Cybersecurity – A Critical Business Risk

A National Security Strategy

The four highest-priority risks faced by nation states 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 are:

- There is an advanced persistent threat posed by organized crime and state level entities, with enterprises like Google, Citigroup, the IMF and RSA all apparently attacked;
- Titan Rain (the multi-year series of attacks on US Critical National Infrastructure that began in 2005 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 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 closely 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 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 Eurpol, "serious organized 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 organizations, cyberattacks at a lower level are more widespread and are initially automated and indiscriminate – any organization with an Internet presence will be scanned and potentially targeted. Vulnerable targets, with potentially interesting, or valuable, data, can then be attacked further.

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 2010 PwC ISBS Breaches Survey was headlined: "Cybercrime losses double in two years". High-profile cyberattacks and data protection compliance failures have led to significant embarrassment and financial loss for organizations 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.

Cybersecurity – A Critical Business 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, a significant proportion of which are likely to be 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 Ponemon Institute's Global Cost of a Data Breach Survey 2010 identified the average cost of a data breach in 2009 – across five economies (USA, UK, Germany, France, Australia), and including detection, notification, remediation and lost business – as $3.4 million.

The median annual number of security breaches per organization is 45 – a threefold increase on 2008.

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 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,
- Organizational survival itself.

Protect Your Business from Cyber Risk

Cybersecurity – A Critical Business 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 organizations. In an environment where the survival of individual organizations is, at least, partially dependent on the security of critical national infrastructure, all organizations 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 organization, 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 organizations 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 Center 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 cyber crime**. Increasing numbers of organizations 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 organization 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 organization's approach to securing its information assets.

ISO27001 – The Cybersecurity Standard

ISO/IEC 27001, together with the international code of practice, ISO/IEC 27002, provide a globally recognized best-practice framework for addressing the entire range of risks which, taken together, may be described as cyber risks. ISO27001 and ISO27002 are 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 recognized framework for information security controls.

Accredited Certification to ISO27001

Accredited Certification to ISO27001 gives an organization internationally recognized 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 organization in the United States 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 recognized best practice.

Cyber Resilience

The idea of resilience – that an organization'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 cybersurvival, 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 organization'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 organization'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 organization:

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 – 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.

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 – 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.

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 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 recognize 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.
6. 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.
7. Adopt ISO27001 and ISO27031 as standards for developing and implementing comprehensive cybersecurity and business resilience management systems.

IT Governance Cybersecurity Products & 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

Cybersecurity standards kit – all four standards (ISO27001, ISO27002, ISO27031, ISO27035):
http://www.itgovernanceusa.com/product/2371.aspx

Books on Cybersecurity

Above the Clouds: Managing Risk in the world of Cloud Computing

Cyber Risks for Business Professionals

CyberWar, CyberTerror, CyberCrime

E-mail Security: A Pocket Guide

Mobile Security: A Pocket Guide

Security: The Human Factor

The Insider Threat

Cyber Resilience Toolkits

ISO27001 & Cyber Security Toolkit:

http://www.itgovernanceusa.com/product/258.aspx

Social Media Governance Toolkit:
http://www.itgovernanceusa.com/product/2049.aspx

Business Continuity Toolkit:
http://www.itgovernanceusa.com/product/2255.aspx

SERVICES – CERTIFIED TRAINING

ISO27001 Certified ISMS Foundation Training
http://www.itgovernanceusa.com/product/2358.aspx

Information Security Foundation Based on ISO27002

http://www.itgovernanceusa.com/product/2359.aspx

ISO27001 Certified ISMS Internal Auditor Training

http://www.itgovernanceusa.com/product/2363.aspx

ISO27001 Certified ISMS Lead Auditor
http://www.itgovernanceusa.com/product/2363.aspx

ISO27001 Certified ISMS Lead Implementer Masterclass Training
http://www.itgovernanceusa.com/product/2360.aspx

ISO27001 Information Security Management Standard

IT Governance is a leading international authority on ISO27001 information security management. You can access a comprehensive range of information, advice, standards, books, tools, consultancy and training through the ISO27001 portal: http://www.itgovernanceusa.com/infosec.aspx

Business Continuity, Disaster Recovery, ISO22301 & ISO27031

IT Governance is also a leading international authority on business resilience standards and, again, you can access a comprehensive range of information, advice, standards, books, tools, consultancy and training through the business resilience pages on our website: http://www.itgovernanceusa.com/disaster-recovery-bs25999.aspx

Cybersecurity Tips: http://www.itgovernanceusa.com/cyber-security.aspx