

Information security policies

– awareness and enforcement –

Author: **Alex Kelley**

MBA/MS-MIS candidate

Joseph M. Katz

(Graduate School of Business)

Coordinator: **Dr. Brian Butler**

Head of MIS department

Joseph M. Katz

December 4, 2008

Summary

As the world of information technology has evolved, the damage of poor security towards corporate and personal information has increased tremendously. The security of data and information is not a new issue, but it is nevertheless challenging. There are multiple threats from an IT security point of view: malicious code, hacker attacks, unauthorized access, and so on.

Sometimes overlooked is the employee. For an outside hacker, the first obstacle towards achieving his goal is access to the information. He needs to either get physical access, which can be difficult depending on the measures in place (badge, for instance), or get electronic access through wired channels by finding a weak link on the IT side and exploiting it, which typically requires some effort. The employee, on the other hand, received physical access by simply being hired within that company, and also can access a number of application that give him or her permission to see and even update internal information that is not available to an outsider. Thus, the potential damage is much higher from the employee, as he has direct access to more data. The case when an employee intends to do damage aside, there is still the issue of making him aware and informed of the threats.

This paper presents background information on the issue, then reviews some of the current practices in implementing security policies and their content. There are many articles and publications debating the issue and offering solutions; however, since it still is a current issue, my thesis is that most recommendations are either difficult to implement or have serious drawbacks.

The case for information security

Not only do regulations impose a strict control of internal information of a company, but so does the need to remain viable when faced with aggressive competition and public disclosure of internal practices.

The security of information is not a new issue, but it is nevertheless challenging. PrivacyRights.org maintains a record of all declared breaches since January 2005ⁱ and shows a total of over 245 million people in the United States who had their personal information (social security numbers, financial data) inadvertently released to non authorized persons. This list only reflects, as mentioned, the breaches that have been discovered and made public (due to specific regulations), and only if they affected end users, as opposed to company data. Given that the population of the United States as estimated for July 2008 is almost 304 million peopleⁱⁱ, of which 20% are under 14 years of age, one could argue that each individual's personal data has been compromised to a certain extent (depending on the severity of the breach and the type of information that was released), and potentially not only once.

Information security has created a tremendous amount of hype, especially with the development of Internet, which connects an estimated 541.7 million computers in more than 250 countries on every continent as of January 2008ⁱⁱⁱ, and the more and more intense use of technology in the workplace. The concept broadly refers to protecting the data that an entity owns at a certain point in time. This data can be top secret (usually encountered in government agencies or contractors), of strategic value (the loss of it would mean the loss of a competitive advantage a company currently sustains), of private concern (employees personal information, medical history etc.). In a word, the information that is at stake would cause problems of some kind if it is intercepted, modified, stolen, lost or deemed unusable or unavailable.

In addition, careless access^{iv} could also result in unpleasant legal actions against the company, or could be detrimental in current or future law suits. The Internet Library of Law and Court Decisions^v has a large database with examples of lawsuits that have a root in electronic access; while not all of them are strictly related to security of information, there is still a wide array of cases that address the issue of misuse or loss of confidential data.

Principles and problems

The core principles of information security are known as the CIA Triad^{vi}, which stands for confidentiality, integrity and availability. The *confidentiality* of data is the part of the core principles that is most obvious; it refers to the ability to hide the information from the people that are not authorized to see or access it. The *integrity* refers to the ability to ensure that the data is authentic and complete^{vii}. Finally, the *availability* ensures that the information is readily accessible to an authorized user at all times.

In addition, two more principles have surfaced as suggested by the legislation pertaining to information security: *accountability*, which determines the controls necessary to trace actions back to their source, and *assurance*, which works towards creating the confidence that technical and operational security measures work as intended^{viii}.

All these principles are guarded through well-placed systems that have the sole scope to protect the company's databases and to ensure that the data respects the recommendations in the principles. Among the *technical* products that help ensure the C-I-A of data are firewalls, virus and intrusion detection software, and the use of encryption^{ix}. However many the technical solutions

are, the contingency planning and training for a breach take place at the operational level, while higher management should be responsible for creating a security policy, conducting risk assessments and identifying comprehensive security architectures^x.

A look along the list mentioned above, from PrivacyRights.org, shows a decrease in the number of hacked servers or breached systems in the past couple years and an alarming increase in the cases of employees that left an unsecured laptop in a public place or mistakenly made some otherwise private records public via the Internet. This suggests the premise that the technology has improved over the years and even though is not perfect, it is now ready to face the attacks with greater chances to success; however, there are still many cases when the employee that has access to confidential data does not entirely understand or chooses not to respect the company's security policy with regard to that information.

Issue statement

In the growing development of technology and its impact upon corporate operations, a key element in protecting an entity's confidential information is reflected in every employee that has a certain level of access to either the actual data or to

the physical facilities of that entity; any access underlines a certain degree of trust that the company has placed in the particular employee. A large part of this paper is be dedicated to the corporate security policies: what they are, how they are created, presented, applied and enforced – and where their weaknesses lie.

According to a study^{xi} done at the end of 2007, among the vulnerabilities in information security lie the insufficient attention to human factors in systems design and implementation; management that does not understand that security is the entire company's responsibility, not only IT; ignorance, carelessness negligence or idle curiosity from by users; an apparent disconnect between solid information security and commercial success which usually leads to inadequate investment in security controls. All these vulnerabilities are potentially exploited by either the company's employees or by outside users that target the employees. The important idea is, however, that it becomes more and more evident that the human factor is essential in its alignment with the overall understanding of security in any given corporation and the implementation of adequate policies and controls.

This represents a clear change from a similar assessment five years before^{xii}, where the technology challenges seemed much more pervasive and the

only human-related issues perceived referred to inadvertently downloads of potentially malicious code from browsing the internet, or to renaming files and not being able to retrieve them later due to the change in the name or extension.

Many companies do not always create the security policies in a clear and actionable manner. In addition, even if they cover all issues of access and forbidden actions, the biggest difficulties come in the actual monitoring of how the policy is implemented, as well as in raising awareness of the issue among the employees.

Stakeholders

A stakeholder represents an individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services^{xiii}. From a corporate security perspective, stakeholders' interests are likely to be expressed around enhancement and preservation of the company's reputation, protecting the privacy of the corporation's information, availability and reliability of services offered to internal and external customers^{xiv}.

Given the above-mentioned stakes, all the company's employees have a loss

potential from the failure of security policies, from the CEO of the company to the summer intern in the finance department.

Advantages of understanding the issue

Typically, the correct application of internal information security policies translates in seamless business processes and uninterrupted operations – from the point of view of diminished privacy concerns and limited loss of critical enterprise information. A well understood and applied security framework leads to a higher level of expectations from the business activity, but is not really noticed until something goes wrong.

Potential dangers of understating the issue

Not implementing correct and adequate security measures, both technologic and human resources, could lead to negative consequences as the company would find itself faced with loss¹ of strategic information (which could affect its position among the competitors), or with loss of private – client or employee – information (which would potentially

¹ The “loss” of data is used here in a larger sense to mean unavailable, incomplete/corrupt, or missing information

imply legislation non-compliance fines, and diminished trust from investors and clients).

Legislation and industry standards

Evidently, one of the reactions with regard to security is related to existing legislation. Companies have spent millions of dollars in solutions meant to ensure their systems are in accordance with the specifications and thus diminish the risk of having to pay heavy penalties for non-compliance.

There are a few acts^{xv} that touch on security, and they come from different areas: financial institutions, health care, state law etc. The main requirements found in the legislation are directions towards what the systems should be able to provide, but no clear steps are given.

On the other hand, certification processes and ISO standards tend to have more detailed and better defined requirements – but they do not always address security directly, representing only a set of processes and associated technology that can be applied at any level in the hierarchy of a system’s structure^{xvi}. The ISO 9000 family of quality management standards define quality as the customer-required features of a product or service^{xvii}, which inherently involves some measures of security; the expectation is that the certification will portray a

secure organization^{xviii} given the ISO certification.

ISO 27001 and 27002², on the other hand, are information security management standards, meant to provide a more detailed framework for information systems managers in addressing risk assessments, technologies and internal policies. They are part of a larger family of standards, the 27000s, currently in development^{xix}. An important element of the series is recognizing the importance of involving^{xx} the senior management in the implementation of the standard, with its benefits and costs.

The Information Systems Audit and Control Association (ISACA) has developed separately a set of guidance for IT governance called COBIT³, which is dedicated to understanding and managing the risks associated with IT by bridging the gaps among business requirements, control needs and technical issues. A detailed assessment of the maturity for a specific critical area can be realized, under COBIT, by considering the three dimensions of the framework, capability, coverage and control^{xxi}, in the context of the overall business requirements.

² Created by the International Organization for Standardization (ISO)

³ The acronym COBIT stands for Control Objectives for Information and related Technology

How the security issue appears in press, vendor whitepapers and academic research

Press

The issue of employee as a security threat to the company is not addressed too often in business publications. There, security of information technology is regarded more from the point of view of reporting regulations^{xxii} or describing cases^{xxiii}.

The in depth analysis is left for the technology-oriented publications, which target a “how to” approach in providing advice on addressing parts of the issue. There are articles concerning the strengthening of password policies^{xxiv}, containing advice on how to identify an insider threat^{xxv}, listing best practices^{xxvi}, or pointing out that the employees are the biggest danger^{xxvii} to a company’s information.

Vendor whitepapers

The vendor whitepapers show an understanding of the issue and are trying to provide solutions and advice by analyzing the causes and identifying possible courses of action that would diminish the risk. Most of these are technical solutions, yet they address aspects of the main issue by

either simplifying employees' activities with a single sign-on application^{xxviii} meant to decrease the risk of writing passwords on sticky notes as fewer would need to be remembered, or by providing an overview of common means of communication (like e-mail) with recommendations on how to monitor it and thus prevent potential threats, thus using information tools to self-promote the vendor's products⁴ for information security in general^{xxix}.

Academic research

From the education side, Carnegie Mellon⁵'s Computer Emergency Response Team (CERT) offers a series of research materials on insider threat^{xxx} and analyzes in depth the characteristics of an effective security governance^{xxxi}. The Information Warfare Site has a list^{xxxii} of educational initiatives throughout the United States, with most major schools offering an orientation towards information security.

Government

⁴ For instance, Sophos (www.sophos.com) is a vendor of anti-virus and anti-spam software and has become well known through similar analyses and reports not necessarily strictly related to the products that the company is currently offering, but providing important information and thus creating a name for itself.

⁵ CMU was designated as a Center for Academic Excellence in Information Assurance Education by the National Security Agency

Finally, governmental organizations like NSA (National Security Agency) and NIST (National Institute of Standards and Technology) also address the issues of information assurance^{xxxiii} security management^{xxxiv}, and provide useful resources for the private sector. NIST is also supporting the Federal Information Security Management Act (FISMA), which is directed towards security measures^{xxxv} at federal agency level.

Current knowledge

As of present, there are many guidelines, standards and recommendations on what to do, from an IT perspective, to both keep all employees content and maintain the security of the company's data. It is interesting, however, to take a look at pieces of the recommended actions and identify their strengths and weaknesses, or try to give an answer to why they are not implemented.

Best practices and recommendations analysis^{xxxvi}

Policies

In regards strictly to the policies that employees acknowledge when they start work, core IT specialists agree that the information technology department of a company is not the owner, but the facilitator of

enforcement of these policies, in which quality it provides the technical controls for support. As the policy is enforced by human resources and top management, there needs to be a clear understanding of what is needed and the risks that this policy would address.

However, this is rather easier said than done, as most companies face a misunderstanding of the boundaries of the role of IT^{xxxvii}.

Limited trust

Another view is the opinion that the employees should be trusted only to the extent that the company is willing to take on a level of risk. In this regard, technology should restrict the access, be able to track down lost laptops, lock access when triggered to do so, and so on. In this situation, biometrics solutions would take care of limiting physical access and even technological.

The downside of this approach is that the employees would sense the limited level of trust, which in turn would typically lead to lower retention rates throughout the company. In addition, when an employee changes departments or leaves the company, the access is not always removed.

However, two of the less radical applications of this practice are relatively successful as preventive measures and strongly recommended throughout the industry: the principle

of least privilege and the separation of duties.

The *principle of least privilege* requires that a user be given no more than access than necessary to perform a job, thus limiting the damage that can be done by one individual^{xxxviii}.

The *separation of duties* has long been a common policy in the financial sector and is typically oriented towards preventing conflicts of interest and detecting control failures^{xxxix}. The separation of duties is necessarily determined by conditions external to the computer system^{xl} and in this quality it constitutes a fundamental principle of regulatory controls (SOX, GLBA).

Training

There seems to be a high stress on awareness and training. Most HR and IT professionals alike suggest that employees should be trained periodically on security issues even outside their daily routine, with examples on how to maintain security of their personal information first, then with regard to the company that employs them. In order for this to be functional, a feedback mechanism should be put in place so that users can both ask questions and report on misuse from colleagues, without revealing their identity if they so wish.

Intentional versus accidental information loss

Finally, there are studies that address the intentional rather than the

accidental misuse of accessible information technology^{xli}. In this case more so than in any other one, it is very important to create a culture of trust in the company^{xlii} and to observe any abnormal behaviors that could betray malevolent intentions.

Classic practices

A few common practices in the policies are highly recommended in various publications. However, the reason they are hard to implement or to follow is that they are not 100% proof. This is also the main rationale that lies at the basis of security being a hard issue when one is addressing the employee.

- *Password policy*: Most companies specify that passwords should not be shared with co-workers, some don't allow the same password to be used for different systems. In addition, password policies recommend creating a strong password and changing it often, at pre-determined time intervals. A too rigid password policy can create more problems than it solves: for instance, if the employee needs to have a different password for each system used, the likelihood that it will be forgotten increases with the level of complexity required for password validity. An easy solution is to write it down, although that is typically not accepted in the policy.

- *Single sign-on*: To address the issue mentioned above, some companies

implement a single sign-on solution, which provides the end user the flexibility of using only one password, to the repository system, then have access to all the systems that he uses. Among the benefits are: decreased amount of time used for the administrative tasks of logging on various systems, easiness in having to remember one password, and a perception of general simplicity. The drawback here lies in the idea of a single point of failure: if that one password is shared or written down and an unauthorized user obtains it, he can access all the systems that the rightful employee has access to, especially if the password chosen was weak^{xliii}.

- *Limited usability of features*: This refers to typical actions of blocking access to blacklist websites, not allowing the use of USB drives etc. However, most of these measures only address the "innocent" employee, as when a user's intent is towards stealing information, it is not impossible to find ways around these relatively simple measures.

- *Timely access*: The timely access is tied to the principle of least privilege discussed above. When the need for access to a new system is determined, the employee is granted access to this system by the department that is responsible for it. The drawback lies in the escalation system that is commonly in place for all internal

requests; usually, providing access is not a top priority, which in turn can lead to password sharing or other temporary fixes.

- *Employee exit procedures*: Typically, if an employee was terminated, the access is canceled faster than in the case of a leave by own consent. Even in this case, however, it is not unusual for a cumbersome exit process, where the request goes from department to department and, in effect, permits the internal systems to treat the former employee as still current for days or weeks after the employment ended.

- *Mobile device policies*: In companies with an intensive use of smart phones and laptops, it is important that action be taken in a timely fashion in the case of an employee termination or a stolen device. Improperly trained first contacts (a service center, for instance) can sometimes undermine the process by not attributing the correct priority to the request, which may lead to higher usage costs on the device itself, and also potential theft of proprietary information.

Writing security policies

One of the most common mistakes is to take a standard format of a security policy and implement it with only minimal impact analysis. The risk here is that the policy is either unsuitable for the specific company, or that the terms used are too hard to understand for the average user. Either case can

result in discarding the information and not taking into account the recommendations.

Monitoring compliance

Use of internal systems is typically monitored through logs, but difficult to analyze due to the very high volume of raw data from these systems. Best practices recommend paying attention to signals like heavy internet usage, for instance, to do a more in depth research on the employee.

Recommendation steps

In ensuring security of company information and clients' personal data, the company should *first* conduct a risk assessment, to identify the types of information that it contains and that, if lost or stolen, would create a negative impact of some scalable importance. The *second* step is to organize a technology roadmap to address the gaps in the information security determined through the risk assessment. Suitable technology solutions should be identified according to the roadmap, in the *third* step. Along with selecting the technology that will be put in place, the company should formulate written policies for the current and future employees, as well as determine and address the need for physical security within the company.

The *next* step is the actual implementation of both the IT measures and the security policies to the users of the company's information systems. Just as the software and hardware in place need to be checked periodically for full functionality, the employees should be trained towards first understanding and then following the policies within the work place, within the *fifth* step. Here should be created also measures to determine if and who is not respecting the company's principles with regard to security (logs, data volume examination etc.). *Finally*, enforcement deals with measures taken if the policies are violated. This should go gradually from minor admonition and retraining to the extreme measure of termination.

From the above-mentioned perspectives, the issues of *training and awareness*^{xliv} seem to stand out. From an employee perspective, if the only contact with policies happens on the first day at work – when typically a large number of different documents are quickly reviewed and signed –, then it is likely that the information about the security policy will be hard to remember. If, instead, the employee is provided with an easily accessible link towards a controlled document that describes in non-technical terms what the expectations are, and then is reminded periodically about the security practices through online training with quizzes or inter-

departmental reviews, then there is a much greater chance for those practices to be at least understood, if not respected. It is likely that a certain level of trust in the employee is still required – in which case the link between awareness and compliance is addressed.

Brief conclusion

As the internal use of technology is still growing, it is important for any company to make sure the correct safeguards are in place to allow it to comply with the legislation and to remain competitive by protecting its information. The technology, albeit extremely important, represents only a step in the greater security plan; a clear strategic view of information security throughout the company should set the stage both for the technology and for the employees. Thus, a well-written, understood and enforced security policy, together with a comprehensive set of controls, would greatly help towards ensuring that the company will remain viable. In addition, companies should increase the number of resources concentrated in training their employees towards a better understanding of the policies involving information security.

Sources cited

(with the date on which they were accessed mentioned in parentheses)

- ⁱ *** - "A chronology of data breaches", Privacy Rights Clearinghouse
<http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>
(November 18th, 2008)
- ⁱⁱ *** - "The World Factbook (United States)", CIA
<https://www.cia.gov/library/publications/the-world-factbook/print/us.html>
(December 1st, 2008)
- ⁱⁱⁱ *** - "Introduction to Information Security", CERT
http://www.us-cert.gov/reading_room/infosecuritybasics.pdf
(November 20th, 2008)
- ^{iv} Nash, Kim S. – "How text messaging and Facebook can get you in legal trouble", CIO magazine, October 29, 2008
<http://www.cio.com/article/457925/How-Text-Messaging-and-Facebook-Can-Get-You-in-Legal-Trouble>
(November 30th, 2008)
- ^v The Internet library of law and court decisions, <http://www.internetlibrary.com/>
- ^{vi} *** - "What is security analysis?"
<http://www.doc.ic.ac.uk/~ajs300m/security/CIA.htm>
(November 28th, 2008)

- ^{vii} *** - "The information security glossary"
http://www.yourwindow.to/information-security/gl_confidentialityintegrityandavailability.htm
(November 18th, 2008)
- ^{viii} *** - "IT examination handbook", Federal Financial Institutions Examination Council, July 2006
http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf
(November 17th, 2008)
- ^{ix} Grance, Tim; Hash, Joan; Stevens, Marc; O'Neal, Kristofor; Bartol, Nadya – "Guide to information technology security services – Recommendations of the National Institute of Standards and Technology", NIST special publication 800-35, October 2003, pg. 53-56
<http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf>
(December 2nd, 2008)
- ^x Grance, Tim et al., op. cit., pg. 43
- ^{xi} *** - "Top information security risks for 2008" (a collaborative project by the professional information security communities at CISSPforum and ISO27k implementers' forum), December 31, 2007
http://www.iso27001security.com/Top_information_security_risks_for_2008.pdf
(November 22nd, 2008)
- ^{xii} Gaudin, Sharon – "Top 10 enterprise security risks", eSecurity Planet (reproduced), July 11, 2002
<http://www.esecurityplanet.com/trends/article.php/1384081/Top-10-Enterprise-Security-Risks.htm>
(December 3rd, 2008)

xiii *** - "Interoperability ClearingHouse glossary of terms", ICH architecture resource center
<http://www.ichnet.org/glossary.htm>
(November 28th, 2008)

xiv Allen, Julia – "Governing for security: protect stakeholder interests", News at SEI (Software Engineering Institute), Carnegie Mellon University
http://www.sei.cmu.edu/news-at-sei/columns/security_matters/2005/4/security-matters-2005-4.htm
(November 14th, 2008)

xv *** - "Information privacy laws", Wikipedia
http://en.wikipedia.org/wiki/Information_Privacy_Laws
(November 15th, 2008)

xvi *** - "Security related ISO standards", ISO 27001 security
http://www.iso27001security.com/html/ot_hers.html#ISOstds
(November 14th, 2008)

xvii *** - "ISO 9000", Wikipedia
http://en.wikipedia.org/wiki/ISO_9001#Future_version:_2008
(November 20th, 2008)

xviii Gupta, Arun – "Is information security important to your enterprise?", CIOL, September 12, 2008
<http://www.ciol.com/Enterprise/Opinion/Is-information-security-important-to-your-enterprise/12908110299/0/>
(November 17th, 2008)

xix *** - "An introduction to ISO 27001, 27002 ... ISO 27008", The ISO 27000 Directory
<http://www.27000.org/>
(November 16th, 2008)

xx *** - ISO 27001 and 27002 Open Guide

http://iso-17799.safemode.org/index.php?page=Hints_and_Tips
(November 22nd, 2008)

xxi *** - "COBIT frequently asked questions", ISACA
http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/FAQ6/COBIT_FAQ.htm#27
(December 1st, 2008)

xxii Krebs, Brian – "OMB sets guidelines for federal employee laptop security", The Washington Post, June 27, 2006
<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/27/AR2006062700540.html>
(November 30th, 2008)

xxiii Epstein, Keith; Elgin, Ben – "Network security breach plague NASA", Business Week, November 20, 2008
http://www.businessweek.com/magazine/content/08_48/b4110072404167.htm
(November 21st, 2008)

xxiv Carey, Bill – "How to encourage employees to strengthen password security", eWeek, November 3, 2008
<http://www.eweek.com/c/a/Security/How-to-Encourage-Employees-to-Strengthen-Password-Security/>
(November 14th, 2008)

xxv Greenemeier, Larry – "How to spot insider-attack risks in the IT department", Information Week, December 11, 2006
<http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=196602853>
(November 29th, 2008)

xxvi Miliefsky, Gary S. – "The 7 best practices for network security in 2007", Network World, January 17, 2007
<http://www.networkworld.com/columnists/2007/011707miliefsky.html>
(December 1st, 2008)

^{xxvii} Daniel, Diann – “Human error tops the list of security threats”, CIO magazine, February 5, 2008

[\(December 2nd, 2008\)](http://www.cio.com/article/179802/Human>Error>Tops the List of Security Threats</p></div><div data-bbox=)

^{xxviii} *** - “eTrust SiteMinder single sign-on for PeopleSoft Solutions”, CA Whitepapers, February 2006

http://ca.com/files/WhitePapers/pplsft_wp.pdf

(November 17th, 2008)

^{xxix} *** - “Effective email policies: Why enforcing proper use is critical to security”, Sophos, April 2008

<http://i.i.com.com/cnwk.1d/html/itp/sophos-email-acceptable-use-policies-wpna.pdf>

(November 21st, 2008)

^{xxx} Insider threat research, CERT

http://www.cert.org/insider_threat/

(November 25th and 26th, 2008)

^{xxxi} Allen, Julia H.; Westby, Jody R. – “Governing for Enterprise Security (GES) implementation guide – Article 1: Characteristics of effective security governance”, CERT, February 2007

http://www.cert.org/archive/pdf/GES_IG_1_0702.pdf

(November 30th, 2008)

^{xxxii} IWS, The Information Warfare Site
<http://www.iwar.org.uk/directory/information-security/academia.htm>

(December 1st, 2008)

^{xxxiii} Information Assurance Research, National Security Agency – Central Security Service

<http://www.nsa.gov/niarl/index.cfm>

(November 28th, 2008)

^{xxxiv} *** - “Security management and assistance”, NIST

<http://csrc.nist.gov/groups/SMA/index.html>

(November 27th, 2008)

^{xxxv} *** - “FISMA – detailed overview”, NIST

<http://csrc.nist.gov/groups/SMA/fisma/overview.html#background>

(November 27th, 2008)

^{xxxvi} LinkedIn answers, with thanks to: Tarun Gupta; Josh Chernin; Donna Hogan, CISSP, PMC; Ed Wawrzaszek; Steven Podvoll; Rick Lawthorn, CISA, CISSP;

<http://www.linkedin.com/answers/technology/information-technology/information-security/TCH ITS ISC/355943-16709142?browseIdx=0&sik=1228150126510&goback=%2Eamq>

(November 22nd, 2008)

^{xxxvii} McKeen, James D.; Smith, Heather A. – “IT strategy in action”, Pearson – Prentice Hall, 2008, pg. 37-50 (Chapter 4 – Managing perceptions of IT)

^{xxxviii} *** - “The principle of least privilege”, IT Business Edge, January 12, 2007

<http://www.itbusinessedge.com/item/?ci=23379>

(December 3rd, 2008)

^{xxxix} Coleman, Kevin – “The key to data security: Separation of duties”, Computerworld, August 27, 2008

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113647>

(November 29th, 2008)

^{xl} *** - “Separation of duties”, NIST

<http://hissa.nist.gov/rbac/paper/node6.html>

(November 22nd, 2008)

^{xli} *** - “Insider threat study: Illicit cyber activity in the Government sector”, US Department of Homeland Security / US Secret Service; and CERT at Carnegie Mellon University, January 2008

http://www.cert.org/archive/pdf/insiderthreat_gov_execsummary2008.pdf

(November 17, 2008)

^{xlii} Slay, Jill; Quirchmayr, Gerald – “A formal model for the relationship between culture and trust within IS security”, University of South Australia
<http://scissec.scis.ecu.edu.au/publications/aism2004/Slay-Quirchmayr.pdf>
(December 1st, 2008)

^{xliii} Ellison, Gary; Hodges, Jeff; Landau, Susan – Sun Research, October 18, 2002
<http://research.sun.com/liberty/RPSSOA/index.html>
(November 28th, 2008)

^{xliv} *** - “18 best practices in security awareness training”, Information Security Resource Center, Oregon
<http://www.oregon.gov/DAS/EISPD/ISRC/bestpractices.shtml>
(December 3rd, 2008)