ICAEW THOUGHT LEADERSHIP
AUDIT INSIGHTS

Audit insights: cyber security

COPING WITH INCREASING COMPLEXITY

Summary

COMPLEX LEGACY IT ENVIRONMENTS HINDER GOOD CYBER SECURITY

Many large organisations struggle with complex legacy IT environments made up of fragmented, non-standard systems that often need to be supported by information held in spreadsheets. These complex IT environments are typically the result of many years of business and IT decisions, and one of the unintended consequences is that it makes good cyber security, such as patch management, much harder.

In the longer term, organisations need to reduce the complexity of their IT architecture and simplify their systems. Yet even if companies were to rip their systems out and start again, the continual level of change means that complexity could easily creep back into the IT environment. Consequently, the most fundamental improvement that businesses can make is to embed cyber risk into decision-making across all business activities.

DESPITE IMPROVEMENTS, THERE IS A SUBSTANTIAL GAP IN CYBER SECURITY MATURITY LEVELS

There have been significant improvements in cyber security in most organisations over the last five years, reflecting substantial investment in cyber security programmes. There has been a particular emphasis on getting basic security practices right. Following the real-world impact of some high-profile breaches, such as Wannacry and NotPetya, businesses are also placing much greater emphasis on resilience, recovery and response to breaches.

However, there is a wide range of maturity levels in cyber security practices. The most mature companies are typically found in sectors such as financial services and technology, and are spending a lot of money combatting intensive cyber attacks.

BUSINESS NEEDS A SMARTER APPROACH TO CYBER SECURITY LAWS AND STANDARDS

Greater board engagement has been driven to some extent by regulators and governments, who have increased the pressure around cyber security over the last two or three years. This includes hard legal requirements. For example, the General Data Protection Regulation (GDPR), which updates personal data laws across Europe, will have a widespread impact as it comes into force.

There has also been a proliferation of cyber security standards around the world. While these all may be well intentioned, and aim for the same broad objectives, there is little co-ordination between initiatives. Consequently, businesses must become more proactive in developing a specific strategy around cyber security laws and standards that maps different requirements and builds broad capabilities to comply.

ISBN 978-1-78363-938-0

Introduction

FIVE YEARS OF AUDIT INSIGHTS: CYBER SECURITY

The first audit insights cyber security report, written five years ago, in 2013, highlighted four key challenges and priorities for boards in managing cyber risks.

- **Businesses should consider cyber risk in all their activities:** the challenge here is to move cyber risk from being pigeonholed as 'IT' to be seen as an integral part of all business risks.
- **Businesses need to accept their security will be compromised:** this emphasised a different mind-set, recognising some level of compromise as inevitable and broadening cyber security activities beyond prevention to include intelligence, detection and response.
- **Businesses should focus on their critical information assets:** given the inevitability of breaches, businesses need to prioritise their security activities around their most valuable pieces of data, although identifying these was often a major challenge.
- **Most businesses don't get the basics right:** the real challenge for businesses of all sizes is achieving basic cyber hygiene.

The three subsequent reports (2014, 2015, 2016) highlighted a number of related themes – the need for more meaningful board conversations; the real difficulties in changing employee behaviour; the challenges of managing cyber risks across integrated supply chains; and a growing government frustration that businesses are not doing enough, fast enough, to improve cyber security.

CYBER ATTACKS AND SECURITY BREACHES CONTINUE

There has been no let-up in cyber attacks and security breaches since the last Audit insights: cyber security report (October 2016). According to World Economic Forum's latest Global Risk Report (2018), cyber crime is expected to cost businesses US$8 trillion over the next five years. The UK government's 2017 cyber security breach survey showed that 46% of UK businesses had suffered cyber attacks or breaches over the previous 12-month period. For medium and large businesses, that figure rose to 66%. Furthermore, online fraud became the most common crime in England and Wales, accounting for half of all computer misuse and cybercrime, according to the Crime Survey of England and Wales, published in January 2017.

These statistics are reflected in a variety of high-profile incidents over the last 18 months that demonstrate the real-world impact of cyber breaches, the sophistication of some cyber attackers and the impact of a poor response to a major breach.

HIGH-PROFILE INCIDENTS (2016–17)

- **Bangladesh Central Bank (February 2016):** this was highly sophisticated and based on a good understanding of financial value chains. Attackers gained access to Bangladesh Bank's Swift credentials, which they then used to transfer money.
- **Yahoo (2013, 2014; revealed in February 2017):** while the breaches of 1bn and 500m customer accounts took place in 2013 and 2014, this was only disclosed in 2017 and consequently, Yahoo's sale price was dropped by $350m when Verizon bought it in February 2017.
- **Wannacry (May 2017)**: this involved the fast spread of a ransomware virus that encrypted data and demanded payments for unencrypting the data. It reportedly infected over 200,000 computers in 120 countries, including computers in many smaller businesses.
- **NotPetya (June 2017):** this ransomware attack, which closely followed Wannacry, was focused on Ukraine but also spread to a number of multinational companies, such as Maersk and TNT.
- **Equifax (May/June 2017):** around 143m customers of the credit ratings agency had their data stolen by hackers. This was one of the largest data breaches in the US.
- **Uber (revealed in November 2017):** hackers accessed data related to 57m customers and drivers worldwide in 2016. However, Uber did not disclose this to authorities or the affected individuals.

Looking to the future

The Audit insights series offers a snapshot of the current state of cyber security in businesses. This report reflects in particular on ongoing issues related to the complex nature of security in many businesses, as well as the improvements made over the last five years, since the series began.

Another key challenge in cyber security stems from the continually changing nature of the risk, especially given the fast pace of change in technology. New technologies provide both opportunities and challenges for cyber security. Big data, artificial intelligence and all types of automation, for example, create new risks and new targets for attackers. Greater reliance on algorithms and data for all business operations increases the potential impact of breaches and attacks. These technologies also provide great opportunities to improve cyber security through more automated controls, better understanding of anomalies on networks, and better prediction around the behaviour of attackers.

Although we recognise cyber security needs to be an ongoing and sustainable process in order to cope with this changing environment, this report does not focus on these new technologies, or reimagine how cyber security could look as a result. Future work will consider more fundamentally the extent to which current approaches adequately cope with changing cyber risks and whether new thinking is needed.

Complex legacy IT environments hinder good cyber security

COMPLEXITY AND BASIC SECURITY

Many large organisations struggle with complex legacy IT environments made up of fragmented, non-standard systems that often need to be supported by information held in spreadsheets. While they may support the business, such complex legacy IT environments make it harder to implement good security practices in a timely manner. Furthermore, attackers are increasingly exploiting these weaknesses in areas such as patch management.

TAKING TIME TO APPLY PATCHES

Patches are fixes to vulnerabilities in software code. Attackers can exploit these vulnerabilities while they remain unfixed and therefore it is a very basic principle of cyber security that organisations should update software with patches as soon as possible to minimise their risks.

However, many organisations fail to do this in a timely manner. Where there are complex legacy architectures, implementing patches is not as simple as it appears. Patches are changes to the system and therefore they should be fully tested to make sure that they do not interfere with any other existing software and are safe to apply into the live system. With so many systems to consider, this process can take a lot of time and resources. This time lag of applying patches is increasingly being exploited by attackers, for example in the Wannacry and NotPetya cases highlighted earlier. While the organisation is going through its processes to test and apply the patch, the attackers target the vulnerability.

Another process that is made harder by complex legacy IT environments is asset (hardware, software, data) management, as the sheer variety of assets in place can make this very time-consuming to achieve in practice. This also undermines other areas of basic security, as it is difficult to ensure assets are appropriately protected and up-to-date if the organisation does not have good visibility of what and where those assets are.

In the longer term, organisations need to reduce the complexity of their IT architecture and simplify their systems, most likely through moving into an environment that is more modern, cloud-based and agile. This is a highly complex task involving substantial investment and significant migration risks. Nevertheless it would still leave businesses with many security risks to manage, yet, at the same time basic cyber hygiene would be easier to achieve.

Where a full transition to a more modern architecture is not possible, organisations can mitigate the security risks by segregating older legacy systems or ensuring effective controls to manage the risks between older and newer environments.

THE IMPACT OF BUSINESS DECISIONS

These complex IT environments are typically the result of many years of business and IT decisions, for example:

- decentralisation of management structures, whereby subsidiaries develop and implement their own systems independently;
- development of bespoke systems to meet specific business needs, rather than using off-the-shelf packages;
- historic under-investment in systems, resulting in a variety of old legacy systems;
- purchase or management of systems or connected devices by non-IT staff, eg, control systems or scanners; and
- mergers and acquisitions, whereby the systems of acquired companies are not integrated.

As highlighted in this section, one of the unintended consequences of complex and disparate systems is that it makes good cyber security much harder. It requires significant resources just to keep things going securely – money most companies would rather spend on innovation. This also makes it extremely difficult to be agile, responsive and adaptable to new threats. It also makes it harder to communicate effectively about cyber risks.

Simplifying and standardising IT environments is an important step in this context. But even if companies were to rip their systems out and start again, the continual level of change means that complexity could easily creep back into the IT environment. Furthermore, much of the complexity is a result of broader business and IT decisions, such as bespoke systems or acquisitions.

Consequently, the most fundamental improvement that businesses can make is to embed cyber risk into decision-making across all business activities. As long as businesses treat cyber as a technical, bolt-on activity, rather than an underpinning of all operations, they will continue to create unintended challenges for security. As connected devices proliferate across organisations, eg, through the internet of things, the need for an integrated approach will become more urgent.

IMPROVING DECISION SUPPORT AROUND CYBER

These challenges are amplified by the need to improve the information available to many boards around cyber risk. This is reflected in a growing frustration in many boards at the slow pace of change from investments in cyber security and the lack of tangible impact of remediation programmes. These programmes can seem opaque for many board members, with little clarity on where problems lie and what needs to be done to increase the impact of the investment.

Translating complex operational information into something meaningful for board members is a crucial task for security specialists. The information needs to support good decision-making about cyber security, and boards need to have confidence in the accuracy of the information. Dashboards are an increasingly popular way of doing this. However, in many cases, boards still receive relatively poor-quality information.

Delivering better information needs clear thinking about the relationship between boards and security specialists. Boards are never going to be experts in cyber security – so what do they realistically need to know and understand? What information will help them to make decisions and fulfil their duties around the management of the risks? A better definition of the role of boards and their relationship with security specialists will greatly help the development of meaningful information.

RECOMMENDATIONS FOR BUSINESSES

- Integrate cyber risk: embed thinking about cyber risk into all business decisions and systems planning.
- Reduce complexity of IT environment: simplify and standardise the IT environment where possible; mitigate risks through, for example, effective controls between legacy and modern environments.
- Improve cyber risk reporting: make cyber risk reporting more transparent, qualitative and focused on the impact of security investments, for example, threat analysis and the extent to which investments have reduced cyber risk.

Despite improvements, there is a substantial gap in cyber security maturity levels

INVESTMENT IN BASIC SECURITY PRACTICES

There have been significant improvements in many organisations over the last five years, reflecting substantial investment in cyber security programmes. There has been a particular emphasis on getting basic security practices right, building on the estimate from the UK intelligence agency Government Communications Headquarters (GCHQ) that 80% of breaches could be prevented by good basic security (sometimes termed 'cyber hygiene'). The UK standard Cyber Essentials emphasises these basic security controls.

CYBER ESSENTIALS – THE FIVE BASICS

The UK government launched Cyber Essentials in 2014 with a view to providing a universal standard of cyber hygiene that would apply to all businesses, whatever their size and sector. It selected five technical controls, based on an assessment by GCHQ, around which controls would prevent indiscriminate, unsophisticated attacks. The five controls cover:

- boundary firewalls and internet gateways;
- secure configuration;
- access control;
- malware protection; and
- patch management.

Adoption is being encouraged by its inclusion in some UK government tendering processes.

Following the real-world impact of some high-profile breaches, such as Wannacry and NotPetya, businesses are also placing much greater emphasis on resilience, recovery and response to breaches.

And yet, most companies still struggle to achieve good basic security in practice, for many different reasons. Smaller businesses may not have the knowledge or skills to implement good practices. There can still be a lack of awareness, or security is not seen as relevant or a high enough priority. Most breaches have a human component, such as the downloading of an infected file; and making behavioural changes stick is proving difficult.

Furthermore, many organisations simply do not apply detailed processes consistently. Such application takes significant effort, time and resources, and detracts from more innovative activities. However, without improvements in basic discipline around cyber security, many businesses will continue to be vulnerable to many types of cyber attacks, whether directly or via their supply chains.

IMPROVEMENTS IN BOARD ENGAGEMENT

Board awareness has increased greatly in the past five years, and most boards now have cyber security on their agenda to some degree. Many boards have invested significant time and energy in cyber training, and knowledge levels have improved accordingly. Non-executive directors have played an important role in sharing knowledge across organisations, and many boards now have at least one member who focuses on cyber risk. Boards have generally improved their understanding of their critical data assets.

Many businesses are also working to improve the integration of security into business activities. The role of the Chief Information Security Officer has evolved from a technical focus to a more business- and board-orientated role. There has also been greater emphasis on training and testing of all employees with regard to phishing attacks, for example.

However, there continues to be a significant communications gap between boards and security specialists though. This increasingly reflects the difficulty in finding security specialists who are sufficiently business-savvy and credible to boards. In particular, there is a limited number of people who can perform the more business-orientated Chief Information Security Officer role effectively, and the turnover of senior staff is high. This compounds skills shortages in technical areas throughout organisations, increasing reliance on consultants and contractors, and making it harder to develop effective and trusted relationships between boards and security leaders.

There has been investment in new cyber security education and training, for example new university degrees. However, there is a significant time lag for newly qualified specialists to gain both the technical experience and the business knowledge and credibility to move into senior roles. As a result, the industry will need to find other ways to fill this shortage in the short to medium term.

VARYING MATURITY LEVELS

While many organisations have improved their security capabilities, there is a wide range of maturity levels in cyber security practices. The most mature companies are typically found in sectors such as financial services and technology, and are spending a lot of money combatting high levels of intensive cyber attacks. For example, they have established Security Operational Centres (SOCs) to focus on better intelligence and detection, and broaden their focus beyond traditional controls and preventative measures. They are also investing in new technologies such as artificial intelligence to improve cyber security. They are analysing different threat actors to help understand who might attack the business and tailor their response accordingly. Furthermore they recognise the importance of continually improving their process maturity in this area, in contrast to many other companies, which typically see security as a series of one-off tactical activities, such as new joiner security training or an annual board review.

Greater maturity does give significant advantages, sometimes in unexpected areas. Information sharing, for example, is an important part of a broad strategy to improve cyber security. As most attackers will use similar methods at other companies, sharing information about attacks among peers can provide intelligence to sharpen the defences of others.

However, not every company has the skills and ability to gain maximum benefit from this intelligence, and smaller businesses can be particularly disadvantaged. It takes significant technical resources to participate in these processes. Formal information sharing also does not replace informal networks among peers. However, there are some mechanisms, such as the UK Cyber Information Sharing Partnership (CiSP), which recognise these challenges for smaller businesses. Suppliers may also be able to help smaller businesses benefit from information sharing activities.

RECOMMENDATIONS FOR BUSINESSES

- **Apply discipline:** focus on applying strong discipline around security and consistently complying with good practices.
- **Continuously improve:** instil a culture of continuous improvement and integrated thinking around security, rather than seeing it as a series of one-off tactical activities.
- **Manage talent:** build a talent management strategy at all levels of the organisation to cope with skills shortages and reduce reliance on contractors and consultants.
- **Share information:** join formal and informal networks to contribute to, and benefit from, information sharing activities where possible.

Business needs a smarter approach to cyber security laws and standards

GROWING PRESSURES ON LAWS AND STANDARDS

Greater board engagement has been driven to some extent by regulators and governments, who have stepped up the pressure around cyber security over the last two or three years. This focuses primarily on the protection of personal data and the resilience of organisations in critical national infrastructure sectors such as financial services.

For example, the General Data Protection Regulation (GDPR), which updates personal data laws across Europe, will have a widespread impact. While it goes further than cyber security, and covers a range of privacy practices, it will increase regulatory interventions in the event of security breaches and require reporting of breaches to authorities. New personal data laws have also been passed in many other countries including China, Singapore, and Australia. The EU's Network and Information Security Directive covers 'operators of essential services' and specifies cyber security practices which need to be implemented for companies working in a range of critical national infrastructure sectors.

Other third parties – for example customers, insurance companies and investors – are also increasingly looking for cyber security standards to provide confidence that a business is following good practices. In addition, taking a proactive approach to adopting appropriate standards offers a stronger line of defence to regulators in the case of a breach.

DIFFERENT NEEDS AND DIFFERENT STANDARDS

Any cyber security standard needs to balance two elements:

- sufficient flexibility in implementation, as the specifics of the IT environment will vary substantially across different organisations and continually change; and
- sufficient rigour for the standard to be consistently applied and provide a meaningful baseline.

Different standards reflect different approaches and third-party needs. Some cyber security standards are high-level, risk and principles-based; others are more prescriptive about specific security practices which need to be in place. Some are industry focused and others are more generic. Some are suitable for small businesses, while most are more applicable to large businesses. This has led to a proliferation of standards and regulations around the world, some of which are highlighted below.

KEY CYBER SECURITY STANDARDS

ISO 27001 is the best-established information security standard. It is a management system that provides a long list of potential controls that organisations can choose to adopt, based on their risk assessment. It is supplemented by a variety of more specific security standards in the 27000 series, such as business continuity.

Cyber Essentials was created in 2014 by the UK government, after it concluded that none of the existing standards met their specific needs. This aims to provide a baseline of cyber hygiene for all organisations and is being pushed down supply chains for government contracts.

NIST (National Institute of Standards and Technology) is a US framework that incorporates risk-based cyber security standards based on different industry sectors. They are also often pushed down supply chains, such as defence, and are fairly prescriptive in nature.

PCI-DSS (Payment Card Industry Data Security Standard) is a standard that is specific to payment cards – anyone processing payment card transactions has to pass the assessment and show compliance. This is a highly prescriptive standard, identifying the controls to be adopted with regard to payment card data.

The AICPA (American Institute of CPAs) published a framework, known as SOC for Cybersecurity, for reporting about cyber risk management, and for providing assurance opinions on the cyber risk management programme and associated controls. While it is US-centric, it shows the potential demand for better reporting and assurance around cyber risks.

While these all may be well intentioned, and aim for the same broad objectives, there is little co-ordination between initiatives. Where it is possible to align or repurpose standards, this should be done. However, while better coordination would be welcome, a single integrated standard that can be used for multiple purposes is highly unlikely in practice. Indeed, simplicity in this case would make it a lot easier for hackers to launch an attack. Consequently, businesses must become more proactive in developing a specific strategy around cyber security laws and standards that maps different requirements and builds broad capabilities to comply.

ALTERNATIVE APPROACHES TO STANDARDS

There are also different approaches that put less emphasis on standards and point-in-time accreditation which should be explored by businesses and regulators. For example, the Bank of England has taken an approach more akin to stress testing, whereby large financial institutions undergo penetration testing based on the latest intelligence about attackers. This provides specific insights into how the company copes in practice with sophisticated attackers. Approaches that are based more on testing or real-time monitoring may be more realistic, fruitful and less onerous on businesses.

This raises opportunities for the audit profession to help to improve confidence between third parties. Cyber risk is not currently included in the scope of statutory audit, other than in the context of financial data. Other established approaches, such as section 3402 reports, frequently do not give high levels of assurance. There is an opportunity for the profession to take a more proactive role and pioneer different approaches, for example, making more use of continuous auditing.

There may also be different ways that companies can collaborate and work together on cyber security. A large company needs to ensure that its suppliers are following good practices, and while standards can help, companies can also share information and expertise to help smaller companies in their supply chain. More collaborative approaches may improve the security of integrated supply chains more meaningfully, rather than just add administrative burdens.

RECOMMENDATIONS FOR BUSINESSES:

- **Be proactive:** build an effective strategy around cyber security laws and standards enabling compliance as efficiently and effectively as possible.
- **Apply standards:** demand that suppliers comply with relevant cyber security standards where appropriate.
- **Collaborate across supply chains:** consider other forms of cyber risk assurance which do not rely on point-in-time assessments, and explore other ways to collaborate across supply chains.

ICAEW IT FACULTY

ICAEW's IT Faculty is a leading authority on technology and the finance profession. It provides its members with information that allows them to make the best possible use of IT and keep up to date with IT issues and developments. Membership is open to finance professionals with an interest in technology, to join visit icaew.com/joinitf

---

There are over 1.7m chartered accountants and students around the world – talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future.

Over 150,000 of these are ICAEW Chartered Accountants. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair.

We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com

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

T +44 (0)20 7920 8100
E generalenquiries@icaew.com
icaew.com

ICAEW IT Faculty
@ICAEW_ITFaculty

Chartered Accountants Worldwide
Member

Global Accounting Alliance