An Interactive Visual Library Model to Improve Awareness in Handling of Business Information

Petrus M.J. Delport, Mariana Gerber, Nader S. Safa
Centre for Research in Information and Cyber Security
NMMU
Port Elizabeth, South Africa
S211253502@nmmu.ac.za, Mariana.Gerber@nmmu.ac.za, sohrabisafa@yahoo.com

***Abstract*— Information technology has changed organisational processes significantly. However, information security is still a controversial issue among experts in this domain. Information security breaches lead to loss of reputation, competitive advantages, intellectual properties, productivity, and revenue and in the worst scenario leads to bankruptcy. In this regard, awareness plays a vital role to mitigate information security threats. This study aims to present different threats that effect confidentiality, integrity and availability of information, pertaining to administrative employees, in an integrated and informative design, based on a review of literature. In addition, a possible interactive visual library is proposed, through a proof of concept that contributes to administrative employees' information security awareness. The results shed some light on this information security awareness issue, and provides the means for further academic study.**

Keywords-Information security; administrative employees; business information; sensitive data; awareness; threats

I. Introduction

Information has become the lifeblood of modern organisations and core to most business processes [1]. Due to this, an organisation could seriously be harmed or even become bankrupt if proper information security is not implemented and maintained. According to the reputable company named Bitdefender, employees of an organisation remain the weakest link in the organisational sphere and may consequently pose a serious threat to information security [2]. Another study undertaken by Whitman, suggests that the third highest information security threat in an organisation is the act of human error or failure [3]. This clearly shows the importance of employees' behaviour in the domain of information security. One can clearly see that without proper awareness, an organisation's employees could compromise business information. The term business information is used as an amalgamation of valuable data, sensitive data and information within a business environment, essentially any information that is considered an asset to the organisation. In reference to an organisation's employees, this paper focusses purely on the role that administrative employees, sometimes called administrative assistants, play whilst handling business information. An administrative employee is defined as a person that is employed to assist with various clerical tasks in an office setting such as correspondence, keeping records, making appointments, and carrying out similar tasks [4]. This paper classifies administrative employees as the main point of contact in most organisations, whether by phone, email or physical contact due to the role of liaising with customers, and even potential attackers, on a daily basis.

Consequently, without administrative employees having proper knowledge of existing threats, the organisation may undergo severe repercussions. Therefore, the objectives of this paper is to firstly, focus on the role of administrative employees and actions they perform, especially when encountering certain threat scenarios and how these threats can compromise business information. Secondly, it will also propose a possible solution, through a proof of concept, which can contribute in raising the administrative employees' awareness on secure handling of business information.

With the mentioned background in mind, this paper will continue to discuss the research approach. Thereafter the problem will be explored in more detail by contextualizing information security threats. The paper will then end off by providing a proof of concept to the proposed interactive visual library.

II. Methods/Approach

The following methods were used to address the objectives of this paper.

Firstly, a literature review was done in order to identify top threats that exist within a typical organisation. After comparing the top threats from various sources, the top five threats that focus on organisational environments were extracted which provide the input into the survey.

Secondly, a survey in the form of a questionnaire was done. Typically a questionnaire is done to identify a specific pattern or behavioural existence within a certain group [5]. The questions were adopted from previous studies in this domain [3]. The focus of this survey is administrative employees within an organisation. In order to have participated in this survey, the participant had to adhere to the following three characteristics. These characteristics are as follows:

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

- Participant must be an administrative employee within any sector except the IT sector, as it might provide a bias result.
- Participant has to work with a computer on a daily basis.
- Participant must handle business information on a regular basis

Only when a participant adhered to these three characteristics, was the participant able to participate in the survey. Each participant, which belong to various institutions or organizations, received the same questions and a specific pattern or behavioural existence was identified. The data were analysed and reported on, which showed a sample of the current awareness levels regarding administrative employees within organisations.

Thirdly, argumentation was used in order to identify critical aspects in creating an interactive visual library, which aims to address the awareness levels of administrative employees within a typical organisation.

Lastly, a prototype was discussed which served as a proof of concept. Using this research approach, the following section will start contextualizing information security threats

III. Administrative Employees Vs. Threats

Information security techniques may lose their usefulness if misused, misunderstood, or not used by end-users. Due to this, information security awareness is a crucial activity in any organisation [6]. It is clear that without awareness or knowledge of information security threats, one might become a victim within an organisational environment and most likely compromise business information. As mentioned previously, information is the lifeblood of an organisation and therefore administrative employees must securely handle business information.

It is essential to have a clear understanding of what a threat is within an organisation; therefore, the following subsection will identify typical threats within an organisation.

A. *Threats Within an Organisation*

In order to address the objective of this paper, the first step is to identify the top five threats administrative employees might encounter whilst handling business information within an organisation.

A threat, regarding information security, is a category of entities that present a danger to a current asset [7]. The asset is anything that the organisation finds vital to keep secure in order to continue normal business operation. The threat typically moves the asset from a secure state to an unsecure state whereby compromising either confidentiality, integrity or the asset's availability. When an asset is compromised, the organisation could suffer tremendously. Many threats exist which could lead to compromised assets, however this paper focusses on the threats that fall under the category of "Act of human error, or failure" as identified by Whitman [3]. By combining literature [8] and various online threat reports, such as the annual Threat Horizon report [9], a cross examination, based on highest occorrence, revealed the top threats that exist within a typical organisation [10][11]. Table 1 displays a list of the top five internal threats.

TABLE I. Top Five Threats Inside an Organisation

Threat:	Description/Example:
1) *Malicious attacks*	- Due to internal employees with privileged system access performing deliberate attacks on company. - Disgruntled employees/ Outsider attacks.
2) *Social engineering*	- The trusting nature of internal employees is exploited by extracting sensitive information. - E.g. a perpetrator pretending to be an IT technician, asking employees for personal passwords to fix underlying problems, however the perpetrator uses this information to breach security in.
3) *Downloading malicious internet content*	- Employees use the organisation's internet for personal use during working hours. - Employees might use the internet to watch a video clip, log onto social media sites or play games, hereby dramatically increasing chances of hidden malicious files entering organisation's network.
4) *Information leakage*	- Technological advances enable one to carry data easily through portable devices such as USB flash-disk, MP3 player and cell phones. - Employees use these methods daily without thinking about consequences. - E.g. business information is stored on employee's flash-disk, and the flash-disk with sensitive business information is misplaced. The leakage of business information can have a devastating effect on the business. - Employees give out their passwords/credentials to other employees, not considering the consequences it may have on the organisation.
5) *Illegal activities*	- Piracy is a major issue. - Could have major reputational damage on organisation. - Employees often save personal files or programs on organisation's network; these include pirated software, movie files, or even pornography. - Effective policies should be in place to monitor for such files together with effective policy enforcement.

Administrative employees interact with business information and might subsequently confront various threats. Therefore, awareness about these threats are critical, and simultaneously, from an organisational perspective, to have effective policy control and enforcement in place. The following subsection will discuss the organisation's responsibility towards awareness.

B. *Awareness Within an Orgnization*

Security awareness is how well users understand the importance of information security and how well they exercise information security controls to protect the organisation's data and networks [13]. According to Ernst & Young, for the effective protection of information, it is recommended that organisations invest more in training and awareness programs to help prevent information security breaches [14].

Without these awareness programs, administrative employees typically have one of two standings with regard to awareness: either the employee is ignorant or the employee is negligent. Whether ignorant or negligent, the administrative employees' insecure handling of data may be a vulnerability that could lead to the compromising of business information.

The impact of compromised business information may lead to a business losing reputation, competitive advantages, intellectual properties, and in the worst scenarios, lead to bankruptcy in the business sector. It is therefore imperative to eradicate any lack in knowledge that may exist with administrative employees about secure handling of business information. A fundamental point is firstly to be aware of threats. If one's awareness is deficient, one is more likely to be the cause of compromised business information.

To address this deficiency, it is of utmost importance to properly educate, train, and raise awareness on how to handle business information securely. This raises a question: how does one raise administrative employees' awareness? Different methods of effectively establishing awareness amongst administrative employees exist. One of the most efficient methods to raise awareness is to make use of the Information Security Awareness Training (ISAT) which provides awareness and training or workshops to educate administrative employees on issues related to information security [13].

Some guidelines in combination with an ISAT program from Cisco, a network technology company, suggest that an organisation should establish a security awareness and education practice. This is vital in gaining employee support, due to the fact that employees who believe that security programs are important, are more likely to follow specific procedures [12]. Cisco further suggests that a practice should:

- Educate and train employees about company expectations for protecting data.
- Include security awareness and practices in new-hire orientation events.
- Train employees about security considerations when answering the phone and connecting to the internet, social networking, and collaboration sites.
- Train employees about physical security concerns, such as allowing only employees with badges to enter buildings.

By using a combination of these suggested guidelines, it is possible to have a proper awareness program. As mentioned before, employees are seen as the weakest link inside an organisation, concerning information security. In agreement to this, the following section will determine the actions of administrative employees when facing the top five identified threats.

IV. Analysis and results

In further addressing the objective of this paper, the next step is to determine the level of knowledge and awareness administrative employees possess when encountering threats while handling business information. This is done using a survey in the form of a questionnaire.

A. *Instrument Design and Categorization*

For the design of the questionnaire, suggestions from Rowley [5] are followed which formulates the different questions. Not only the suggestions, but also the predominant threats, that were identified from literature, are integrated into the design of questions asked to participants. This will enable one to find a correlation with facts from literature and results from the survey.

The questionnaire consists of fifteen questions. Twelve of the fifteen questions are scenario-based questions. Each question will contain a scenario, allowing the participant to select one of four provided answers. Depending on the chosen answer of a participant, a different outcome is calculated.

The twelve scenario based questions are divided into three main categories, allowing an easy method of determining the level of awareness. The different categories are abstracted from the well-known McCumber Cube as seen in Figure 1. The three different categories are confidentiality, integrity, and availability (CIA) respectively. Also from Figure 1, the three different information states are important namely: transfer, storage, and processing state.

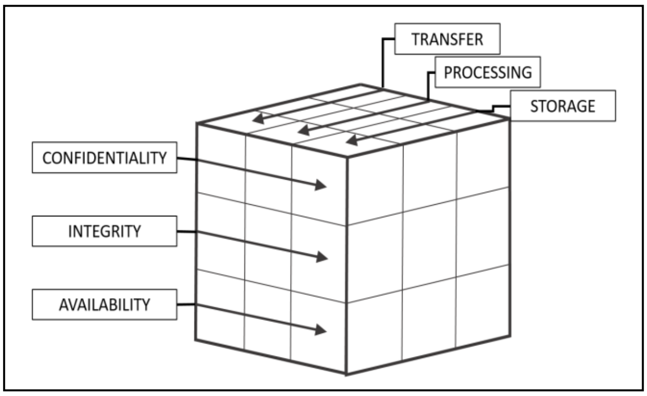


Figure 1. The Well-known McCumber Cube

For the exact explanation of the questionnaire, Figure 2 is used for reference. From Figure 2, one can identify the three categories on top. Underneath each category, any of the three different states may be used in a scenario. For instance, scenario 1, 4, 7, and 10 will be based on either the transfer, storage, or processing state. However, all four of these scenarios will focus only on the category of confidentiality.

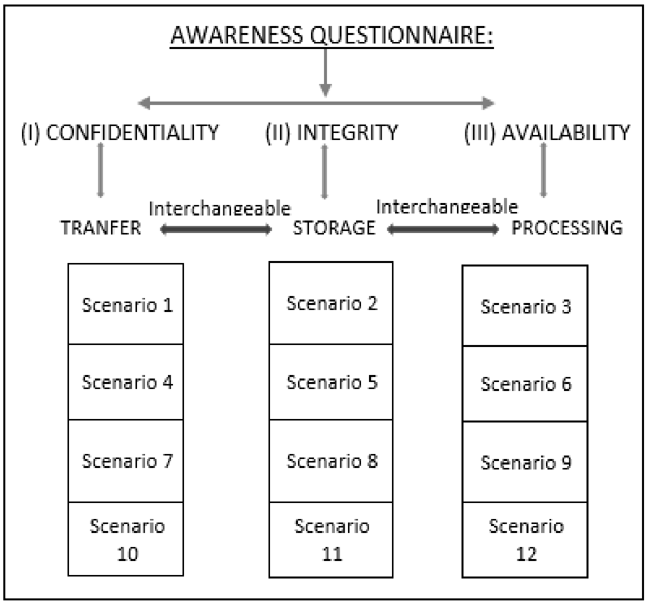
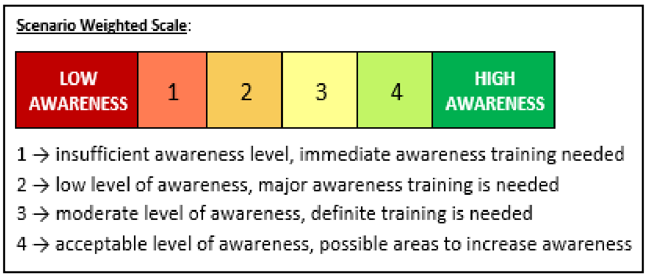


Figure 2. Visual Representation of Questionnaire Structure

Each scenario question was designed to test a specific category's awareness level. The following subsection highlights the method behind measuring the awareness level.

B. Weighted Ranking Scale

In order to collect usable quantitative data from the survey, a weighted ranking scale was designed. This weighted ranking scale allows the participant's awareness level to be determined. For instance, depending on the answer that a participant selects for a particular scenario, the participant will be ranked on the weighted ranking scale. Figure 3 shows the weighted ranking scale together with the association of each number. This weighted ranking scale is used in the following subsection to explain the overall working of the questionnaire.



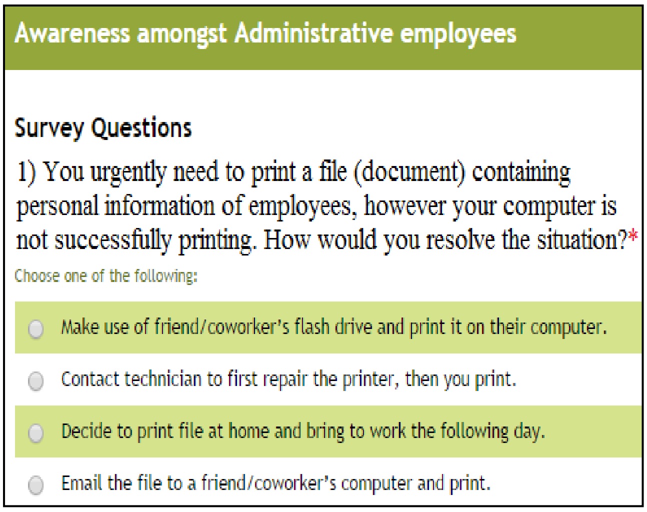
1 → insufficient awareness level, immediate awareness training needed
2 → low level of awareness, major awareness training is needed
3 → moderate level of awareness, definite training is needed
4 → acceptable level of awareness, possible areas to increase awareness

Figure 3. Weighted Ranking Scale

C. Example and Explanation

As mentioned earlier, each individual category (CIA) has four underlying scenarios. These four scenarios not only test the awareness level of its underlying category, but also the awareness level of the top identified threats respectively. Consequently, one is able to adequately test for awareness amongst administrative employees on various threats and categories.

The first scenario of the questionnaire is now used as an example to explain the overall working of the questionnaire. The participant will be given the scenario as shown in Figure 4.



Awareness amongst Administrative employees

Survey Questions

1) You urgently need to print a file (document) containing personal information of employees, however your computer is not successfully printing. How would you resolve the situation?*

Choose one of the following:

○ Make use of friend/coworker's flash drive and print it on their computer.

○ Contact technician to first repair the printer, then you print.

○ Decide to print file at home and bring to work the following day.

○ Email the file to a friend/coworker's computer and print.

Figure 4. Sample Scenario Based Question from Questionnaire

After reading the scenario, the participant will then have to choose one of the four provided answers. The answers are not sorted in any particular order when presented to the participant. However, when the answers are reviewed, to determine the awareness level, the answers will be sorted according to most suitable answers. Below is how the answers are sorted when determining the level of awareness:

1) Make use of friend/co-worker's flash drive and print it on their computer.

2) Email the file to a friend/co-worker's computer and print.

3) Decide to print file at home and bring to work the following day.

4) Contact technician to first repair the printer, then you print.

The value next to the answer enables the researcher to determine the awareness level of the participant. For instance if the participant chose the answer "Decide to print file at home and bring to work the following day". This issues the participant a weight of three (3). The three (3) on the weighted scale shows that the participant has a moderate awareness level; definite awareness training is needed for this particular scenario. Some scenarios allow the participant to select a fifth option named "I don't know". The weight of this option holds a value of one (1). This symbolizes that the participant is unaware and/or unknowledgeable of the threat. The sum of all the weight values allows one to determine the participant's overall awareness of the three categories, and the top identified threats.

The example scenario given above for instance, tests the participant’s knowledge regarding the threat of information leakage, under the confidentiality category while business information is in the transferring state. Table 2 lists all the scenario questions from the questionnaire, including a brief explanation of what is being tested.

TABLE II. EXPLANATION OF EACH SCENARIO IN QUESTIONNAIRE

Scenario No:	Explanation:
1	This scenario is determining the level of awareness concerning information leakage while in the transferring state. Transferring the sensitive file to another computer may result in information leakage.
2	The level of awareness is determined concerning integrity of business information while in a state of storage. If one changes the file, the integrity is compromised.
3	The level of awareness is determined concerning availability of business information while in a state of storage. If one removes the record, the availability of that information is compromised.
4	The level of awareness is determined concerning social engineering breaches. If the employee is not aware of these threats, it might compromise security and confidentiality of business information.
5	The level of awareness is determined concerning malicious attacks and integrity of business information while in a state of processing. If one use outdated logs, the business information might unreliable due to malicious activity
6	The level of awareness is determined concerning illegal activity and availability of business information while in a state of transferring. Surfing particular websites might severely affect the network availability and provide an open door into network
7	This scenario is determining the level of awareness concerning business information confidentiality and social engineering while in the processing state. If sensitive information is seen by unauthorized personnel, it might have a major effect on company.
8	The level of awareness is determined concerning integrity of business information while in a state of storage. Changing information without proof of validity can easily breach business information’s integrity.
9	The level of awareness is determined concerning availability and illegal activity while in a state of storage. Storing personal files at work can compromise the availability for necessary space needed for business information also creating an unsafe environment.
10	This scenario is determining the level of awareness concerning business information confidentiality while in the storage state. Not locking up hardcopies of sensitive information could easily have information leakage as effect.
11	The level of awareness is determined concerning malicious attacks and integrity of business information while in a state of processing. Using special privileges to change business information may cause a breach of integrity.
12	The level of awareness is determined concerning availability of business information while in a state of processing. Turning off or restarting a server will most definitely reduce the availability of business information for all employees.

Each of the twelve scenarios was weighted using the weighted ranking scale. The following subsection will report on the results of the questionnaire.

D. Questionnaire Results

Seventy-five questionnaires were distributed, by using email, amongst eleven sectors. Fifty responses were received which are categorized in the different organisational sectors as shown in Table 3.

TABLE III. DISTRIBUTION OF DEMOGRAPHIC SECTORS

Demographic Sector:	Number of respondents:
Academic Sector	4
Engineering Sector	4
Financial Sector	12
Human Resource Sector	2
Insurance Sector	1
Marketing Sector	5
Medical Sector	1
Production Sector	3
Public Service Sector	5
Safety & Security Sector	7
Secretarial Sector	6

After collecting all the responses, an average score was calculated, and mapped to a percentage value, for each category. A zero (0) percentage means no awareness exist compared to a hundred (100) meaning excellent awareness exist.

In order to have calculated an average percentage for each participant, each value of the weighted scale was given a certain percentage. The following list shows the percentage value for each weighted scale ranking.

- Weight of 1 → 0% to 25%
- Weight of 2 → 26% to 50%
- Weight of 3 → 51% to 75%
- Weight of 4 → 76% to 100%

By using this list, Figure 5 was created to represent the percentage for the overall average score of the three individual categories.

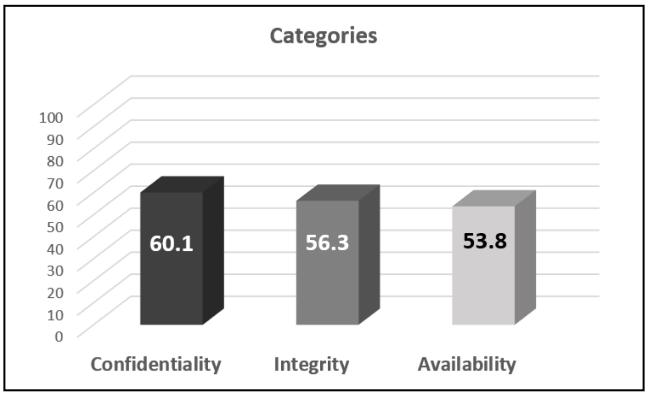


Figure 5. Overall Category Results

One can see that in the Confidentiality category, the participants scored 60.1%. This percentage is equal to a three (3) on the weighted ranking scale. The three (3) shows a moderate level of awareness, which is acceptable, however still suggesting that definite training is needed to increase awareness in this category. In the Integrity category, the participants scored 56.3%. This places them on a weight of three (3), just rising above a two (2). This also shows a moderate level of awareness exists, however it is in the early stages of awareness, and more awareness straining is necessary. Lastly, in the Availability category, the participants scored 53.8%. The weighted ranking is a three (3) however; it is extremely close to a two (2), which emphasises a need for major awareness training in the availability category.

Al three categories might seem acceptable at first, however the following three figures focus on the percentage value for each underlying scenario. This highlights specific threat areas that need attention within its respective category.

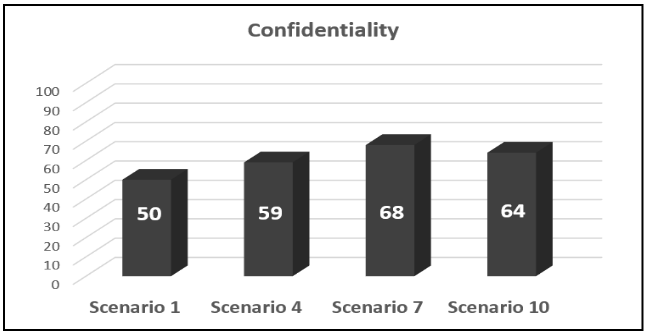


Figure 6. Results of Category: Confidentiality

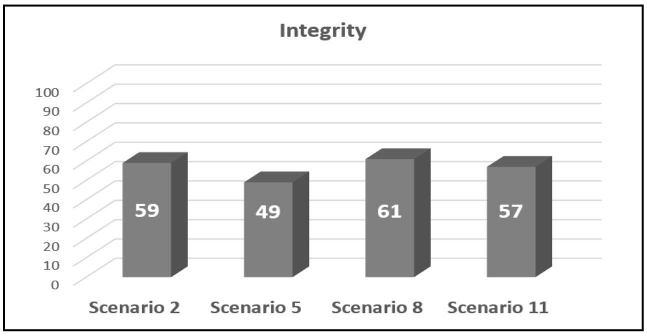


Figure 7. Results of Category: Integrity

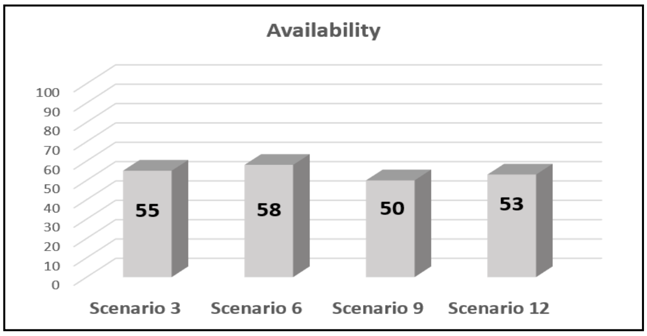


Figure 8. Results of Category: Availability

The previous three graphs highlight the three lowest scenarios, which is scenarios 1, 5 and 9. The following subsection will discuss the scenarios in more detail.

E. *Questionnaire Findings*

The three scenarios can be mapped to an individual threat area. Scenario 1 maps to threat of information leakage. Scenario 5 maps to the threat of malicious attacks and lastly scenario 9 maps to the threat of illegal activity. These three threats require more awareness training than the rest; however, it is essential that all threats receive proper awareness training. Further findings collectively suggest that there is a need for proper awareness training especially under the category of availability. If one were to look at the overall percentage score of the survey (56.7%) one would realize that it is barely a moderate level of awareness. This implies that overall; there is a definite need for awareness training on certain areas whilst major awareness training is needed in other areas. It is essential that this is addressed accordingly, otherwise without proper awareness training in these areas; administrative employees can become vulnerable, in turn leading to compromising an organisation's business information.

In order to address the much-needed awareness training, the following section proposes a possible solution that could aid in raising administrative employees' awareness.

V. Interactive Visual Library

From the previous sections, it is clear that awareness has to be raised regarding administrative employees. A possible way of raising awareness is in the form of an interactive visual library. For the purpose of this paper, an interactive visual library can be defined as a dynamic method in which theory principles are provided. The theory principles are presented in a holistic manner by which knowledge is transferred in an engagement between a person and computer. The question however is, what aspects are important in creating an interactive visual library? To answer the question, the following section will highlight the aspects that are deemed critical in creating such a library.

A. *Critical Aspects*

The first critical aspect to consider is the learning style. Three different learning styles can be derived from Neil Fleming's VAK model. The three styles are visual, auditory and kinaesthetic learning styles [15]. The three different styles are individually explained as:

- **Visual** – Visual material is preferred and helps with better remembrance.
- **Auditory** – Learners use the form of auditory sound waves to study and remember.
- **Kinaesthetic** – Prefer to work in groups together with the fact that a classroom affects the learner negatively.

According to Woda and Kubacki-Gorwecki [15] a staggering 65% of learners are visually orientated learners. The proposed solution therefore only focusses on the visual learning style. Providing a visual interactive library to promote awareness with administrative employees is suited considering the fact that a majority of administrative employees would better comprehend with a visual learning style. Ultimately, the interactive library promotes satisfaction, usability, and acceptance with the administrative employees.

The second critical aspect is to consider the fact that it is interactive. With regards to computers, Stevenson defines interactive as a two-way flow of information between a computer and a computer-user; the reaction of the computer responding to a user's input [4]. From the definition, it is clear that it allows the user to interact with the computer. The fact that the solution is interactive, allows the user to control the library according to his or her needs. An example of the interactive requirement, for instance, would allow the user to use a swiping gesture to rotate the threats in order to select a desired threat.

The third and final critical aspect to the proposed solution is that the solution is in the form of a library. To clarify, the proposed solution holds a collection of threats in one single integrated library. This negates the need for a user to search online for threats. As it is difficult to search for a threat online if one is not aware that a particular threat exist. Therefore, this library would ease the searching of threats. Thus, the third aspect promotes ease of use with users.

A combination of these three critical aspects forms the basis of the interactive visual library. In the following subsection, an example of such an interactive visual library is given, which serves as a proof of concept.

B. *Interactive Visual Library Prototype*

As mentioned in the previous subsection, the first aspect of the prototype is for it to be of visual nature. Figure 9 serves as a demonstration on how the prototype is structured. As seen from Figure 9, the prototype is in the visual form of a three-dimensional rotating wheel. The wheel is visually stimulating to promote satisfaction, usability, and acceptance with the administrative employees.

Each three-dimensional block is interactive in the sense that one could click on it. Depending on the platform it operates on, one uses either a computer mouse or even a finger on a touch display such as a smartphone. Each three-dimensional block represents a threat in itself. Each threat listed on the blocks is not only abstracted from literature's top five threats, but also on the results of the survey. In this main screen, one is able to rotate by swiping the blocks like a wheel. A user can rotate through all the blocks and select a specific block.

Once an administrative employee clicks on a specific block, another screen will be displayed. Figure 10 shows a clear view of the block that was clicked on. This screen educates the administrative employee on the specific threat. Details are given regarding the threat, such as description of the threats and possible examples of the threat, amongst others. Tips on how to protect against the specific threat will also be highlighted.

Figure 10 serves as an example for each of the three-dimensional blocks. Each threat has the same layout of information as well as interactive in the same way. As mentioned previously, the fact that all the threats are together in one library negates the need for an administrative employee to search for threats on the internet. This adheres to the third aspect of being an integrated library. Functionality is also embedded to allow an educational video to be played.

Figure 11 is a view of the tips specifically concerning the threat of social engineering. Once the user clicks on the button called "Tips to keep safe", this screen will appear. Typically, the same happens when the user clicks on the "More examples" button. The proposed solution currently serves as a prototype for a proof of concept on raising awareness amongst administrative employees. This prototype should be modified to extend its functionality. However, the fundamental part is to incorporate the three critical aspects into the design of the library.

VI. Conclusion

The first objective of this research has been achieved by identification of different threats through a review of literature, pertaining to acts of human error, or failure. The second objective was attained by integrating threats with three main elements in security – confidentiality, integrity, and availability of information. Consequently, this led to an integrated and informative design. Finally, a possible interactive visual library, through a proof of concept, was proposed which can possibly contribute to employees' information security awareness.

Further research can be done by other researchers in this domain to reveal other approaches that can improve information security awareness in organizations. Further research will also be beneficial in expanding the scope of identified threats, to incorporate more areas coexisting with acts of human error, or failure. In addition, further research is required to assess the contribution of the interactive visual library in raising administrative employees' awareness. Although the research focusses on adminstrative employees, further research can be done by expanding the scope to encompass all employee groups within an organization, such as IT personnel, executive management as well as support personnel. It would be benificial to compare the results from future research with the results of this study in order to identify possible patterns.

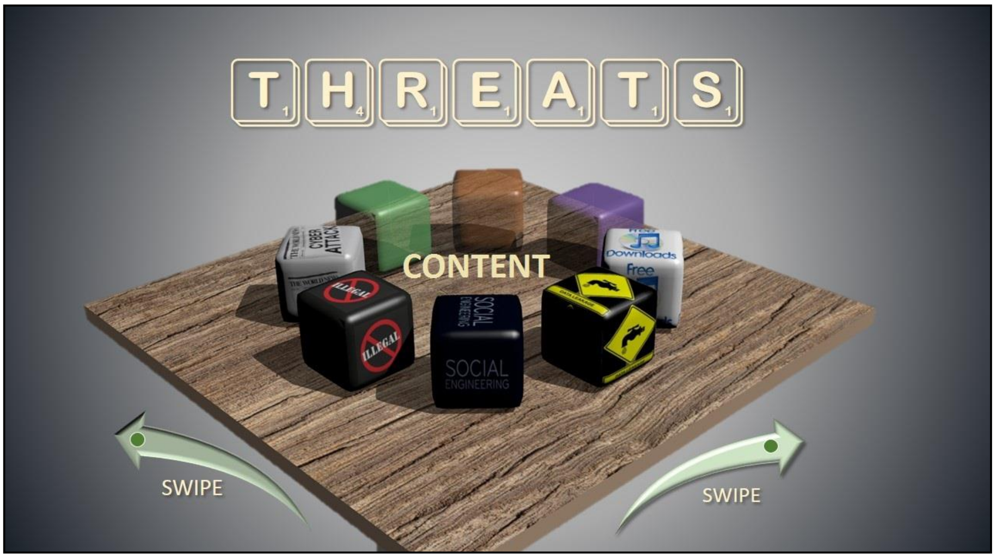
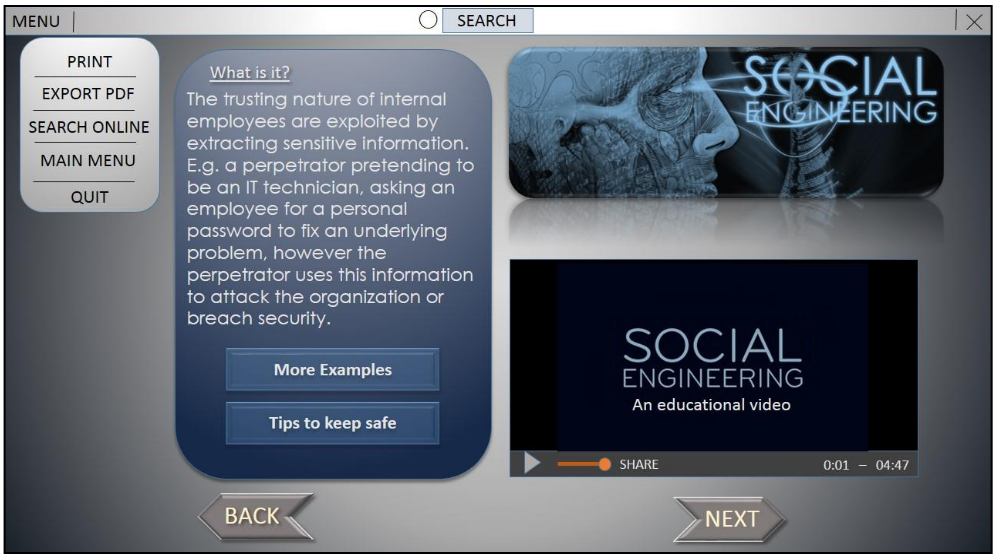


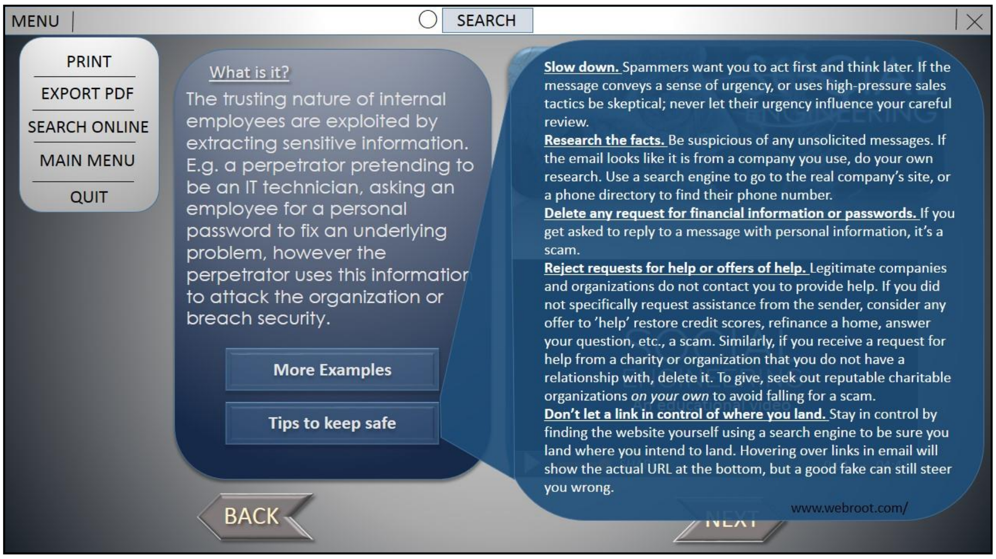
Figure 9. Demonstration of Visual Nature



What is it?

The trusting nature of internal employees are exploited by extracting sensitive information. E.g. a perpetrator pretending to be an IT technician, asking an employee for a personal password to fix an underlying problem, however the perpetrator uses this information to attack the organization or breach security.

Figure 10. Block Containing Information of a Particular Threat



What is it?

The trusting nature of internal employees are exploited by extracting sensitive information. E.g. a perpetrator pretending to be an IT technician, asking an employee for a personal password to fix an underlying problem, however the perpetrator uses this informatior to attack the organization or breach security.

Slow down. Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.

Research the facts. Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.

Delete any request for financial information or passwords. If you get asked to reply to a message with personal information, it's a scam.

Reject requests for help or offers of help. Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, answer your question, etc., a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations *on your own* to avoid falling for a scam.

Don't let a link in control of where you land. Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

www.webroot.com/

Figure 11. Tips to Keep Safe

Acknowledgment

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors, and are not necessarily to be attributed to the National Research Foundation.

References

[1] R. von Solms and S. H. (Basie) von Solms, “Information Security Governance: A model based on the Direct–Control Cycle,” Comput. Secur., vol. 25, no. 6, pp. 408–412, Sep. 2006.

[2] DBIR, “Verizon, Data Breach Investigation Report.” [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf. [Accessed: 22-Apr-2014].

[3] M. E. Whitman, “Enemy at the Gates: Threats to Information Security,” Commun. ACM, vol. 46, no. 8, pp. 91–95, 2003.

[4] Oxford Dictionaries, “Oxford Dictionaries,” Oxford University Press, 2016. [Online]. Available: www.oxforddictionaries.com/definition/english/administrative-assistant. [Accessed: 10-Apr-2016].

[5] J. Rowley, “Designing and using research questionnaires,” Manag. Res. Rev., vol. 37, no. 3, pp. 308–330, 2014.

[6] M. T. Siponen, “A conceptual foundation for organizational information security awareness,” Inf. Manag. Comput. Secur., vol. 1, no. 8, pp. 31–41, 2000.

[7] M. E. Whitman and H. J. Mattord, Principles of Information Security. Boston, USA: Cengage Learning, 2012.

[8] M. E. Whitman, “In defense of the realm: understanding the threats to information security,” Int. J. Inf. Manage., vol. 24, no. 1, pp. 43–57, Feb. 2004.

[9] Threat Horizon, “Threat Horizon 2013: Information security-related threats of the future,” 2013. [Online]. Available: https://www.securityforum.org/research/. [Accessed: 24-May-2014].

[10] C. Waxer, “The Top 5 Internal Security Threats - IT Security,” ITsecurity.com. [Online]. Available: http://www.itsecurity.com/features/the-top-5-internal-security-threats-041207/. [Accessed: 24-May-2014].

[11] Whittle, “The top five internal security threats.” [Online]. Available: http://www.zdnet.com/the-top-five-internal-security-threats-3039363097/. [Accessed: 24-May-2014].

[12] CSO Staff, “The Ten Habits of Highly Secure Employees.” [Online]. Available: http://www.csoonline.com/article/2123078/access-control/the-ten-habits-of-highly-secure-employees.html. [Accessed: 25-May-2014].

[13] E. B. Kim, “Recommendations for information security awareness training for college students,” Inf. Manag. Comput. Secur., vol. 22, no. 1, pp. 115–126, 2014.

[14] Ernst and Young, “Ernst & Young’s 2008 Global Information Security Survey,” 2008. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf. [Accessed: 20-Apr-2014].

[15] M. Woda and K. Kubacki-gorwecki, “Students Learning Styles Classification For e-Education,” in ICIT 2011 The 5th International Conference on Information Technology, 2011.