	
2	Businesses need to accept that their security will be compromised	UPDATE ▼
	<p>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.'</p>	<p>Businesses are investing more in their monitoring, detection and response capabilities. Leading organisations are also focusing on building intelligence on potential attacks and sharing information with peers.</p> <p>Breaches remain underreported. However, the new breach notification requirements in the GDPR will see a radical change in reporting and provide much more information to authorities on what is happening in practice.</p>
	<p>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.</p>	
	<p>There also needs to be a change of mindset, which emphasises collaboration and information sharing rather than secrecy.</p>	
	<p>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.</p>	
	<p>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.</p>	



2013 findings ▼

3	Businesses should focus on their critical information assets	UPDATE ▼
<p>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.</p>		<p>The growing adoption of the internet of things in businesses is leading to new vulnerabilities in networks and many new points of potential attack. This is increasing the need for businesses to categorise their data and focus resources on the areas of greatest impact and risk.</p>
<p>Most businesses are not very good at doing this and greater discipline and understanding of organisational data will be required.</p>		
<p>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.</p>		
<p>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.</p>		
4	Most businesses don't get the basics right	UPDATE ▼
<p>Up to 80% of security breaches could be prevented by having basic cyber hygiene in place, such as anti-malware software.</p>		<p>Most businesses are still struggling to make significant progress on getting basic security right. While awareness is high, changing behaviour in particular is proving to be very challenging.</p>
<p>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.</p>		
<p>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.</p>		<p>Businesses are also experiencing skills shortages for cyber security roles. This could be exacerbated by the new GDPR, as cyber security specialists could be attracted to new Data Protection Officer roles.</p>
<p>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.</p>		
<p>Recommendation 2: boards should demonstrate commitment to a strong security culture and show leadership to encourage behavioural change where needed.</p>		

Audit insights

A comprehensive series of publications offering unique practical insight and guidance from auditors, across a number of areas: retail, insurance, corporate reporting, cyber security, manufacturing, banking, construction and small businesses. Access all of the current reports at icaew.com/auditinsights

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 145,000 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 8635

E itfac@icaew.com

icaew.com/auditinsights

 [linkedin.com](https://www.linkedin.com/company/icaew) – find ICAEW

 twitter.com/icaew

 [facebook.com/icaew](https://www.facebook.com/icaew)

