

SUCCESS FACTORS IN INFORMATION SECURITY IMPLEMENTATION IN ORGANIZATIONS

Maryam Al-Awadi

University of Glasgow

Computing Science, 17 Lilybank Gardens, Glasgow G12 8RZ

mawadi@dcs.gla.ac.uk

Karen Renaud

University of Glasgow

Computing Science, 17 Lilybank Gardens, Glasgow G12 8RZ

Karen@dcs.gla.ac.uk

ABSTRACT

This paper will explore and identify success factors related to the implementation of information security in organizations. It will explore these factors from the expert's perspective. Qualitative analysis of the organizations' employees' experiences will be analysed and discussed. The purpose of this research was to identify those factors required to ensure successful implementation of information security, particularly in government organizations. This study revealed many experiences and insights which will have widespread applicability.

KEYWORDS

Information security, Success factors, Security management, Awareness.

1. INTRODUCTION

Information is an asset, and having specific, relevant and correct information can make a massive difference to an organization's efficiency. With the huge number of available technologies; it is possible for information to be collected, shared, sold, exchanged and distributed without citation or notice to the owner (Varney, 1996). It is necessary to ensure information security so that it becomes a natural phase in the daily activities of an organization. Organizations must define the threats and vulnerabilities to their information resources to ensure the confidentiality, integrity and availability thereof (Gollmann, 1999; Pfleeger, 1997; Sebastiaan et al., 2003).

"Information security relates to an array of actions designed to protect information and information systems" (Gordon & Loeb, 2006, p.121). However, information security does not cover only the information itself but also the entire infrastructure that facilitates its use. It covers hardware, software, threats, physical security and human factors, where each of these components has its own characteristics. Consequently information security plays a major role in the internet age of technology. Given that the number of organization security breaches is increasing daily, and the more accessible the information, the greater the hazards, it is inevitable that security will need to be tightened (Brown & Duguid, 2000).

As the number of employees, applications and systems increase, the management of the organization's information becomes much more difficult and consequently vulnerabilities potentially increase. To determine secure use of hardware and software as well as facilitating and encouraging secure employee behaviour, organizations make use of information security *policies*. An information security policy is a combination of principles, regulations, methodologies, techniques and tools (Tryfonas et al., 2001) established to protect the organization from threats. These policies also help organizations to identify its information assets and define the corporate attitude to these information assets (Canavan, 2003).

Von Solms (1999); Canavan (2003); and Doherty & Fulford (2005) all agree that established standards, such as the international standard ISO 17799, are a good starting point for shaping the information security policy to improve information security in an organization. ISO 17799 presents some guidelines related to successful implementation of information security, and is mainly aimed at senior management to help them make decisions and then pass the essential actions to those in management positions. ISO 17799 deals with:

- security policy, objectives and activities that properly reflect business objectives,
- clear management commitment and support,
- proper distribution and guidance on security policy to all employees and contractors,
- effective 'marketing' of security to employees (including managers),
- provision of adequate education and training,
- a sound understanding of security risk analysis, risk management and security requirements,
- an approach to security implementation which is consistent with the organization's own culture,
- a balanced and comprehensive measurement system to evaluate performance of information security management and feedback suggestions for improvement.

Siponen (2001) disapproves of ISO 17799 from the perspective of philosophy of science and disagrees that these standards are scientifically justified since they are based on personal observation and are not universally valid. However, Von Solms (1999) concludes that ISO 17799 "can certainly provide the basis to ensure safe driving on the information super highway". Indeed the organization does not need to start from scratch to address information security in their organization; using ISO 17799 will help them to develop an overall picture of security in order to ensure overall security of information assets.

There has been little empirical investigation of the factors that make information secure in an organization. Nevertheless, a policy alone cannot make an organization safe or reduce threats without some external factors that must be in place to direct the successful maintenance of the information security policy. The aim of this paper is to report upon the results of an exploratory empirical study to pinpoint the critical success factors that play a vital role in ensuring that an information security policy leads to enhanced information security in an organization.

2. LITERATURE REVIEW

Von Solms (1996) explains that information security has evolved through three stages: the first stage began in the 1960's when information security's major concern was to ensure and control physical security of the facilities; eg. that printouts were circulated in a protected ways. The second stage started in the mid-1970s when information security was tailored to the specific needs of individual organizations, despite the fact that the scope of information security had extended radically. In the third stage, with the advent of advanced technology, organizations needed to link their IT services together and move from a closed environment to complex environments that work in distributed and connected networks of machines.

What makes information security very important nowadays in organizations is the type of environment people work in. Organizations depend more and more on computers and computing control has been brought down to the individual desktop. More employees are interacting with technology to undertake their daily tasks, and employees constitute a greater threat (Madigan, et al. 2004) because they have direct access to an organization's assets.

Lampson (2002) argues that organization's systems still remain vulnerable to attack after thirty years of accumulated work on security. The reason is probably that security setup is costly and difficult to sustain. There is a perception amongst employees that security *gets in the way* and that it interferes with employees' ability to accomplish tasks (Sandhu, 2003).

Straub and Welke sum up the situation as follows: "Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary" (Straub & Welke, 1998, p. 441). In order for organizations to achieve a stronger protection of their information the recognition of the main threats facing organizational information is urgently required (Whitman, 2003).

Threats are "circumstances that have the potential to cause loss or harm" (Pfleeger, 1997, p.3) to information and can be classified as *external* and *internal* (Hinde, 2002). Many publications and surveys such

as (Whitman, 2003; Ernst & Young, 2004; Doherty & Fulford, 2005; and DTI, 2006) quantify the sources and consequences of threats to information faced by organizations. The following threats have been identified by these surveys:

- **External threats:** computer viruses; natural disaster; spam emails and hacking incidents.
- **Internal threats:** installation or use of unauthorized hardware, peripherals; abuse of computer access controls; physical theft of hardware or software; human mistake; damage by displeased employee; use of organization resources for illegal communications or activities (porn surfing, email harassment) and installation or use of unauthorized software.

Information security has been regularly considered to be a technological problem with a technological solution. That is simply untrue because information security is about managing risk (Whitman, et al. 2005) and managing risk is about discovering and measuring threats to information assets (Lampson, 2002; and Garbars, 2002) in the organization and taking actions to respond to those threats. When organizations fail to manage their information security, the organization's integrity will be compromised and loss of money could occur. The UK's biggest building society Nationwide was given almost one million pounds fine after a lost laptop with customer details was stolen from an employee's home (BBC, 2007). The inescapable conclusion is that *information security is people* and is actually more of a managerial problem than a technical problem. It therefore cannot be purely dealt with by technically. There is a need to highlight effective approaches and strategies that might help organizations to achieve good information security.

3. RESEARCH DESIGN METHODOLOGY

Our research is aimed at governmental organizations' implementation of information security. The study is exploratory using a semi-structured qualitative method for collecting data and grounded theory to analyze the data. The data has been categorized by identification of patterns or themes and organized to derive meaning. This study is based in the sultanate of Oman because of the relative infancy of information security in Oman.

Currently there are approximately 52 governmental organizations in Oman. The selected samples for the semi-structured interviews were a mixture representing a cross-section of ten IT & information security experts. Almost an hour was allowed for the IT & information security experts. Experts selected for the interviews represented a cross-section of the population of different government organizations. All experts are at a senior level of information technology or information security in their organization with more than five years' experience in the field of information technology and all of them have a generally high level of education (graduate level and above).

A semi-structured interview questionnaire was developed for the experts. The questions were of an open-ended type to encourage respondents to explore their own experiences, perceived success factors and measures undertaken to secure information. The reality as perceived by the respondents had to be described in terms of the meaning respondents attach to the elements of the field of study they were questioned about. The data needed multiple sources of their knowledge, including insight into their values, experiences, cultures and the ways they interpret and understand these. The small selective sample is related to the in-depth nature of the qualitative approach (Carr, 1994).

The questions posed during the semi-structured interviews were validated through the approval of the method by experienced people in the field of social science research, and an information security expert.

The interview was arranged and conducted with all of the participants at the convenience of the interviewee and took place in the interviewees' offices. Confidentiality of the data was guaranteed. All participants requested that anonymity also be guaranteed.

4. RESEARCH FINDINGS AND DISCUSSION

The qualitative responses reported in this paper are supported by verbatim quotes from the interviews. The views collected from the overview interviews of IT & security expert employees have been used in the discussions of the related responses.

Different success factors were derived from the findings. These success factors are presented below, in decreasing order of frequency.

4.1 Awareness and Training

The interviews show that organizations all wished to secure their information. However, they believed that information security would be achieved simply by increasing awareness and providing training. All experts stressed the need of security awareness and training for employees. One of the experts commented: *"The problem that we faced seven years ago is IT awareness, the awareness of security was zero, a lot of people thought that all they needed to be protected was to have login name and password, and then we worked on training our employees to raise the awareness to make the implementation of security easy"*. Furthermore they stressed that information security would need a continuous and ongoing awareness and training programme for employees to deal with the ever-changing security arena. Dhillon (1999) argues that, organizations must have ongoing education and training programs to achieve the required outcome from the implementation of an information security policy. The 2002 security awareness index report cited by McKay (2003) concluded that organizations around the world are failing to make their employees aware of the security issues and the consequences. However, there is no evidence in the literature that awareness programs play any decisive role in reducing insecure behaviour or that it makes a difference in ensuring information security and in increasing compliance to information security policies.

The interviews revealed that the most security incidents that the organizations face came from their own users, known as insider threat damage. As described by one expert *"we faced some incidents, there have been attempts at sabotage by our users, our employees sabotage us..."*. This confirms what Katz (2005) finds that employees are the biggest threat to information security. Another expert said *"Outsider (threats) we did not face any hacking attacks, the only thing we face is viruses and spam"*. The viruses were installed when employees opened spam emails or attached files that had embedded viruses which then affected the organization's system.

Furthermore, hackers rely on well known human weaknesses to get into computer systems. Kevin Mitnick, one of the most famous social engineers, cited by the Economist 2002, explained that: *"The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain"*, where the weakest link is people (Lampson, 2002). Employee failings can weaken even the strongest security measures. For example, common practices are employees leaving machines logged on while out for breaks; recording passwords on sticky note on the computer's monitor; or revealing confidential information to unauthorised people. The accepted wisdom is that there is a need to put effort into training and educating the employees, because they are the ones who are going to need to comply with the information security mechanisms and norms. No matter how powerful the technical security underpinning of the system is, or how strong the regulations, or policies, there is still the possibility that they will be broken simply because someone subverts them.

Such a person is a continuous threat, and a disturbance to the sustaining of a secure information environment because technology is a tool that can either be used or misused. We recommend that a training and awareness program be employed for employees all levels in the organization with the consideration of the job type or the environment they work or deal with. For example, awareness training for managers will vary from other employees in the IT department and so forth. It is true that we do not currently have any clear understanding of the efficacy of such training and awareness programs, but at the current time it is the only tool in our arsenal and we can only hope that it will do some good.

4.2 Management Support

In all organizations we surveyed and understanding and identification of the need for security comes from the IT department or the person in charge of information security. One of the experts said *"Us (the experts), the top management does not know everything, we have to explain to them and make them understand the need of security"*. This confirms what Fung & Jordan (2002), claims that management tends not to initiate measures to ensure the security of organizational information because generally they feel that the IT department is responsible for choosing the proper technologies, installing the required software,

maintaining the technology in the organization and keeping the organization's information secure. The majority of experts emphasised their perception of importance of management perceptions in the implementation of information security policies. One of them commented "*top management, we can't do anything without their authorization they have to support us in implementing information security in the organization*". One expert stressed the support of management as "*...we have to understand if the top management don't support or understand the need of information security the implementation of information security will fail*". Another expert said "*... it is an important issue because if they believe in the importance of information security for the organization they will work on enforcing it and also the employees will take it seriously*". Hone & Eloff (2002) explain that the behaviour and attitudes of employees towards information security will be more in line with secure behaviour if top management demonstrates concern, therefore it is suggested that the tone of security is set by the attitudes of those at the top of the organization (Hinde, 1998). Management won't act to support the information security unless they can see that it supports the organization's core business function (Blake, 2000). Hence they must be convinced of the importance of information security before they will to provide sufficient budget, and act to enforce the information security policy (Von Solms, 1999).

4.3 Budget

The interviews revealed that all the experts define budget as an important aspect of implementing information security in the organization. One expert commented on the budget "*One day my boss asked me 'are we protected?', I told him if you have a house and you want to protect it you will need money to do so... so the level of security or the protection you will get depends on how much money you will spend. According to the budget we plan for information security*". The budget needs to be adequate: "*Without enough money, we can't have security in the organization; money will bring software, hardware, and consultants*". Without a proper budget, organizations won't be equipped with sufficient resources to ensure information security. Bjorck (2002) describes *budget* as the financial facility which firstly rationally estimates the costs and secondly assesses the access required to the resources to achieve successful implementation of information security. Organizations require adequate funding (Doherty & Fulford, 2005) to achieve effective information security. "Budgets generally depend on the manner in which individuals' investments translate to outcomes, but the impact of security investment often depends not only on the investor's own decisions but also on the decisions of others" (Anderson & Moore, 2006, p.612). Lack of information security budgeting in organizations leads to under- investment in appropriate controls (Dinnie, 1999).

When it comes to technology, new products appear frequently and are sold as the security "silver bullet". This happens because the information security vendors and consultants naturally about selling their latest products and services. What they don't say is that the software often needs to be updated frequently in order to address the continuously changing and emerging threats. It is therefore challenging to meet Gordon and Loeb's maxim: "From an economics perspective, firms should invest up to the point where the last dollar of information security investment yields a dollar of savings" (Gordon & Loeb, 2006, p.121). Specifically, information security expenses should be analysed in cost-benefit conditions. Organizations do *not* need to invest in expensive software or hardware to achieve an effective level of information security. What *is* required is a careful plan that ensures that the user behaves securely, and this cannot be achieved by means of any new technology or software product. However, such training is expensive and it is hard to demonstrate the efficacy thereof, which makes it difficult, if not impossible, to demonstrate the return on investment that management needs in order to justify expenditure.

A few experts in the interview mentioned the organization's resources as the base of information security in the organization. "*Security software or IT technology within the organization is a part of the requirement to conduct information security which is a mandatory need...*". There are essential operating systems, applications and other technologies which are required to support the implementation of information security in the organization (Canavan, 2003). Organizations with lack of proper software or hardware will face difficulties in handling some security issues such as access control mechanisms or helping employees to apply good security practice like an automatic logoff or regular password changes. Resources in organizations are the foundation requirement to enforce and monitor the implementation of information security.

4.4 Information Security Policy Enforcement and Adaptation

The information security policy is a plan identifying the organization's vital assets together with a detailed explanation of what is acceptable, unacceptable and reasonable behavior from the employee in order to ensure security of information (Hone & Eloff, 2002). Moreover, Fung et al. (2003) explains that an information security policy is the keystone of good information security management. There is no doubt that the adoption of an information security policy is the initial measure that must be in place to minimize the threat of unacceptable use of any of the organization's information resources. On its own it cannot ensure information security. It is a *necessary* but not *sufficient* requirement for the security of organizational information.

One of the experts from the interviews explained, "*Performance of the organization will be successful when we create a policy, effective implementation of the policy, acceptance from employees, and stick to our rules and don't manipulate them*". Many experts mentioned that the policy should be straightforward, easy and clear: one said "*it should be a straightforward policy and you should exclude any process not required, they should exclude any one not in sequence reading of the policy*", and it is also important that the policy be reviewed and updated frequently.

Madigan, et al. (2004, p.48) clarifies that policy enforcement involves "*assuring that the policies are understood by all interested parties, regularly checking to see if the policies are being violated, and having well-defined procedure guidelines to deal with incidents of policy violation*". Hone & Eloff (2002, p.15) state, "*at the end of the day, an effective information security policy will directly result in effective information security*". Canavan (2003) explains that the information security policy can only be enforced by means of implementation. When an organization puts an information security policy into practice, employees can be requested to follow the rules and be made aware of their rights and responsibilities (Hone & Eloff, 2002). A security policy can mitigate some threats, such as viruses, and work towards preventing incidents caused by these threats from re-occurring (Hinde, 2003). The aim is to change the habits of employees in the organization. Below are some criteria that the organization should consider in order to implement the information security policy effectively and to secure organization assets properly (Canavan, 2003; Doherty & Fulford, 2005; Hone & Eloff, 2002; Salter et al. 1998; Madigan, et al. 2004; Tryfonas et al., 2001; and Dhillon, 1999). The policy must: fit the organizational culture; have a style which is consistent with the organization's general communication style; not read like a technical document, but use simple language to ensure it is not difficult to understand; be effective and dynamic; use a concrete language rather than abstract language; specify the job responsibilities; state the purpose of the policy and the scope of the organization; and explain what activity is acceptable and what is not.

Many of the experts mentioned that adaptation of the information security policy to the needs of the organization is important. One of the experts commented that "*The information security required a lot of customization to fit our organization's culture*". Each organization provides different services, that's why they require an adaptation of the security policy but the underlying principles should be the same: "*In general terms the information security policy should be the same but the rest varies from place to place in terms of implementation. For example security is different from a tent to a house*". It appears that it is advisable for organizations to implement a customized information security policy which reflects the culture of the organization. This is reflected in the literature. Barman (2001) argues that the content of the information security policies may vary from one organization to other but that all policies have some topics in common. The policy should be developed based on the security needs and business goals of the organization (McKay, 2003).

4.5 Organization Mission

Siponen (2001) explains that in terms of security, organizations usually do nothing as long as nothing goes wrong, but when things *do* go wrong, they suddenly pay attention and a lot of effort is required to recover from the situation, even though sometimes full recovery is impossible.

Some of the experts said that the organization's clear goals and objectives are essential in implementing information security policies and that having a culture of secure information in the organization will affect its success. This is illustrated by a statement from one of the experts "*It is successful when understanding what*

we want to achieve, defining what we want to achieve by setting goals and objectives, will support the information security implementation", also "what makes it not successful is when the users don't understand and believe the need for information security. In other words incomplete culture change will reflect on the success on information security". McKay (2003) clarifies that if the organization's mission is not addressed, the organization will continue to struggle to secure its information and employees will not take responsibility seriously and will not follow and respect the guidelines in the information security policy.

5. CONCLUSION

What has been discovered from the study is that there are a number of essential factors which will information security experts have identified as being essential if an organization wants to achieve a level of information security. The results suggest that organizations *must* institute information security policies to prevent unauthorized access to their resources. Steps must be taken to ensure that employees get the required awareness and security training to make them aware of the security issues and the consequences of insecure behavior. Moreover, the results suggest the ethos of information security must come from the top of the organization to encourage a serious attitude from employees and an expectation that they will comply with the organization's security policy rules and regulations. Implementation of information security won't be possible if a sufficient budget is not allocated. Furthermore, we hope that clear organizational mission statements and goals result in positive employee behaviour and positive attitudes towards securing the organization's information assets. The results suggest that the identified factors are connected and linked to each other and therefore it is difficult to prioritize one factor over another.

It is very likely that the factors identified by this study would have a significant impact in helping organizations to achieve effective information security. When adhered to, these factors should lead to fewer security breaches within the organization. While the study highlighted the requirements for good information security practice there is a need for follow-up studies using different methods or different tools to help organizations to understand what is required to improve the effectiveness of their information security policy.

While the whole issue of information security is under-developed in Oman, the outcome of this research will be able to contribute to both governmental organization and non-governmental organizations in terms of best practice in enhancing information security. As the research unfolds, it is expected that the findings will help organizations everywhere to better understand and determine the steps that are needed to improve the organization's information security.

REFERENCES

- Anderson, R. and Moore, T., 2006. The Economics of Information Security. *Science*, Vol. 314, No. 5799, pp. 610-613.
- Barman, S., 2001. *Writing Information Security Policies*. SAMS. 1st Edition.
- Bjorck, F., 2002. Implementing Information Security Management Systems – An Empirical Study of Critical Success Factors.
- Black, S., 2000. Protecting the Network Neighbourhood. *Security Management*, Vol. 44, No. 4, pp. 65-71.
- Brown, J. S. and Duguid, P., 2002. *The Social Life of Information*. Boston, Harvard Business School Press.
- Canavan, S., 2003. An Information Security Policy Development Guide for Large Companies. *SANS Institute*.
- Carr, L.T. 1994. The Strengths and Weaknesses of Quantitative and Qualitative Research: What Method for Nursing? *Journal of Advanced Nursing*, Vol. 20, pp.716-721.
- Dhillon, G., 1999. Managing and Controlling Computer Misuse. *Information Management & Computer Security*, Vol. 7, No. 4, pp. 171-175.
- Dinnie, G., 1999. The Second Annual Global Information Security Survey. *Information Management & computer security*, Vol. 7, No. 3, pp. 112-120.
- Doherty, N. F. and Fulford, H., 2005. Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal*, Vol. 18, No. 2, pp. 21-39.
- DTI, 2006. http://www.dti.gov.uk/industries/information_security, last reviewed September 2006.
- Ernst & Young, 2004. Global Information Security Survey 2004.
- Fung, P. and Jordan, E., 2002. Implementation of Information Security: A Knowledge-based Approach.

- Fung, P., Kwok, L. & Longley, D. 2003. Electronic Information Security Documentation. *Australian Computer society*, Vol. 21.
- Garbars, K. 2002. Implementing an Effective IT security Program. *SANS Institute*, As part of the information security reading room. GSEC Version 1.4.
- Gollmann, D. 1999. *Computer Security*. New York. John Wiley & Sons Ltd.
- Gordon, L. A. & Loep, M. P. 2006. Budgeting Process for Information Security Expenditures. *Communications of the ACM*, Vol. 49, No. 1, pp. 121-125.
- Hind, S. 2002. Security Surveys Spring Crop. *Computers and Security*, Vol. 21, No. 4, pp. 310-321.
- Hone, K. & Eloff, J.H.P. 2002. What makes an Effective Information Security Policy. *Network Security*, Vol. 20, No. 6, pp. 14-16.
- <http://news.bbc.co.uk/1/hi/programmes/moneybox/6371089.stm>, last reviewed 17 January 2007
- <http://www.cisecurity.org/charter.html>, last reviewed 3 October 2006.
- http://www.economist.com/surveys/printerfriendly.cfm?story_id=1389553, last reviewed January 2007.
- I.S.O. 2000. *Information security management systems: specification with guidance for use*. London: British Standards Institute.
- I.S.O. 2001. *Information technology: code of practice for information security management*. London: British Standards Institution
- Katz, F. H. 2005. The Effect of a University Information Security Survey on Instruction Methods in Information Security.
- Lampson, B. W. 2002. Computer Security in the Real World. *Principles of Computer Systems*. www.research.microsoft.com/lampson.
- Madigan, E. M., Petrulich, C. and Motuk, K. 2004. The cost of Non-Compliance-When Policies Fail. *Proceedings of the 32nd annual ACM SIGUCCS conference on User services*, pp. 47 – 51, USA.
- McKay, J. 2003. Pitching the Policy: implementing IT Security Policy through Awareness. *SANS Institute*.
- Pfleger, C. P. 1997. *Security in Computing*. Prentice Hall PTR. 2nd Edition.
- Sebastian, H. Van. Solms & Jan HP Eloff. 2003. *Information Security*. B & D Printers.
- Sandhu, R. 2003. Good-Enough Security Toward a Pragmatic Business-Driven Discipline. *IEEE Computing Society*.
- Siponen, M. T. 2001. A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security*, Vol. 8, No. 1, pp. 31-41.
- Straub, D. W. & Welke, R. J. 1998. Coping with System Risk: Security Planning Models for Management decision Making. *MIS Quarterly*, Vol. 22, No. 4, pp. 441-470.
- Tryfonas, T., Kiountouzis, E. & Poulymenakou A. 2001. Embedding Security Practices in Contemporary Information systems Development Approaches. *Information Management & Computer Security*, Vol. 9, No. 4, pp. 183-197.
- Varney, C. A. 1996. Consumer Privacy in the Information Age: A View from the United. States. *Remarks before the Privacy and American Business National Conference*, Washington. <http://www.ftc.gov/varney/priv%26game.htm>
- Von Solms, R. 1996. Information Security Management: The Second Generation. *Computer & Security*, Vol. 15, pp. 281-288.
- Von Solms, R. 1999. Information Security Management: Why Standards are Important. *Information Management & Computer Security*, Vol. 7, No. 1, pp. 50-57.
- Whitman, M. E. 2003. Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, Vol. 46, No. 8, pp. 91-95.
- Whitman, M. E., Caylor, J., Fendler, P. & Baker, D. 2005. Rebuilding the Human Firewall. *Information Security Curriculum Development Conference*, Kennesaw, GA, USA. ACM, pp. 104-106