CYBERSECURITY:

A CRITICAL BUSINESS RISK

February 2013

Protect • Comply • Thrive

CYBERSECURITY: A CRITICAL BUSINESS RISK

UK National Security Strategy

The UK's most recent National Security Strategy, published in 2010, identified that the four highest-priority risks faced by the UK are those arising from:

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

Cyberattack is the most pervasive of these four high-priority risks. The reasons for this were:

- There is an advanced persistent threat posed by organised crime and state level entities, with enterprises like Google, Citigroup, the IMF and RSA all apparently attacked;
- Operation Aurora (the series of attacks on large US companies that began in 2009 and have been ascribed to China), the 2007 attacks on Estonia's critical national infrastructure, the Stuxnet worm in Iran and the Duqu Trojan all demonstrate that an international military crisis is also likely to be accompanied by a cyberattack.
- The information on which our responses to any major national incident depend is stored in electronic information systems.

Advanced Persistent Threats

Advanced Persistent Threat (APT) is the description applied to the co-ordinated cyberactivities 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, able to combine multiple targeting methods, a range of tools, technologies and techniques to reach and compromise and maintain access to a target, 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 suck information out of it at a slow, undetected pace. The successful APT is the one you probably don't 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 Eurpol, "serious organised crime groups are increasingly multi–commodity and poly-criminal in their activities, with extensive, diverse portfolios of business interests and significant collaborative activity" – all taking advantage of, or underpinned by, the Internet.

While APTs are usually targeted on specific government or private sector organisations, cyberattacks at a lower level are more widespread and are initially automated and indiscriminate – any organisation with an Internet presence will be scanned and potentially targeted. Vulnerable targets, with potentially interesting, or valuable, data, can then be attacked further.

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

Not surprisingly, the PwC Global State of Information Security Survey 2011 said that "increasing the focus on data protection is the single most common IT strategy worldwide for the second year in a row". The 2012 PwC Information Security Breaches Survey began with the words: "The vast majority of respondents had a security breach in the last year", continuing to say that 93% of large organisations and 76% of small had experience a security breach in the previous year. High-profile cyberattacks and data protection compliance failures have led to significant embarrassment and financial loss for organisations around the world in both the public and private sectors.

Cyber Insecurity

Cyberspace is unregulated; cybercops exist only in films. In cyberspace, no-one can hear you cry, and a digital version of the Tragedy of the Commons is there for all to see. That means cyberattacks could come from any direction. Cyberattacks have multiple vectors, and initial attacks may be completely automated and totally undiscriminating. Critical national infrastructure (CNI) and ordinary businesses with an Internet presence are all at risk – and it's impossible to determine whether the suspicious activity you're detecting on your firewall is an APT attack or an ordinary cybercriminal. Internet programmes seek out vulnerabilities in websites and Internet connections for further attention. Phishing, pharming and straightforward malware attacks penetrate wherever there are security weaknesses and then exploit target systems for the benefit of their creators. Social engineers exploit human characteristics to penetrate secure areas or technologies and steal information.

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, yesterday's average employee wasn't much of a 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.

And a mobile, fragmented working population – made possible by that exciting combination of the Cloud and mobile computing technologies – creates more opportunities for cybercriminals, and opens up more potential data breaches.

Cyberbreach Costs

Cyber insecurity has significant financial implications, including fines, legal fees and punitive damages. Forrester Research, in a 2011 report, put the average cost per record of a breach at between $9 and $305, commenting that discovery, response, and notification costs are usually substantial, at about $50 per lost record. These costs include legal fees, breach notification costs, and increased operational, marketing and PR costs. The UK's ISBS 2012 put the average cost of a serious breach for a large organisation as between £110k and £250k and £15k-£30k for small.

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,
- Organisational survival itself.

Protect Your Business from Cyber Risk

In today's information economy, the protection of information assets (information security) is a key element in the long-term competitiveness and survival of commercial organisations. In an environment where the survival of individual organisations is, at least, partially dependent on the security of critical national infrastructure, all organisations must contribute to improved cybersecurity. With the Internet becoming a ubiquitous communication and application platform, the greatest risk to your business is not cyberwar, but cybercrime.

Your Business Plan – Risk & Reward

The assessment and prevention of cyber risks associated with your information assets are crucial to the success of your business. Participants at an RSA Washington DC APT Summit, in September 2011, recommended that CEOs in every industry sector should NOT DELAY devoting attention and funding to combat advanced persistent threats and, moreover, to "plan and act as though you've already been breached".

As in any organisation, it is management's responsibility to minimise risk and to maximise all business opportunities and return on investment. No-one else is going to do it for you. The adoption of an appropriate balance of cyber risk and reward must be an essential part of your business plan.

Effective Cybersecurity

Effective cybersecurity 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 cybercrime or for APTs; the very nature of an APT is that it is designed to evade standard security controls.

Effective cybersecurity requires a strategy – and money. Although the average company is spending 6% of its IT budget on information security, the benchmark against which their expenditure should be compared is closer to the 13% average of organisations where management genuinely cares about information security.

In fact, as the 2010 Cyber Security Watch Survey (conducted by CSO Magazine with help from the US Secret Service, Carnegie Mellon Software Engineering Institute (CERT) and Deloitte's Centre for Security and Privacy Solutions) found, respondents to the survey reported an increase in the number of incidents, but a decline in severity. The survey attributed this impact reduction to a 42% increase in IT security spending by respondent companies and an 86% increase in corporate/physical security spending over the past two years.

There is, in other words, a direct correlation: spend more on information security and you drive down the severity and cost of cybercrime. Increasing numbers of organisations realise this. In a recent ESG survey, 32% of the security professionals in the survey said the APT issue "will cause us to increase security spending by 6% to 10%" and 11% of the respondents expected their spending to increase by more than 10%.

Cybersecurity Standards

Cybersecurity 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 organized and structured framework for tackling its cyber risks. ISO27001, as a specification for an information security management system, is clear and precise; it also lists 133 key security controls that should always be at the heart of any organisation's approach to securing its information assets.

"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 ISO27001."

ISO27001 – The Cybersecurity 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. ISO27001 and ISO27002 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. ISO27001 is also used as the basis for supplier audits and supply chain assurance.

ISO27001 and ISO27002 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 a legal exposure, there is real sense in basing your information security management system on an international standard that provides a recognised framework for information security controls.

Accredited Certification to ISO27001

Accredited Certification to ISO27001 gives an organisation internationally recognised and accepted proof that its system for managing information security – its ISMS or cybersecurity readiness – is of an acceptable, independently audited and verified standard. Accredited certification enables an organisation in the United Kingdom to demonstrate to a potential client elsewhere in Europe, in North America, in 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.

Cyber Resilience

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 ISO27001. Incident response is one aspect of business resilience and ISO/IEC 27035 is best practice for incidence response.

Business continuity for information and communications systems is even more fundamental to cyber survival, and ISO/IEC 27031 now provides detailed and valuable guidance on how this critical aspect of business resilience should be tackled. Also capable of working within a broader enterprise-wide business continuity management system (such as that specified in the new business continuity management system standard ISO22301), ISO27031 should form part of every organisation's planning for cyber resilience.

Business Resilience

Cyber resilience should, of course, form part of a wider business resilience strategy. 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 still to be developed.

Seven-Step Cybersecurity Strategy

There are seven key actions that should form part of an effective cyber security strategy for any organisation:

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 – penetration testing, remediation and confirmatory re-testing – has been completed, schedule regular network tests. Depending on risk, these should take place either quarterly or, at least, every six months.

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.

Secure the inward: and outward-bound communication channels – e-mail, instant messaging, Live Chat. Make sure there are appropriate arrangements for data archiving and an appropriate balance between protecting confidentiality, integrity and availability.

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.

Train 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, therefore, be trained to recognise and respond appropriately to social engineering attacks that range from tailgating through to phishing, spear phishing and pharming. Also ensure that you have a well-thought through social media strategy that minimises information loss through social media websites, such as Facebook, LinkedIn and Twitter.

Develop and test a security incident response plan (SIRP): sooner or later, your defences will be breached and you, therefore, 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.

Adopt ISO27001 and ISO27031 as standards for developing and implementing comprehensive cybersecurity and business resilience management systems.

About the author

Alan Calder is an acknowledged international cybersecurity 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 ISO27001/ISO27002 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 ISO27001).

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 Cybersecurity 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.

Standards

- ISO27001: www.itgovernance.co.uk/shop/p-1261.aspx
- ISO27002: www.itgovernance.co.uk/shop/p-721.aspx
- ISO27031: www.itgovernance.co.uk/shop/p-733.aspx
- ISO27035: www.itgovernance.co.uk/shop/p-739.aspx
- All available as one set from www.itgovernance.co.uk/shop/p-504.aspx.

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.
www.itgovernance.co.uk/shop/p-345.aspx

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.
www.itgovernance.co.uk/shop/p-505.aspx

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.
www.itgovernance.co.uk/shop/p-511.aspx

E-mail Security: A Pocket Guide

This is a concise reference to the main security issues affecting those that deploy and use e-mail to support their organisations.
www.itgovernance.co.uk/shop/p-540.aspx

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.
www.itgovernance.co.uk/shop/p-941.aspx

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.
www.itgovernance.co.uk/shop/p-1110.aspx

The Insider Threat

The insider threat poses a significant and increasing problem for organisations. The use of highly connected computers makes controlling information much more difficult than in the past. This pocket guide sheds light on those key security issues

www.itgovernance.co.uk/shop/p-1178.aspx

Toolkits

- ISO27001 & Cyber Security Toolkit: www.itgovernance.co.uk/shop/p-716.aspx
- Social Media Governance Toolkit: www.itgovernance.co.uk/shop/p-1134.aspx
- Business Continuity Toolkit: www.itgovernance.co.uk/shop/p-1039.aspx

Training

- ISMS Implementation – Masterclass: www.itgovernance.co.uk/shop/p-713.aspx
- Implementing Business Continuity: www.itgovernance.co.uk/shop/p-695.aspx
- Digital Forensics Readiness: www.itgovernance.co.uk/shop/p-487.aspx

IT Governance Solutions

IT Governance source, create and deliver products and services to meet the evolving IT governance needs of today's organisations, directors, managers and practitioners.

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 also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk, 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/free_trial.aspx 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.aspx 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

Our company is 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.aspx 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.aspx for more information.

Contact us: + 44 (0) 845 070 1750

www.itgovernance.co.uk servicecentre@itgovernance.co.uk