Managing human factor to improve information security in organization

Areej A. AlHogail

College of Computer and Information Sciences,
Imam Mohammed bin Saud Islamic University, Riyadh, Saudi Arabia.
aalhogail@imamu.edu.sa

Abstract:

There are many security risks to the organizations’ information assets; nonetheless, among the major threats to achieve a secure information environment are the actions and behavior of the employees when handling information. Insiders, intentionally or unintentionally, can cause serious risks, despite investments usually made on security control measures and other security related products. Neglecting the human factor could lead to security breaches as human factor determine the behavior of the employees toward information security. This paper attempts to focus on the role of human factor in achieving the required level of security and suggest a best practice recommendation guideline that is based on the Human Factor Diamond (HFD) framework. HFD focus on the human factor issues that can influence employees’ behavior toward information security in organizations. The framework is structured in two dimensions, and four domains. Each domain has been mapped to a set of guideline in order to give practical guide to organization management and security practitioners to minimize threats posed by the employees’ behavior to information security.

Keywords: human factor; information security; human behavior; information security controls; insider (employee) threats, best practice guideline.
1. INTRODUCTION
For years the focus on information security was purely technical which is no longer enough and suitable to the dynamic nature of organizations today [1]. Human factors such as knowledge, skills and personality can impact on the behavior of employees when interacting with information assets and security controls. Despite the amount of money and efforts spent on the technical measures and solutions, the effectiveness of these technologies lies in the behaviors of the humans who access, use, administer, and maintain information resources [2]–[4]. In addition, this human dimension of information security cannot thoroughly be solved only by procedural and technical measures. The human is the weakest link in the security chain [5], [6].

In most organizations, managing information security threats focuses on managing technology and process, but little efforts are paid at managing people. It is crucial to understand how employees are expected to assist in keeping the organization’s information secure and understand the factors behind their behaviors. In the literature there is a lack of frameworks that guide the analysis of the human factor in information security [7], [8] and it is often left unaddressed [9], [10].

The purpose of the work presented in this paper is to provide a best practice recommendation guideline that is based on the Human Factor Diamond (HFD) framework by AlHogail et al. [11]. HFD focus on the human factor issues that can influence employees’ behavior toward information security in organizations. The framework domains have been mapped to a set of recommendation in order to give practical guide to organization management and security practitioners to minimize threats posed by the employees’ behavior to information security. The recommendations is based on expert survey of opinion towards the most appropriate practices. In addition, it will include different methods of enforcement, motivation, reward and deterrence and so on to ensure the obedience to information security requirements.

2. LITERATURE REVIEW
Business environments are now depending heavily on information systems, Internet, cloud computing, mobile computing and so on to achieve competitiveness and remarkable advantages. However, this has opened the doors for new kind of threats to appear that need to be dealt with in order to protect the organizations’ information assets. Information is vulnerable as it could fall in the hands of unauthorized people. Loss, misuse, or damage to the information assets could have devastating effects on the overall organization’s wellbeing that could range from lost employees hours to negative publicity or even financial damage. This has raised a number of concerns connected with the protection of organizational information assets.

Focusing on the technical aspects of security in organization without appropriate consideration of the human interaction with the system is evidently inadequate [12]. Different studies shown that a significant emerging threat to information security is from the employees themselves [13], [14]. A security breach survey by PWC (Price Waterhouse Coopers) in 2015 showed that 75 % of large organizations suffered a staff-
related breach and 31% of small organizations had a similar occurrence. 50% of the worst security breaches were caused by unintentional human error in comparison to 31% in the previous year [14].

This ‘insider human-related threat’ is one of the greatest information security challenges that organizations face and one of the hardest to protect against [2], [13]. 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 [15], [16]. Moreover, the lack of skills, knowledge, and commitment by employees when it comes to the protection of information could be a challenge for organizations [9].

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 [9]. Thomson et al. [9] assumed that well trained and conscientious employees can form the strongest link in any organization’s security infrastructure. Even though, many organizations have no plans to deploy relevant countermeasures to avoid threats posed by humans, as 35% of organizations surveyed in 2015 have not provided any security awareness nor training to their staff [14]. This highlights the vital need for organizations to adopt security solutions that address the human factors.

Colwill [17] believes that key reasons behind the ignorance of insider threat and human factor in organizations are: (1) Organizations are not aware of the risks posed by its employees; (2) Organizations fear of the bad publicity, so they deny it; or (3) Organization know about the threat but don’t know how to deal with it. Many organizations do not report insider errors or attacks making the estimation of the scale of the problem very difficult and inaccurate. According to [18], 70% of organizations do not report their worst security incident.

On the other hand, strict requirements, based on the perception that employees pose a potential hazard, could lead to dissatisfaction, ignorance, frustration, and, attempts at bypassing regulations and policies. Therefore, a well-balanced security and usability should be in place.

2.1 THE HUMAN FACTOR DIAMOND (HFD) FRAMEWORK

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 [19]. 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.

Alhogail et al. [11] presented the Human Factor Diamond (HFD) framework to identify the human factors that influence human behavior when interacting with information in order to reduce human related security threats. The framework is structured according to two main dimensions, with each dimension having two domains, forming the diamond shape as shown in Figure 1.

![Figure 1 The Human Factor Diamond (HFD) framework](image)

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

- The “society and regulations” 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.
2.1.1. The “society and regulation” domain

The organization “society and regulation” domain includes: the national culture, the internal security culture of the organization, and the related 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 [20]. 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 [13].

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 [21], [22]. The process of information security must be compatible with the society ethics and reflects essential society values [23], [24]. Moreover, the national culture (unchangeable) should be taken into account when designing information security policy and guidelines. In addition, employees should be made aware of all relevant government information security related legislation [25].

2.1.2 The “management” domain

The organization “management” domain includes management practice, security policy and communication. The attitude of the senior management toward security highly affects how employees perceive the importance of information security [13], thus, on their security behavior. Ruighaver et al. [26] 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 [27], it has been found that the lack of security policies was rated as one of the top inhibitors to achieving security effectiveness in organizations. 72% of organization where the security policy was poorly understood had employees' related breaches, [14]. 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 [28]; thus the effectiveness was only related to how well it is developed, implemented and maintained.

2.5 The “preparedness” domain

The employee “preparedness” domain include awareness and training and change. 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. Information security awareness shall be integrated with the employee induction process so that employees understand the significance of information security to the organization.
Continuous awareness and training programs help employees to understand security requirements and security policy documentations [12]; and keep them current 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. The language used in training has a great impact on the success of the program. For instance, security issues that are addressed in a complicated way may lead employees to misunderstandings and may disturb and affect their judgment, or even make them stressed and afraid of taking decisions. Moreover, training and awareness should not interrupt employees from their duties and should be enjoyable.

Furthermore, 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. The transition periods could expose the information assets to security risks. No matter how carefully the changes in security are introduced into an organization, resistance could be present [29]. Therefore, change management principles should be implemented to help in reducing the resistance to change, thus their information security threats.

2.6 The “responsibility” domain
The employee “responsibility” domain includes employee’s acceptance of responsibility, monitoring and control, and reward and deterrence. 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 requirements [27]. Van Nikkrek [30] 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 [31]. Employees should view security as an essential element when interacting with information assets [24]. In addition, employees should feel responsible to act in a supportive manner to prevent, detect and respond to security incidents.

Employees monitoring should be in place to prevent any security risks [12], [17]. 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 [32]. Organization shall have a clear policy and role assignments to achieve an accurate access rights.

In addition, some researchers suggest that strong human resource policies should be applied to monitor employees to identify financial problems or changes in behavior. Also they suggest that
employee online activities should be logged, monitored and audited regularly [32]. Continuous monitoring would prevent costly threats to the organization information assets.

Promoting good user behaviors and constraining bad user behaviors could provide important benefits for information security [2]. Formal procedures for penalty found to be effective in shaping employees' security behavior. Deterrence forms could include laws, policies and even technical controls. However, there should be fear of penalty: fear of being caught and penalty should be actually applied [33]. This could be useful to reduce errors, carelessness and negligence and to prevent illegal and unethical activity [34].

Not only punishment, but a reward system should also be in place [20] as a great way to encourage employees to show a desired healthy security behavior and greater participation in achieving organizational security goals. Recognition must be given to employees for their security efforts [27]. Nevertheless, if it is not clear and reasoned, it may increase complaint or other negative emotions about oneself being underestimated.

The HFD framework 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 guides information security professionals in taking proactive measures to guard against insider threats rather than reactive procedures after the occurrence of the threat.

3. MANGENG THE HUMAN FACTOR GUIDELINES

Ten experts in information security have been invited to participate in reviewing the suggested framework domain mapping by rating the importance of suggested recommendations with regards to their influence on the employees security behavior. The views are derived through a questionnaire.

The results of each recommendation are reported in weight. 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. 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
Based upon the results, this paper present a best practice recommendations guidelines that aims at improving the state of information security by guiding organizations' management and information security professionals at managing the human behavior. The recommendations are high level and generic and are intended to be applicable to all type of organizations, regardless of type, size and nature. This best practice recommendation should be used in conjunction with the HFD to protect the information assets from internal risks caused by employees' behavior. Other procedures should be taken to protect the information assets from the external risks.

It is recommended that the responsibility for information security and risk analysis in general should be delegated to a person, function or team based on the organization size. They should have authority to contact other departments with awareness information and should get the highest support from the top management. This team is responsible for developing and maintaining the appropriate information security culture based on the following recommendations. The guidelines leave the details to the organization to decide how to shape it based upon their requirements.

Management:

• Establish and gain management support
• Analyze and identify the information security scope and requirements based on the organization characteristics of the business, and information assets nature
• Perform appropriate risk assessments taking into account insider risks
• Define written information security strategy that includes policy, guidelines and so on
• Align the information security strategy with the IT and business strategies
• The strategy should clearly state what is expected from the employees
• The strategy should address the prevention, detection and response to information threats
• Make the policy available for employees to access
• Inform organization members about the policy and how to get access to it
• Make the message clear that complying to information security policy is not optional and use different enforcement measures
• Prepare a copy of the policy in an easy to digest format such as bullet point or graphics to ensure the maximum attentiveness of the policy

Society and regulations

• Ensure that all employees are aware of the code of ethics (or code of conduct) and all related regulations.
• Consider the national culture values when developing the information security strategy and awareness programs to avoid any behavior that may risk the security of the information assets

• Educate employees about the values of confidentiality and privacy of organization and third parties information

• Information security strategy should be complied with legislative, regulatory, international standards and contractual requirements

Preparedness

• Coach and train employees to develop skills and knowledge base that support the policy, ethical conduct, law and regulations and safe use of different IT technologies

• Educate employees of how to effectively use any technical security controls

• Provide technical assistance and help desk

• Use a variety of communication channels such as email, portal, newsletter, posters, banners, screen savers, workshops, e-learning and so on to improve employees’ information security awareness

• Identify small wins, measures and milestones to generate momentum and track the success of the change

• Select change agents at each department to facilitate the change and communication with other departments

• Employees should be made aware of the changes in practices, the objectives of the change and the alternatives to increase their acceptance

• New employees should receive special orientation to educate them about information security and their roles and responsibility

Responsibility

• Enhance the sense of ownership and responsibility for the security of information assets

• Set a procedure to measure employees’ information security awareness level and responses to security threats on a continuous basis

• Encourage information sharing regard information threats among organization members

• Establish executive information security committee with representatives from key business department to conduct regular meeting to discuss emerging issues

• Involve the stakeholders in the decisions and policy development to gain their support and mobilize the commitment

• Employees should be accountable for their information security actions
- Set reward and deterrence policy to motivate good security behavior
- Access to information should be controlled and segregation of duties should be implemented
- Monitor and audit the compliance to policies and controls
- Employment termination or change of role responsibilities should be clearly defined

4. CONCLUSIONS AND FUTURE WORK

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 practical use of the HFD is supported in this paper through best practice guidelines that is based on it and could be used by information security specialists as a checklist to minimize security threats posed by organizations insiders. The guidelines cover four domains: management, society and regulation, employees’ preparedness and employees’ responsibility. Each domain has been translated into set of recommendations to manage the human factor in information security at organizations.

Future work can consider specific types of organizations and this may require additional elements to be added, and may be some changes in the subdomains. Moreover, knowledge management could be integrated to develop a model that can assist organizations to efficiently predict and improve security behavior. The knowledge management component could be used to capture, acquire and encode knowledge to help decision making. This will definitely benefit from knowledge sharing between organizations and will increase the efficiency of handling security incidents from insiders. The best practice guidelines could be further investigated to recommend practical standards that could be enhanced with performance indicators and indexes for improving security behavior. The indicators should include assessment, evaluation, planning, implementation, and provide criteria for measuring the actual performance.

REFERENCES


Managing Human Factor To Improve Information Security In Organization

Dr. Areej A. AlHogail
Department of Information systems, Imam University
OUTLINE

• INTRODUCTION

• HUMAN FACTOR IN INFORMATION SECURITY

• HUMAN FACTOR DIAMOND FRAMEWORK (HFD)

• BEST PRACTICE RECOMMENDATION

• CONCLUSION AND FUTURE STUDIES
INTRODUCTION

• Human factors such as knowledge, skills and personality can impact on the behavior of employees when interacting with information assets and security controls

• Employees’ behavior and security incidents
  
  • 75% of large organizations suffered insiders related security breaches.
  
  • 50% of the worst security breaches were caused by unintentional human error in comparison to 31% in the previous year (Information Security Breaches Survey 2015)

• Security is a ‘people issue’, as well as a ‘technical issue’.

• Managing the human factor in information security is essential.
The Human Factor in Information Security

• In most organizations, managing information security threats focuses on managing technology and process.

• Human behavior is the weakest link in the security chain [2].

• Understand how employees are expected to assist in keeping the organization’s information secure and understand the factors behind their behaviors.
The Challenge

• Humans are not very predictable because they do not operate as machines

• Accepting that individuals in the organization have personal and social identity [3, 4].

• Lack of skills, knowledge, and commitment by employees
• There are a number of critical human factors ensure that secure environment is developed and maintained

• Thomson et al. [5] assumed that well trained and conscientious employees can form the strongest link in any organization’s security infrastructure.
• Organizations have implemented a range of administrative and technical measures within an overall information security management system

• Different standards touch on the human behavior: ISO27001:2013, ISO 27032:2013, OECD, etc.

• Lack of frameworks that guide the analysis of the human factor in information security [6, 7]
THE HUMAN FACTOR IN INFORMATION SECURITY FRAMEWORK

The Social Cognitive Theory
<table>
<thead>
<tr>
<th>Environment</th>
<th>Human Factor</th>
<th>Examples of previous studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Security policy</td>
<td>Soltanmohammadi et al. (2013), Hu et al. (2012), Cappelli et al. (2009), Colwill (2009), Goh (2003), and Whitman &amp; Mattord (2010)</td>
</tr>
<tr>
<td></td>
<td>Practice</td>
<td>Goh (2003), Leach (2003), Ruighaver et al., (2007), lacey(2009), and Soltanmohammadi et al., (2013)</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>Koskosas et al. (2011), Hu et al. (2012), and Ruighaver et al., (2007)</td>
</tr>
<tr>
<td>Cognitive</td>
<td>Preparedness</td>
<td>Awareness and training</td>
</tr>
<tr>
<td></td>
<td>Change</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitoring &amp; control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reward &amp; deterrence</td>
<td></td>
</tr>
</tbody>
</table>
BEST PRACTICE RECOMMENDATIONS

• List of action for every dimensions
• Recommendations are high level and generic
• Focus on internal threats
BEST PRACTICE RECOMMENDATIONS

Management

• Establish and gain management support
• Analyze and identify the scope and requirements
• Perform risk assessments
• Define written information security strategy
• Align it with the IT and business strategies
• Address the prevention, detection and response to information threats
• Clearly state what is expected
• accessible
• use different enforcement measures
• Prepare a copy with an easy to digest format
Best Practice Recommendations

Society and regulations

• Ensure that employees are aware of the code of ethics (or code of conduct) and all related regulations.
• Consider the national culture values
• Educate employees about the values of confidentiality and privacy
• Information security strategy should be complied with legislative, regulatory, international standards and contractual requirements
BEST PRACTICE RECOMMENDATIONS

Preparedness

- Coach and train employees to develop skills and knowledge base
- Educate employees of technical security controls
- Provide technical assistance and help desk
- Use a variety of communication channels to improve employees' information security awareness
- Identify small wins, measures and milestones to generate momentum and track the success of the change
- Select change agents at each department
- Employees should be made aware of the changes to increase their acceptance
- New employees should receive special orientation to educate them
BEST PRACTICE RECOMMENDATIONS

Responsibility

- Enhance the sense of ownership and responsibility
- Set a procedure to measure employees’ information security awareness level and responses to security threats on a continuous basis
- Encourage information sharing regarding information threats
- Establish executive information security committee with representatives from key business departments
- Involve the stakeholders
- Employees should be accountable for their actions
- Set reward and deterrence policies
- Controlled access and segregation of duties should be implemented
- Monitor and audit the compliance to policies and controls
- Employment termination or change of role responsibilities should be clearly defined
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 best practice guidelines could be used by information security specialists as a checklist to minimize security threats posed by organizations insiders.

On the other hand, strict requirements, based on the perception that employees pose a potential hazard, could lead to dissatisfaction, ignorance, frustration, and attempts at bypassing regulations and policies. Therefore, a well-balanced security and usability should be in place.
FUTURE WORK

• Dedicated studies to produce domain-specific best practice

• Knowledge management component to capture, acquire and encode knowledge to help decision making

• Practical standards enhanced with performance indicators and indexes
REFERENCES


THANK YOU
aalhogail@imamu.edu.sa