Human Excellence in Information Security: A Complexity Theory Perspective

A. Shayan[1], K. Soheili[2] and B. Abdi[1]

[1]Department of Information Technology Management, University of Tarbiat Modares, Tehran, Iran
[2]Department of Social Communication Science, University of Tehran, Iran
e-mail: ashayan@modares.ac.ir; komeil.soheili@gmail.com

Abstract

Information technology has become an indispensable part of the business world today. Organizations have been dependent to information it more than ever. Such dependency has been followed by its own information security issues. Specialists have highlighted the critical role of human and organizational factors. The employees should be creative in relation with information security. In this way, collective knowledge sharing is crucial. Furthermore, balancing between perform routine security and having creative and improving employees is the delicate function of information security officers. This paper intended to present this optimized condition according to the "edge of chaos" concept of the complexity theory. The scrutiny of the equilibrium had done from several important dimensions.

Keywords

Information security, Human excellence, complexity theory, edge of chaos, culture

1. Introduction

Nowadays, information is critical in the organizations and its interruption and vulnerability may be caused the organizations failure (Dohertty and Fulford, 2006). Also, a steady rise in the occurrence of cyber attacks has meant that Cyber security is an issue which is becoming increasingly important as computer networks become more widespread. The level of sophistication and speed of development of the tools being used to create security breaches and attacks are growing exponentially (Sharma and Sefchek, 2007). These events have followed by unpleasant consequences such as information vulnerability and cyber crimes (Eloff and Eloff, 2005). It is predicted that the information security threats are being vaster, vaguer and more complex (Mitchell, 1999). Public and private organizations have gradually noticed that the importance of information security in such connected and multi aspect environment has increased. Research has shown that security is by far the most frequent IT issue considered by states in promulgating or establishing policies and standards (Gil-Garcia, 2004). Technical controls alone will not ensure the safety of the information assets of an organization and will not solve information security related problems (Thomson and Solms, 2006). Also, Birman (2000), Stout (2006) and Schultz (2005) have highlighted the critical role of human and organizational

factors for ensuring security and claim that security is more than purely a technical concern; it is also strategic and legal concern.

It could be induced that one of the biggest threats to the success of information security in an organization is the erroneous actions and behaviour of employees when handling information (Thomson et al, 2006). At the present time, organizations are responsible for their employees and customers privacy in order to attracting their trust. This means fostering and improving of human resources in the organization is the critical function of effective managers. Traditionally, there are three fundamental qualities of information which are vulnerable to risk and which, need to be protected at all times, namely availability, integrity and confidentiality. It is obvious that keeping all these three attributes in the organization requires aware employees. The employees should be creative and they should participate in the organizational collaboration. In this way, we could have a collective knowledge among them. Furthermore, balancing between doing routine security function and having creative and improving employees is a delicate issue. This paper intended to present this optimized condition according to the "edge of chaos" concept of complexity theory.

2. The roles of human resources in the information security

Seen from a distance, it might be easy to think that the field of information security is primarily about technology. Up close, it is clearly a multidisciplinary field that draws from economics, sociology, technology, business, and law. Also, one of the most important aspects of information security is human resources. For decades, security authorities recognized that solving security problems requires managerial attention (Knapp et al, 2006). A 2004 key issues study of 874 certified information security professionals showed that top management support was ranked number one from a list of 25 security issues (Knapp et al., 2004). In the same study, organizational culture ranked sixth and policy-related issues ranked seventh (Knapp et al, 2006). Also, CSO Magazine conducted a survey Based on 7,596 responses from chief level executives in 54 countries, the survey determined that businesses that suffered security breaches did not spend any less on security technologies than businesses who did not suffer any security incidents(CSO, 2003). So, we should find the reasons in the other factor: human abilities.

In addition, corporate culture is a strong driving force in organizations which largely affects the behavior of employees and, consequently, the success of the information security practices. Therefore, any attempt in an organization to implement technical and physical information security controls without considering the culture in the organization could have disastrous consequences (Shaurette, 2004). Furthermore, a number of recent surveys indicate that few organizations have recognized this matter as an issue, so investment in security awareness (SA) initiatives remains low (Purser, 2004). The base of security in any organization is informed, educated, and loyal employees (Trček, 2003). As a result, managing and auditing the employees, become sensitive practices of chief security officers which should cover both behaviour and outcomes of their performances (Vroom and Solms, 2004).

Information and communication systems are confronted by a great variety of threats. Attacks originating from outside usually get public attention. Insider threats, on the other hand, pose a significantly greater level of risk (Schultz, 2002) and have a heavier cost for organizations. An oft-quoted statistic nowadays is around 80% of the risk to information systems comes from insider (Walton, 2006). The dissemination of illegal or offensive material can cause bad reputation or even legal prosecution for organizations. Such reasons lead many organizations to explore ways of information controls by their employees (Mitrou and Karyda, 2006).

It is considerable that this perspective is pessimistic and it considers employees as treats. by the way, With the term ‘‘insider threat’’ they refer to threats originating from employees of an organization, who have been given access rights to information and communication systems, and misuse their privileges, performing actions that violate the security of these systems. Security controls used for protecting information systems from externally initiated attacks are not effective in detaining insider threats, since the latter requires a different approach (Porter, 2003; Lee and Lee, 2002). It has been suggested that insider threats are impossible to control by technological means because they are often socially or organizationally based (Williams, 2008). Therefore, the role of the employees is vital to the success of any company, yet unfortunately they are also the weakest link when it comes to information security. It is imperative to minimize human errors in order to improve organizational security awareness. However, very little evidence could be found that auditing of the behaviour of the employee With regard to information security occurs in practice (Vroom and Solms, 2004).

Insiders enjoy privileged access that enables them to do serious damage far more easily than anyone attacking from outside. Some of this may be due to inadequate defence mechanisms, but for the most part, the access that enables them to cause so much damage is also essential to enable them to do their jobs. It is this ease of doing deliberate damage that makes the insider threat so serious. Nevertheless, almost all insiders are going to be loyal and can be trusted. To some extent at least, the insider threat is within the organization’s control, whereas the outsider threat is not. This is an important distinction between the two sources of risk and governs the measures that need to be taken (Walton, 2006).

Some researchers tried to design several controls to manage employee’s behaviour. For example, Dhillon and Moores (2001), while advocating traditional technical safeguards to limit access to computer systems and their programs, further note the need for formal and informal controls. Formal safeguards include written policies for clarifying the appropriate security responsibilities and roles of staff. These are complemented by informal controls, such as education and awareness campaigns, which directly aim to influence the security behaviour of employees.

While we talking about human resources, we mean the whole organization's members include managers, employees and information security department. A company’s security must start at the top of the company, this means from the CEO on down to the lowest level employee. Management support for a security policy is

crucial. Management's goal should be to make employees and customers an integral part of the solution. Management should understand that security requires them to show the same leadership initiatives as they do with other parts of the business that have a direct bearing on profitability (Smith, 2004). The vacuum between top and down side of organization can be resulted to the unawareness of employees about information security plans and strategies. On the other hand, People do not behave like machines-they are erratic and unpredictable. Therefore constant monitoring of employees would be impractical, expensive and time-consuming. The problems mentioned above are only a few of many that would be encountered when attempting to evaluate people and their behaviour in the organization. A formalized, structured approach would prove to be extremely difficult, both logistically and practically. For these reasons, an alternative approach needs to be found. In order to do this, the organization and the interaction between the employees need to be studied (Vroom and Solms, 2004).

Also, a huge change had observed in the business models of modern organizations. The increasing rate of virtual organization growth is due to the increasing rate of tele-workers (Rana and Hilton, 2006). So, the security issues of these employees will be intensified. Peacey (2006) presented some solutions for Protecting the tele-worker's environment. This separate and scatter individuals require different approaches to increasing their performance. So, for acquisition and use of this knowledge, the organization should fitly adopt strategies (Rohmeyer, 2006).

Information Security as a concept has developed both breadth and depth and it needs the overlay of a strong management system to determine how these aims can be achieved efficiently and coherently (Ashenden, 2008). ISO 27001 defines the management aspects of Information Security as, 'that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve Information Security'. It states that this includes, 'organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources' (ISO/IEC 27001). Security is to combine systems, operations and internal controls to ensure the integrity and confidentiality of data and operation procedures in an organization. With the advent of information technology, users' roles in information systems have evolved from IT specialists for access information facilities, to non-IT personnel for regular operations and unspecified individuals from outside. That is to say, with the serious threat of unauthorized users on the Internet, information security is facing unprecedented challenges, and effective information security management is one of the major concerns (Hong, 2003). Security tools and mechanisms have a limited effectiveness for the reason that security is primarily a "people issue", as well as an "organization issue" (Hinde, 2003). Under this perspective, the importance of security management in the context of the organization becomes evident and therefore requires all levels within the company to be conscious of the vulnerabilities and risks facing the company. Thereby they have a sensitive duty to direct the employees in a way that they become autonomous in their responsibilities and become beneficial motivated.

3. Human excellence for information security

Users play an important role in the information security performance of organizations by their SA and cautious behaviour. Awareness alerts employees to the issues of IT security and prepares users to receive the basic concepts of IT security through a formal training program. Training and awareness programs can be used to influence the culture of an organization by promoting favourable security practices and mindsets (Knapp, 2005). Many researchers (Furnell et al, 2002; Stanton et al., 2005) and practitioners (Hulme, 2001; Ramanathan, 2004) note the importance of SA during strategic, tactical, and operational security decision-making.

There are several information security abilities indicators such as security fraud detection and having security knowledge (Post and Kagan, 2007). A user's view on information security is created by several interlocking organizational, technological and individual factors. Furthermore, social norms and interactions at the work place influence individual understanding of information security. The quality of information security management also affects users' awareness, motivation and behaviour in some way. Motivation, knowledge, attitudes, values and behaviour also influence individual views on information security. How people perceive risk is a part of the explanation for users' view on information security. In a survey, the interviews of users at an IT-company and a bank shown that some main patterns of information security were: (1) users state to be motivated for information security work, but do not perform many individual security actions; (2) high information security workload creates a conflict of interest between functionality and information security; and (3) documented requirements of expected information security behaviour and general awareness campaigns have little effect alone on user behaviour and awareness. The users consider a user-involving approach to be much more effective for influencing user awareness and behaviour (Albrechtsen, 2007).

The role of users is an important part of a holistic approach to information security management. Dhillon and Backhouse (2000) have argued that the role, responsibility and integrity of users are important principles of information security management in new forms of organizations, which can be characterized by blurred organizational and geographical borders; use of mobile equipment; and information and knowledge being the organization's most important resources. Stanton et al (2005) make taxonomy of security behaviours and had considered two dimensions: expertise and intentions. They had suggested six possible behaviors of users.

Employee's SA programs need to begin growing out of their infancy. That means a fully realized multi-phased approach that follows a specific methodology that can be tailored to meet any organization's specific needs, paying close attention to specific security weak points (valentine, 2006). Kruger and Kearney (2006) consider three dimensions for any SA programs. It includes promotion of knowledge, attitude and behaviour of employees. It's difficult to get well trained security specialists, and even more difficult to get them to be well-motivated and stay with you (James, 2006). One way to be vigilant against information security attacks is for information security controls and practices to become part of the corporate culture of an

organization (Thomson and Solms, 2006). Albeit, the organizations should regard the principles of visualization in the implementation of security controls, because it enhances efficiency and effectiveness of these controls (Paula et al, 2005). The vision of senior management with regard to information security must be outlined in the Corporate Information Security Policy of the organization. The Policy should be 'translated' into procedures that will positively affect the attitude and behavior of employees (Thomson and Solms, 2006). The Corporate Information Security Policy must work within the organization, where the corporate culture exists, and must address the security needs of the specific organization. Therefore, if the corporate culture is not taken into consideration when enforcing the Information Security Policy in an organization, the behavior of employees may not change to reflect the 'wishes' embedded in the Information Security Policy (Thomson and Solms, 2006).

Kerry-Lynn Thomson and Rossouw von Solms (2006) illustrated Information Security Competence Maturity Model. In their model, The Conscious Competence Learning Matrix is generic and could cover a wide variety of skills. At Stage 1, employees are at the Unconscious Incompetent stage and unaware of the role they should be playing in terms of information security and not aware of their ineffectiveness. In order for employees to progress from Stage 1 to Stage 2 an effective SA Program should be run in the organization. Ideally, an SA Program should prepare employees for Information Security Training by encouraging a change in employee attitude towards information security. Once employees have participated in the SA Program, and they have been made aware of all the potential threats to information assets, they progress to Stage 2. Stage 2 is Conscious Incompetence. At this stage employees are already aware of their information security roles and responsibilities. For employees to move from Stage 2 to Stage 3, they must participate in Information Security Training. Through Information Security Training, employees will learn "how" information assets must be protected and employees will learn vital skills enabling them to perform information security practices. Once employees have participated in the Information Security Training program, and gained the required skills, they are ready to progress to Stage 3. At Stage 3 of the Information Security Competence Maturity Model, Conscious Competence, employees need to consciously focus on the information security practices they need to perform. These practices are performed correctly, but are neither second-nature nor part of the employees' corporate culture. Employees will only be able to legitimately progress to Stage 4 when they apply the skills they have learnt through Information Security Awareness, Training and Education and have gained Experience by performing the information security practices incessantly and become accustomed to the newly learnt practices. Positive reinforcement will help promote employees from Stage 3 to Stage 4. Reinforcement should be used as confirmation that the employees are performing the correct information security practices and to solidify the benefit of information security practices to the employees. The ultimate goal of the Information Security Competence Maturity Model is for the employees of an organization to reach Stage 4, through awareness, training and experience, and become Unconsciously Competent in the critical information security practices which support the information security vision of senior management. If this is achieved, then Information Security Obedience has been

realised. The progression of employees from Unconscious Incompetence to Information Security Obedience is depicted in the Figure 1.

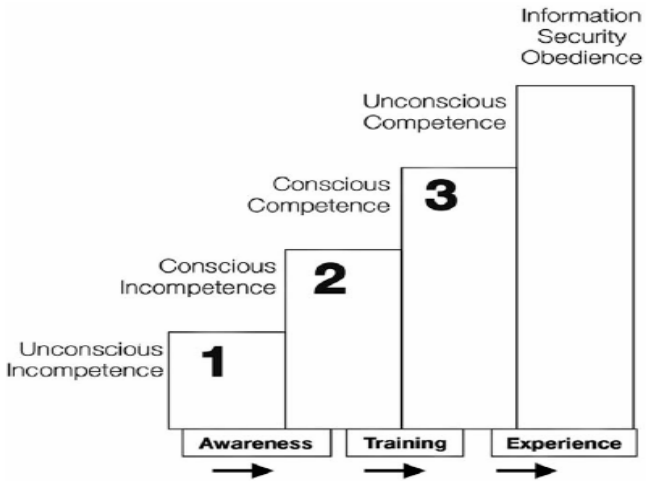

Figure 1: Information Security Competence Maturity Model (Thomson and Solms, 2006)

4. Complexity theory perspective

One of the most important popularizers of complexity theory, Gleick (1987), has argued that 20th century science will be remembered for three things: relativity, quantum mechanics and chaos. All of them are a revolutionary transformation in the nature of modern science. Earlier models of organization can be seen as emphasizing order and regularity at the expense of the erratic and discontinuous. Complexity theory focuses attention on those aspects of organizational life that bother most managers most of the time-disorder, irregularity and randomness. It accepts instability, change and unpredictability and offers appropriate advice on how to act. The pioneer in the development of chaos theory is usually considered to be the Edward Lorenz. During the theory development, the original term 'chaos theory' was giving way to the grander conception of 'complexity theory. Chaos theory is limited to the mathematics of non-linear dynamic behaviour in natural systems. Complexity theory, by contrast, is represented as being applicable to the behaviour over time of complex social as well as natural systems.

In this theory Order is an emergent property of disorder and it comes about through self-organizing processes operating from within the system itself. System and environment change in response to one another and evolve together. This paper brings concept of 'the edge of chaos' from complexity theory into human aspects the information security. The edge of chaos is a narrow transition zone between order and chaos that is extremely conducive to the emergence of novel patterns of behaviour. A system driven to the edge of chaos is likely to exhibit the sort of spontaneous processes of self-organization. The edge of chaos notion has proved

powerful in many different fields, including management and organization. In dynamic environment, Managers may not be able to predict and control organizations, but they can ensure their flexibility and responsiveness by propitiating favourable conditions for learning and self-organization. Learning requires an empowered workforce operating under favourable group dynamics that allow new mental models to emerge (Jackson, 2003). The existence of a strong, shared culture that stifles innovation must be avoided at all costs. Kauffman (1995) suggests that organizations should be broken up into networks of units that can act autonomously in their local environments, but are in continuous interaction with each other.

Stacey (1996) uses the 'edge of chaos' concept to articulate the most detailed account of how learning and self-organization can be promoted in organizations. He notes the complexity theory conclusion that all complex adaptive systems can operate in one of three zones: a stable zone, an unstable zone and at the edge of chaos, a narrow transition zone between stability and instability. In the stable zone they ossify, in the unstable zone they disintegrate, but at the edge of chaos spontaneous processes of self-organization occur and innovative patterns of behavior can emerge. This seems to be the best place for organizations to be. At the edge of chaos, in a state of 'bounded instability', they behave like dissipative structures and display their full potential for creativity and innovation. The edge of chaos is difficult to reach and sustain because it requires a kind of balance between the forces promoting stability in an organization and those continuously challenging the status quo. In Stacey's terms, it demands that an appropriate degree of tension exists between an organization's 'legitimate system' and its 'shadow system'. Stacey outlines five control parameters' to ensure an organization remains at the edge of chaos. These are: 'information flow', 'degree of diversity', 'richness of connectivity', 'level of contained anxiety' and 'degree of power differential'.

5. Human excellence and edge of chaos

Inspired from complexity theory, three situations can be imagined about employee's security. One of them is stable, which brings indolence to the organizations. Another one is unstable situation which brings turmoil and tumble. The last one is the 'edge of chaos' which shows proper, dynamic and productive of organizations. This Status appears when there is a balance between two other types. The erudite managers attempt to create this preferable condition. Figure 2 shows these three positions.

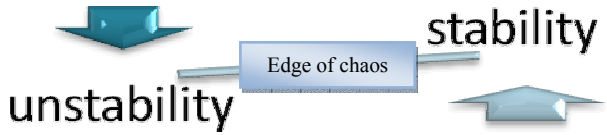

Figure 2: Balance in the edge of chaos

In this section, some important features of each situation will be described. One of the main aspects of information security controls is access management. It ensures

that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services, and applications. If this kind of control prevents interaction between employees, then it can be extremely harmful to foster knowledge and behaviour of them. Implementation of such balanced controls is a delicate function of elite chief security officers.

In recent years, auditors have shifted their approach by using their expertise gained over the decades, to controlling risk. Auditors have moved from a control-based audit model to a risk based model (Hunton et al., 2004). Rather than just controlling, auditors evaluate risks related to the company's strategy and objectives by selecting cost-effective controls that best mitigate the company's risks. However, it appears that the auditing profession may be making another shift from historic ex-post audits to near real-time audits (Flowerday, Solms, 2005). As complexity theory claims, predict the future of this turbulent world is impossible. So, the managers should prepare all staffs for response to any conditions proactively. In advance, auditing of information security should support this manner.

Inherent in the success of a SA program is to ensure that employees achieve three levels of awareness of security risks: perception, comprehension and projection. As more employees of an organization make progress along these three levels, the ‘‘people" side security can be heightened. The heightening of end user SA can help inculcate security cultures and values, thereby developing better security competency (shaw et al, 2009). There are three levels of organizational behaviour that should be influenced by each SA program: The individual, the group and the formal organization (Thomson and Solms, 2006). The methods for teaching should base on the concept of active and just-in-time learning. The SA programs should design for unpredictable future needs. As Confucius advised "Give a man a fish and he will eat for a day. Teach a man to fish and he will eat for a lifetime. ". And also Imam Ali, the Muslim's imam, advised: "teach your children for their time, not yours". so, determined teaching would not work anymore. Managers should consider the new way of teaching that persists on the basic comprehensive awareness for various kinds of events. To creativity taking root, the programs should consist of teamwork and reasonable knowledge sharing. It will be resulted to the collective learning.

It would be beneficial to change the information security culture to one that is more in line with the security policies of the business. Organizational behaviour is used to change the shared values and knowledge of the group. Once group behaviour begins to alter, it would influence the individual employees and likewise have an eventual effect on the formal organization. The artefacts of the organization would reflect these changes that have been put in place. According to three zones of complexity theory, strong culture can caused lethargy and indolence. Also, haywire and mess culture can results to the disorder and chaos. Therefore, the managers should try to establish a creative, dynamic but structured culture. Table1 summarize the distinctions between three situations according to the several important features.

Feature	Stable	Edge of chaos	Unstable
Employee's responsibility	To procedures	To objectives and environment	To their desires and Tendencies
Interaction's Structure	bureaucratic	Adaptive and flexible	Disorder
Learning	collected	Collective	Chancy and casual
Empowerment	regulations	Teams	Individuals
Culture	Strong and shared	Creative	haywire and mess
Organizing	Top-down	Spontaneous processes of self-organization	Disorganized
Knowledge networks	Separated knowledge	Autonomous knowledge networks	Mess knowledge networks
Source of power	Position and hierarchy	Expertise knowledge	Turbulent and illegitimate
Employee's trait	Passive	Proactive	Unpredictable
Goal Setting	By top management without any attention to the employee's needs	Common goal setting	Ramble or not transmitted to the employees
Feedback	Single-loop	Double or multiple loop	Not exist
Employee's changes and rotation	Usual routine	Intentional changes of heterogeneous Employees	Continuous and irrational changes
Awareness program	Limited, passive and retrospect	interactive, prospective and provident	Unfitness with duties
auditing	Based on procedures and tasks	Based on objectives, conditions and competence	Weak auditing
Motivation	Apathetic	Motivated and loyal	Affected by another stronger motivator

Table 1: distinctions between three human's situations of information security

Furthermore, there are other factors which affect on human's situation of information security in an organization. The quality of information security standard could lead organization toward each situation. In fact, standards determine the level of accepted actions which forms the performance and interactions across the organization. It is noticeable that support and participation of senior managers can result to desirable transmission of objectives and employees would achieve the ability of innovation through the obtained confidence. Likewise, the sense of equity and justice can results to motivation. Another impressive force is ethics, which can play an important role for establishing controls without any external controls. This may lead to reduction of organization's costs and omit troublous actions.

As the organization's borders pales and interactions between organizations increased, the importance of human development in this convergence rises and special needs for influenced individuals should be determined (Elahi et al, 2007). It is remarkable that all mentioned practices should be internalized in the employees; otherwise, they would be temporal and unfruitful. Thus, we can improve knowledge, attitude and behaviour of the employees.

6. Conclusion

The growth and availability of the Internet created serious vulnerabilities in connected systems. The most critical success factor of organizations is human abilities, which needs continuously improvement. Their prerequisites are to create a dynamic and creative environment which along with the goal-based direction of top management. This paper outlined a framework to forms a balance between stability and instability, which called edge of chaos, extracted from complexity theory. The paper suggested Employee's responses to the objectives and environment, design adaptive and flexible structure and collective learning through organization. This article prizes team work, creative culture and self-organization processes. Therefore, the organization can be flexible and each part could response to the unpredictable changes, instead of slow top-down organizing. This idea highlights the importance of each individual and offer a new way of thinking. Also, it noted that individual's power should dependent on their expertise. Hence, they tend to participate in the knowledge networks. Thereupon, managers should consider interactive, prospective and provident awareness programs. In summary, there should be a primitive situation for creative behaviour and proactive readiness. This debate can generalize to the public policy which the Governments can create several security programs for society. The methods for prepare such creativity and dynamism in the information security area among people can be appropriate subject for future researches.

7. References

Albrechtsen, E., (2007), "A qualitative study of users' view on information security", *Computers & Security*, 26, 276 – 280.

Ashenden, D (2008), "Information Security management: A human challenge?", *information security technical report* 13 195–201

Birman KP.(2000), "The next-generation internet: unsafe at any speed", *IEEE Computer*;33(8):54-60.

CSO (2003), "The state of information security", *CSO Magazine*, October.

Dhillon G and Backhouse J.(2000), "Information system security management in the new millennium", *Communications of the ACM*;43(7):125–8.

Dhillon, G., and Moores, S. (2001), "Computer crimes: theorizing about the enemy within", *Computers and Security*, 20(8), 715–723.

Dohertty F. and H. Fulford (2006), "Aligning the information security policy with the strategic information systems plan", Computer & security, 25: 55-63.

Elahi, S., A. Shayan and B. Abdi (2008), "Designing a framework for convergent information security management among federated organizations", *World Applied Sciences Journal*, Volume 3 (Supplement 2), 2008.

Eloff J. and M. Eloff (2005), "Information security architecture". Computer Fraud & Security, November: 10-16.

Flowerday, S. and Von Solms, R., (2005), "Real-time information integrity=system integrity+data integrity+continuous assurances", *Computers & Security*, 24, 604-613.

Furnell, S.M; Gennato, M.; and Dowland, P.S. (September, 2002), "A prototype tool for information security awareness and training", *Logistics Information Management*, 15(5/6), pages 352 – 357.

Gil-Garcia, J. Ramon. (2004), "Information technology policies and standards: A comparative review of the states", *Journal of Government Information* 30 548–560.

Gleick, J. (1987), "Chaos: The Making of a New Science", *Abacus*, London.

Hinde, S. (2003), "The law, cybercrime, risk assessment and cyber protection", *Computers and Security*, Vol. 22 No. 2, pp. 90-5.

Hong, K., Chi, Y., Chao, L.R. and Tang, J., (2003), "An integrated system theory of information security management", *Information management & computer security*, 11/5 243-248.

Hulme, G. V. (September, 2001a), "Management takes notice", *InformationWeek*, issue 853, pages 28 – 34.

ISO/IEC 27001: "Information security management systems: Requirements", *http://www.iso.org*

Jackson, M.C. (2003), "Systems Thinking: Creative Holism for Managers", *John Wiley and Sons Ltd*, p 113-135.

James, M., (2006), "Outsourcing- security outgrows fear of the dark", *Infosecurity Today*, November/December.

Kauffman, S. (1995), "At Home in the Universe", *Oxford University Press*, New York.

Knapp, K.J., (2005), "A model of managerial effectiveness in information security: From grounded theory to empirical test", *A Dissertation Submitted to the Graduate, Faculty of Auburn University for the Degree of Doctor of Philosophy Auburn*, Alabama December 16.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Morrow, D.W. (2004), "Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium" *(ISC) 2 Survey Results*, Auburn University, Auburn, AL.

Knapp, K.J.; Marshall, T.E.; Rainer, R.K. and Ford, F.N. (2006), "Information security: management's effect on culture and policy", *Information Management & Computer Security* Vol. 14 No. 1, pp. 24-36.

Kruger, H.A., Kearney, W.D., (2006), "A prototype for assessing information security Awareness", *Computer & Security*, 25, 289 – 296.

Lee, J., Lee, Y.(2002), "A holistic model of computer abuse within organizations", *Information Management & Computer Security* 10 (2), 57–63.

Mitchell, R., R., Marcella, and G., Baxter (1999)," Corporate information security management", *New Library World*, 100(1150): 213-227.

Mitnick, K.D. and Simon, W.L. (2002). "The art of deception – controlling the human element of security", Indianapolis, Indiana : *Wiley Publishing, Inc.*

Paula, R.d., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D.F., Ren, J., Rode, J.A. and Filho, R.S., (2005), "In the eye of the beholder: A visualization-based approach to information system security", *Int. J. Human-Computer Studies*, 63, 5–24.

Peacey, A., (2006), "Teleworkers – extending security beyond the office Network Security", *Network Security*, November, 14-16.

Porter, D.(2003), "Insider fraud: spotting the wolf in sheep's clothing", *Computer Fraud & Security* 1 (4), 12–15.

Post, G.V. and Kagan, A., (2007), "Evaluating information security tradeoffs: Restricting access can interfere with user tasks", *computers & security*, 26, 229 – 237.

Purser, S.A. (2004), "Improving the ROI of the security management process", *Computers & Security* 23, 542-546

Ramanathan, R. R. (December, 2004), "Information security top-down", *Security*, 41(12), pages 30 – 34

Rana, O., Hilton, J. (2006), "Securing the virtual organization – Part 1: Requirements from Grid computing", Network Security, April, 7-10.

Roberts, M. (2002), "Guarding the electronic gates", *Chemical Week*, Vol. 20 No. 27, pp. 41-2.

Rohmeyer, P., (2006), "An evaluation of information security management effectiveness", Ph.D. *dissertation At Stevens institute of technology*, 30 September.

Ryan, J., (2006), "A comparison of information security trends between formal and informal environments", *A Dissertation for the Degree of Doctor of Philosophy the Graduate, Faculty of Auburn University,* Alabama August 7.

Schultz E. (2005), "The human factor in security", *Computers & Security*;24(6):425-6

Sharma, S.K and Sefchek, Joshua (2007), "Teaching information systems security courses: A hands-on approach", *computers & security* , p290–299.

Shaurette, K.M. (2004), "The building blocks of information security – information security handbook fifth edition", Boca Raton, London, New York, Washington D.C. : *Auerbach Publishers.*

Shaw, R.S. , C. Chen, Charlie ,. Harris, Albert L, Huang, Hui-Jou, (2009), "The impact of information richness on information security awareness training effectiveness", *Computers & Education* ,52 , 92–100.

Smith, A. (2004), "E-security issues and policy development in an information-sharing and networked environment", *Aslib Proceedings: New Information Perspectives*, 56(5): 272-285.

Stacey, R.D. (1996), "Complexity and Creativity in Organizations", *Berret-Kohler*, San Francisco.

Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J., (2005), "Analysis of end user security behaviors", *Computers & Security*, 24, 124-133.

Stout, D. (2006), "Data theft at nuclear agency went unreported for 9 months", *New York Times*, June 10.

Thomson, K.L. and Solms, R.v. (2006), "Towards an Information Security Competence Maturity Model", May - *Computer Fraud & Security*, p 11-15.

Thomson, K.L., Solms, R.v. and Louw, L. (2006), "Cultivating an organizational information security culture", October - *Computer Fraud & Security*, p7-11

Trček, D. (2003), "An integral framework for information systems security management", *Computers & Security* Vol 22, No 4, pp 337-360.

Valentine, J.A., (2006), "Enhancing the employee security awareness model", *Computer Fraud & Security*, June, 17-20.

Walton, R., "Balancing the insider and outsider threat", *Computer Fraud & Security*, November 2006, p 8-11.

Ward, P., Smith, C.L., (2002), "The Development of access control policies for information technology systems", *Computer & Security*, Vol 21, No 4, pp356-371.