Challenges in Implementing Information Security Policies

A. Reichard[1], G. Quirchmayr[1, 2] and C.C. Wills[3]

[1]University of Vienna, Faculty of Computer Science, Multimedia Information Systems Research Group, Liebiggasse 4/4-6, A-1010 Vienna
[2]University of South Australia Division of Information Technology, Engineering and the Environment, School of Computer and Information Science, Mawson Lakes, SA 5095, Australia
[3]Kingston University, Faculty of Computing Information Systems and Mathematics, Penrhyn Road, Kingston Upon Thames, KT1 2EE
e-mail: Andreas.Reichard@gmx.net, Gerald.Quirchmayr@univie.ac.at, Gerald.Quirchmayr@unisa.edu.au, ccwills@kingston.ac.uk

Abstract

The goal of the research described in this paper is to identify challenges related to the successful implementation of information security policies and to develop an approach for overcoming them. Based on an analysis of the literature and the results of interviews with domain experts in the telecommunications industry, a framework for addressing the identified challenges is introduced.

Keywords

Information security policy, information security policy implementation, information security management, implementation framework.

1. Introduction

Every kind of information carries a specific value. The exact amount of that value depends on factors such as its content, confidentiality, and owner. In some cases, especially in business environments, this amount can be expressed as a monetary value; in other cases this is not possible. Consequently, the uncertainty about possible consequences of sensitive information getting into the wrong hands has led to the extensive planning of methods to prevent this from happening. Dealing adequately with information – not only highly sensitive information, but information in general, in a way that does not constrain business processes unnecessarily, while still protecting the information (which is a valuable asset), from illicit access, clearly falls into the field of information security.

In a recent case in January 2011, Vodafone Australia had to admit a breach of privacy in a supposedly 'secure web portal'. An unknown number of customer data records were publicly accessible through the web as a consequence of the mishandling of sensitive information by a dealer or an employee, (see the website of the Australian Information Commissioner, 12 January 2011).

Recognizing the danger of such an information exposure, many businesses have invested considerable time and effort into the creation of an information security programme. The creation of such a programme, as described by Desman (2002) is a complex task in its own right, worthy of recognition. The effort devoted to such a programme, however, does not guarantee the efficacy of its implementation, i.e. the crucial issue of whether staff affected by it will also comply with it and, if they do, to what extent. That is "… because controls affect system users, the (security) plan should incorporate user's views, especially with regard to usability and the general desirability of controls" (Pfleeger and Pfleeger 2003, p.499).

Investing a substantial effort in the design of an information security programme without sufficiently acknowledging how co-workers will be affected, will be likely to lead to a significant gap between the conception and the application of such a programme. In a worst case scenario, this may even render the entire information security programme useless, if staff do not recognize an overall benefit of compliance with the programme for their own work, or for the organisation as a whole. On the contrary, if staffs see little or no benefit in compliance, accomplishing day-to-day tasks in the most efficient and time saving manner will receive a much higher priority than that of information security. This usually results in information security measures being ignored, avoided and circumvented. What is required to prevent this from happening is "… a procedural and technical information security infrastructure, as well as a corporate information security culture that support the information security policies, procedures, methods and responsibilities of the organisation, in such a way that information security becomes a natural aspect of the day to day activities of all employees of the organisation, and endures long after those who originally created these infrastructures, have gone" (Von Solms 2000, p.616).

Our paper recognizes, and also partially assumes, that there is a substantial difference between the design and the implementation of an information security programme. It is this difference, which is responsible for the existence of a possible gap between the conception and application of an information security programme. The question this paper seeks to answer is how the gap between conception and application can be reduced, and at its core, how information security can be communicated to employees and management alike, in a way to make them recognize the overall value of information security – both for their own workplace and, more generally, for the organisation for whom they are working. Staff compliance with an information security programme can only be achieved and the system will only work as intended through the staff buying into the idea of information security, being aware and committed to taking ownership of its importance.

Although the successful implementation of an information security programme is closely related to its design and creation, this paper is not focused on the design of such a programme per se, but rather offers an additional insight into aspects of the design of an information security programme. This paper's central topic then, is how to overcome any obstacles that are met during the implementation phase that reduce the efficacy of the application of the information security programme. Overcoming

such obstacles will increase the acceptance of an information security programme on the part of those staff affected by it, because it is seen as necessary to protect information as a common asset.

2. Recognizing the increasing value of information

Every organisation has information assets that have a specific value. The loss of these assets represents a loss of value to the organisation that owns them. This loss becomes even greater if these assets are connected to the organisation in some specialized way. By that definition, an organisation's information is specialized in many ways. Different kinds of information can have different values for different individuals. For every kind of information there is someone for whom this information has value. This is true even for seemingly unlikely cases. As a consequence, every kind of information should be protected against unauthorised access and its possible consequential exploitation for unlawful purposes. Incidents such as that of Vodafone Australia in January 2011, show that companies are still having trouble establishing robust and dependable protective measures. The loss of value to companies in such a case, can be expressed in relation to the number of clients who lose their confidence in that organisation's ability to keep their sensitive information secure.

Seemingly harmless information in the hands of a person who knows how to use it can still cause great damage to an organisation. Some 'social engineers' are able to use linguistic and psychological methods to extract information from unsuspecting employees. This information can later be put to use to damage a targeted organisation. Dorothy E. Denning offers the following definition of this practice: "Social Engineering refers to operations that trick others into doing something they would not do if they knew the truth, for example, giving out a secret password or sensitive corporate information. Any medium that provides one-to-one communications (sic) between people can be exploited, including face-to-face, telephone, and electronic mail" (Denning 1999, p.111). Typical contexts in which these methods are being used are corporate espionage, blackmail and privately motivated enrichment, e.g. via identity theft.

Identity theft is one of the most widespread examples of stolen information. Many people have created a number of virtual identities for themselves through the spread of online communities, e-commerce etc. The reason for the existence of such virtual identities, from the perspective of an institution (e.g. an e-commerce organisation), is to have a representation of the identity's owner with whom it can communicate and do business with. This means that in the eyes of such an institution, this identity *is* effectively the owner. Anything that is done via the use of this virtual identity is traced back to its owner and is deemed to have happened with his/her knowledge and compliance.

The growth rate of e-commerce over the Internet has proven that the concept and growing use of virtual identities has helped to open markets throughout the world, enabling companies and costumers to gain access to each other and do business.

Unfortunately, this concept has also introduced a set of problems, a crucial one of them being the illegal use of a virtual identity by a third party who is not the original owner of that identity. This is 'identity theft' and represents a problem insofar as, from the point of view of the institution handing out these identities, any action committed through the use of a virtual identity is seen as having been committed by the person to whom this identity is registered. Obtaining such a virtual identity by illegal means and using it for criminal activities is therefore one way to frame the original owner of the virtual identity for actions that they person did not commit and obscure the identity of the real perpetrator.

The theft of a virtual identity is one of the scourges caused as a consequence of the expansion of Internet access throughout the world. This problem, however, is not solely Internet-based. There are numerous situations in which individuals present their identities to others in order to gain access to restricted information (bank account numbers, pin numbers etc.). In every one of these situations, opportunities exist for identity theft from a person or institution that enable the thief to pose as the true and original owner of that identity

3. The Role of Information Security Policies

The value assigned to a specific piece of information may be the result of a subjective decision made by one individual. Based on that decision, the information will be regarded as having a particular level of confidentiality in the opinion of this individual. As such a subjective decision will vary from person to person, so too does the level of confidentiality ascribed to that piece of information. In an environment where information security is taken seriously, such a large margin of variation is not acceptable.

Information security policies need to be designed in such a way so as to deal with these kinds of challenges. Their objective, as put by Mark B. Desman, is "… to present a picture as to how the organisation views its information assets, what each employee's responsibility is with regards to protecting those assets and how to go about doing so" (Desman 2002, p.47). They "… define the security philosophy and posture the organization takes, and are the basis for all subsequent security decisions and implementations" (Whitman 2003, p.92).

It is essential not to overlook the impact that information security measures have on the staff affected by them. Establishing and maintaining a good relationship with staff, being aware of concerns expressed by them and respecting different viewpoints on the value of information security is therefore imperative. Only then can an implementation of an information security policy have a reasonable chance of success. Ignoring this requirement can result in theoretically well-designed information security policy not being effectively applied as a consequence of staff apathy.

This fact is often overlooked, as technology solutions are presented to deal with human-based challenges, which need to be addressed first and accordingly, as stated by Whitman (2003, p.93).

Additionally, an implementation of an information security policy needs to take heed of the following highly relevant issues:

Responsibilities concerning information security policies must be clearly defined within an organisation and its roles (as stated by Piper 1994, p.7/1). These responsibilities include the establishment of information security policies, management, maintenance, review and updates, enforcement, adherence in cases of policy violations and criminal prosecution where necessary. Documentation must also detail what life-cycle policies exist before information security policies have to be reviewed, updated or superceded by a newer policy.

The scope of information security policies depends upon the size of the organisation, the environment in which it operates and its business or organisational connections. Information security policies directed at only one organisation on its own are not sufficient if that organisation has partners who do not share an agreed view on information security. Since these partners often have access to sensitive information which is protected by the information security policy of the organisation, their handling of this information may be in violation of the information security policy of a partner organisation. This essentially renders the information security policy useless. At this point information security has not been addressed by the information security policy, it has only been outsourced to a business partner who now represents a potential information and security risk. It is therefore imperative that guidelines for the treatment of information within organisational partnerships are established in compliance with the relevant information security policies. Moreover, differences between national and international organisational partnerships need to be taken into account, because of different regulations that may exist in different countries.

Incident Management: A functioning chain of reactions must operate in situations where information security incidents occur. This must necessarily include the classification of the incident and proper response and reporting. The response to an information security incident depends on the classification it receives. These classifications, as well as established response actions and other details, must therefore exist as an integral part of any information security policies.

Policy Life Cycle: A vital part of an information security policy's life cycle is that of regular review and update. This implies that the responsibility of keeping up to date with new threats to information security, recent information security incidents and new vendor offerings to counter these threats must be clearly defined. A good overview over these matters as well as the organisation's resources is necessary to develop a realistic understanding of what may yet become a threat to the organisation and how it can be dealt with.

4. Challenges in Implementing Information Security Policies

Implementing information security policies includes many measures that have to be taken, but also requires that staff affected by these measures will accept changes that will make their work life more complicated than would otherwise be the case.

The importance of this fact is also underlined by Thomson and Von Solms (1993, p.168), if one is to achieve a lasting change in attitude towards information security.

Lack of interest is one of the greatest challenges in the implementation of an information security policy. The average member of staff is usually less interested in information security matters than in getting his or her work done as quickly as possible. This is especially so during times of stress, when security measures are usually one of the first things to be ignored in order to speed up a process. When confronted with such measures, particularly with the trade-off between security vs. availability of services, staff often experience a feeling of hostility against these measures and those responsible for their implementation. Any attempt to implement information security policies under such adverse circumstances is sure to fail.

In order for such an implementation to succeed, allies in other departments are needed to ensure staffs cooperation to the extent required. This can only happen if everyone understands the reasons for the implementation of such a policy. In order to win the users as allies, one must understand their viewpoints when it comes to information security.

User awareness is therefore key in the process of implementing information security policies. However, simply being aware of the dangers that these policies are trying to protect users from may not be enough. Ideally, they must be brought to a point of awareness where they willingly act as eyes and ears of the information security department throughout the entire organisation. This is the only way that such a department within a large organisation will be able to handle the enormous task that information security represents, if users can be brought to carry out their daily activities in a security supporting manner (as described by Thomson and Von Solms 1993, p.168). This is especially difficult in the face of concerns about the possible invasion of privacy consequent upon the application of security measures.

When everyone knows what is at stake and understands the potential consequences of a failure in information security, the adherence of users to the policies increases. Members of the information security department are no longer seen as disablers, but as enablers of a more secure work environment for all employees. They become simply one more part of the organisation, doing its part for the success of the organisation rather than merely making other people's lives harder than is necessary.

Allies and budget: The effective implementation of information security policies normally requires a generous budget. In practice, the budget for information security is always tight, as many managers still tend not to see information security as a key factor in a business' success. Since maintaining information security policies is an

ongoing and evolving process, further investment is always required, but this subject is often viciously fought over during budget meetings. One challenge is therefore to convince management of why information security must be a top priority within the organisation and obtaining management's public support, top-down, for every employee to see. One way to do so is through the help of allies and so-called 'hidden opinion leaders', supporting one's position and arguments in this matter when they are presented to management. This paper uses the term 'hidden opinion leaders' to denote staffs that have significant influence on the decisions made by management. These members of staff, through extensive know-how and competence in their field, have a level of expertise that has made them management's choice when it comes to obtaining reliable opinions on something that falls into their field of work and deciding whether further budget is to be granted. Winning them as allies and getting their support is therefore crucial to inform decisions taken over budget issues.

Proactive approach: As has already been suggested, information security is by definition an ongoing process. As such, it requires constant attention and maintenance and such efforts must always endeavour to stay ahead of the dangers an organisation needs to be shielded from. If this goal is to be achieved, information security processes must try to follow a proactive instead of a reactive approach. Since not every scenario can be anticipated, this is something that cannot be guaranteed, yet best efforts as well as proper training are required to raise and maintain the necessary level of awareness among all employees of an organisation.

Finally, regular audits and penetration tests should also be performed in order to evaluate the efficiency of current information security and its compliance with legislative and contractual commitments.

5. Suggested Approach

When approaching the challenges faced in the implementation of information security policies, one has to start by familiarizing oneself with the organisation requiring information security. This includes corporate design and structure, management style etc., all of which form part of a series of phases that will be explained using the following process model:

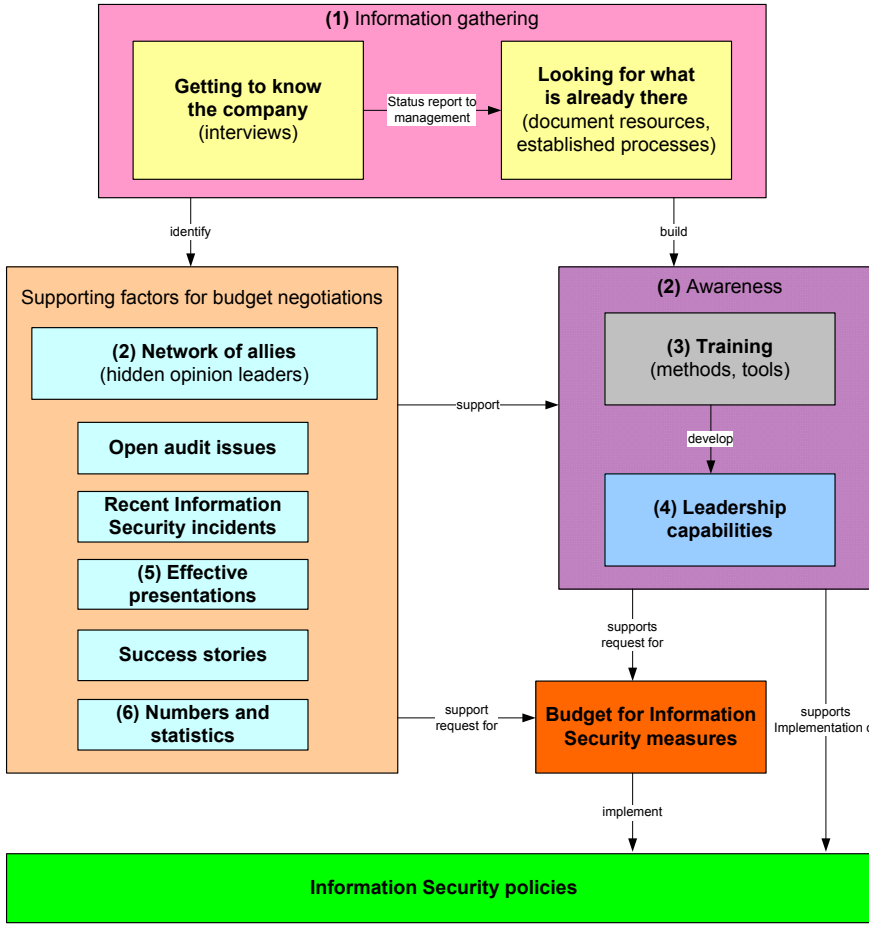

Figure 1: Process model for implementing information security policies

The proposed phases are as follows:

(1) The first phase is that of information gathering. An audit needs to be conducted in order to form an overview of the organisation's current information security provision. Besides conducting interviews, all documentation materials, policies, guidelines and information about currently applied information security tools and procedures need to be scrutinised and reviewed for their reusability. Additionally, staff responsible for these materials need to be identified, as they may become valuable allies. Of equal value, is any information about unfinished or abandoned information security projects and the reasons for their abandonment. In many cases, such abandoned projects are founded on a perfectly adequate idea and were cancelled only for budgetary reasons. Knowing this and talking to staff responsible for these projects can make the process of information security policy implementation that much easier, as problems that the staff have encountered in the past are recognized

and can be avoided in the future. Old audit documentation can also give valuable insight into what went wrong in the past in terms of information security and what the consequences were. At the end of this phase, one should have an overview of the existing materials and documentation and know what can be of use. Everything else should simply be discarded.

(2) The next phase is the search for allies within other departments, especially user management and user support, Human Resources, Public Relations, Corporate Security, Legal and Documentation. These departments' areas of expertise are of great value during the process of implementation of information security policies. Keeping a good relationship with them is therefore imperative. Beyond these departments and the fact that one goal of information security policies is to have each and every member of staff acting as the organisation's eyes and ears regarding information security, other important allies include 'hidden opinion leaders' (as mentioned before) and auditors. If treated as allies, auditors are likely to respond as such and assist one in the common struggle of improving an organisation's information security. By making them allies, one can place ideas directly in front of management by letting the auditors present them. An auditor's report goes directly to management; it states what has to be done to improve the organisation's current situation. If one's ideas find their way into these reports, they will more likely get approved by management, along with the necessary budget.

Also during this phase, one needs to identify the ways in which information spreads within the organisation, i.e. established communication channels, and who controls them, and make these people allies as well (if they are not already). These channels can then be used to spread information security content, raise knowledge and interest in information security and, along with combined training, raise the awareness of its audience.

(3) Besides awareness, another major factor in building and maintaining the necessary level of employee awareness is proper training.

"Whilst training, awareness and practice are arguably associated with each other, simply undertaking training or having an awareness of an issue does not necessarily imply practice" (Shuhaili *et al.* 2010, p.196).

This requires state-of-the-art training methods and tools as well as frequent repetition and attendance control. A specialized training is presented to new employees, starting with orientation day. If the necessary resources for this are not to be found within an organisation, this task can be outsourced to companies specialized in this area.

(4) It is not enough for members of staff to simply know that there is *someone* within the organisation who is responsible for information security. This person/department has to be known or, even better, respected for his/her/its work and the ability to make a positive contribution to the organisation's operations by making them more secure. Essential in achieving this is the development of networking and leadership skills

that support one's efforts to implement information security policies (as described in Whitman and Mattord 2007, p.107).

(5) Every effort undertaken for the implementation of information security policies requires budget. Getting the budget can be seen as a sales process with information security presented as ideas and goods, where management is viewed as the prospective buyers. The best way to close such a deal is through getting the necessary support from allies and 'hidden opinion leaders' whose influence can make a substantial difference in getting essential budget approved. Beyond that support, the ideas that are to be sold must be presented in a way that leaves no doubt about why an approval of the necessary budget is needed. The key to this are simple messages with an easily recognizable, bottom-line conclusion. This should be repeated throughout the presentation as well as in the summary documents sent out to management and involved departments after the presentation.

(6) Inevitably, management will want to evaluate the effort expended in implementing information security policies. This often presents a dilemma, as the success of all security measures is reflected by the absence of security incidents. In other words, if nothing has happened, this most likely means that the security policies were successfully implemented and are working as intended. By itself, however, that will not get the next budget approved; what is needed instead are data, hard facts, numbers and statistics that can be reviewed by management which justify the introduction of the information security policies and prove the success and return on investment of their implementation.

"Successes create credibility and credibility reassures management that you are going about it the right way" (Desman 2002, p.184).

6. Outlook and Conclusion

The implementation of information security policies is not a simple task. During the process of implementation, one might even reach the surprising conclusion that the greatest challenges faced in information security have nothing to do with malicious persons or criminals intending to steal an organisation's valuable information assets, but with the very people whose information assets one is trying to protect through security measures. An adversarial approach, however, in which one tries to force information security onto employees, is sure to fail. Indeed, success in the implementation and efficiency of the information security policies and their application can only come through working together, with an organisation's employees and within an organisation's culture, not against them. This is also pointed out in Karyda *et al.* (2006, p.405).

This realization has its value, yet good will alone will not suffice, as the relationship between information security professionals and other members of staff is often tense. This stems from an unfortunate, but inevitable downside of information security: As a result of optimizing work processes in terms of information security, these processes become more complex than they were before. A natural and up to a point,

even understandable reaction to this fact is therefore that employees resist information security measures. Such resistance needs to be overcome, as the most significant asset in one's arsenal for protecting an organisation's information assets is the awareness of those very employees – awareness of the value of information, the threats that they face while handling information assets, and the need for information security, with all the implications this has for an organisation's business.

As if this were not enough of a challenge already, working in a field where success is defined through the absence of incidents, an information security department constantly needs to justify its existence in the eyes of management. Securing the budget to build and maintain an ongoing information security programme, devising policies and conducting their implementation is another substantial challenge faced by the information security department of any organisation.

Both of these challenges can only be overcome by accepting that the implementation of information security policies is, in fact, a sales situation in which one needs to sell the principles and benefits of information security and associated measures to the members of an organisation. This is in order to encourage both, users and management to adhere to the measures included in the policies. This requires not only in-depth knowledge about the organisation in question, but also its members, management and culture. However, persuasive strategies can only work with the help of allies throughout the organisation. Such allies are thus necessary for their support of the principles of information security as a continuous process and to establish the necessity for information security policies within an organisation.

While technology-based challenges for information security become more advanced as time passes, so too do the technical means to counter these challenges. The implementation of information security policies, however, remains a challenge that is and will remain primarily a people matter that requires corresponding approaches to solve it. Bruce Schneier, in his book 'Secrets and Lies', stated that "It's clear to me that computer security is not a problem that technology can solve. Security solutions have a technological component, but security is fundamentally a people problem" (Schneier 2000, p.xii). Although this quote refers more generally to Computer Security, its conclusions can be extended to Information Security as well. While this paper's goal was to present such an approach, it must be acknowledged that such approaches may be as diverse as people's attitudes towards information security, making the further study of viable approaches for the implementation of information security policies a subject of continuing interest.

7. References

Anderson, R. (2001), "Security Engineering – A Guide to Building Dependable Distributed Systems", John Wiley & Sons, Indianapolis, ISBN: 0-471-38922-6

Bishop, M. (2005), "Computer Security: Art and Science", Pearson Addison Wesley, Upper Saddle River, ISBN: 0-201-44099-7

Denning, D.E. (1999), "Information Warfare and Security", Pearson Addison Wesley, Upper Saddle River, ISBN: 0-201-43303-6

Desman, M.B. (2002): "Building an Information Security Awareness Programme", CRC Press LLC, Boca Raton, ISBN: 0-8493-0116-5

Furnell, S.M., Gennatou, M., Dowland, P.S. (2002), "A prototype tool for information security awareness and training", *Journal of Enterprise Information Management*, Emerald Group Publishing Limited, Bingley

Gupta, M. and Sharman, R., G. (2009), "Handbook of Research on Social and Organizational Liabilities in Information Security", Information Science Reference (an imprint of IGI Global), ISBN: 978-1-60566-132-2 (hardcover) – ISBN: 978-1-60566-133-9 (ebook)

International Standard Organisation, "ISO/IEC 27001:2005", http://www.27001-online.com/iso-27001.htm

Karyda, M., Mitrou, E. and Quirchmayr, G. (2006), "A framework for outsourcing IS/IT security services", *Journal of Information Management & Computer Security*, Emerald Group Publishing Limited, Bingley

Kurose, J.F. and Ross, K.W. (2003), "Computer Networking – A Top-Down Approach Featuring the Internet", Pearson Addison Wesley, Upper Saddle River, ISBN: 0-201-97699-4

McClure, S., Scambray, J. and Kurtz, G. (2005): "Hacking Exposed 5th Edition", Mcgraw-Hill Professional, Emeryville, ISBN: 0-07-226081-5

Mitnick, K.D. (2002), "The Art of Deception – Controlling the Human Element of Security", John Wiley & Sons, Indianapolis, ISBN: 0-471-23712-4

Mitnick, K.D. (2006), "The Art of Intrusion – The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers", John Wiley & Sons, Indianapolis, ISBN: 0-7645-6959-7

Office of the Australian Information Commissioner (2011), "Australian Privacy Commissioner to investigate Vodafone allegations", http://www.oaic.gov.au/news/media_release_vodafone.html, (Accessed 12 January 2011)

Pfleeger, C. P. and Pfleeger S. L. (2003), "Security in Computing 3rd Edition/International Edition", Pearson Addison Wesley, Upper Saddle River, ISBN: 0-13-120199-9

Piper, F. (1994), "The Management of Security", IEE Colloquium on Security and Cryptography Applications to Radio Systems, London

Schneier, B. (2000), "Secrets and Lies – Digital Security in a Networked World", John Wiley & Sons, Indianapolis, ISBN: 0-471-45380-3

Siponen, M.T. (1993), "A conceptual foundation for organizational information security awareness", *Journal of Information Management & Computer Security*, Emerald Group Publishing Limited, Bingley

Skoudis, E. and Liston T. (2006): "Counter Hack reloaded", Prentice Hall, Upper Saddle River, ISBN: 0-13-148104-5

Talib, S., Clarke, N.L. and Furnell, S.M. (2010), "An Analysis of Information Security Awareness within Home and Work Environments", *In the proceedings of 2010 International Conference on Availability, Reliability and Security*

Tsohou, A., Kokolakis, S., Karyda, M. and Klountouzis, E. (2008), "Investigating Information Security Awareness: Research and Practice Gaps", *Information Security Journal: A Global Perspective*, Vol. 17, Issue 5-6

Von Solms, B. (2000), "Information Security – The Third Wave?", *Computers and Security Volume 19*, No. 7, Elsevier Science Limited, Elsevier Amsterdam

Whitman, M.E. (2003), "Enemy at the Gate: Threats to Information Security", Communications of the ACM , Volume 46 Issue 8, August 2003.

Whitman, M.E. and Mattord, H.J. (2008): "Management of Information Security 2nd Edition", Course Technology, Florence, ISBN: 13: 978-1-4239-0130-3 and 10: 1-4239-0130-4