Top information security risks for 2008

A collaborative project by the professional information security communities
at CISSPforum and ISO27k implementers' forum

FINAL 31st December 2007

Introduction

This document stems from a posting to CISSPforum by Tim Bass asking for input to his Top Ten Cybersecurity Threats for 2008. We decided to draw up a better 'top ten' list than those bandied about every new year by the antivirus companies and others with vested interests. Taking Tim's idea a stage further, we decided to list the top information security threats, vulnerabilities *and* impacts separately, and then generate a consolidated list of information security risks, and finally a list of recommended controls. We are using 'top' in the sense of 'most important from the perspective of experienced information security professionals, both today and looking forward to the year ahead.

This document was created by an international virtual committee or rather a willing group of volunteers from the CISSPforum and ISO27k implementers' forum, who collaborated on a shared document thanks to Google Docs (thanks Google!). Please see the credits at the end for their names.

A note on terminology and taxonomy

We are frustrated by those who confuse "threats" with "vulnerabilities" and/or "risks". This is more than just a matter of semantics and taxonomy: they are distinct concepts as Bill Murray would surely agree. That said, we had a fair amount of discussion about the terms when writing this.

The current 3rd Committee Draft of ISO/IEC 27000 (which is still in development and will probably change before publication) defines the key terms we are using as follows, within the context of information security management systems:

- **Threat**: a potential source of an incident attack [*sic*] that may result in adverse changes to an asset, a group of assets or an organization
- **Vulnerability**: weakness of an asset that can be exploited by a threat
- **Impact**: a measure of the effect of an event
- **Risk**: the combination of the likelihood of an event and its impact
- **Control**: means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management or legal in nature

The NSW Dept of Commerce Information Security Guidelines suggests these variant definitions:

- **Threat**: a potential cause of an unwanted event which may result in harm to an organisation
- **Vulnerability**: a characteristic (including a weakness) of an information asset or group of information assets which can be exploited by a threat

Warning for journalists and other readers of this document

We may be information security professionals but we are not soothsayers with mysterious magical powers (although it may seem so, and some of us may even believe it to be true). This is not a definitive or comprehensive document, just a community project by people who bring their own experiences and prejudices to bear on the topic. Individual organizations should regularly assess information security risks in their specific situation and respond accordingly. This is most certainly not legal advice. Your mileage may vary. Do not climb above top two rungs.

The CISSPforum / ISO27k implementers' forum information security risk list 2008

Information security threats

Threats (or 'threat sources') are the actors or situations that might deliberately or accidentally exploit vulnerabilities causing information security incidents:

- Imposition of legal and regulatory obligations, such as the need for adequate information security controls to protect personal data and enforced breach disclosures
- Organized crime or terrorist groups using identity theft and other forms of compromise or extortion (*e.g*. denial of service and DNS attacks) to finance or support criminal activities.
- Cyber-criminals, either skilled Black Hats themselves or able to direct or pay others to do their bidding
- Malware authors responsible for viruses, worms, Trojans (particularly key loggers)
- Phishers including spear phishers targeting individuals with carefully crafted attacks
- Spammers and other obnoxious, self-serving marketers wasting network bandwidth and filling our inboxes with junk, using their botnets and malware
- Negligent staff such as programmers, technical architects, testers and project managers who cause or fail to prevent the vulnerabilities listed at #1 just below
- Storms, tornados, floods - Acts of God or intentional acts such as arson that may disrupt, damage or destroy information assets and services (plus worse/unpredictable weather due to global warming)
- Fraudsters who simply use IT whilst exploiting control weaknesses in the IT-enabled business processes, or directly exploit control weaknesses within the IT systems themselves, or exploit other control weaknesses involving printed or other information rather than computer data and systems
- Hackers, ranging from evil Black Hats down to naive and curious Grey or White Hats (who may be well-meaning but also cause security incidents)
- Unethical competitors (*e.g*. using industrial espionage to steal trade secrets, customer lists *etc*.) or foreign powers targeting commercial and national secrets through espionage, social engineering, physical/network penetration, phishing and/or malware
- Disgruntled/untrained/ignorant employees who make genuine if naive human errors, misuse/misconfigure system security functions, or ignore security policies and good practices
- Saboteurs who destroy, or threaten to destroy, information assets or who [threaten to] deny access to same (extortion)
- Unauthorized access to, or modification or disclosure of, information assets (hardware, software, data, information)
- Nation states with advanced information warfare capabilities attacking critical information infrastructures to cause disruption or denial of service.
- Technical advances such as quantum computing (it's only a matter of time before all current encryption algorithms are effectively rendered obsolete)

Information security vulnerabilities

A flaw or weakness in a system's security procedures, design, implementation or internal controls (*e.g*. lack of or inadequate physical, logical, procedural or legal protection of information assets) that could be exploited and result in a security breach, violation of the systems security policy or other impact:

- Software bugs and design flaws, particularly those in mass-market software such as, um, Windows and TCP/IP [usually exploited by hackers, fraudsters & other criminals]
- Complexity in IT, including “bloatware” and "richness" generally (modern, general purpose computers and internets are BAD for security) [usually 'exploited' inadvertently causing errors or deliberately by hackers, fraudsters & other criminals]
- Inadequate investment in appropriate information security controls, at least partly due to the apparent disconnect between solid information security and commercial success [potentially exploited by all threats if security controls are weak or missing]
- Insufficient attention to human factors in systems design and implementation, including cognitive biases and "laziness" [causes errors and is exploited by hackers, ID thieves, fraudsters & other criminals]
- Unwarranted confidence in inherently flawed or missing security controls, including both a general lack of awareness of the items in these lists and dependence on compliance certificates resulting from incompetent or fraudulent audits [exploited by hackers and fraudsters]
- "Management" who, in the main, still just doesn't get information security and insists that it be buried deep out of sight, out of mind in the bowels of IT [exploited by all threats, for the same reasons as lack of investment in security]
- Ignorance, carelessness, negligence or idle curiosity by users [exploited by untrained or mis/uninformed people who accidentally cause damage or discover exploitable control weaknesses]
- Poor or missing governance of information assets such as lack of accountability for their protection, incomplete/inaccurate asset inventories, lack of risk analysis and security controls design and implementation [exploited by all threats for the same reasons as lack of investment in security]
- Frequent change in the business, IT and security arenas, leading to a degree of helplessness and consequent denial or abdication of responsibilities [exploited by all threats for the same reasons as lack of investment in security]
- Inadequate contingency planning and preparedness for unpredictable/unusual or extreme information security incidents [exploited by accident or perhaps deliberately by a competitor, criminal, saboteur or terrorist creating a crisis to eventuate a disaster]
- Legacy systems (*e.g*. SCADA, safety-certified medical, space, aerospace & other systems) running on legacy platforms, often unsupported and no longer security-patched, that form part of a critical business process/data chain [exploited by accident or by hackers targeting old well-known vulnerabilities]
- Bugs in microprocessor designs and microcode that create opportunities for hackers to subvert trusted kernel routines including encryption and virtualization (one to watch in 2008) [potentially exploitable by skilled hackers and later by script kiddies]
- Lack of will, concern and/or ability to impress the need for information security on youngsters and young adults [exploited by all threats for the same reasons as lack of investment in security]

Information security impacts

Impacts are the [adverse] consequences or outcomes on the individual, organization or community at large resulting from information security incidents:

- Disruption to organizational routines and processes with consequent interruption to trading capabilities, loss of income *etc*.
- Direct financial losses through information theft and fraud, whether simply the "background noise" or exceptional and obvious in nature
- Decrease in shareholder value because of negative impact on customer relations, lost sales, and decline in public confidence (a very significant impact for those at Board level)
- Loss of privacy, including Big Brother snooping on ordinary citizens by their governments and authorities, the generalized decay of personal privacy inherent in modern society, and the result of criminal activities such as identity theft
- Reputational damage causing brand devaluation, lost customers, customer complaints and defection (affects individuals on Facebook *etc*. as well as corporations!)
- Loss of confidence in IT, seeding doubts and holding back valid commercial or noncommercial exploitation of IT
- Jail time, fines, suspension of licenses and/or other sanctions for those held accountable for serious legal or regulatory noncompliances and other information security breaches (another key motivator for the Board of Directors, strangely enough)
- [Necessary] Expenditure on information security controls at every stage of the systems and process development lifecycles
- Replacement costs for equipment and data damaged, stolen, corrupted or lost in incidents
- Loss of competitive advantage - that nagging feeling that a competitor has the inside track on your secret strategy to Rule The World (affects nations as well as corporations!)
- Reduced profitability, growth and bonuses caused by the background noise of security incidents, control costs and unspecified doubts about the effectiveness of security
- Impaired growth due to inflexible and/or overly-complex infrastructure/system/application environments
- Injury or loss of life if safety-critical systems fail, misbehave or are maliciously controlled [this item would clearly be #1 on the list for the individuals and families concerned, but is thankfully very rare, so far ...]
- Global thermonuclear war [this is more than just an obscure reference to an old sci-fi/hacking flic: we've been warned for years that cyber-terrorism is on the rise and that nation states are actively building their capabilities for information warfare. As the 'practice' attacks on Estonia in 2007 surely demonstrate, it's only a matter of time before one nation/state/organization/boundaryless entity launches a devastating cyber attack against one or more others. Imagine the sheer horror: no Internet access, for anyone, forever! This is no joke.]

Information security risks

For the purposes of this analysis, risks are defined as the coincidence of threats acting on vulnerabilities to cause impacts.

- Theft of personal data by criminals, or loss of laptops and computer media, leading to criminal prosecution of senior management, regulatory fines, loss of public confidence in trusted organizations, and significantly increase the probability of identity theft for the data subjects concerned. [There have been many such incidents in 2007 with many more to come in 2008. Proving cause-and-effect linkages between data exposure and ID thefts is tricky unless the criminals are rash enough to exploit compromised data sets in their entirety]
- Information leakage, extraction or loss of valuable and/or private information and introduction of unauthorized/malicious software through widespread unauthorized and/or uncontrolled use of portable devices and transportable computer media (*e.g*. USB memory sticks and iPod schlurping), with some potential for deliberate attacks propagated on such devices/media (Trojan-infected USB sticks, CD-ROMs *etc*. left in the corporate parking lot or simply given or posted to targets)
- Social engineering/pretexting or targeted phishing and malware attacks on call centre staff to obtain unauthorized access to personal data that can be exploited by fraudsters for identity theft (*e.g*. Norwich Union fined £1.26m for incidents like this)
- Environmental disasters due to acts of God or intentional acts that severely affect the business survivability of organisations due to a lack of business continuity and disaster recovery planning and management.
- Poor information security studies, risk assessments, projects/assignments and/or staffing/organization, causing failed, wasteful, excessive or otherwise inadequate controls and practices selection, implementation, performance measurement, monitoring and/or auditing.
- Deception including frauds (such as identity theft through phishing, social engineering, spyware *etc*.), repudiation (*e.g*. someone denying that they made an online purchase, and perhaps manipulating and falsifying transaction histories) and false allegations (*e.g*. accusing a teacher of having pornography on his PC)
- Endangerment - accidentally or intentionally putting information or systems "in harm's way" (*e.g*. someone accidentally publishing highly sensitive internal information on the Internet, leading to loss of personal privacy and/or commercial disadvantage and perhaps prosecution)
- Unauthorized exploitation of intellectual property including plagiarism and outright theft of text, audio/visual content by unethical members of the public or organizations, causing 'opportunity costs' (lost sales) and investigation/prosecution costs for the rightful IP owners if they choose to defend their rights

Information security controls

Controls or countermeasures are intended to reduce or constrain information security risks by addressing the threats, vulnerabilities and/or impacts. The following controls address the risks identified above:

- Investment in a comprehensive and systematic ISMS (Information Security Management System) incorporating high quality information assurance processes, ideally but not necessarily one based on internationally-accepted good security practices such as those embodied in the ISO/IEC 27000-series and NIST SP800 standards, the Information Security Forum's Standard of Good Practice for Information Security and others
- Data confidentiality controls to protect personal and proprietary data against unauthorized access or disclosure including physical, legal and logical access controls, both technical and procedural in nature (*e.g*. proper encryption of laptop hard drives, data backups and CD ROMs being sent to the auditors!)
- Data integrity controls to improve the quality, completeness and accuracy of data in the computer systems through data entry, processing, output and transmission controls
- System integrity controls to avoid computer and telecomms systems being undermined by unauthorized or otherwise undesired changes such as malware infections and hacks
- Proactive technical vulnerability management including timely identification of vulnerabilities, patching and updating of systems, and even more proactive system hardening such as choice of secure operating systems, de-installation of unnecessary applications and services, and intensive security testing
- "Anti-everything" software to minimize the malware, spam, spyware and intrusion incidents on systems, both client workstations and servers
- Proactive IT auditing, monitoring and reporting processes to identify and respond to risks before they cause incidents, in addition to more traditional reactive/after-the-fact auditing and post-incident analysis
- Enforcement of rights and compliance obligations in relation to IP ownership, IT governance, personal data protection etc. through moral, legal, regulatory and other means
- Resilience engineering: designing, building, testing, operating and maintaining both business processes (*i.e.* business continuity) and IT systems to provide reliable and secure services by reducing vulnerabilities and single points of failure and hence minimising unplanned downtime and other disruptive incidents even if threats materialise
- Contingency arrangements including backups, redundant assets, IT disaster recovery plans, audits and exercises of same, and insurance - all control measures that you hope never to need but are invaluable if (when!) you do
- Information security awareness, training and education. Helping people understand and fulfil their security obligations (*e.g*. recognizing and responding appropriately to potential social engineering attacks). Motivating them to 'do the secure thing' and avoid the insecure. Creating a security culture.

Conclusion

While some will hopefully find the lists of interest in themselves, the process by which the lists were created was fascinating. Along the way, we have discussed taxonomic issues such as the difference between "threats", "threat sources" and "threat agents"; the distinction between "risk" and "threat"; and whether "vulnerability" is the same as the lack of control. We've found items that could have been classified on several lists, with only slight changes of wording perhaps. And due to the many-to-many relationships, we've not managed in this project to follow a rigorous process for relating threats, vulnerabilities and impacts to risks and ranking them objectively - all we've really done is generate some potential risk scenarios that reflect most of the elements listed. Some would argue that any attempt at a mechanistic numerical analysis of the risks would be misleading in any case. Finally, the suggested controls have ended up being very generic but one only needs to read the headlines to find examples of organizations that have failed to adopt them.

References and further reading

- Australia/New Zealand standard AS/NZ 4360 (2004) provides a generic guide to managing risk in a wide range of activities, decisions or operations. An accompanying handbook is also available.
- CISSPforum and ISO27k implementers' forum (daily) - this document would have rather more imperfections if it were not for the ongoing professional discussions around information security risks and controls on these friendly mailing lists
- Eight New Year's security resolutions for 2008 and other similar security risk and control lists, predictions *etc*. that appear at this time of year, generally based on the authors' experience and prejudices (as indeed is this document, although we have tried to be more systematic and objective than most, and comprise a team of professionals giving, we hope, better balance)
- ISN (Information Security News and GigaLaw (both daily) - ideal ways to keep up with the news of recent information security breaches, prosecutions *etc*.
- ISO/IEC 27001 and 27002 (2005) - promote good practice in ISMS design and aide the selection of appropriate information security controls (and watch out for the imminent release of ISO/IEC 27005 on information security risk management)
- New South Wales Department of Commerce Information Security Guidelines (2003) - useful descriptions of information security risk models and, in section 2, plenty of examples of information security threats and vulnerabilities
- NIST SP 800-30 Risk Management Guide for Information Technology Systems offers 55 pages of sound advice
- RISKS (monthly) - mailing list with news relating to IT risks around the world
- The Information Security Forum Standard of Good Practice for Information Security (2007) does what it says on the tin
- Tim Bass' Top Ten Cybersecurity Threats for 2008 was the bright spark that set fire to this project
- Tom Peltier's book Information Security Risk Analysis (2001) is a practical and worthwhile guide to the process if you want to take this paper to the next level
- World Bank Information Technology Security Handbook (2003) offers nearly 300 free pages of well-written pragmatic advice
- Your favourite information security textbook, CISSP/CISM course book *etc*. such as Computer Security Handbook (2002), the Handbook of Information Security: Key Concepts, Infrastructure, Standards, and Protocols (2006), or Beyond Fear (2003) - start there for the basic information security risk-control concepts

Credits

I'd like to express my sincere thanks to all those willing volunteers who actively participated in the project, either directly writing and editing this document or providing input and helpful comments on the drafts.

The following people have been generous with their time and intellectual input on this project: Tim Bass (www.thecepblog.com) who instigated the idea of listing threats, specifically; Mike Iacovacci (suggested carelessness); Donn Parker (suggested 'endangerment' and others); Sunette la Grange; Chris Norman; Richard O. Regalado (introduced 'threat sources'); Peter Hillier; Geoff Choo; Mike Smith; Les Bell for the infosec risk models (especially the one based on figure 4); Anton Aylward for his thoughts on the taxonomy.

I've benefited from your inputs and perspectives and enjoyed the discussion. Happy new year to you all. I trust 2008 will be more controlled and less risky than 2007.

Dr Gary Hinson CISSP, "Project leader", 31st December 2007