CYBER RESILIENCE

Cyber security and business resilience

January 2015

Protect • Comply • Thrive

CYBER RESILIENCE

Why cyber security is not enough

As more information is held in digital databases by more organisations, and as the reliance on cyberspace now affects every sector of modern life, so the risks involved for all of us naturally increase. For the enterprising cyber criminal there has never been more to gain, and it has never been easier to gain it.

For organisations of any size or type the costs of a data breach, from short-term financial penalty to long-term reputational damage, are incalculable. The days of implementing an information security system and then sitting back, safe in the knowledge that you were secure, are gone. Nor is there safety in obscurity: if your organisation has a web presence then it is necessarily vulnerable. Automated attacks make no distinction between targets.

The scale of potential cyber security vulnerabilities is only going to increase, so it is essential to act now to prepare for future threats. Two major recent surveys provide food for thought:

- Figures from the Department for Business, Innovation and Skills (BIS) 2014 Information Security Breaches survey[1] show that 81% of large organisations and 60% of small organisations suffered a security breach in 2013.
- The same source shows that the average cost to a large organisation of its worst security breach of the year was between £600,000 and £1,150,000, and for a small business was between £65,000 and £115,000.
- The Verizon 2014 Data Breach Investigations Report[2] found that 85% of data breaches took weeks or more to discover and that 99% of incidents were discovered by a third party.

It is almost inevitable, then, that you will suffer a data breach, and there is no way of knowing how badly you'll be affected. Even if you think you're perfectly secure, the chances are that you're actually not: you may well have already suffered an attack that you don't even know about.

It's no longer sufficient to suppose that you can defend against every potential attack: you must accept that, sooner or later, some attacks will succeed. Traditional cyber security is not enough; it is an organisation's resilience in identifying and responding to security breaches that will become a critical survival trait in the future. If you're going to get hit, make sure you're not hit hard.

The risks you face

According to the National Audit Office (NAO)[3], there were 44 million cyber attacks in the UK in 2011, at an annual cost to the economy of between £18 billion and £27 billion. Cyber attacks are ranked as one of the top four UK national risks. As Amyas Morse, the head of the NAO said, "The threat to cyber security is persistent and continually evolving. Business, government and the public must constantly be alert to the level of risk if they are to succeed in detecting and resisting the threat of cyber attack."

Cyber Security Strategy

The UK Government, as part of its Cyber Security Strategy[4], has allocated £860 million to national cyber security up to 2016. One of the main objectives of the strategy is that the UK should "be more resilient to cyber attacks and better able to protect [its] interests in cyberspace". The future importance of cyber resilience cannot be underestimated.

"If you're going to get hit, make sure you're not hit hard."

Cyber resilience or cyber security?

So what do we mean by cyber resilience and how does it differ from cyber security?

As basic definitions:

- **Cyber security** is the state of protecting your information from attack by identifying risks and establishing appropriate defences.
- **Cyber resilience** accepts that there is a risk that an attack may be successful no matter how well prepared your defences are, and stresses the additional importance of incident management and business continuity planning.

Cyber security requires compromise. In order for your systems to be entirely secure they would have to be locked down to such an extent that they would be unusable even by you. The compromise you therefore have to make is that in everyday operations there will always be an element of risk.

Cyber resilience is a broader approach that encompasses cyber security and business resilience, and aims not only to defend against potential attacks but also to ensure your survival following any successful attack. An effective approach to cyber resilience is therefore twofold:

1. Ensure your cyber security is as effective as possible without compromising the usability of your systems.
2. Ensure you have robust, integrated business continuity plans in place that cover your information assets so that if an attack is successful you can resume normal operations as soon as possible.

1. Effective cyber security

Risk management

In Cyber Risk Management – A Board Level Responsibility[5], the Department for Business, Innovation and Skills (BIS) states that "cyber security is all too often thought of as an IT issue, rather than the strategic risk management issue it actually is."

Effective cyber security depends on coordinated, integrated preparations for rebuffing, responding to, and recovering from a range of possible attacks throughout the entire organisation. In practice, however, this approach is often not adopted, with inevitably negative results.

Alignment of security with business objectives

Only 42% of respondents to the PwC Global State of Data Breaches Survey 2015[6] say that their board actively participates in the overall security strategy. The report further highlights that diminished budgets have resulted in degraded security programmes for many organisations, which are generally struggling to keep up with security threats. Risks are not well understood or being properly addressed.

Budget

According to the ISBS 2014 survey[7], UK organisations on average now spend 10% of their IT budget on security (with no change from 2013), but many businesses still struggle to implement effective security defences due to ineffective leadership, weaknesses in risk assessment, and skills shortages. Developing a cyber security strategy and identifying key areas of investment is therefore essential for effective targeting of cyber security expenditure and ROI.

There is, in other words, a direct correlation between expenditure and safety: spend more on information security training and technologies and you drive down the severity and cost of cyber crime. Increasing numbers of organisations realise this. In a recent ESG survey[8], 58% of all responding organisations said they planned to increase their information security spending this year. This follows several years of increases, and is up more than 10% on the previous year.

How do you ensure your money is well spent?

The first step in an effective cyber security plan is to implement an information security management system (ISMS) that encompasses the whole organisation, as stipulated by the international standard ISO/IEC 27001:2013. ISO27001 ensures information security through a cohesive, enterprise-wide approach which encompasses people, processes and technology, in recognition that effective cyber security is as much a cultural practice as a technological practice. ISO27001 sets out specific requirements against which an organisation's ISMS can be audited and certified, giving the organisation a robust framework for information security, which will reassure stakeholders that best practice is followed. ISO27001 will give you the best chance of ensuring the robustness of your systems.

Your data having been secured as well as possible, you should now move on to the second stage: what to do if an attack is successful.

2. Business continuity and disaster recovery planning

Given that some 90% of organisations that suffer a significant data loss are not in business two years later, business continuity management must therefore be an essential part of effective cyber resilience to ensure that you can recover, and recover quickly.

Business continuity for information and communication systems is fundamental to an effective ISO27001-compliant ISMS. ISO/IEC 27031 provides detailed and valuable guidance on how this critical aspect should be tackled.

While development of a broad business resilience strategy should fit within an organisation's enterprise risk management framework, there is no reason to delay dealing with cyber resilience because a wider business resilience strategy has yet to be developed. Published by GCHQ, the 10 Steps to Cyber Security framework sets out a simplistic approach to handling cyber risk in order to help secure your information and ensure your business thrives. A robust assessment of your performance in each of these ten areas can be carried out by IT Governance, providing you with a tailored and usable action plan that will help you close the gap between recognised good practice and what you're actually doing.

A cyber resilience summary

- If your systems fail due to attack, the consequences could be catastrophic.
- Cyber security isn't enough to ensure your safety.
- A cyber resilience strategy will ensure you're prepared if an attack gets through your defences.
- Cyber resilience amounts to cyber security plus business continuity, and is the sensible approach to business continuity and disaster recovery.

Cyber resilience standards

The idea that an organisation's systems and processes should be resilient against outside attack or natural disaster is a key principle underpinning a number of international standards, including ISO27001 and ISO22301.

- Certification to ISO27001 will provide an organisation with an effective structure on which to build cyber resilience. By establishing a sturdy information security management system (ISMS) framework based on the best practice laid out in ISO27001, and the guidance in ISO27002, resilience to cyber attacks is naturally bolstered.
- Equally, adherence to the results-driven PAS 555 framework can provide resilience in an organic way, by adopting a framework that focuses upon the key goals.
- ISO27032 provides guidance for improving cyber security, and covers

information security, network security, Internet security and critical information infrastructure protection (CIIP).

- ISO22301 specifies the requirements for a business continuity management system (BCMS), an essential approach to ensuring your organisation is prepared for the unexpected. An ISO22301 BCMS is wholly compatible with an ISO27001 ISMS.
- ISO27031 (ICT business continuity) is designed to work within a broader enterprise business continuity management system, as laid out in ISO22301, and should form part of every organisation's planning for cyber resilience.
- ISO27035 for information security incident management provides a structured approach to detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.
- ISO27036-3 provides guidance on information and communication technology supply chain security, to help ensure that supply chains are not the weak link in your security systems.
- ISO24762 covers disaster recovery, which is essential in the event that you suffer a severe cyber attack, and to protect your organisation from opportunistic attacks during other disasters.

All of the guidance offered by the ISO27000 family of standards is mutually compatible.

Other approaches

As well as international standards, there are a number of recommended steps an organisation can take towards cyber resilience if they are not yet ready to implement a standards-based approach.

10 Steps and 20 Controls

In conjunction with GCHQ (Government Communications Headquarters) and CPNI (Centre for the Protection of National Infrastructure), the UK's Department for Business Innovation and Skills (BIS) has developed its 10 Steps to Cyber Security, which aims to highlight methods of recognising and pre-empting cyber risks in order to offer the best defence. The 10 Steps offers a management framework that can sit at the top of your cyber security programme alongside other management/governance level guidance, such as PAS 555, providing a comprehensive structure for your cyber security programme.

The 10 Steps states that basic "information risk management can stop up to 80% of the cyber attacks seen today, allowing companies to concentrate on managing the impact of the other 20%."

The 10 Steps covers:

- An information risk management regime
- Home and mobile working
- User education and awareness
- Incident management
- Managing user privileges
- Removable media controls
- Monitoring
- Secure configuration
- Malware protection
- Network security

For organisations involved in national infrastructure, the Council on Cyber Security's 20 Critical Controls[9] will be of interest.

The 20 Critical Controls is a set of additional controls developed for organisations involved in critical national infrastructure, and has much to offer larger organisations. Of those 20, there are five 'critical tenets'.

"The five critical tenets of an effective cyber defense system as reflected in the Critical Controls are:

• Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
• Prioritization: Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in your computing environment.
• Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
• Continuous monitoring: Carry out continuous monitoring to test and validate the effectiveness of current security measures."

Seven-step cyber security strategy

IT Governance has developed its own seven-step strategy for implementing your cyber security regime, which aims to give structure to the whole cyber security project.

1. Secure the cyber perimeter

Test all of your Internet-facing applications and network connections to ensure that all known vulnerabilities are identified and patched. This should include testing all wireless networks. Make sure that OWASP and SANS Top 10 vulnerabilities and security weaknesses are patched. Once this exercise has been completed (penetration testing, remediation and confirmation testing) regular network tests should be scheduled. Depending on risk, these should take place either quarterly or, as a minimum, every six months.

2. Secure mobile devices beyond the perimeter

Encrypt and secure access to all portable and mobile devices (laptops, mobile phones, BlackBerrys, USB sticks, etc.) to ensure that the increasingly elastic network perimeter remains secure and that data taken beyond the perimeter remains secure.

3. Secure the inward- and outward-bound communication channels

This encompasses channels such as email, instant messaging, Live Chat, and so on. Make sure there are appropriate arrangements for data archiving and an appropriate balance between protecting confidentiality, integrity and availability.

4. Secure the internal network

Identify risks and control against intrusions from rogue wireless access points, from unauthorised USB sticks and from mobile data storage devices (including mobile phones, iPods and so on).

5. Train your staff

Attackers understand that employees are the weakest link in the security chain and take advantage of natural human weaknesses through a style of attack known as social engineering. Staff must be trained to recognise and respond appropriately to social engineering attacks that range from tailgating to phishing, spear phishing and pharming. Also ensure that you have a considered social media strategy that minimises information loss through social media websites such as Facebook, LinkedIn and Twitter.

6. Develop and test a security incident response plan (SIRP)

Sooner or later your defences will be breached, and you need an effective, robust plan to respond to that breach. Your response plan should include developing a digital forensics capability so that you have the in-house competence to secure areas of digital crime long before outside experts arrive on the scene.

7. Adopt appropriate information and cyber security standards

The adoption of key standards not only assures you of your organisation's security and response capability, but certification assures business partners and customers that their information is safe in your hands. It also provides the combined wisdom of

years of best practice, which helps to ensure that all salient points are met in protecting your information.

"For the safety of your organisation you need to prepare for cyber resilience, not cyber security."

Useful Cyber Resilience Resources

IT Governance offers a unique range of cyber resilience products and services, including books, standards, pocket guides, training courses and professional consultancy services.

IT Governance offers a unique range of products and services designed to help you protect your business from the impact of cyber risk and to ensure business continuity in the case of an unplanned disaster.

ISO27001 Packaged Solutions

ISO 27001:2013 implementation packages

IT Governance's packaged ISO27001 implementation solutions will enable you to implement an ISO 27001:2013-compliant ISMS at a speed and for a budget appropriate to your individual needs and preferred project approach. Each fixed-price solution is a combination of products and services that can be accessed online and deployed by any company in the world.

www.itgovernance.co.uk/iso27001-solutions

Standards

- **ISO27002 (ISO 27002) Code of Practice for ISM**

  ISO/IEC 27002:2013 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation.

- **ISO27031 (ISO/IEC 27031) Guidelines for ICT Readiness for Business Continuity**

  ISO/IEC 27031:2011 is the international standard that describes the concepts and principles of information and communication technology (ICT) readiness for business continuity.

- **ISO27032 (ISO/IEC 27032) Guidelines for Cyber Security**

  ISO/IEC 27032: 2012 provides guidance for improving the state of cyber security, drawing out the unique aspects of that activity and its dependencies on other security domains.

- **ISO27035 (ISO 27035) Information Security Incident Management**

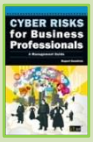
  Given the increasing risks from cyber attack from external and internal sources, your organisation will inevitably experience a security breach at some time in the future.

- **ISO22301 (ISO 22301) BCMS Requirements**

ISO 22301:2012 specifies the requirements for a business continuity management system (BCMS). The requirements for a BCMS can be employed by any organisation, no matter their size, type or location.

Books

- **Cyber Risks for Business Professionals - A Management Guide**



Cyber Risks for Business Professionals - A Management Guide is a general guide to the origins of cyber risks and to developing suitable strategies for their management. It provides a breakdown of the main risks involved and shows you how to manage them.

- **CyberWar, CyberTerror, CyberCrime & CyberActivism, Second Edition**

Understand the scale of the risk we face from criminals and other attacks mounted across the Internet, and learn about the measures that organisations and individuals can take to protect themselves.

- **IT Governance - An International Guide to Data Security and ISO27001/ISO27002**

This manual provides clear, unique guidance for both technical and non-technical managers. It details how to design, implement and deliver an ISMS that complies with ISO 27001.

- **The True Cost of Information Security Breaches - A Business Approach**

This pocket guide uses case studies to illustrate the possible breach scenarios that an organisation can face. It sets out a sensible, realistic assessment of the actual costs of a data or information breach and explains how managers can determine the business damage caused.

- **Security: The Human Factor**

Understand the challenges associated with information security, the consequences of failing to meet them and – most importantly – the steps organisations can take to make themselves and their information more secure.

Toolkits

- **Cyber Security Governance & Risk Management Toolkit**

This toolkit helps you make an enormous leap forward by consolidating five separate approaches (PAS 555, ISO27001, ISO27032, Cloud Controls Matrix & Ten Steps to Cyber Security) into a single, comprehensive, robust framework.

- **Business Continuity Toolkit**

Implement ISO 22301, the international best practice for business continuity, quickly, easily and cost effectively with this toolkit. Containing plans, templates, policies and all the other documents you need.

- **ISO27001 2013 ISMS Standalone Documentation Toolkit**

This toolkit will help you implement ISO 27001, the international best practice for information security, quickly and cost effectively with its customisable and editable templates.

Training

- **ISO27001 Certified ISMS Lead Implementer Masterclass**

If you are involved in information security management, writing information security policies or implementing ISO 27001 – either as a lead implementer or as part of the planning/implementation team – this masterclass covers all the key steps in preparing for and achieving ISMS certification first time.

- **ISO22301 BCMS Lead Implementer Training Course**

The three-day ISO 22301 Certified BCMS Lead Implementer training course provides a comprehensive and practical coverage of all aspects of implementing a business continuity management system (BCMS) and ensuring full compliance to the ISO 22301 standard.

- **Managing Cyber Security Risk Training Course**

This three-day classroom course provides those responsible for cyber security risk management with the knowledge and practical skills to develop and deploy effective cyber security risk management strategies, to protect their organisations in cyber space.

Consultancy and technical services

IT Governance consultancy services offer a unique blend of cyber security, business continuity and risk management advisory and professional services that will enable you to implement systems and processes to be cyber resilient in the event of a cyber attack.

- Cyber governance assessment and health check
- Cyber security consultancy
- Information/Cyber security risk assessment
- Business continuity assessment and implementation, and ISO 22301
- Information security management system implementation and ISO 27001 certification – end-to-end consultancy)
- Penetration testing services

Visit www.itgovernance.co.uk/consulting for more information.

Software

vsRisk is the risk management solution for cyber security that helps you take stock of the threats and vulnerabilities your information assets are exposed to, and provides a database of ISO27001-compliant controls to apply as a risk treatment plan.

Visit www.itgovernance.co.uk/software for more information.

Third-party products

IT Governance is a reseller of many other products and software tools that cover a wide range of subject areas that will help put you on the right track toward developing cyber resilience in your organisation.

The following additional software products and books provide encryption solutions and information on building cyber resilience:

Boldon James Classifier software

IT Governance solutions

IT Governance writes and publishes extensively on IT governance subjects, including IT service management, project governance, regulation and compliance, and have evolved a range of tools for IT governance, information security and regulatory compliance practitioners. This expertise is pulled together by the technical writing team to develop a number of products and services, including toolkits, books, training materials and green papers. IT Governance is your one-stop shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and can also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk/shop, we sell the most sought after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/product-demos to view and trial all of our available toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT practitioners and Certified Lead Implementers and Auditors.

Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/training for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy

We are an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit www.itgovernance.co.uk/consulting for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit www.itgovernance.co.uk/software for more information.

Contact us:

+ 44 (0) 845 070 1750

www.itgovernance.co.uk

servicecentre@itgovernance.co.uk

[1] http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf
[2] http://www.verizonenterprise.com/DBIR/2014/
[3] http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Exec-Summ.pdf
[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf
[6] http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml
[7] http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf
[8] http://www.esg-global.com/research-briefs/2014-networking-spending-trends/
[9] http://www.counciloncybersecurity.org/images/downloads/Critical%20Controls%20v4.1.pdf