Journal of Theoretical and Applied Information Technology
20th August 2015. Vol.78. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A COMPREHENSIVE HUMAN FACTOR FRAMEWORK FOR INFORMATION SECURITY IN ORGANIZATIONS

[1] AREEJ ALHOGAIL, [2] ABDURRAHMAN MIRZA, [3] SAAD HAJ BAKRY

College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia.

[1] Alhogail@ccis.imamu.ed.sa, [2] amirza@ksu.edu.sa, [3] shb@ksu.ed.sa

ABSTRACT

Human factor represent an essential issue in the security of information in organizations, as human factor determine the behavior of the employees toward information security. This paper attempts to integrate related human factors, recognized by previous work, into a structured comprehensive framework. The framework has four main domains that take the form of a diamond. Two domains are concerned with the environment and management issues representing an organization dimension; while the other two are related to preparedness and responsibility issues giving an employee dimension. The domains at the four corners of the diamond interact with one another influencing the human behavior toward information security. Expert views on the framework have been collected through a survey that addresses the importance of its various components to human behavior. The framework provides a base for the future investigation of information security protection in organizations, and the development of controls for this purpose.

Keywords: *Human Factor; Information Security; Human Behavior; Information Security Controls; Insider (Employee) Threats.*

1. INTRODUCTION

This introductory section has three main parts. It presents the subject of the paper, and emphasizes its importance. This is followed by a review of the literature associated with the topic considered. The work described by the paper is then introduced.

1.1. The Human Factor in Information Security

Information security is not a purely a 'technical' issue; it is also an issue associated with 'people'. Using only traditional technical approaches are no longer enough and suitable; as the traditional approaches focuses into technical fixes, which are not suitable to the dynamic nature of organizations today [1]. Security controls often require some form of human involvement that is very important in the information security process [2] and strategic decisions should be taken to ensure that users are aware of the aspects of information security. Human factors such as knowledge skills and personality can impact on the behavior of employees when interacting with information.

There are common security risks and threats to the information assets, nonetheless, the users of a system can be the biggest enemy [3] and can cause serious risks despite the amount of money spent on the technical measures and on security related products [4]. The effectiveness of these technologies lies in the behaviors of the humans who access, use, administer, and maintain information resources [5]–[7]. In addition, this human dimension of information security cannot thoroughly be solved by procedural and technical measures regardless of the effectiveness of these measures.

The human factor can be considered as one of the most significant vulnerability; but unfortunately, it is often left unaddressed [8]. Organizations will not be able to protect the integrity, confidentiality, and availability of information assets if they ignore the human factor. In most organizations, managing information security threats focuses on managing technology and process, but little efforts are paid at managing people. A study by Ashenden [9] reaches that the human factor of information security management has largely been neglected. In fact, a small number of publications have actually addressed the human aspect of information security [9]–[11].

1.2. Literature Review

Human behavior represents the weakest link in the security chain [12]–[14]. Focusing on the technical aspects of security, without appropriate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

consideration of how the human interaction with the system is evidently inadequate [15]. Studies revealed that a significant emerging threat to information security is from the employees themselves [16], [17]. This 'insider human-related threat' is one of the greatest information security challenges that organizations face and one of the hardest to protect against [5], [16]. These incidents based on severity could cost organization from few lost employees hours to negative publicity or even financial damage.

Numerous surveys continue to suggest that employees' misuse, errors or damage could have devastating effects on an organization's overall well-being [17]. The [18] revealed that 58% of large organizations suffered insiders related security breaches. Also, 36% of the worst security breaches in that year were caused by unintentional human error. Introducing mobile networks and cloud computing has also presented more security risks to the organization information assets. To illustrate, employees carry sensitive data on mobile laptops, smart phones and USBs which when lost or stolen could compromise the data. Even though, many organizations have no plans to deploy relevant countermeasures to avoid threats posed by humans, 46% of organizations surveyed in 2014 have not provided any current security awareness and training to their staff [18]. This highlights the vital need for organizations to adopt security solutions that address the human factors.

Insider threat refers to "intentionally disruptive, unethical, or illegal behavior performed by individuals who possess internal access to the organization's information assets" [5]. Moreover, insider threats could also include unintentionally disruptive actions from individuals who have internal access to the organization's information assets [8]. The human that should be considered are all the individuals in the organization who have access to information, from top-level managers to clerical staff; whether a current employee or an ex-employee.

Humans are usually difficult to manage in the context of information security. In fact, humans are not very predictable because they do not operate as machines where if the same situation happened they will operate in the same way, time after time. Human challenge lies in accepting that individuals in the organization have personal and social identity (i.e. unique attitudes, beliefs and perceptions) that they bring with them to work as well as their work identity conferred by their role in that organization [19], [20]. While information security management activities comprise processes and procedures, it seems that there are a number of critical human factors ensure that secure environment is developed and maintained [8].

One of the major concerns facing the security of the organization's information is the lack of skills, knowledge, and commitment by employees when it comes to the protection of information [8]. Dhillon & Backhouse [21] mentioned that users have developed 'security blindness' with their daily interaction with information assets. Nevertheless, individual attitudes, perceptions and core values could be changed to achieve a secure environment to the organization's information assets and to a successful information security management. Thomson et al. [8] assumed that well trained and conscientious employees can form the strongest link in any organization's security infrastructure.

As a response to insider human posed risks, many organizations have implemented a range of administrative and technical measures within an overall information security management system that is based on policies, procedures and practices [22]. However, there is a lack of structured frameworks that provide a reference guide to practitioners of the human factors that should be considered to eliminate the insiders' threat. This is the main concern of this paper.

1.3. The Presented Work

The purpose of the work presented in this paper is to provide a comprehensive framework of the human factor issues that can influence employees' behavior toward information security in organizations. The framework is based on collective previous studies associated with the subject and on the social cognitive theory. It is structured in two dimensions, four domains, and eleven subdomains. Experts' views on the importance of the various components of the framework are collected through a survey that validates the framework. The framework provides a base for the future investigation of information security protection in organizations, and the development of controls for this purpose.

2. THE PROPOSED COMPREHENSIVE FRAMEWORK (HUMAN FACTOR DIAMOND: HFD)

This section presents the targeted framework. It starts with the basic structure of the framework, which takes the form of a four-domain diamond, which will be called the Human Factor Diamond (HFD). It emphasizes the scope of the framework in

Journal of Theoretical and Applied Information Technology
20th August 2015. Vol.78. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

accommodating a wide scope of factors associated with human behavior. This is followed by describing the details of each of the four dimensions.

2.1. Framework structure

The framework is structured according to two main dimensions, with each dimension having two domains, forming the diamond shape shown in Figure 1. These dimensions and domain are introduced in the following text.

The first dimension is the "organization" dimension, and it is concerned with the following two domains:

- The "environmental" domain, which is mainly related to cultural and regulation issues.
- The "management" domain, which is mainly concerned with security policy, practice, and direction and interaction issues.

The second dimension is the "employee" dimension, and it is associated with the following two domains:

- The "preparedness" domain, which is mainly concerned with training and awareness, knowledge acquisition and change of old practice.
- The "responsibility" domain, which is mainly related to employee's practices and performance such as monitoring and control, reward and deterrence, and employee's acceptance of responsibility.

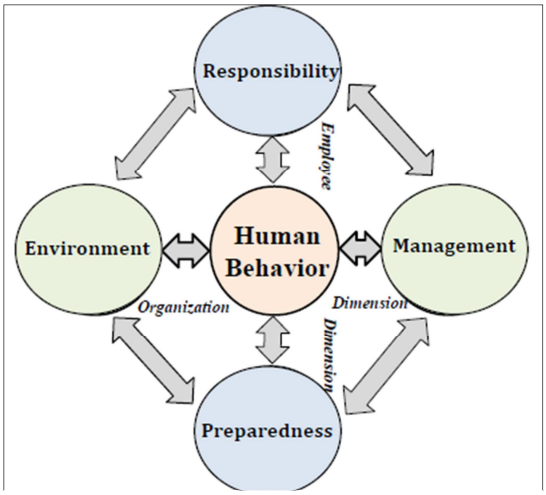


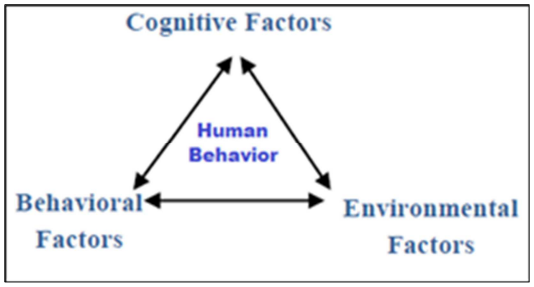
Figure 1 The Human Factor Diamond (HFD) framework

2.2. Framework scope

The framework enjoys a wide scope. This is emphasized here through the following of two main considerations; the Social Cognition Theory (SCT) on the one hand [23]; and with previous various investigations of the human factor in information security on the other hand.

The SCT framework explains how people acquire and maintain certain behavioral patterns and shows that the human behavior is the result of the relationship between behavioral factors, environmental factors and cognitive factors. All factors are interrelated and influenced by each other's in a bidirectional mutual way. The SCT framework is illustrated in Figure 2.

It can be viewed that the HFD domains corresponds to the SCT factors in two main ways. Firstly, the environmental factors of the SCT framework are related to the environment and management domains of the HFD framework (Organization dimension). Secondly, the cognitive and behavioral factors of the SCT framework are related to the employee dimension of the HFD framework that is



to the employee preparedness and responsibility.

Figure 2: The framework of the Social Cognitive Theory (SCT)

This correspondence is emphasized further in Table 1. It enhances the claim of comprehensiveness of the HFD framework.

The claim of HFD framework comprehensiveness is enhanced further by identifying subdomains of its four main domains and mapping factors considered by various previous investigations to these subdomains. The domains and subdomains of HFD framework are given in Table 2 together with references to previous studies that correspond to the various HFD framework subdomains. It should be observed that as shown by

Journal of Theoretical and Applied Information Technology
20th August 2015. Vol.78. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1 Correspondence Between The Human Factors Diamond (HFD) Framework And The Framework Of The Social Cognitive Theory (SCT)

HFD			SCT Factors
Dimensions	**Domains**	**Examples of issues**	
Organization dimension	**Environment**	Social norms; culture; rules; standards; and practices	**Environmental**
	Management	Security policy; commitment; interaction	
Employee dimension	**Preparation**	Awareness; knowledge; training; perception.	**Cognitive & Behavioral**
	Responsibility	Commitment; Practices; skills; performance;	

Table 2 Table 2 2Issues Of Human Factors Considered By Previous Studies And Integrated As Subdomains Into The HFD Domains

HFD Dimension: *Domain*	**Human Factor**	**Examples of previous studies**
Organization: *Environment*	National culture	Alumaran et al. (2015), Alfawaz et al. (2010), Alnatheer & Nelson (2009).
	Organizational culture	Soltanmohammadi et al., (2013), lacey(2009), Da Veiga & Eloff (2010) , Leach (2003), Von Solms (2006) and Zakaria (2006)
	Standards and regulations	Da Veiga & Martins (2015)Alfawaz et al. (2010), Dojkovski et al. (2010)
Organization: *Management*	Security policy	Soltanmohammadi et al., (2013) , Hu et al. (2012), Cappelli et al. (2009) , Colwill (2009), Goh (2003), and Whitman & Mattord (2010)
	Practice	Goh (2003), Leach (2003) , Ruighaver et al., (2007), lacey(2009), and Soltanmohammadi et al., (2013)
	Communications	Koskosas et al. (2011), Hu et al. (2012), and Ruighaver et al., (2007)
Employee: *Preparedness*	Awareness and training	Soltanmohammadi et al., (2013) , Stanton el al. (2005), Colwill (2009), and Goh (2003)
	Change	Da Veiga & Eloff (2010), lacey(2009), Colwill (2009), and Goh (2003)
Employee: *Responsibility*	Employees' acceptance	Van Niekerk (2010), Goh (2003) and Leach (2003)
	Monitoring & control	Cappelli et al. (2009), Colwill (2009), and Goh (2003)
	Reward & deterrence	Soltanmohammadi et al., (2013) , Leach (2003), Knapp et al. (2006), and Whitman & Mattord (2010)

Table 2, some previous studies were concerns with proposing some human factor that correspond to subdomains of the HFD framework. The right column lists the studies that cited the human factor on left column. The factors are listed without specific order. The selection criterion was that the human factor must be supported by at least two studies.

2.3. The "environment" domain

The organization "environment" domain has been divided into three subdomains; and for each of these subdomains a number of elements have been considered according to the following:

- The "natural culture"
- The "internal security culture"
- The "standards and regulations"

Employees tend to behave as what they see more than as what they are told; therefore, in most cases, an informal norm like culture is more important than formalized norms like policies [26]. Researchers suggest that that information security culture has a serious impact on employees' information security behavior and it is possible to manipulate informal norms in order to reduce internal threats [20]. It has been recognized that organizational culture may be a key critical lever by which managers can direct and influence and the action of their employees [16].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Usually, national culture determines organization's members' values and beliefs as it influences how people view their duties and interact with others, and define the acceptable and the unacceptable behavior [24], [27]. The process of information security must be compatible with the society ethics and reflects essential society values [25], [28]. . Moreover, the national culture (unchangeable) has been taking into account when designing information security policy and guidelines

Applying a set of security standards and regulations would have a great impact on shaping user security behavior [11], [29]. In addition, employees should be made aware of relevant government information security related legislation.

2.4 The "management" domain

The organization "management" domain has been divided into three subdomains (human factor); and for each of these subdomains a number of elements have been considered according to the following:

- The "practice"
- The "security policy".
- The "communication"

The attitude of the senior management toward security highly affects how employees perceive the importance of information security [16], [26], thus, on their security behavior. Ruighaver et al. (2007) suggested that to achieve better employee security behavior, management support and prioritization of information security should be visibly demonstrated.

moreover, in a study by Goh [31], it has been found that the lack of security policies was rated as one of the top inhibitors to achieving security effectiveness in organizations. 93% of organization where the security policy was poorly understood had employees' related breaches, whereas, it was only 47% where the security policy was well understood [32]. However, it has been found that the only presence of security policies has no impact on the number of incidents or the seriousness of incidents [33]; thus the effectiveness was only related to how well it is developed, implemented and maintained. Moreover, poor implementation of security policies is as bad as the lack of security policies and could place organization information assets at risk [31].

In addition, effective interactions and communications are essential to achieve a mutual understanding about security risks among different stakeholders in the organization [16], [34]. Koskosas et al. (2011) study suggest that communication have a significant role of security management and have an effect on the setting of organizations' security goals. The effective communication has proven to have a great effect on security behavior [30].

2.5 The "preparedness" domain

The employee "preparedness" domain has been divided into two subdomains; and for each of these subdomains a number of elements have been considered according to the following:

- The "awareness and training" human factor.
- The "change" human factor.

Stanton el al. (2005) have documented, in a deep study of 1167 end users, evidence that good password practices were related to training and awareness. They have concluded that with a relatively small increase in security expertise or awareness, naïve mistakes could be avoided. Continuous awareness and training programs help employees to understand security requirements and securities polices documentations; and keep them up-to-date to security risks and various security issues. Security awareness and training programs should include training on technical skills and systems, security policies and standards, security threats, ethical and safe computing practices, and updates on new threats and security topics.

Employees must change their behavior in order to protect information assets [36]. The transition periods could expose the information assets to security risks. To change the behaviors and attitudes of employees, managers must clearly communicate with the employees in order to make them feel that they are part of the change and that change will affect them. Management support, empowerment and great participation of all organization members could help in reducing the resistance to change, thus their information security threats.

2.6 The "responsibility" domain

The employee "responsibility" domain has been divided into three subdomains; and for each of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

these subdomains a number of elements have been considered according to the following:

- The "employee's acceptance of responsibility" subdomain
- The "monitoring and control" subdomain
- The "reward and deterrence" subdomain

The "employee's acceptance of responsibility human factor is affected by the employee's perceptions, norms, values and beliefs. It is also affected by employees' security knowledge. This could be measured in employees' willingness to act according to the interest of organization information security requirement [31]. Van Niekerk (2010) noted that even if the user has the necessary knowledge but views security as an obstacle to performing daily jobs, or as being not important, may behave in insecure manner. Their commitment could also be affected by the degree of difficulty of compliance to security countermeasures even if they understand that they should follow the requirements. IT skills and knowledge has been found to highly affect how employees view security [38]. Employees should view security as an essential element when interacting with information assets [28] . In addition, employees should feel responsible to act in supportive manner to prevent, detect and respond to security incidents.

Employees monitoring and control should be in place to prevent any security risks [36]. Policies, password, and account management system should be implemented to enforce duties separation and different access privileges to information. It is effective in limiting access to information assets that should not be reached. This access limitation plays a major role in reducing the threats posed by insiders [39]. Organization shall have a clear policy and role assignments to achieve an accurate access rights. Continuous monitoring would prevent costly threats to the organization information assets. However, monitoring could contradict with employees' privacy, liberty and responsibility. Therefore, a balance between a security and usability is required.

In reward and deterrence human factor, promoting good user behaviors and constraining bad user behaviors could provide important benefits for information security [5]. Formal procedures for penalty found to be effective in shaping of employees' security behavior. This could be useful to reduce errors, carelessness and negligence and to prevent illegal and unethical activity [40]. Not only punishment, but reward system should be in place [26] as a great way to encourage employees to show a desired healthy security behavior and greater participation in achieving organizational security goals.

The resulting comprehensive framework has two dimensions; four domains; eleven subdomains. The subdomains has been translated into "45" key elements represented as statements. The final structure has been put for experts to review as described in the next section.

3. EXPERTS VIEWS

This section presents views provided by experts on the importance of the various components of the HFD framework to employees' security behavior in organizations. The views are derived through a survey. The results obtained are described and discussed.

3.1. A survey

A number of experts in information security have been invited to participate in reviewing the proposed framework. Nine experts have accepted to participate through a questionnaire. The survey aims at assessing the importance of the various components of the framework with regards to their influence on the behavior of employees toward information security. Each domain has been assessed in a hierarchical manner according to its subdomains and their elements. The assessment scale given in Table 3 has been used for this purpose.

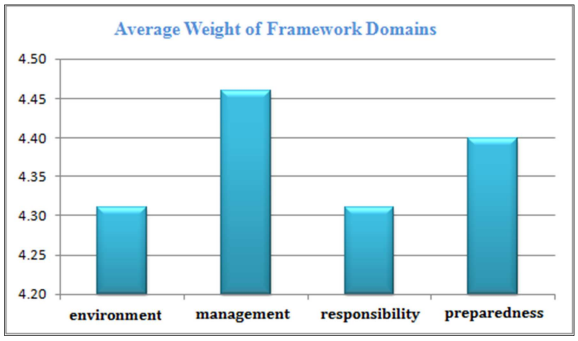


Figure 3: Average importance weight of the four domains of the HFD framework (out of 5)

Table 3 Assessment Scale

Grade	N/A	Very low	Low	Average	High	Very high
Value	0	1	2	3	4	5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The results of each factor are reported in weight and frequency. The weight distribution is used to distinguish positive versus negative perceptions. It has been considered that an element with very low weight should be excluded as this indicate that experts believe it has little relation or effect on the human behavior. On the other hand, high and very high indicate a positive relevance. The statistical aggregation of group response allows for a quantitative analysis and interpretation of data [41].

Any element fall in middle weight range, should be restudied and either improved or removed as this indicates that experts are unsure about its importance to the human security behavior. An action table (Table 4) has been used as a guide.

Table 4: Action Table

Weight	Action	Weight	Action	Weight	Action
0-1	Reject	2-3	Restudy	4-5	Accept

3.2. The results obtained

After all the responses have been collected and combined, analysis of the results was conducted in order to validate the framework. The data was quantitatively analyzed using the Statistical Package for the Social Sciences (SPSS) software. The data preparation process ensured that the data set have no missing values and not distorted significantly by the different opinions of specific groups.

The average weight given by expert for each element and subdomain that belongs to the same domain has been accumulated and used to evaluate each domain. The average weight in the survey to each domain is given in Figure 3.

It can be noticed from Figure 3 that all four domains fall in the acceptance area. Organization and employee dimensions have gained the same impact, showing the importance of both dimensions to the achievement of suitable employees' behavior.

The resulting average weight of the subdomains is given in Figure 4. It can be seen from the Figure that every subdomains has an average weight above 4; and like the above, this falls in the positive acceptance area and indicates that the respondent experts feel positive about the validity of the framework

The outcome of the statistical analysis of results is given in Table 5. It shows that the mean of the average weight of the impact of studied key elements is 4.37 which fall in the positive area. This indicate a positive attitude toward the four domains. With a 95% confidence interval, the small range between 4.31 and 4.42 shows a precise indication of acceptance of the tasks. This also suggests that the mean is adequately representative. In addition, the standard deviation of 0.1 indicates a deviation of 0.1 point from the mean of the average that is close to zero emphasizes the positive perception of the different presented human factor and assures that the mean is a good representative for the data set. Therefore, the sample would represent an accurate reflection of the population and the mean value can be used as a representative for the data set.

Table 5 Statistical Analysis

Mean	4.37
Standard Error	0.027
Standard Deviation	0.10
Confidence Interval	{4.31-4.42}

Cronbach's alpha, a coefficient of internal consistency, was used to measure reliability of the model [42]. Cronbach's alpha values must meet the minimum accepted criteria (above 0.7) to confirm the consistency and reliability of the framework [14]. The results of the reliability analysis are presented in Table 6.

Table 6 Reliability analysis

Factor	No of items	α value
Preparedness	10	0.933
Responsibility	13	0.925
Management	14	0.941
Environment	8	0.903

The values of the Cronbach's alpha are above 0.9 which is larger than the threshold indicating a good internal consistency and reliability. Therefore, the instrument appears to be composed of a set of consistent variables for capturing the meaning of the framework.

4.3. Discussion of results

The response of the experts confirmed the validity of the four-domain and eleven-

Journal of Theoretical and Applied Information Technology
20th August 2015. Vol.78. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

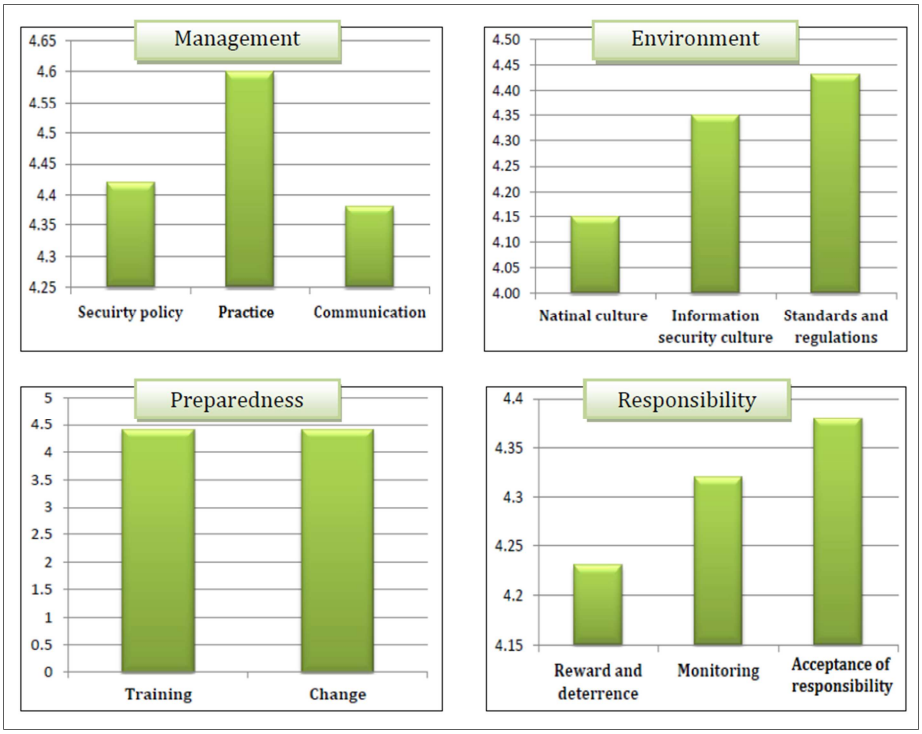


Figure 4 Average Weight Of The Subdomains Associated With The Main Domains Of The HFD Framework

subdomain HFD framework. Here are some comments on the results obtained.

- Considering the four-domain level, the management domain received the highest score followed by the preparedness domain. The environment and the responsibility domains came together in the third position. However, differences were not significant. The difference between the highest score and the lowest one is around 3%.
- For the subdomains of the environment domain, the standards and regulations subdomain scored first followed by information security culture, and then the national culture. Differences were also insignificant, at around 6% between the highest and lowest scores.
- For the subdomains of the management domain, the management practices subdomain scored first followed by information security culture, and then the national culture. Differences were also insignificant, at around 6% between the highest and lowest scores.
- For the subdomains of the employee preparedness domain, both the awareness and training subdomain and the change subdomain scored high with no difference between the two.
- For the subdomains of the employee responsibility domain, employees acceptance of security responsibility scored high followed by monitoring and then rewards and deterrents. Differences were insignificant, at around 2.5% between the highest and lowest scores.

4. CONCLUSIONS AND FUTURE WORK

The application of information security technologies do not always result in an improved security as security is largely associated with 'people. The interaction between human and information systems have always opened the chance for many security risks. To improve the security of information assets, an understanding of the human factor is required. The proposed framework provided a comprehensive view of the human issues that influence human behavior toward information security in organizations. One of its two dimensions considers organization issues according to the domains of: environment and management. The other dimension emphasized employees' issues using the domains of preparedness and responsibility. The four domains were related to the main factors of the Social Cognitive Theory (SCT); and the subdomains resulting from the refinement of the domains were related to previous work.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The eleven subdomains (human factor) were refined into "45 elements" that influence information security; and these were put before experts to view their importance. The various components of the framework structure received high scores by the experts reflecting the validity of the framework for future use.

The four domains of the framework are associated with organizations in general; no specific type of organization has been specified. Future work can consider specific types of organization and this may require additional elements to be added, and may be some changes in the subdomains. In addition, the comprehensiveness of the framework is limited to the inside of the organization, future work can provide extra-dimensions that can accommodate global issues.

The outcome of the work has the following main benefits.

- It provides information security tools for both: risk analysis originated by human behavior within organizations; and risk management for the achievement of protection.
- It enhances the development of special controls that contribute to the protection of information security from human behavior.
- It contributes to the enablement of deriving improved frameworks and models that deal with specific types of organization, and with global human threats to information security.

It is hoped that the framework will be used by information security professionals in organizations toward better human-related information security management; and it is also hoped that researchers in the field will also use the framework for further improvements and newer development.

REFERENCES:

[1] A. Norman and N. Yasin, "An analysis of Information Systems Security Management (ISSM): The hierarchical organizations vs. emergent organization," *Int. J. Digit. Soc.*, vol. 1, no. 3, pp. 230–237, 2010.

[2] J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, Jun. 2010.

[3] R. Von Solms and B. von Solms, "From policies to culture," *Comput. Secur.*, vol. 23, no. 4, pp. 275–279, Jun. 2004.

[4] B. von Solms, "Information Security – The Fourth Wave?," *Comput. Secur.*, vol. 25, no. 3, pp. 165–168, 2006.

[5] J. Stanton, K. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Comput. Secur.*, vol. 24, no. 2, pp. 124–133, 2005.

[6] J. Eloff and M. Eloff, "Information security architecture," *Comput. Fraud Secur.*, vol. 2005, no. 11, pp. 10–16, 2005.

[7] A. da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Comput. Secur.*, vol. 49, no. 2015, pp. 162–176, 2015.

[8] K. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," *Comput. Fraud Secur.*, vol. 2006, no. 10, pp. 7–11, 2006.

[9] D. Ashenden, "Information Security Management: A Human Challenge?," *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 195–201, 2009.

[10] G. Dhillon, *Principles of information systems security*. John Wiley & Sons., 2007.

[11] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: a behaviour compliance conceptual framework," in *8th Australasian Information Security Conference (AISC 2010)*, 2010, pp. 47–55.

[12] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*. Indianapolis, IN: John Wiley & Sons, Inc., 2000.

[13] A. Martins and J. Eloff, "Information security culture," in *Security in the information society*, Boston: Kluwer Academic Publishers, 2002, pp. 203–214.

[14] A. Da Veiga, N. Martins, and J. Eloff, "Information security culture-validation of an assessment instrument," *South. African Bus. Rev.*, vol. 11, no. 1, pp. 146–166, 2007.

[15] K. Parsons, A. McCormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security: Individual, Culture and Security Environment," *Command, Control, Communications and Intelligence Division, Defenses Science and Technology Organization, Department of Defense, Australian Government*. Command, Control, Communications and Intelligence Division Defenses Science and Technology

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Organization, Department of Defense, Australian Government, Australia, 2010.

[16] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*," *Decis. Sci.*, vol. 43, no. 4, pp. 615–660, 2012.

[17] (Price Waterhouse Coopers PWC, "Managing insider threats," 2014.

[18] Information Security Breaches Survey, "2014 Information Security Breaches Survey," 2014.

[19] R. Hagberg and J. Heifetz, "Corporate Culture /Organizational Culture: Understanding and Assessment." Hagberg Consulting Group (HCGH)., 2000.

[20] A. Da Veiga and J. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[21] G. Dhillon and J. Backhouse, "Technical opinion: Information system security management in the new millennium," *Commun. ACM*, vol. 43, no. 7, pp. 125–128, Jul. 2000.

[22] S. Dojkovski, S. Lichtenstein, and M. Warren, "Enabling information security culture : influences and challenges for Australian SMEs," in *ACIS 2010 : Proceedings of the 21st Australasian Conference on Information Systems, ACIS*, 2010, p. 61.

[23] A. Bandura, "Social cognitive theory: An agentic perspective," *Annu. Rev. Psychol.*, vol. 52, pp. 1–26, 2001.

[24] S. Alumaran, G. Bella, and F. Chen, "Culture Dimensions of Information Systems Security in Saudi Arabia National Health Services," *Int. J. Soc. Educ. Econ. Manag. Eng.*, vol. 9, no. 2, pp. 510–514, 2015.

[25] M. Alnatheer and K. Nelson, "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," in *Proceedings of the 7th Australian Information Security Management Conference, December 2009*, 2009, pp. 6–17.

[26] J. Leach, "Improving user security behaviour," *Comput. Secur.*, vol. 22, no. 2, pp. 685–692, 2003.

[27] M. Selamat and D. Babatunde, "Mediating Effect of Information Security Culture on the Relationship between Information Security Activities and Organizational Performance in the Nigerian Banking Setting," *Int. J. Bus. Manag.*, vol. 9, no. 7, pp. 33–38, 2014.

[28] OECD, "The promotion of a culture of security for information systems and networks in OECD countries (OECD)." OECD (Organization for Economic Cooperation and Development) "(OECD), 2005.

[29] A. Colella, A. Castiglione, and A. Santis, "The Role of Trust and Co-partnership in the Societal Digital Security Culture Approach," in *2014 International Conference on Intelligent Networking and Collaborative Systems*, 2014, pp. 350–355.

[30] A. Ruighaver, S. Maynard, and S. Chang, "Organisational security culture: Extending the end-user perspective," *Comput. Secur.*, vol. 26, no. 1, pp. 56–62, Feb. 2007.

[31] R. Goh, "Information Security: The Importance of the Human Element," unpublished PhD thesis, Preston University, 2003.

[32] Information Security Breaches Survey, "2013 Information Security Breaches Survey," 2013. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf.

[33] T. Wiant, "Information security policy's impact on reporting security incidents," *Comput. Secur.*, vol. 24, no. 6, pp. 448–459, 2005.

[34] R. Werlinger, K. Hawkey, and K. Beznosov, "An integrated view of human, organizational, and technological challenges of IT security management," *Inf. Manag. Comput. Secur.*, vol. 17, no. 1, pp. 4–19, 2008.

[35] I. Koskosas, K. Kakoulidis, and C. Siomos, "Information Security: Corporate Culture and Organizational Commitment," *Int. J. Humanit. Soc. Sci.*, vol. 1, no. 3, pp. 192–198, 2011.

[36] C. Colwill, "Human factors in information security: The insider threat – Who can you trust these days?," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, Nov. 2009.

[37] J. Van Niekerk, "Fostering Information Security Culture Through Integrating Theory And Technology, Unpublished PhD Thesis," Nelson Mandela Metropolitan University, , South Africa, 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[38] A. Munteanu and D. Fotache, "Enablers of Information Security Culture," in *Procedia Economics and Finance*, 2015, vol. 20, no. 2015, pp. 414–422.

[39] D. Cappelli, A. Moore, R. Trzeciak, and T. Shimeall, *Common sense guide to prevention and detection of insider threats*, 3rd ed. CERT, Software Engineering Institute, Carnegie Mellon University, 2009.

[40] K. Knapp, T. Marshall, R. Rainer, and F. Ford, "Information security: management's effect on culture and policy," *Inf. Manag. Comput. Secur.*, vol. 14, no. 1, pp. 24–36, 2006.

[41] G. Skulmoski and F. Hartman, "The Delphi Method for Graduate Research," *J. Inf. Technol. Educ.*, vol. 2007, no. 6, pp. 1–21, 2007.

[42] A. Field, *Discovering Statistics using SPSS*. London, United Kingdom: Sage Publications, 2005.