A Framework of Information Security Integrated with Human Factors

Ahmed I. Al-Darwish and Pilsung Choe(✉)

Department of Mechanical and Industrial Engineering,
Qatar University, Al Tarfa, Doha 2713, Qatar
aal709549@student.qu.edu.qa, pchoe@qu.edu.qa

Abstract. Information systems support organizations to achieve strategic competitiveness over other organizations and assist senior management in the decision-making process. In addition, they help organizations in timely implementation of projects and effective risk management. A reliable and coherent Information System requires a solid security framework that ensures Confidentiality, Integrity, Availability, Authenticity and Auditability of the critical information assets; therefore, managing security is essential for organizations doing business in a globally networked and competitive environment whilst seeking to achieve their objectives and goals and ensuring the continuity of business. This paper provides an integrated framework that classifies and holistic view of challenges in Information Security Systems, and their interrelationships. The framework is expected to provide a basis that can be used to evaluate individual organizational members' behavior and the adequateness of existing security measures.

Keywords: Information security management · Information security culture · Human factors · Organizational factors · Technological factors · Security challenges · Organizational security

1 Introduction

Uncertainty and risks are growing due to increased dynamic, complex and interrelated economy and enhanced threats from a wide range of forces, such as financial instability, political movements and terrorism, societal requirements, extreme nature events due to climate change, cyber-attacks and others. In the past years there were different low-probability and high-impact events, Black Swan events [1, 23], which are almost impossible to forecast (e.g., drought, earthquake, floods, cyber-attacks). Depending on how uncertainty is handled, it can become opportunity or threat. Traditionally, organizations managed risks in "silos" [13, 14, 23], such as finance, market, compliance, regulation, human resources, innovation, Information Security and others. But risks interrelate in a cybernetic way. Recently organizations adopt more comprehensive approaches and aggregate the results of the different risk assessments into an organization-wide risk profile [4, 12, 15, 23, 30].

Organization must protect their information assets from unauthorized access and quickly resume business activities after a security breach. It is necessary to broaden the

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 217–229, 2019.
https://doi.org/10.1007/978-3-030-22351-9_15

study of Information Security risk to include not only the technical, but also the non-technical issues [10, 12, 16, 21, 23].

To date, studies have shown that non-technical risks are as important as technical risks in safeguarding an organization's sensitive information and in addressing Information Security management strategies or issues [17–19, 22]. However, little attention has been paid to the role of human factors (e.g. individual choice and behavior) or to organizational factors such as national and organizational culture, environment, and levels of Information Security awareness, and how these factors relate to attitudes about Information Security and its management.

For a long time, Information Security was seen as a technical job and an integral part of the IT department. Corresponding frameworks start at the process level and go down through all technical levels accordingly an IT enterprise architecture approach [23]. Despite the common goals of Information Security and enterprise risk management, we found no systemic framework for extending Information Security management to enterprise risk management. In addition, although there have been studies of specific challenges of Information Security management [1, 6, 7, 20] or sets of challenges along one of the factors, none have provided a comprehensive integrated overview of the challenges faced by Information Security management. A better understanding of how different human, organizational, financial and technological elements interplay could explain how different factors lead to sources of security breaches and vulnerabilities within organizations [5, 8, 20].

This paper provides an integrated framework that classifies and holistic view of these challenges, and their interrelationships (Fig. 1). This framework can help organizations identify their limitations with respect to implementing security standards and determine if they are spending their security resources effectively. It also provides a way to understand how different factors interplay. The integrated Information Security framework described in this paper will provide a sound basis that can be used to evaluate individual organizational members' behavior and the adequateness of existing security measures [20, 22, 25–27].

2 Social Engineering

A major concern within Information Security is the threat of Social Engineering Attacks. Social engineering attacks are made to collect sensitive information, and this information is often used maliciously. Social Engineering Attacks can cause a great deal of disruption to business activities and create financial, social and technical mayhem. Their impacts can extend beyond geographical borders and organizational boundaries. Therefore, dealing with Social Engineering Attacks would be in a great interest of any organization. Janczewski and Fu (2010) identified five main causes of Social Engineering Attacks: people, lack of security awareness, psychological weaknesses, technology and defense and attack methods and provided a conceptual model in order to understand the impact of Social Engineering Attacks on individuals and businesses and present a defensive approach to mitigate these risks [14].

According to the Verizon Report of Data Breach Investigation Report (2016), human factors are a main source of successful attacks, even using the latest security

techniques and protocols, most information systems still face numerous security breaches. Human factors are at the heart of the vast majority of security breaches, however, human factors in Information Security are very complex to define because, they are intertwined with organizational culture and individual perceptions and characteristics. Providing a global solution to Information Security is a big challenge in the organizational context. Therefore, this paper define human factors as one of the major components responsible for inadequate Information Security and risk to organizational assets [14].

3 Human Factors in Information Security

People work falls into four categories: individual, team, management and customer/interested party. Human factors within these categories can become uncontrollable forces, because people have different perceptions of security, and their reactions to Information Security procedures are diverse and highly subjective and hard to measure. People have their own culture, attitudes, skills, knowledge, understandings, behavior and interests that depend upon the role that they play within the organization. Individuals' interaction with computers and decisions made with regard to Information Security are certainly very dynamic and complex issues. We can classify human factors into direct and indirect human factors based on the directness of the impact on the Information Security System [31].

3.1 Direct Human Factors

Direct human factors are based on individuals who have a direct impact on the overall Information Security System. These individuals are involved in an organization's efforts to meet its goals and objectives. They are also social entities within the Information Security System and cannot be measured using a technical approach. A socio-technical approach enables these entities to be defined in an Information Security System and is constructed upon social and technical sub-systems alike. These direct human factors include errors, usability, security awareness, training and education, skills, experience, employee engagement, incentive and disincentive policies, ignorance and negligence, and stress as follows [14]:

Errors: Swain and Guttman (1983) distinguish five different types of human factor errors, which can be used to explain Information Security breaches. First, there are acts of omission, in which people forget to perform a necessary action. For instance, in an Information Security domain, this could involve the failure to regularly change passwords. Second, errors are commonly acts of commission, in which people perform an incorrect procedure or action, such as writing down a password. Third, a number of errors are caused by extraneous acts, which involves doing something unnecessary. Fourth, errors can be caused by sequential acts, which involve doing something in the wrong order. Finally, time errors, caused by people failing to perform a task within the required time [16].

Usability: There is a trade-off between security and usability. According to Wilde (2001), there are four motivating factors that influence this trade-off between security and usability. Users are influenced by the expected costs and benefits associated with the risky behavior, and the expected costs and benefits associated with the safe behavior. Hence, if the potential gains associated with undertaking a risky activity are quite high, or if the adherence to a security system is a great inconvenience, then people are less likely to obey the policy, and are more likely to take risks. This is supported by Schneier (2003), who indicates that an understanding of the trade-offs associated with security is essential. Similarly, the security of information technology could be greatly improved through a drastic reduction in users' access and privileges. However, people are unlikely to tolerate such stringent restrictions, and it is therefore necessary to find an adequate balance between security and usability [16].

Security Awareness, Training and Education are some of the most effective countermeasures against the human factor threats to Information Security. According to the National Institute of Standards and Technology (NIST) report on security awareness and training, "learning is a continuum; it starts with awareness, builds to training, and evolves into education". The goal of awareness is to ensure that individuals are aware of potential IT security concerns and know how to recognize and react to such concerns. Training goes a step beyond this and aims to produce the required security skills and competencies. The aim of education is to integrate those security skills and competencies into a body of knowledge, and education "strives to produce IT security specialists and professionals capable of vision and pro-active response" [16, 27, 28].

Besnard and Arief (2004) emphasize the education of staff, stressing that although education may not alter behavior on its own, education makes people aware of the consequences of their actions. It ensures that individuals are conscious of the threats and the potential damages that can result from insecure behaviors.

Skills are one of the main forces in dealing with Information Security issues such as incident response. The absence of adequate and appropriately skilled staff contributes to a weak performance of Information Security policy. Employees are required to possess adequate skills to deal with the requirements of Information Security policy. Education and training are crucial in developing skills and demonstrating a commitment to preserve professionalism and competency [14, 25, 27].

Experience: Scholars have different views on the factor of experience with respect to the Information Security System. Some argue that people's understanding of Information Security procedures relies upon a few human factors, including their experience, whilst some go further and claim that a successful implementation of an Information Security System depends greatly on people's knowledge and experience. Although there is disagreement on the level of influence the factor of experience has, both sides would not deny its important role [14, 25, 27].

Employee Engagement in an organizational context can be seen as the unwillingness of employees to contribute to the achievement of the organization's goals and objectives in situations where they should demonstrate pro-social behaviour. Disengagement will lead to apathy, which creates significant issues in organizations due to a lack of

willingness to implement organizational security policies and procedures. It creates an environment in which employees believe they have no responsibilities. Whereas a positive attitude, motivation and optimal working conditions contribute to better performance. Alavi (2016) argues that positive attitude serves the effectiveness of a security system; and the miscommunication between employees and senior management contributes to misunderstanding that leads to employee apathy [14].

Incentive and Disincentive Policies in organizations reward good behaviour and punish bad attitude. There are certain connections between people's attitudes and incentive and disincentive policies; even a little persuasion invariably increases motivation. Kabay (2002) argued that even a simple comment on Information Security policy made by an employee should be considered seriously, considering how it can ultimately affect the entire Information Security System in an organization. This factor has an impact on people's motivation to go along with Information Security policies. Organizations sometimes focus on punishment when instead they should divert their attention towards training and reward policy [14].

Ignorance and Negligence: Employees in organizations, sometimes unintentionally, do not pay enough attention to security policy. One example of user negligence and ignorance is when software piracy occurs because employees have little knowledge of software installation for various reasons such as a lack of training. The impact on an Information Security as a result of ignorance or negligence requires decisive action and must be addressed by Information Security professionals. Organizations pay far more attention to reinforcing technical facilities to overcome this issue, but ignorance and negligence are human issues and must therefore be confronted differently [14].

Individuals' stress in corporations can be caused by heavy workloads and tight project deadlines. People react maladaptive to stress and work overload despite any training programs they may receive. Stress leads to human error. Those under stress may tend to bypass Information Security policies. Stress and fatigue have a direct relationship to Information Security vulnerabilities [14, 25].

Security behavior can be described using a two-factor taxonomy, where the two factors are intentionality and technical expertise, which creates six categories of security behaviors, where two of those behaviors (Aware Assurance and Basic Hygiene) are positive, designed to increase security, and four of the behaviors may result in breaches to security. Intentional Destruction covers the actions of malicious insiders, who have technical expertise and the intent to do harm, whereas Detrimental Misuse involves personnel who have malicious intent, but lack technical expertise. Dangerous Tinkering covers behaviors that require technical expertise, but where there is not an intention to do harm. Perhaps the most common behavior, which will be covered in the most detail in this report, is Naïve Mistakes, in which individuals with low expertise and without malicious intentions perform an action which was not intended to harm the organization, but yet could result in a security breach.

3.2 Indirect Human Factors

Indirect factors have a certain influence on direct factors, as well as on Information Security System. However, these factors affect people through elements that are largely controlled by organizations and which individuals have no jurisdictional power over; therefore, these factors are collective matters managed by organizations. These indirect human factors include budget, return on investment, culture, Information Security and safety climate, communication, security policy enforcement, management support, Information Security business dashboard, risk perception and information processing biases and audit and compliance process as follows [14]:

Budget: Information Security experts widely believe that budgets have a significant impact on the efficiency of Information Security System. To ensure that an Information Security System fulfils its objectives effectively, organizations must have an effective cost strategy, which should be adopted for addressing the technical and personal requirements of the Information System. For instance, organizations will not be able to deal with Information Security System goals sufficiently if an access control mechanism has not been implemented or if employees have not been receiving adequate training. The importance of training emerges when the element of cost effectiveness is highlighted. Some measures to reduce cost, such as automated user access provisioning, require training programs that are less costly. This demonstrates the relationship between budget planning and direct human factors [25].

Return on Information Security Investment: Security cannot tolerate any performance delays in protection mechanisms and requires extra attention to ensure its success and at the lowest possible cost. Cost and urgency in organization's procurement processes thus become a priority, especially dealing with security requirements. Nevertheless, the way security is designed and implemented varies from one organization to another and depends upon the nature of the business, organizational culture and how the business risk management approach is adopted [24]. Information Security management systems are now increasingly based on economic principles such as cost-benefit analysis. Balancing Information Security costs and benefits is essential for organizations. However, organizations will invest in Information Security to a greater extent if the cost of investment is less than the cost of potential risk [14, 25, 27].

Culture: Organization's culture has a strong impact on organizational security. In order to understand security culture, it is important to have a grasp on the wider literature of organizational culture. Culture is defined differently, measured differently and evaluated differently. Schein's model of culture consists of three levels: artifacts and creations, values and beliefs, and basic assumptions. Artifacts and creations comprise the first level and represent the most visible and apparent aspects of an organization. According to Schein (1985), this level includes the elements of culture that can be seen and heard and easily interpreted by employees, customers and the public, including furniture and clothing, symbols, objects, the language used within the workplace, as well as slogans, rituals and stories [32]. The second level of culture comprises values and beliefs that underpin artifacts and creations. Values are the wants and desires that guide behavior; they are devised by senior management to provide

direction and guidelines for the behavior of their employees. Third level of culture, basic assumptions, which represents and captures an organization's culture. Basic assumptions are hidden, elusive and invisible, making the core concepts of culture difficult, not only to understand, but also to assess. These basic assumptions include the "assumptions individuals hold about the organization and how it functions, they relate to aspects of human behavior, the nature of reality and the organization's relationship to its environment" [32]. Culture evolves and develops over time and this complexity is a contributing factor to the debate over what the construct of culture represents [16, 27].

Information Security and Safety Climate: The concept of organizational climate is similar to that of organizational culture. Organizational climate is a concept that is described as "shared perceptions of organizational policies, practices, procedures, both formal and informal". The constructs of culture and climate do overlap and share many similarities. They are both used to explain the ways in which individuals make sense of their work environments. Both concepts stress that culture and climate are learned through socialization and interaction with others. Importantly, both attempts to "identify the environment that affects the behavior of people in organizations". Parsons (2010) identified eight dimensions of a safety climate: the importance of safety and training, the effects of safe conduct on promotion, the effects of required workplace safety, the effects of safe conduct on social issues, the management's attitudes towards safety, the level of risk in the workplace, the status of safety officer and the status of safety committee. All eight dimensions are based on employee perceptions of their workplace environment [16].

Chan and colleagues (2005) found a relationship between safety climate and Information Security compliance behaviors. Their findings show that compliant behavior in Information Security is influenced by both organizational factors and personal factors. The overall results suggest that compliant behaviors can be increased by promoting self-efficacy, ensuring that there is a positive perception of Information Security climate, and ensuring that all levels of the organization (co-workers, supervisors and upper management) apply security guidelines to their everyday behaviors. Essentially a positive relationship between safety climate and employee behavior will more than likely improve the level of Information Security within an organization [16, 25].

Communication: O'Neill (2004) describes risk communication as: *"An interactive process of exchanging information and opinions between stakeholders regarding the nature and associated risks of a hazard on the individual or community and the appropriate responses to minimize risks".*

The manner in which Information Security is communicated can strongly influence how it is interpreted and whether it is then acted upon. Communication is far more likely to be effective if there is an adequate understanding of the gaps in current beliefs, and a clear and concise message of what the target audience needs to know [29]. Evidence also suggests that aspects of individuals' personality or cognitive style are likely to influence the manner in which they respond to information regarding risk. Finally, the effectiveness of risk communication could be increased if the message is framed towards the various cognitive styles, with different messages for different styles [16, 27].

Security Policy Enforcement: A security policy is an organizational document in which the Information Security procedures and rules are outlined. Employees at all levels of the organization must understand the security policy and participate in its implementation according to their position [1]. Enforcing a security policy is a major issue for an Information Security System and its successful implementation should be supported by management. Network security, access control, IT personnel job descriptions and password policy are examples of factors that are required to be covered by security policy [14, 25].

Management Support: To enforce policies relating to the Information Security in organizations, management must support it from the design stage through all evaluation stages. The role of management in an Information Security System is not only to advocate but also to deliver a clear message of Information Security policy to the rest of the organization. An obvious example of management endorsement of an Information Security System in organizations is the allocation of an adequate budget, which is entirely under the control of senior management. The general perception of senior management is that an Information Security System is entirely the responsibility of an IT department, who should ensure the installation of appropriate and adequate software systems to preserve the security of information [14, 25].

Information Security Business Dashboard: Information Security management and business decision-making are intimately interconnected with risk management. Executive boards require an understanding and monitoring of the risks that have the potential to obstruct their organization's ability to achieve its goals. These risks are characterized by Key Risk Indicators (KIRs), which stem directly from the organization's long-term strategy. The Business Intelligence Dashboard (BID) guides organizations towards a suitable information security posture whilst providing answers to key questions often raised by executives. Providing a meaningful BID for organizations and their senior executives helps them to receive some extended analytical insights on security metrics and Key Security Performance Indicators (KSPIs), a non- technical method that can be grasped by non-technical senior executives [14, 25].

Risk Perception and Information Processing Biases: When making behavioral decisions, individuals will often decide based on their estimates of the risks associated with the various options. Hence, the manner in which IT users perceive threats will influence their behavioral responses [27]. People often take shortcuts in the decision-making process, by using a number of information processing biases and heuristics to simplify the task. These biases and heuristics can affect risk perception, and evidence suggests that people generally have an inaccurate perception of risk [29]. Although there is a great deal of research in risk perception in general, there is little empirical study examining individuals' perceptions of risk within the Information Security domain. Huang and colleagues (2007) concluded that perceptions of Information Security risks could be described using six factors, namely knowledge, impact, severity, controllability, possibility and awareness. A few other authors have inferred perceptions of security risks from research in other areas. For example, Pattinson and Anderson (2005) suggest that perceptions of security risks are generally influenced by factors such as the individuals' mood at the time, recent media reports, past experiences, and knowledge of

technical aspects, such as viruses. A few psychological, social and cultural factors can also affect the way that people perceive risk [16].

Audit and Compliance Process: It is not all that difficult to discover risk exposure gaps, or improvement opportunities. Neither is it that difficult to implement some solutions to address these. The trick, however, is that closing a gap improperly can sometimes be worse than not closing it in the first place. By "closing" a gap one can gain a sense of misplaced confidence and security that may in fact be more damaging than recognizing that a gap still exists and needs to be cautiously managed. What's worse is that improperly/inadequately closing gaps uses up resources and introduces additional variation potentially further destabilizing processes. The lesson here is to focus more on the quality of gap closure and improvement, rather than quantity.

4 Conclusion: Integrated Framework

The Information Security framework is based upon the conceptual understanding of an Information Security System within an organizational context and its integration with other concepts such as security incident, risk, technical and non-technical factors and return on investment within an organizational setting. All these concepts are necessary to determine the adequate and appropriate level of control mechanism required to effectively address risks to information assets through effective Information Security framework. The conceptual Framework address the Information Security from four angles: Business, Enterprise Risk Management, Technology & Human. These four elements are most relevant to achieve a balance between Information Security goals and organizational goals, as a defiance mechanism against attackers' goals and Human Factors [2, 9].

An effective Information Security System depends as much on knowledge of the business as on software architecture. Security professionals require the translation of business requirements and goals into an Information Security System solution capable of meeting those goals and requirements. This also extends to technology, human factors and the specific use of processes that should be aligned with business objectives and security goals. An organization's business goals and IT strategy are two factors that most influence the adoption of security countermeasures. Technology, risks and critical human factors all provide sources for Information Security System requirements (Fig. 1) [9, 11].

The risks and human factors from the business domain are mapped to the functions and objects of the Information Security System. The business processes and functions are understood through IT, which aggregates one or more functions from the Information Security System. The direct and indirect human factors identified include: Errors, Awareness, Skills, Experience, Ignorance and Negligence, Stress, Budget, Culture, Communication, Security Policy Enforcement, and others. These have been mentioned in many academic and professional reports as the source of Security Incidents; this is because they have direct and substantial impacts on Security Incidents [3, 25].

Tools and strategies are essential in keeping organizations cost effective whilst Information Security professionals endeavor to demonstrate the value of and Return on

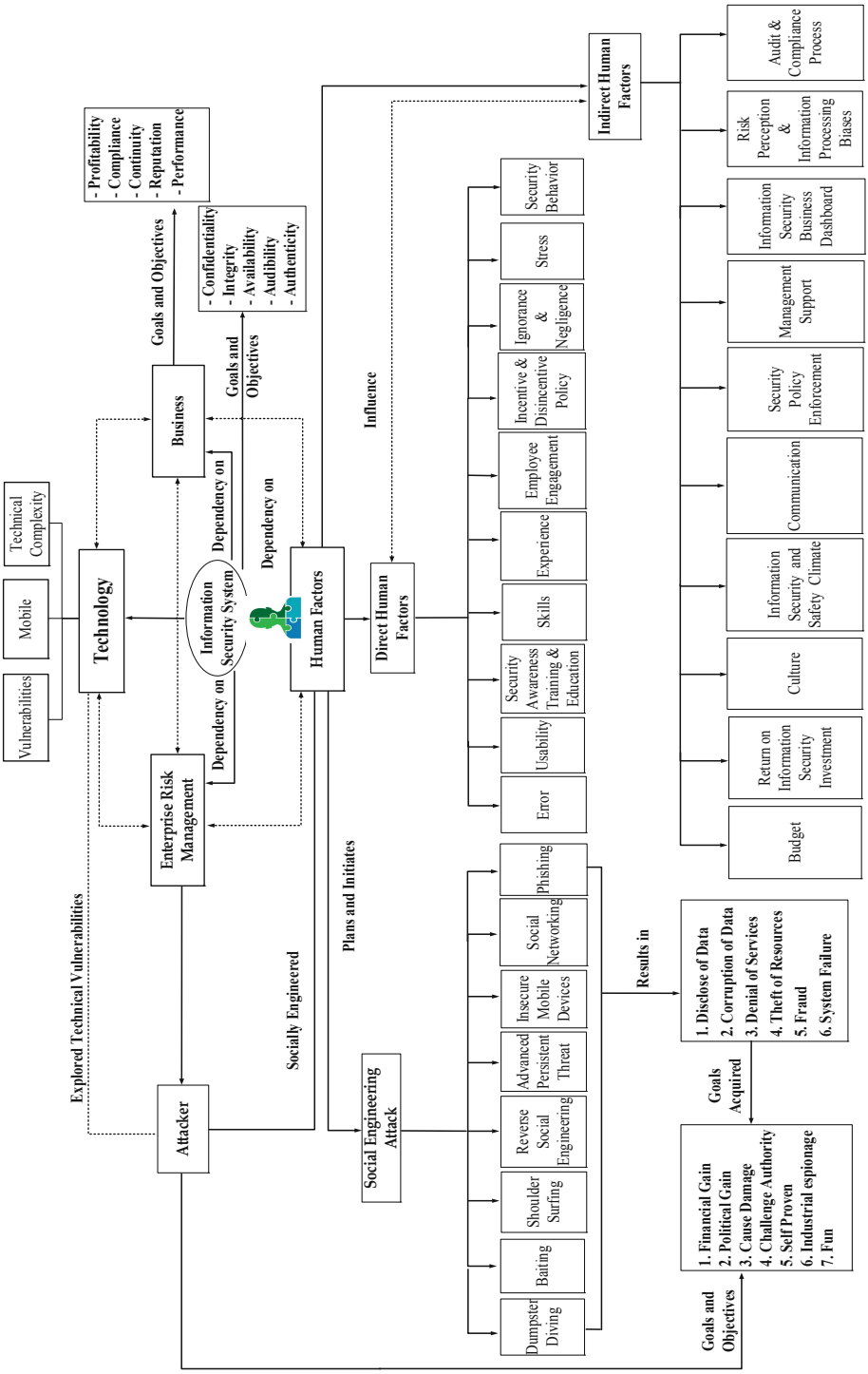

Fig. 1. The integrate information security system framework

Information Security Investment. Information Security Systems research literature indicates that there is a clear relationship between investments in Information Security System and enhanced organizational performance. Available tools and methods allow organizations to calculate and analyze the financial impact of a specific security control but cannot be used to analyze the cost-benefit of other factors such as critical human factors. Information Security management systems are now increasingly based on economic principles such as cost-benefit analysis [25].

Effective risk management practice forms the core of an organization's Information Security System. The risk management process is about identifying, analyzing, evaluating and treating risks and sets the stage for protecting organization's assets. An Information Security System combines business, socio-technical and technology concepts, including critical human factors, risks and investment, at every phase of development. Thus, Information Security System are affected by multidimensional factors during the course of their design, implementation and evaluation. Consideration of the influence of critical human factors, risks and security investment in meeting the goals should be given to construct a more consistent and reliable risk assessment methodology.

This study provides a perspective understanding of the role of human factors in relation to Information Security risks based on a literature review. Our study will continue to validate the applicability of the Information Security framework based on quantitative analyses using real security breach incident data in an industry in Qatar.

References

1. Audestad, J.: Four reasons why 100% security cannot be achieved. Telektronikk **1**, 38–47 (2005)
2. Johan, N., Rossouw, S.: Understanding Information Security Culture: A Conceptual Framwork: Centre for Information Security Studies. Nelson Mandela Metropolitan University, South Africa (2000)
3. Adele, V., Jan, E.: An information security governance framework. Inf. Syst. Manage. J. **24**, 361–372 (2007)
4. Kankanhalli, A., Teo, H.-H., Tan, B.C., Wei, K.-K.: An integrative study of information systems security effectiveness. Int. J. Inf. Manage. **23**, 139–154 (2003)
5. Koskosas, I.V., Paul, R.J.: The interrelationship and effect of culture and risk communication in setting internet banking security goals, New York, NY (2004)
6. Kraemer, S., Carayon, P.: Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. Appl. Ergon. **38**, 143–154 (2007)
7. Ernst, Young.: Into the cloud, out of the fog, Ernst & Young's 2011 Global Information Security Survey. http://www.ey.com/Publication
8. Siponen, M., Oinas-Kukkonen, H.: A review of information security issues and respective research contributions. SIGMIS Database **38**(1), 60–80 (2007)
9. Rodrigo, W., Kirstie H., Konstantin, B.: An integrated view of human, organizational, and technological challenges of IT security management, University of British Columbia (2008). www.emeraldinsight.com/0968-5227.htm

10. Kirstie, H., David, B., Rodrigo, W., Kasia, M., Gagne, A., Konstantin, B.: Human, Organizational, and Technological Factors of IT Security, Florence, Italy (2008)
11. Salahuddin, A., Karen, N., Kavoos, M.: Information security culture: a behavior compliance conceptual framework. School of Management, Queensland University of Technology, Brisbane (2010)
12. Margareth S.: Information security management to enterprise risk management. In: Sobh, T., Elleithy, K. (eds.) Innovations and Advances in Computing, Switzerland (2015)
13. Margareth, S., Michael, F., Ruth, B.: Information management for holistic, collaborative information security management. In: Sobh, T., Elleithy, K. (eds.) Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering, vol. 151. Springer, New York (2013). https://doi.org/10.1007/978-1-4614-3558-7_17
14. Alavi, R., Islam, S., Lee, W.: A Risk-Driven Investment Model for Analyzing Human Factors in Information Security, The University of East London, Computing and Engineering (2016)
15. Werlinger, R., Hawkey, K., Beznosov, K.: Human, Organizational and Technological Challenges of Implementing Information Security in Organizations, University of British Columbia (2008)
16. Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L.: Human Factors and Information Security: Individual, Culture and Security Environment. Defense Science and Technology Organization (DSTO-TR-2484) (2010)
17. Chan, M., Woon, I., Kankanhalli, A.: Perceptions of information security at the workplace: linking information security climate to compliant behavior. J. Inf. Priv. Secur. **1**(3), 18–42 (2005)
18. Huang, D., Rau, P.P., Salvendy, G.: A survey of factors influencing people's perception of information security. In: Jacko, J. (ed.) Hum.-Comput. Interact. Part IV. Springer, Heidelberg (2007)
19. ISO: ISO/IEC 17799 Information technology - Security techniques - code of practice for information security management. Second edition 2005-06-15. Reference: ISO/IEC 17799-1:2005(E). pp. 1–115 (2005)
20. Needle, D.: Culture at the level of the firm: organizational and corporate perspectives. In: Barry, J., Chandle, J., Clarck, H., Johnson, R., Needle, D. (eds.) Organization and Management: A Critical Text. Business Press, London (2000)
21. O'Neill, B.: Developing a Risk Communication Model to Encourage Community Safety from Natural Hazards. Paper Presented at the Fourth NSW Safe Communities Symposium, Sydney, and NSW (2004)
22. Reichers, A.E., Schneider, B.: Climate and culture: an evolution of constructs. In: Schneider, B. (ed.) Organizational Climate and Culture. Jossey-Bass Publishers, San Francisco (1990)
23. Richardson, R.: 2007 CSI Computer Crime and Security Survey. Computer Security Institute, Ritov (2007)
24. Schein, E.H.: Organizational Culture and Leadership. Jossey-Bass, San Francisco (1985)
25. Schultz, E.: The human factor in security. Comput. Secur. **24**, 425–426 (2005)
26. Swain, A. D., Guttman, H. E.: Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278, Washington, D.C. (1983)
27. Van der Pligt, J.: Risk perception and self-protective behavior. Eur. Psychol. **1**, 34–43 (1996)
28. Wilson, M., Hash, J.: Computer Security: Building an Information Technology Security Awareness and Training Program. Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8933 (2003)
29. Janczewski, L.J., Fu, L.: Social engineering-based attacks: model and New Zealand perspective. In: 2010 International Multiconference on Computer Science and Information Technology, pp. 847–853. IEEE, October 2010

30. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Inf. Manage. Comput. Secur. **8**(1), 31–41 (2000)
31. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of IT security management. Inf. Manage. Comput. Secur. **17**(1), 4–19 (2009)
32. Wilde, G.J.S.: Target Risk 2: A New Psychology of Safety and Health. PDE Publications, Toronto (2001)