Information Security – new threat - but of a different nature

Introduction

Since their inception in the late 1950 and early 1960s, computer-based information systems have been crucial for most organizations. Since the mid-1990s, the development of Internet has crystallised the role of information technology in the function of a modern organization. Concern with information security has also moved to centre stage since the emergence of the Internet. The importance that one puts on information security is determined by the value placed on it by an organization but factors such as company size and affordability can change that value in the real terms.

Over the years, information security focused largely on technical issues such as encryption, access control and intrusion detection. More recently, economic, financial and risk management issues of information security have become an important concern for today's modern organization. These issues drive, rather than replace, the technical aspects of information security. Today, information security is so much more than just compliance, anti-theft and anti-security breaches and defenses - it's about sharpening your competitive edge for battle in an information-driven age for new business. Information and data is the gold and silver of tomorrow. Controlling access to, as well ensuring the confidentiality and integrity of, vital information assets will be crucial for business with many organizations. Vital information assets would include intellectual property, trade secrets, source code, databases, design / architectural specifications, various forms of internal communications, spreadsheets, logs, non-public information (NPI) entrusted to the organization by customers, business partners, and patient information existing on a variety of computerized devices, such as networks, laptops, and even USB keys. It is the world we live in.

For organizations seeking to balance business requirements with information security needs, achieving ISO/IEC 27001[1] certification makes good business sense, especially because ISO/IEC 27001 controls can actually be mapped directly to multiple regulatory compliance controls and thereby reduce unnecessary overlaps. It allows organizations to build an effective information security program, which addresses current regulatory compliance requirements, pertaining to information security, in a sustainable and cost-effective manner. Now think hard when answering this question, "*Do you want to do business with a company certified to a security management standard or a company that is not*?" Judging by the rate of the global uptake of the ISO/IEC 27001 standard, it would seem that companies based in progressive and the newly emerging knowledge economies have come to the same logical answer that –"*Yes*" – ISO/IEC 27001 certification is a way forward. Irish based companies – or so it would seem – are starting to come out of hibernation and waking up to the need to get certified. Certification will help in the achievement of underpinning business risk and objectives.

In this article, SID2U.com (www.sid2u.com) and eFortresses Ireland (www.eFortresses.ie) jointly take a look at the international standard ISO/IEC 27001, noting that some Irish-based companies (e.g. Elan Corporation Plc.) and government departments (e.g. Department of Defence) are now adopting this internationally accepted standard to help boost their security defences. We also introduce you to SID2U's desktop and network management system 'ASA' (http://www.sid2u.com/downloads.html) and present an opinion on pervasive IT security threats that are constantly lurking and even with Microsoft's current offering 'Vista', the security threat are not going away.

This article is **'Open for feedback'**. We welcome your feedback and encourage interested readers to forward their comments on the subject matter addressed in this article to tom@sid2u.com.

[1] ISO27001: 2005 "Information Technology – Security techniques – Information security management systems – Requirements".

Is Change in the Air?

Network and IT security managers must be aware that the financial and management aspects of dealing with security are as critical to their business as the technical aspects. An organization may be faced with multiple security issues ranging from desktop (e.g. PC / laptop) control, network control, patch management, bandwidth management, network environment infringement management, asset management right through to data access and even USB key usage. These are critical business management issues as well as technical issues, but they are just some of the wide range of issues that require attention to minimise risk of a security breach and ensure the confidentiality and integrity of the business.

Over the past three years, organizations on both sides of the Atlantic felt increased pressure from the introduction of various government regulations and fiduciary requirements pertaining to corporate governance, including information security governance. These requirements include Sarbanes-Oxley Act (SOX), BSA, Basel II, HIPAA, Visa CISP/PCI, GLB Act, California SB-1386 and other state government derivatives, FISMA/NIST 800-53/FIPS 200, UK Data Protection Act, EU Directive on Data Protection and the Canadian PIPEDA to name a few.

We are of the opinion that most information security requirements are really a knee-jerk reaction on the part of regulators and industry groups in response to corporate mishaps and high-impact security breaches. Therefore, the intention is to instill corporate accountability and minimize information security breaches. Most of these regulations are really stipulating common sense best practices and are asking organizations to “do the right thing”, which they should have been doing anyway. Either way you look at it – you know there is a cost.

In 2005, there were over 200 documented high profile security breaches that made national headlines in the US, highlighting a trend that got regulators and industry groups extremely concerned about the protection of personally identifiable information (PII) belonging to customers, business partners and employees. The threat posed by identity theft, including stolen company identities, has also raised the stakes for information security, evolving from an “IT problem” to a business problem, serious enough to keep your average corporate executive up at night.

Globally, organizations are now struggling to keep up with the latest external and internal threats as well as regulatory compliance requirements. As demonstrated by the sensitive information about a Japanese thermoelectric power plant run by the Chubu Electric Power Company being leaked on the Internet following a virus infection, and also demonstrated by the attempted $400 million heist at the London branch of Japanese Sumitomo Bank, and the increased spate of *phishing* attacks on banks and their customers in Ireland, the bad guys are getting smarter and more determined, especially as Cyber-crime becomes more profitable. It is only a matter of time before sophisticated gangs turn to Cyber-crime as the next low-risk and high-return venture. The targets are corporate assets, including financial and identity data. Speed of execution is of the essence and cyber criminals typically target organizations with the least point of resistance. Organizational security weaknesses continue to allow external and internal personnel to perform malicious activity (visit http://www.efortresses.ie/services.htm to see a high profile security breaches matrix for 2005/2006 mapped to ISO/IEC 27001 controls).

Software vendors such *as SID2U.com, AVG, McAfee and eFortresses Ireland* are increasingly echoing the same warning – that software tools *alone* cannot protect organizations from security threats. Organizations need hardened security processes, procedures, software tools and stated policies that are based on internationally accepted best practices, to solidify their information security defenses and meet legal, contractual and regulatory requirements.

Attackers use known security holes to propagate / infiltrate network systems. Many attackers are distributing their source code with the virus, which means that new virus writers have a wealth of proven sample code to craft new viruses. In July 2006, McAfee officially released protection for the 200,000th threat to software systems – such is the volume of threats to a business and the IT network. Today, management must have effective business management processes for security and must implement an effective set of controls, including policies, processes, procedures, organizational structures, software tools, hardware functions and training. In December 2006, Charles Kolodgy, research director for security products at the *IDC* said, "Threat management security solutions are a mainstay of a defence-in-depth strategy designed to protect the network perimeter, internal network, devices, and applications." In January 2007, Jim Allchin (*Microsoft's Co-President for platform and service division*) stated that users should expect vulnerabilities to pop up in Microsoft Vista.[2]

Vulnerabilities within software packages can be exposed and if not addressed can leave an organization open to abuse, interruption and disruption. Yet technology security goes beyond the firewall and anti-virus software protection software. A USB key is an example where a commonly- used device is now viewed as a potential leak threat. Another example is not having the latest version of anti-virus software package on one solitary laptop logged onto the network, locally or remotely. The *cliché* that a network system is "only as strong as the weakest link" is too true for comfort. Viruses and worms infiltrate network systems through the back door. These are just two examples of how the security threats are widening. Management must implement frequent risk assessment as a key security undertaking to protect the business. Sadly, in today's world, it must be an ongoing process. There is no longer time for naivety. There no longer is room for excuses.

Cyber-crime, technology inefficiency threats, Internet fraud, and even a software vendor's decision to drop support for their technology can expose an organization to a breach in security. However, the more knowledge that we have about the causes and the consequences of information security breaches, as well as the way an organization addresses information security issues, the more likely information security defences will improve.

This is where the international standard ISO/IEC 27001:2005 standard can help.

A Brief History: ISO/IEC 27001:2005

The IT security standard revolution began in the UK with the February 1995 publication of the BS7799-1 standard. As a result of the momentum gained, the ISO/IEC 17799 was published in December 2000 and has now achieved international acceptance as the most comprehensive best practices framework available for Information Security Management. Up until October 2005, organizations could only be certified against BS7799-2 and not ISO 17799. In October 2005, industry received the long awaited ISO/IEC 27001:2005, just four months after the publication of the significantly revised version of ISO/IEC 17799 (See appendix A1).

Organizations worldwide can now be certified against ISO/IEC 27001:2005 titled "Information Technology – Security techniques – Information security management systems – Requirements". Unlike ISO/IEC 17799, which is a "code of practice", ISO/IEC 27001:2005 is a certifiable standard that is intended to provide the foundation for a third party audit and is harmonized with other management standards, such as ISO 9001 (i.e. quality management) and ISO 14001 (i.e. environmental management). In other words, the Information Security Management System (ISMS) developed for ISO/IEC 27001 certification can be integrated with existing management systems.

[2] Source: ComputerScope, January 2007

Ireland vs the Globe

Globally, there are over 3309 companies ISMS certificates issued in February 2007 and the breakdown by country is as follows:

Japan	1907*	Austria	11	Oman	2
UK	319	Saudi Arabia	8	Slovak Republic	2
India	269	Spain	8	South Africa	2
Taiwan	123	Sweden	8	Sri Lanka	2
Germany	74	UAE	8	Armenia	1
Hungary	55	Iceland	7	Egypt	1
Korea	48	Philippines	7	Lebanon	1
USA	46	Greece	5	Lithuania	1
China	43	Kuwait	5	Luxemburg	1
Italy	42	Russian Federation	5	Macedonia	1
Netherlands	31	Argentina	3	Moldova	1
Singapore	28	Croatia	3	Morocco	1
Hong Kong	25	France	3	New Zealand	1
Australia	22	Indonesia	3	Pakistan	1
Malaysia	18	Isle of Man	3	Peru	1
Ireland	17	Macau	3	Qatar	1
Poland	15	Romania	3	Serbia and Montenegro	1
Brazil	14	Slovenia	3	Ukraine	1
Czech Republic	14	Thailand	3	Uruguay	1
Finland	14	Bahrain	2	Vietnam	1
Norway	14	Belgium	2		
Switzerland	14	Canada	2		
Mexico	12	Colombia	2	Relative Total	3322
Turkey	12	Denmark	2	**Absolute Total**	**3309***

Fig. 1: Number of Certificates Per Country - sourced by the ISMS International User Group on 22nd February 2007[3]

[3] The total number of ISO/IEC 27001 certificates is now **933** (this includes **432** BS 7799 Part 2:2002 upgrades and **501** new certifications). *The Absolute Total represents the actual number of certificates. This table is copyright © ISMS International User Group 2001-2005*

In July 2005, Ireland had '11' organizations certified to ISO/IEC 27001. SID2U.com tracked the adoption of this standard and noticed that one year later, July 2006, Ireland still had 11 certified. However, by February 2007 the numbers noticeably increased to 17. **Are Irish-based firms coming out of hibernation?** Well hopefully, yes! Many progressive European countries and 'so-called' emerging Asian countries are 'roaring ahead' with certification to the international security standard. Irish-based companies on the registration include *GTech (Ireland) Operations Limited*, *Health Services Executive (HSE) – Health Protective Surveillance Unit*, *Sysnet Ltd*, *Vodafone IT Operations*, *Eircom.net*, *Sentenial Ltd.*, *Elan Corporation and Wyeth Medica (Ireland) Ltd* amongst others. **Do we hear a Celtic Tiger 'roar' in response?**

Since July 2005, more than 1,600 companies were certified globally. The rise is exponential. Business enterprises in Japan, India and Taiwan are strongly positioned for future business. The Japanese government established their own scheme of "ISMS", which is almost identical to ISO/IEC 27001, under the Japanese accreditation body, known as 'JIPDEC' (www.isms.jipdec.jp/en). The acronym 'ISMS' is well promoted and is almost a prerequisite for trade in Japan. In July 2005, India had 118 companies certified to ISO/IEC 27001. By June 2006, the figure rose to 157. By February 2007, 269 companies were certified.

In Europe the UK, Germany and Italy are leading the European charge but perhaps more noticeably for Irish competitiveness, the Czech Republic and Poland are starting to make good progress. Perhaps, they too recognize the importance of the ISO/IEC 27001 standard for future business and their competitiveness!

Let us be clear, certification sends out a clear message: "Our data and information is secure and protected. We are good to do business with."

We believe that public sector departments in the UK are issuing tenders whereby certification to ISO/IEC 27001 is a prerequisite for the tender and that this could soon apply in Ireland. We have no concrete data to support our suspicion, but do you too not think that it is logical step and inevitable? Clive Nightingale, Lead Assessor, *Certification Europe* believes that we are starting to see some signs that public sector organizations are issuing tenders where ISO/IEC 27001 certification is a prerequisite, noting that companies providing highly confidential services are actively implementing security management systems to ensure they remain competitive. As for Irish exports and the potential knock on effect, well, according to *Kable Research (London)*, the UK public sector is now the largest ICT spender; £16bn will be spent on ICT in 2006/2007 and £17.9bn in 2007/2008. The UK is traditionally important for Irish ICT exports. **Will Irish exports suffer? What is your opinion?** We want your feedback! Should *Enterprise Ireland / Shannon Development* take a lead on this? Is more investigative work required? What do you recommend?

Opportunity Knocks

Unlike existing security-related certifications such as SAS 70 and Web Trust, ISO/IEC 27001:2005 certification is much more comprehensive and specifically focused on information security management.

ISO/IEC 27001 certification enables organizations to clearly demonstrate that their information security program is not only effective but also regularly reviewed and updated based on the *plan-do-check-act* (PDCA) process model, covering performance, effectiveness monitoring and review, and continual improvement. The controls defined in the standard are to be implemented to meet the requirements identified by a risk assessment.

The standard is also intended as a common basis and practical guideline for developing organizational security standards and effective security management practices as well as to help build confidence in inter-organizational activities.

Benefits of pursuing ISO/IEC 27001:2005 certification, include:

❑ allow organizations to mitigate the risk of information security breaches

- allow organizations to mitigate the impact of information security breaches, in the event that they do occur
- reduce the penalty imposed by regulators in the event of a security breach, since the organization's security and record-handling procedures will be seen as following internationally accepted best practices
- allow organizations to demonstrate due diligence and due care to shareholders, customers and business partners, through strategic thinking
- allow organizations to demonstrate proactive compliance to legal, regulatory and contractual requirements, as opposed to taking a reactive approach
- provide independent third party validation of an organizations information security management system.

ISO/IEC 27001:2005 certification is the most comprehensive information security management certification that is internationally accepted. Certification programs such as SAS 70 and Web Trust cannot provide all the benefits listed above, due to their limited scope.

One of the companies certified to this standard is *GTech (Ireland) Operations Limited*. Managing Director, Jacinta Kielty, believes that the standard is tremendous for business operations and continues to be valued across the company. Clive Nightingale *(Certification Europe)* believes that this standard demands management commitment to their organization's system, because they have defined and documented policies and processes that in the event of any malpractice the responsibility lies with management and is likely to be reinforced by litigation.

Security Implementation Tips

Some of the critical tasks required for implementing an effective Information Security Management System (ISMS) when pursuing ISO/IEC 27001 certification, include:

- procure the ISO/IEC 27001:2005 standard
- obtain full executive management support
- consider consulting options e.g. Big 4 consultants versus BSI Associate Consultancies
- define the scope and boundary of the ISMS, working in conjunction with your Certification Body
- consider legal, contractual and regulatory requirements
- define an ISMS policy
- define the risk assessment approach
- identify, analyze and evaluate the risks
- identify and evaluate risk treatment options
- consider centralized software tools to reduce the identified risks and manage more effectively
- select controls and control objectives and reasons for selection
- obtain management approval of the proposed residual risks
- obtain management authorization to implement and operate ISMS
- prepare a Statement of Applicability that qualifies the elements of the standard that are being adopted. This document is verified at the time of the certification audit and included in the certificate is reference to the version and date of this document.

Security Threats

If you think that the number of security threats is in decline - well - think again. Fig. 2 (below) serves to highlight that the potential for security attacks considered "high" or "extremely critical" is rapidly rising. Courtesy of Secunia Security Advisories, Fig. 2 shows that overall the number of high and critical advisories continues to rise.

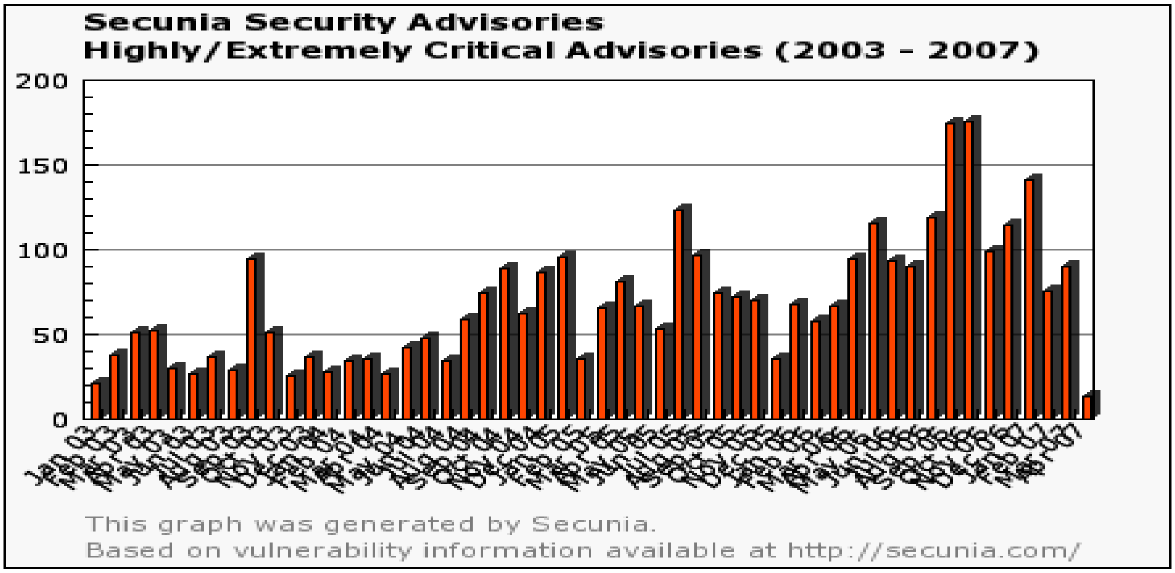


Fig. 2: - Vulnerability graph - Secunia advisories (4th April 2007).

Undoubtedly, a number of organizations experienced security breaches over this period, many going unreported. Negative publicity could hurt the company image, stock markets, etc. and no doubt the competition would use it to their advantage.

Organizations face increasing costs (i.e. both tangible and intangible) as a result of information security breaches and regulatory non-compliance, including heavy fines, loss of customer confidence, loss of reputation, regulatory scrutiny, loss of market share and criminal and civil litigation.

With the recent spate of high profile information security breaches and subsequent hefty penalties being handed down by US regulators, in the information security world, **R**eturn **O**n **I**nvestment (ROI) is now taking on new meanings:

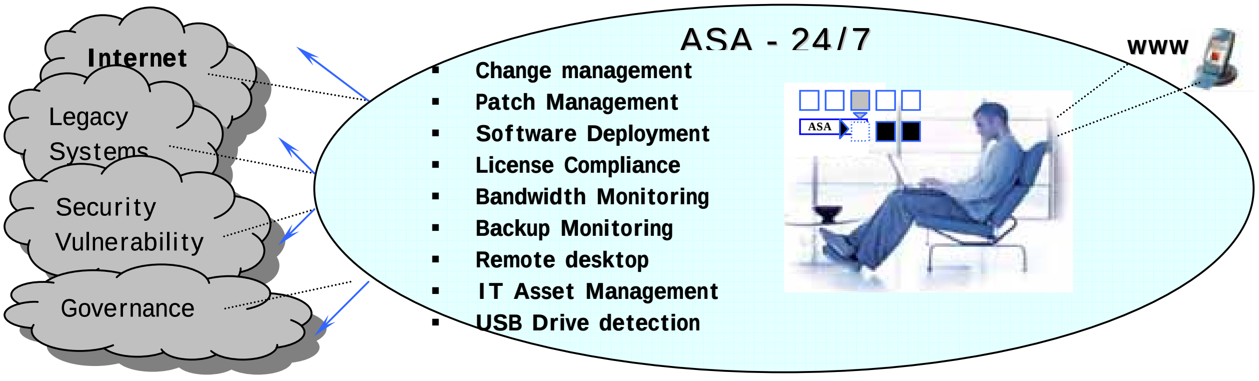
- ❑ **R**isk **O**f **I**mprisonment
- ❑ **R**isk **O**f **I**nvestigation
- ❑ **R**eturn **O**n **I**nsurance
- ❑ **R**eduction **O**f **I**ncidents etc.

A recent *IDC survey* indicates that organizations that take a more integrated approach to security and compliance issues can achieve tremendous cost savings. The days of addressing security and compliance requirements in silos are truly over. Today, a typical network environment consisting of a jumble of disparate technologies (including portals, business intelligence, knowledge management, etc.) and a variety of integrated applications (i.e. broker or otherwise), represents many possible vulnerability attacks. Over 51% of UK businesses believe that their infrastructure is never 100% protected against threats. Just one PC/laptop on the network running a previous version of anti-virus software (e.g. McAfee, AVG) is all that it takes for a virus to disrupt business continuity or damage the business. Disruption or damage could also be caused by the simple use of a USB key drive. Remember – an organization operating singularly or through interconnectivity is only as secure as its weakest link! Remote attacks are quite common. Worms spread without user interaction. According to a *CSI / FBI survey* 2005, over 30% of organizations saw unauthorised access to their data. According to the *DTI / PWC* the average cost of the worst security incident ranged from €12,000 to €26,000 and 56% stated that they suffered data loss. A recent survey published by the *ISSA (Ireland)*[4], stated that over 98% of respondents reported issues, the most common of which were viruses and other malicious software (90%), misuse of systems (88%), asset theft (63%) and phishing (56%). **So what is the cost to your organization?** Consider the following to determine the potential financial impact on your organization:

Downtime:	What is the cost of the computer downtime in your environment? What is the cost of critical business transactions and systems being interrupted?
Remedy time:	What is the cost of fixing a problem that spans your IT environment?
Stolen intellectual property:	What is the cost if any of your intellectual property is stolen or destroyed?
Credibility:	What is the cost if you lose credibility with your customers? What is the cost from negative public relations?

What works best for you will depend on the risks and compliance culture of your organization? One thing is clear is that there is no room for naivety. Reducing human error through automation promises direct and indirect IT savings, as well as more efficient business support. Security costs. It is a business issue.

Developed in Ireland, SID2U.com's Automated Systems Administration (ASA) product is an exciting, cost-effective network and desktop management product recently released in the Italian, German and Irish markets. ASA[5] is a comprehensive product, designed to ease the burden of managing a network environment and comes 'all-in-one' - without the added on integration cost. Its purpose is to *simplify* the administration and management of network and desktops, to *improve efficiency, security, software licence compliance* and to *reduce cost*.



ASA: Intuitive - Easy to use – Easy to Administer - **An 'all-in-one' low cost product**

With ASA, a core set of systems administration tasks are automated, which includes:

- change / infringement management,
- software patch management,
- bandwidth monitoring,
- software deployment,
- software licence control,

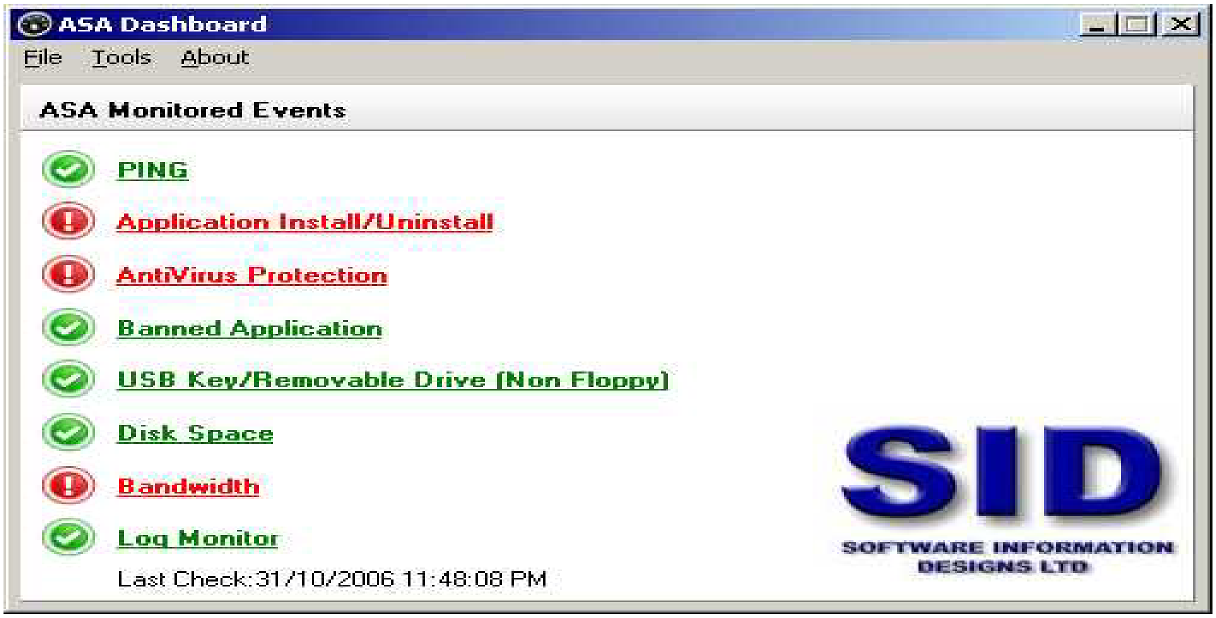
[4] ISSA / UCD Irish Cyber crime Survey 2006: The impact of Cyber crime on Irish Organisations.

[5] ASA: Automated Systems Administration (*visit* http://www.sid2u.com/downloads.html for product brochure).

- IT asset management,
- backup monitoring,
- remote desktop,
- multiple network utilities (e.g. ban applications, USB drive detection),
- ping monitoring for mission critical servers,
- disk space monitoring.

ASA can be configured to detect events or infringements and sends an email / SMS warning notification when an event occurs. Such events can signal new unidentified threats or a system compromise.

A centralised product, ASA, is thin client technology and incorporates useful dashboard technology (example below) as well as the early warning alert system with diagnostic information to mobile phones across multiple network environments.



ASA Monitored Events

✓ PING
! Application Install/Uninstall
! AntiVirus Protection
✓ Banned Application
✓ USB Key/Removable Drive (Non Floppy)
✓ Disk Space
! Bandwidth
✓ Log Monitor

Last Check:31/10/2006 11:48:08 PM

Fig 3: ASA – Sample screen shot

According to Dr. Bernhard Kölmel, IT Director, *CAS Software A.G.*, *Germany*, “We found the ASA product to be extremely comprehensive and useful. It is a well thought out piece of technology and eased the pressure on our internal support resources”.

It is possible to register on-line for a ’30-day free trial’.

ASA is sold at low cost and licensed software. We believe that it is important that companies maximise their ROI. The capability of ASA will go a long way in achieving that objective.

For more details of the capability of ASA please visit www.sid2u.com.

Conclusion

The bottom line is that security is a key business issue in more ways than one.

Clearly, the world's leading and emerging economies are taking the ISO/IEC 27001:2005 standard seriously. We suggest that only organizations that are ISO/IEC 27001 certified will at some point in the future be only invited to tender. We also suggest that this process will gather momentum in the UK and then Ireland will follow the UK Public Sector initiative and then it is snowball time. The Irish exchequer could lose billions. Should we act now or follow at cost?

Economic, financial and risk management issues of information security have become an important concern for today's organization. These issues drive rather than replace, the technical aspects of information security. There is a cost. It depends on how you look at it. Management must have effective business management processes for security and must implement an effective set of controls, including policies, processes, procedures, organizational structures, software tools, hardware functions and training to achieve business best practice information security. Some organizations are taking more of a "check box" approach to compliance, especially since they are finding it difficult to derive real business value from compliance spending. However, a more pragmatic approach is for organizations to seek independent certification to ISO/IEC 27001, which helps to address current and future regulatory compliance requirements in a proactive, cost-effective and sustainable manner. If the rapid uptake of ISO/IEC 9001 certification for Quality Management in the 1980s and 1990s is anything to go by, the uptake of ISO/IEC 27001 certification for Information Security Management is likely to be more intense than that of ISO/IEC 9001, considering the current business driver for effective Information Security Management is not just competitive advantage. In Ireland, Certification Europe is the only indigenous certification body accredited at this time to assess against ISO/IEC 27001.

Organizations now have legal, contractual and regulatory requirements as additional motivators. It remains to be seen if the Government bodies such as Enterprise Ireland and Shannon Development will take a lead to help SMEs. The establishment of a grant-aided incentive scheme dedicated to support SMEs achieve the ISO/IEC 27001 certification would be good for the Irish business community. We encourage this action. Such a scheme could incorporate a database for the registration of software tools, which would help SMEs to address some scope for the international standard (e.g. software patch management, bandwidth monitoring, USB drive detection, etc.). Consultants would also have a role to play too.

We **open this article for feedback**. It is treated as a 'living' document. We look forward to preparing a follow up article on IT security, which will be based on the content of this article and your feedback. Constructive comments are now welcomed. Please direct them to tom@sid2u.com.

Authors

Henry Ojo

Tom Flynn

Henry Ojo, of eFortresses, Ireland is a BS7799 certified auditor and information security expert with a pragmatic holistic approach to the management of information security and regulatory compliance, as well as a subject matter expert on information security governance and compliance relating to regulatory requirements such as HIPAA Security, GLB Act, Sarbanes-Oxley Act, PCI Data Security (Visa CISP), California SB-1386, UK Data Protection Act, EU Data Protection Directive and many others. Henry is a major contributor to the Holistic Information Security Practitioner (HISP*)* Certification Program http://www.hispcertification.org/, the industry's first integration course for security and compliance professionals. For further information contact hojo@eFortresses.com or visit www.eFortresses.ie. The company is also an ISO 27001 Associate Consultancy of BSI Americas.

Tom Flynn is the Managing Director of SID2U Limited, an Irish software development company and the producers of the ASA product, which is comprehensive software for network and desktop management. ASA is a centralised product, which is designed to *simplify* the administration and management of network and desktops, to improve *efficiency, security, software licence compliance* and to *reduce cost*. A core set of systems administration tasks are automated including: software patch management, bandwidth monitoring, software deployment, software licence control, IT asset management, backup monitoring, remote desktop, multiple network utilities (e.g. ban applications, USB drive detection), ping monitoring for mission critical servers, disk space monitoring and change / infringement management. ASA http://www.sid2u.com/downloads.html is designed to aid network managers, system administrators, IT directors, CIO, security and compliance managers, financial managers and IT consultants. Tom has worked for the National Software Directorate, the European Commission and was the President of the 6th European Software Quality Conference. Recently, the company won a significant European project with Hewlett Packard (Italy) for the development of open platform technology, MUSIC. For further information contact tom@sid2u.com or visit www.sid2u.com.

Contribution

The Authors are grateful for the contribution of the following people:

Ian Cowan:	National Standards Authority of Ireland.
Jacinta Kiely:	GTech (Ireland) Operations Limited
Clive Nightingale:	Certification Europe.
Bernhard Kölmel:	CAS Software A.G., Germany.

Remember this is a ‘discussion’ document. Your feedback is welcomed!

Please send your feedback / input to

tom@sid2u.com

Thank you.

An ‘unofficial’ but hopefully useful glossary on security issues and references addressed in the article follows as does a brief introduction to the ISO/IEC 17799:2005.

Glossary

Attacker: Person implementing or organization responsible for the attack.

ASA: Automated Systems Administration product.

Basel II: **Basel II**, also called **The New Accord** represents recommendations by bank supervisors and central bankers from the 13 countries making up the Basel Committee on Banking Supervision (BCBS) to revise the international standards for measuring the adequacy of a bank's capital. It was created to promote greater consistency in the way banks and banking regulators approach risk management across national borders.

BSA: Business Software Alliance is an organisation dedicated to promote a safe and legal online world. The BSA is the voice of the world's software and internet in industry before government and with consumers in the international marketplace.

BS7799: The BS 7799 International User Group that was convened by UK DTI, onto which other national were invited, to revise and internationalize BS 7799: 1995. The NSAI participated because of its perceived importance at the time by the Advisory Group on IT & T Standards (precursor to the ICT Standards Consultative Committee), and this resulted in the publication of I.S. 17799-1: 2000 and I.S. 17799-2: 2000 and 2002, publicly launched in Ireland at the time.

California SB-1386: **Senate Bill 1386** is a California state law regulating the privacy of personal information.

Canadian PIPEDA: *Personal Information Protection and Electronic Documents Act* is a Canadian law governing how private sector organizations collect, use and disclose personal information in the course of commercial business.

CSI: Computer Security Institute (USA) www.gocsi.com

DTI: Department of Trade and Industry (UK)

eFortresses: eFortresses is a risk management software company providing best of breed solutions for information security, privacy and regulatory compliance. Mission is to provide clients with the knowledge and expertise to make informed decisions regarding exposure to regulatory non-compliance and potential theft or compromise of information assets. Knowledge and expertise are provided by a combination of automated assessment, extensive and continuous research, and real world experience gained in projects over several years for government and commercial organizations worldwide. www.eFortresses.ie

Encryption: Allows information to be transmitted or stored securely and ensures that information received can be verified to ensure that it came from the advertised source and not changed in transit.

EU Directive on Data Protection: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Firewall: A firewall controls the access between computer networks – normally between the internal Local Area Network and the Internet. A set of rules is defined on the firewall, which specifies the information that is permitted to pass through. Firewalls can also be used to set up encrypted tunnels across the internet so that information passing between the LAN and a home user, or the LAN and a remote site is encoded.

FISMA/NIST 800-53/FIPS 200: The Federal Information Security Management Act (FISMA) is a law stating the measures to implement in order to secure United States federal property and information. The FISMA assigned the National Institute of Standards and Technology (NIST), the responsibility of defining standards and security procedures to be respected by American governmental agencies and to reinforce the information systems security level. These standards have been published in the Federal Information Processing Standards Publication 200 (FIPS PUB 200), and the security controls to be made have been detailed in the NIST Special Publication 800-53 document.

HIPAA Privacy & Security: **Health Insurance Portability and Accountability Act** (**HIPAA**) The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. It establishes regulations for the use and disclosure of Protected Health Information (PHI).

GLB Act: The ***Gramm-Leach-Bliley Act*** of 1999, a U.S. legislation provides limited privacy protections against the sale of your private financial information. Additionally, the GLBA codifies protections against pretexting, the practice of obtaining personal information through false pretences.

ICT: Information Communication Technology

IDC: International Data Centre

IPS: Intrusion Prevention Systems. IPS will block traffic marked as potentially dangerous. Emails identified with ‘false’ positive can prevent a significant amount of legitimate traffic from entering your network. Ironically, accidentally denying legitimate traffic can equally be catastrophic.

IDS: Intrusion Detection System. IDS will detect only and log as potentially dangerous allowing the ‘false’ positive emails onto the network.

ISMS: Information Security Management System

ISO/IEC 9001: Quality Management Systems standard published to govern the management of quality

ISO/IEC 17799: An information security framework published and most recently revised in 2005 by the International Organization for Standardization and the International Electro technical Commission. It is entitled *Information technology - Security techniques - Code of practice for information security management*. The current standard is a revision of the version published in 2000, which was itself a technical copy of the British Standard BS 7799-1:1999.

ISO/IEC 27001: An information security standard published in 2005. The current standard is a revision of BS 7799-2: 2002, which has now been withdrawn. ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented (ISMS). It specifies requirements for the management of the implementation of security controls. It is intended to be used with ISO 17799:2005, a security Code of Practice, which offers specific security controls to select from.

ISSA: Information Systems Security Association

Mitigation: Software configurations, hardware or procedures that reduce risk in an IT environment.

Node: A node is any piece of equipment that has its own IP address and is therefore uniquely addressable on the network.

NSAI: National Standards Authority of Ireland. http://www.nsai.ie

PDCA: Plan-Do-Check-Act process model

PHI: PHI is any information about health status, provision of health care, or payment for health care that can be linked to an individual[12]. This is interpreted rather broadly and includes any part of a patient’s medical record or payment history.

Phishing: Phishing are online crimes that use spam to direct Internet users to web sites that are controlled by thieves but designed to look like legitimate e-commerce sites. Users are asked to provide sensitive information such as password, bank account number, credit account number, and social security number often under the guise of updating account information.

PWC: PriceWaterhouseCoopers.

Sarbanes Oxley (SOX) Act: A United States federal law passed in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, and WorldCom (now MCI).

SAS 70: Statement on Auditing Standards (SAS) No. 70 ("*Service Organizations*") is an international auditing standard developed by the American Institute of Certified Public Accountants (AICPA)

SID2U.com: www.sid2u.com: Developers of low cost comprehensive desktop and network management software solutions. Thin client architecture. Zero client side maintenance.

Virus: A small program or piece of code inserted into legitimate programs or processes. It will be executed as the carrier or other programs run and will cause something to happen in the system that is abnormal. It attaches itself to a host program. Viruses can be introduced by a numbers means such as by downloading programs from the internet, receiving email, using electronic media, CDs, connecting directly to other PCs or LANs (Local Area Networks), not using the latest version of anti-virus software, using pirate software, logging on to a LAN via an infected portable computer.

Visa CISP/PCI: The Payment Card Industry standard developed by MasterCard International and Visa endorsed and adopted by payment brands. It applies to all members, merchants, and service providers that store, process or transmit cardholder data.

Vista: Microsoft’s latest Operating System. A coalition of companies - rivals to Microsoft - allege that Microsoft's new Vista operating system will perpetuate practices found illegal in the European Union nearly three years ago (i.e. 2004). The group, which includes IBM, Nokia, Sun Microsystems, Adobe, Oracle and Red Hat, said its complaints made last year are yet to be addressed just days before Vista is due for release. (26/1/07) http://www.pcpro.co.uk/news/103207/vista-under-attack-as-illegal-in-europe.html

Vulnerability: Software, hardware a procedural weakness, a feature or a configuration that could be a weak point exploited during the attack. Also often referred to as an exposure.

UK Data Protection Act: A British Act of Parliament that provided a legal basis and allowing for the privacy and protection of data of individuals in the UK.

Virus: A small program or piece of code inserted into legitimate programs or processes. It will be executed as the carrier or other programs run and will cause something to happen in the system that is abnormal. It attaches itself to a host program. Viruses can be introduced by a number of means such as by downloading programs from the internet, receiving email, using electronic media, CDs, connecting directly to other PCs or LANs (Local Area Networks), not using the latest version of anti-virus software, using pirate software, logging on to a LAN via an infected portable computer.

Worms: Can be as malicious as a virus. Worms are self-replicating programs that can spread from computer to computer without infecting files first.

Web Trust: A seal of assurance service developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

Appendix A1 - ISO/IEC 17799:2005 – A Brief Introduction

The last revision of the international security management standard, ISO/IEC 17799: 2005, was published 15th June 2005 to establish guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The prime objective is to outline guidance on the commonly accepted goals of information security management. The standard contains best practices of control objectives and controls in the following areas of information security management:

- ❑ security policy
- ❑ organization of information security
- ❑ asset management
- ❑ human resources security
- ❑ physical and environmental security
- ❑ communications and operations management
- ❑ access control
- ❑ information systems acquisition, development and maintenance
- ❑ information security incident management
- ❑ business continuity management
- ❑ compliance.

Disclaimer:
Any views and opinions expressed are those of the individual authors/sender and are not necessarily shared or endorsed by others and shall not assume any legal liability or responsibility for any incorrect, misleading opinionated or altered information contained.

< This is the final page of the article. Edition 1.0, April 2007 >