CYBER SECURITY:

A CRITICAL BUSINESS ISSUE

January 2015

Protect • Comply • Thrive

CYBER SECURITY: A CRITICAL BUSINESS ISSUE

UK National Security Strategy

The UK's most recent National Security Strategy, published in 2012[1], identified that the four highest-priority risks faced by the UK are those arising from:

- International terrorism;
- Cyber attack;
- International military crises; and
- Major accidents or natural hazards.

Cyber attack is the most pervasive of these four high-priority risks. In recent years we have seen evidence of this in a series of highly advanced attacks:

- An advanced persistent threat posed by organised crime and state-level entities, with attacks against enterprises like Google, Coca-Cola, NASA and Lockheed Martin[2];
- Operation Aurora (the series of attacks on large US companies beginning in 2009, ascribed to China)[3];
- 2007 attacks on Estonia's critical national infrastructure[4];
- Malware such as Stuxnet, Duqu and Flame all demonstrate that an international military crisis is also likely to be accompanied by a cyber attack[5].

Any response to a major national incident also depends on information stored in electronic information systems. This makes the threat of cyber attacks doubly dangerous, as the response to the assault can be compromised by the attack itself.

Advanced persistent threats

Advanced Persistent Threat (APT) is the description applied to the co-ordinated cyber activities of sophisticated criminals and state level entities, targeted on large corporations and foreign governments, with the objective of stealing information or compromising information systems. Groups of attackers, working hand-in-glove with governments and commercial concerns, are able to combine multiple targeting methods, a range of tools, technologies and techniques to reach, compromise and maintain access to a target. They usually have advanced technology skills, state protection, and a wide range of channels through which they can mount their attacks. The goal of an APT is not usually to bring down a business, but to stay embedded and to extract or corrupt information out at a slow, undetected pace. The successful APT is the one you do not know about because it is already inside your network.

Serious organised crime

APTs are a major area of concern. The other is organised crime. According to Europol, "Cybercrime in the form of large scale data breaches, online frauds and child sexual exploitation poses an ever increasing threat to the EU, while profit-driven cybercrime is becoming an enabler for other criminal activity"[6] – all taking advantage of, or underpinned by, the Internet.

While APTs usually target specific government or private sector organisations, cyber attacks at a lower level are more widespread and are initially automated and

"The goal of an APT is not usually to bring down a business, but to stay embedded and to suck information out at a slow, undetected pace."

indiscriminate – any organisation with an Internet presence will be scanned and potentially targeted. Vulnerable targets with interesting or valuable data can then be attacked further.

The fragmented workforce

Inescapable changes in the workplace also bring significant dangers.

Yesterday's workforce was monolithic. Working within tightly controlled corporate perimeters, using computer terminals with limited capabilities and with restricted access to data, the average employee was not a significant security risk.

Technology has fragmented the monolith: today's employee uses high-powered, pocket-sized gadgets to access and manipulate a wealth of data, most of which is stored in the Cloud and all of which is increasingly beyond the employer's oversight. Today's average employee is a significant security risk, and the human factor an increasingly important part of every security strategy.

A mobile, fragmented working population – made possible by that exciting combination of the Cloud and mobile computing technologies – creates more opportunities for cyber criminals, opening up more potential data breaches.

Effective cyber security

Effective cyber security depends on co-ordinated, integrated preparations for rebuffing, responding to, and recovering from a range of possible attacks. There is no single, stand-alone solution for cyber crime or for APTs; the very nature of an APT is that it is designed to evade standard security controls.

According to the ISBS 2013 survey[7], UK organisations now spend 10% of their IT budget on security on average (up from 8% in 2012). A key finding of the survey was that many businesses 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.

The PwC Global State of Data Breaches Survey 2013[8] revealed that only 30% of the respondents say that their security policies and spending are completely aligned with business objectives. 46% believe that they are somewhat aligned, while 14% claim poor alignment and 10% say they are not aligned. The report highlights that diminished budgets have resulted in degraded security programmes for many organisations. Organisations are generally struggling to keep up with security threats and risks are not understood well or properly addressed.

There is, in other words, a direct correlation: 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[9], nearly half (49%) of all responding organisations plan to increase their information security spending this year. This follows several years of increases of 6% to 10%, with more than one in ten organisations increasing their spending on information security by more than 10%.

A two-phase approach

While the risks of attack from external and internal agents may appear to be vast and

The stakes are high!

The potential impact of cyber risk to any individual business includes:

- Financial loss from theft or fraud;
- Loss of invaluable customer information or intellectual property;
- Possible fines from legal and regulatory bodies (e.g. FSA, Information Commissioner) or expensive court actions resulting from breach of data protection or confidentiality regulations;
- Loss of reputation through 'word of mouth' and adverse press coverage; and, under a range of scenarios,
- Survival of the organisation itself.

hydra-like, the fundamental principles of ensuring the security of your organisation's information remain largely unchanged.

There are two key factors that comprise effective protection of your information: cyber resilience and cyber security. The distinction lies in the understanding that protection of information must come first, but the business must continue to adapt and transform in the face of a rapidly changing technological environment.

Cyber security is the state of protecting your information from most attacks. This is achieved by identifying the risks and establishing appropriate defences.

Cyber resilience, meanwhile, accepts that there is a risk that an attack may be successful, no matter how well prepared your defences are. As such, cyber resilience posits the necessity of incident management and business continuity.

In brief, cyber security protects you from attacks while cyber resilience ensures survival following an attack.

The basics of cyber security

At its core, cyber security recognises that there are a limited number of avenues through which an attack can gain access to your information. These can be broadly divided into physical, mobile and digital. In order to protect your information, you need to ensure that each of these avenues is blocked to hostile agents.

Physical

The physical avenue is through gaining direct, physical access to your organisation. An attacker may gain access to computers, hard copies of files, mobile devices such as laptops or tablets, and your employees. Mitigating this risk involves securing the physical perimeter, which is readily achieved and already standard practice in many organisations. Organisations should – at the very least – monitor all entrances and exits, train staff to report strangers within the perimeter, and place security measures on external doors and internal secure areas.

Social engineering is possibly the most difficult aspect of physical security to defend against, as it relies upon fallible humans. Having said this, solutions can often be a disarmingly simple regime of training and awareness.

Mobile

Mobile devices are increasingly popular business tools and require an additional level of control in order to protect the expanding range of the business perimeter. Employees must be trained to secure the devices when not in use, and to ensure that business-owned devices are used in accordance with security policies. Further, a comprehensive and robust Bring Your Own Device (BYOD) policy should be enforced to minimise or prevent the loss of information through employees' personal mobile devices.

Digital

Securing the perimeters is an excellent first step in securing your information, but you should be sure that this information is further protected in case these perimeter defences fail, or in case of a direct cyber attack. Data should be encrypted wherever it is stored, and access to valuable information should restricted by two- or three-key authentication. The digital perimeter should be protected with firewalls, user authentication and other measures to prevent an unauthorised intrusion.

Cyber security and resilience standards

Information security standards are an important element in building a strong, resilient information and communications infrastructure. ISO/IEC 27001 is the most significant international best practice standard available to any organisation that wants an intelligently organised and structured framework for tackling its cyber risks. ISO 27001, as a specification for an information security management system, is clear and precise. It lists 114 key security controls that should always be at the heart of any organisation's approach to securing its information assets.

Protection of information does not comprise the whole of cyber security, however, and the responsible organisation will establish a comprehensive and effective business continuity framework to ensure the organisation can continue to protect its information in the event of a disaster or emergency. ISO/IEC 22301 is the international best practice standard for a business continuity management system (BCMS), and comprises both business continuity – keeping the business running – and disaster recovery – returning to full functionality as speedily as possible.

PAS 555:2013 defines what effective cyber security looks like. While standards such as ISO 27001 are prescriptive (defining the 'how'), PAS 555 does not specify practices or actions – instead, it describes what an effective cyber security regime looks like (the 'what'). This approach allows organisations to choose how they achieve specified outcomes, whether through the use of other standards or through internal best practice.

ISO 27001 – The information security standard

ISO/IEC 27001, together with the international code of practice, ISO/IEC 27002, provide a globally recognised best-practice framework for addressing the entire range of risks which, taken together, may be described as cyber risks. ISO 27001 and ISO 27002 are, together, the basis for the UK's national information security management standards – they are at the core of the NHS Connecting to N3 requirements, the government secure connection (or Codes of Connection – CoCo) requirements, the Gambling Commission Compliance requirements, the Department for Work and Pension's Baseline and Security Plan requirements, and virtually every other security management activity across the UK's critical national infrastructure. ISO 27001 is also used as the basis for supplier audits and supply chain assurance.

"The idea of resilience – that an organisation's systems and processes should be resilient against outside attack or natural disaster – is a key principle underpinning ISO 27001."

ISO 27001 and ISO 27002 are also common reference points for almost all laws and regulations that touch on information security. As almost every data breach is likely also to bring legal exposure, there is real sense in basing your information security management system on an international standard to provide a recognised framework for information security controls.

Business resilience

Cyber resilience should, of course, form part of a wider business resilience strategy. The lack of a broader business resilience strategy, however, is no reason to delay dealing with cyber resilience.

Accredited certification to ISO 27001 and ISO 22301

Accredited certification to ISO 27001 and ISO 22301 gives an organisation internationally recognised and accepted proof that its system for managing information security and business continuity is of an acceptable, independently audited and verified standard. For example, accredited certification enables an organisation in the United Kingdom to demonstrate to a potential client elsewhere in Europe, North America, Japan or anywhere else, that its approach to selecting information security controls and managing its overall approach to information security is in line with internationally recognised best practice. Further, implementation of an internationally recognised framework for business continuity ensures that the gains earned from the ISMS will not be compromised in an emergency.

Cyber resilience

Certification to ISO 27001 and ISO 22301 provides the organisation with a structure on which to build cyber resilience. The idea of resilience – that an organisation's systems and processes should be resilient against an outside attack or natural disaster – is a key principle underpinning ISO 27001. By establishing a sturdy ISMS framework based on best practice, 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.

In order to thoroughly protect the organisation from attack, however, it is necessary to go one step further. While absolute security is likely impossible, ensuring that your organisation is a wholly undesirable target is a readily achievable goal. To this end, the UK's Department for Business Innovation and Skills (BIS) has developed its 10 Steps to Cyber Security. This document –produced in conjunction with GCHQ (Government Communications Headquarters) and CPNI (Centre for the Protection of National Infrastructure) – aims to highlight methods of recognising and pre-empting cyber risks in order to offer the best defence.

Seven-step cyber security strategy

IT Governance has developed a seven step strategy for implementing your cyber security regime. This strategy aims to give structure to the whole cyber security project.

1. Secure the cyber perimeter

Test all 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 confirmatory re-testing – schedule regular network tests should be scheduled. Depending on risk, these should take place either quarterly or, at 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 e-mail, 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 for responding to the 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 with certification it 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.

These standards include ISO/IEC 27001 and the other frameworks and specifications mentioned earlier in this green paper, and should be expanded according to your business needs. Of particular interest should be the BIS Ten Steps to Cyber Security and, for organisations involved in national infrastructure, the CNI 20 Critical Controls.

The Ten Steps offers a management framework that can sit at the top of your cyber security programme. This fits alongside other management/governance level guidance, such as PAS 555, providing a comprehensive structure for your cyber security programme.

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.

About the author

Alan Calder is an acknowledged international cyber security guru and a leading author on information security and IT governance issues. He is also chief executive of IT Governance Limited, the single-source provider for products and services in the IT governance, risk management and compliance sector.

Alan wrote the definitive compliance guide, *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002 5th edition* (co-written with Steve Watkins), which is the basis for the UK Open University's postgraduate course on information security. This work is draws on his experience of leading the world's first successful implementation of BS7799 (now ISO 27001).

Other books written by Alan include *The Case for ISO 27001*, *ISO 27001 – Nine Steps to Success*, *Risk Assessment for Asset Owners*, *IT Governance: Guidelines for Directors*, *IT Governance: A Practitioner's Handbook* and *IT Regulatory Compliance in the UK*.

Alan is a frequent media commentator on information security and IT governance issues, and has contributed articles and expert comment to a wide range of trade, national and online news outlets.

Alan was previously CEO of Wide Learning, and of Business Link London City Partners. He was a member of the Information Age Competitiveness Working Group of the UK Government's Department for Trade & Industry, and a member of the DNV Certification Committee, which certifies compliance with international standards including ISO/IEC 27001.

IT Governance Cyber Security Solutions

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.aspx

Standards

- **ISO27001 (ISO 27001) ISMS Requirements**

  

  ISO/IEC 27001:2013, usually referred to just as ISO 27001, is the best practice specification that helps businesses and organisations throughout the world to develop an Information Security Management System (ISMS).

- **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 latest (March 2011) 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 cybersecurity, 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

- **Above the Clouds - Managing Risk in the World of Cloud Computing**

A comprehensive introduction to the benefits and risks associated with transitioning to cloud computing.

- **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**

Understand the scale of the risk we face from criminal 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.

- **Mobile Security: A Pocket Guide**

This pocket guide aims to raise awareness of the threats to which mobile devices, users and data are exposed, as well as to provide advice on how to address those problems.

- **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 – at 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.

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.

- **ISO 27005 Certified ISMS Risk Management Training**

This course is designed to provide delegates with the knowledge and skills required to undertake information security risk management based on the best practice guidance as outlined in ISO27005 and fully meeting the requirements of the ISO27001 standard.

- **Managing Cyber Security Risk Training Course**

This 3-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.

Contact us: + 44 (0) 845 070 1750
www.itgovernance.co.uk servicecentre@itgovernance.co.uk

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83775/121128-Annual-Report-to-Parliament-on-NSS-and-SDSR.pdf
[2] http://www.bbc.co.uk/news/world-asia-china-21272613
[3] http://nakedsecurity.sophos.com/2010/01/18/security-roundup-google-adobe-0-day-flaw/
[4] http://www.economist.com/node/9163598
[5] http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html
[6] EU Serious and Organised Crime Threat Assessment (SOCTA) 2013, https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf
[7] 2013 Information security breaches survey, http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf
[8] PwC Global State of Date Breaches Survey 2013, http://www.pwc.com/gx/en/consulting-services/information-security-survey/giss.jhtml
[9] 2013 Information Security Spending Trends, http://www.esg-global.com/research-briefs/2013-information-security-spending-trends/