NJRST 1 (2018): 11-18

Namibian Journal for Research, Science and Technology

Vol 1, October 2018

Developing Security Metrics to Evaluate Employee Awareness: a Case of a Ministry in Namibia

D. Tjirare[1], F. Bhunu Shava[1]

[1]Computer Science: Faculty of Computing and Informatics, Namibia University of Science and Technology, Namibia[1]
Email: dkanikin@gmail.com, Cell 0855601000
Email: fbshava@nust.na, Tel and Cell (061) 207 2510, 081 328 9988

ARTICLE INFO

Article History:

Received: July 2017
Published: October 2018

Keywords:

security awareness, security metrics, employee security, employee security awareness, security objectives, information security and confidentiality, integrity, availability (CIA)

ABSTRACT

Employees that lack security awareness may cause a threat to an organisation unintentionally. A mixed research method was used to conduct a case study to evaluate the security awareness levels of employees in one ministry to reduce the risk associated with security threats.
A survey using a questionnaire was carried out with the ministry employees from four different departments. Collected data was quantitatively analysed to gauge the security risk of the organisation. Analysed survey results were used to develop security metrics using the Goal Question Metric approach and security objectives as measurements. The metric evaluated the security awareness level of employees at the ministry. Employees' responses were validated using helpdesk statistics on incident reporting and antivirus statistics.
The security metrics aim to assist the Information Technology department to detect security breaches early, and then develop a security awareness program and policies to promote security best practices. On the other hand the metrics can be used to encourage top management to get involved.
The results show that employees' awareness level was mostly low or elevated. Security standards and best practices are recommended based on the findings of risk rating per security category.

1. Introduction

With the advance of technology, more tools are available for unauthorized users to attack computer resources. Additionally, the open nature of the modern computing environment has also opened up security loopholes whereby without properly securing access to computer resources, there will always be eavesdroppers and hackers, who can use unsecured resources, steal identity, impersonate or take advantage of resources available to the rightful owner. Thus according to Hinson (2014), information security awareness (control) and measure is needed in an organisation in order to:

- Update users on general IS risks as well as assistance where needed.
- Elaborate leadership's assurance and pledge to information security.
- Educate users on the enterprise's information security policies, standards, procedures and guidelines, as well governing laws, rules and regulations.
- Encouraging users to act in a responsible and secure way.
- Improve the rate of detecting and reporting security violations.
- Save on security costs through early mitigation of security violations.

With this in view, a case study strategy was used to evaluate the security awareness level of the case site employees. The case site is committed to be a model

provider of accessible and timely service for all citizens. According to Alshboul (2010) security measures, controls, and policies are put in place to achieve information security objectives (confidentiality, integrity, and availability) and protect information assets.

Security weaknesses result in loss of finances, reputation, and market confidence (Alshboul, 2010). According to Hubbard (2002) if low 'security awareness' is present in an organisation, the vulnerabilities will be greater with respect to that organisation's people, and this is mainly due to ignorance of appropriate security behaviour, they will behave negatively. There is therefore a need to evaluate the security awareness level of the employees so as to provide them with appropriate awareness training and avoid the negative impact associated with a lack of security awareness.

The main research objective was to develop a security metric to measure security awareness level of the employees which was supported by the following sub objectives:

- To determine the confidentiality, integrity, and availability (CIA) awareness level among the case employee. This will be determined by the following security categories incident reporting, data confidentiality, email security, malware, phishing attack, password security, security policy, physical security, desktop security and internet security.
- To develop security metric that will measure employee awareness. The security metric will be a tool to measure the security awareness level.

The research questions used for this research project are listed below

- What is the confidentiality, integrity, and availability (CIA) awareness level among the case employee?
- What kind of security metrics can be used to measure employee security awareness?

2. Materials and Methods

The research project used the mixed research methodology, employing a case study strategy with the case site employees. An explanatory case study was used for this project to investigate and develop a security metrics to evaluate employees' awareness level as it strives to find factors that have an effect or compare findings to existing theories to identify theories better suited to (Oates, 2006, p. 143).

Four departments, namely Human Resources, Internal audit, Legal and Finance were selected for conducting the research because most employees that deals with the public belong to those departments. The researcher saw a need to measure the awareness level of MOJ employees as to determine their security risk levels, since they provide service to the public, their employee(s) need to be educated on security issues, to ensure that they understand the information security objectives to mitigate security risk. The project was conducted in two phases. The first phase was a survey using a questionnaire, where participants were requested to respond to questions on different security categories. Phase two was the development of a security metric using the results from the first phase. The metric development can be done using the bottom up approach or top down approach.

2.1 Security awareness survey

Data collection occurred in three phases, namely environment analyses, pilot studying and the actual survey with a questionnaire.

The questionnaire was divided into different security categories namely incident reporting, data confidentiality, email security, malware, phishing attack, password security, security policy, physical security, desktop security and Internet security. An online questionnaire link was emailed to the systems administrator to distribute to the four identified departs.

A concurrent, identical sampling method was used for this project to collect quantitative and qualitative data from the same participants (Onwuegbuzie & Collins, 2007). A random purposeful sampling scheme was used to select the identical samples, which were the four departments selected for the project to increase credibility (Robert Wood Johnson Foundation, 2008). An online questionnaire link was emailed to the departments.

There were mail server challenges at site, where by employees couldn't receive emails. This instigated a change in the data collection strategy to a manual distribution of questionnaires. Employees' manually

distributed the questionnaire to colleagues. Due to time constraints, willingness to complete the questionnaire was a huge challenge whilst a constraint, the sampling method was changed to the convenience sampling method because of the poor response from employees. Questionnaires were collected from employees that were available and willing to complete.

Table 1: Metric generation approaches (Payne, 2006)

Top down approach		
Define the aims of the security policies	To increase policy awareness in the organisation	Example objective for :to increase policy awareness levels among employees to 100%
Identify metrics to measure the improvement to policy awareness	Current ratio of policy awareness compared to baseline figure	Current employee awareness compared to total number of employees
Determine measurements for each policy awareness	Number of people trained on security policies in the organisation	Calculate the ration to target figure

2.2 Metrics development process using Goal Question Method (GQM)

The survey results informed the development of the metrics. In this research a top down approach of GQM was applied because its method was appropriate to answer the research question. The top-down approach starts with the objectives of the security program, and then works backward to identify specific metrics that would help determine if those objectives are being met, and lastly measurements needed to generate those metrics (Payne, 2006). Payne (2006) also states that the metric development should follow the following seven steps:

- Define the metrics program objectives and goals (evaluate the CIA levels of the organisation).
- Decide on which metrics to generate (using a top-down approach by finding the metrics can evaluate the objectives of the overall security program - for example as shown in Table 1).
- Develop approaches for identifying the metrics (How will the data be collected, methods of collection (survey, helpdesk statistics), frequency of collection, data analysis techniques, metric generation).
- Identify the standards and aims.
- Decide how to convey the metrics
- Make an action plan and implement it.
- Create a prescribed program review/refinement cycle.

Table 1 shows how the top down approach can be applied as an example of metric generation.

3. Results

Data analysis was conducted both qualitatively and quantitatively. The ordinal data was quantitatively collected from the questionnaire using Likert scale based questions. Each question response is assigned a risk value (1 for lowest - 5 for highest). The results of the survey were used to determine the overall risk score level of the organisation (Table 2).

Table 2: Awareness rating for security categories

Security Categories	Risk Value	Risk levels
Overall risk rating	38	Low
Incident reporting	28	Low
Data confidentiality	26	Low
Email security	47	Elevated
Malware, Viruses, worms, Trojans, Spyware and Adware	47	Elevated
Phishing	41	Elevated
Password security	32	Low
Security policy	34	Low
Physical security	54	Elevated
Desktop security	35	Low
Internet security	29	Low

The formula used to calculate the risk level:

- Add the total risk values from each survey to determine the cumulative total
- "Divide the cumulative total by the number of participants to get the organisation's risk score" (Bond, n.d).

- Using the risk score table, (Table 3) the researcher evaluates the organisation's overall risk level

Table 3: Risk levels adopted from Bond (n.d)

Risk Levels	Description
Low (25 – 39)	Employees are knowledgeable about good security practices and threats; they are well consentised and apply organisational security practices and policies.
Elevated (40 – 60)	Users have been on organisational Employees are taught about security principles and policies, they know the threats, however they do not implement good security practices and practices.
Moderate (61 – 81)	Employees know the threats and acknowledge that they should implement good security practices and procedures; however they need to be educated on organisational security principles and rules. They might not be able to recognise or act on a security incidents.
Significant (82 – 96)	Employees do not know good security practices and vulnerabilities and they are not submissive to organisational security values and rules.
High (97 – 120)	Employees do not know of security vulnerabilities and do not follow established security principles and rules. Their behaviour exposes them to attacks.

The outcome of applying the criteria was an identification of security critical factors which should be considered for security awareness programs in the case organisation.

The figures below present some highlights of the research findings from the quantitative data in pictorial form.

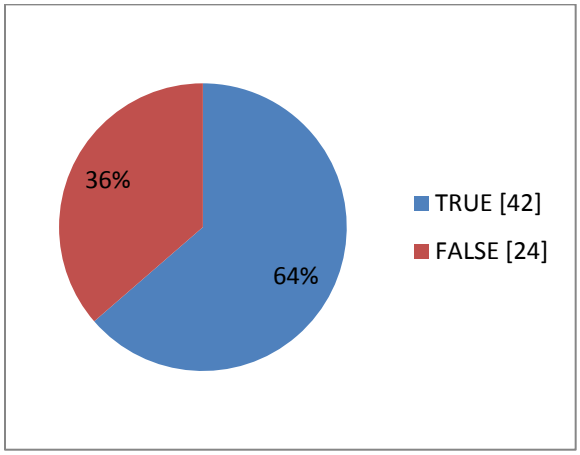

Figure 1. Computer cannot become infected if it has anti-virus program

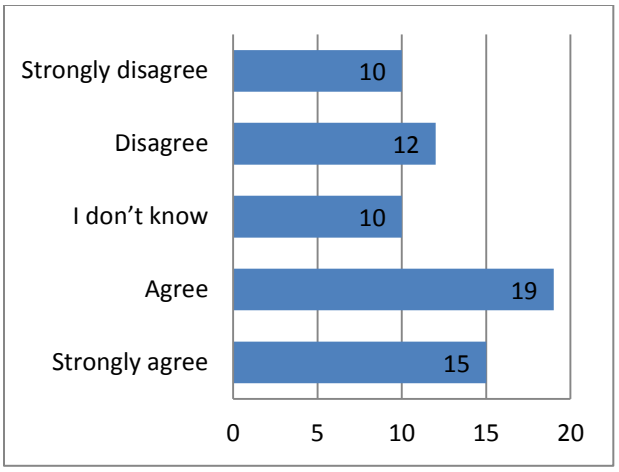

Figure 2. Protecting devices or information is the IT department responsibility

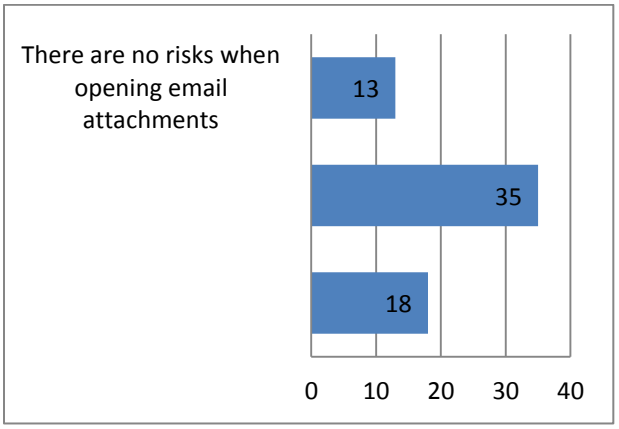

Figure 3. Opening an attachment in an email

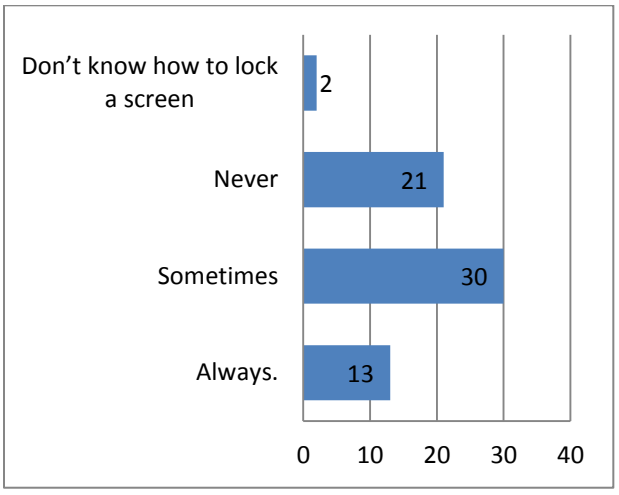

Figure 4. Locking a computer screen

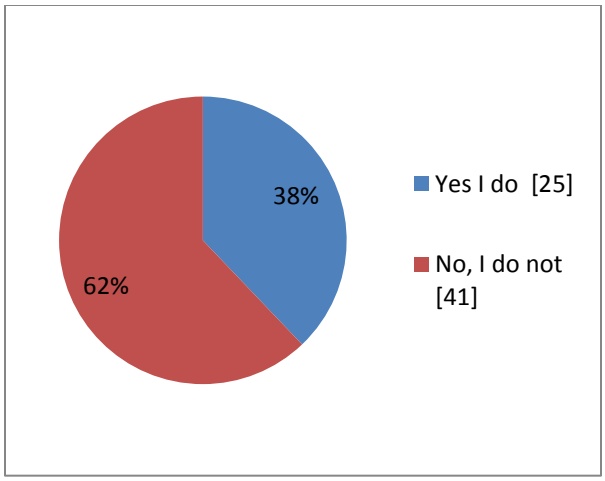

Figure 5. Identifying an email scam

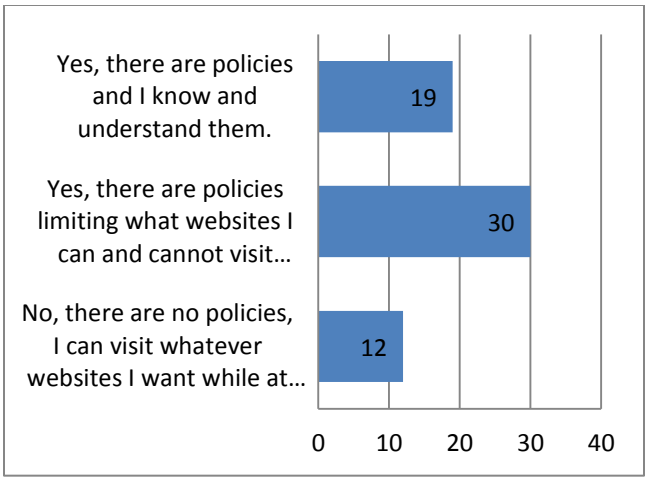

Figure 8. Internet policy

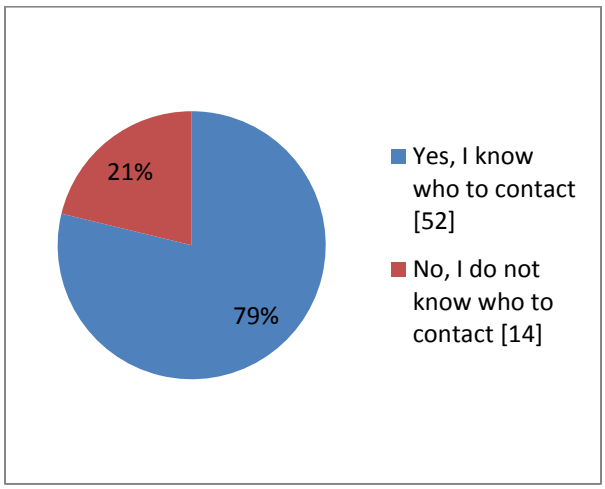

Figure 6. Incident Reporting

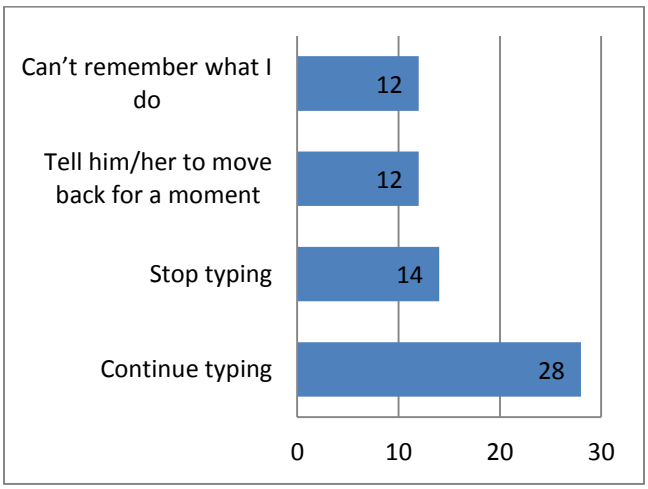

Figure 9. Reaction when a colleague goes behind your screen

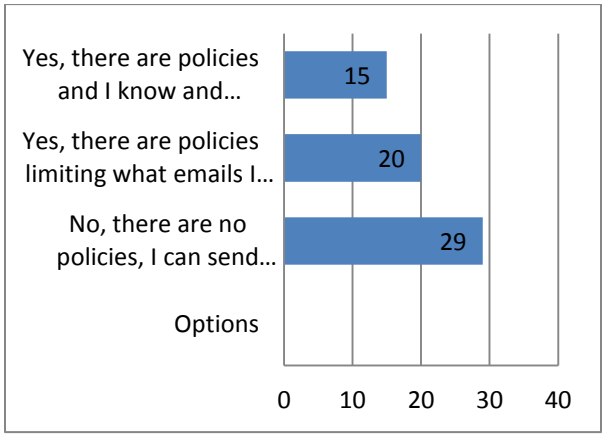

Figure 7. Email policy

The qualitative data was analysed using text identifying and coding theme. For example when analysing the ability to identify if the computer had been hacked, the following patterns emerged: Slow and freezing; unusual behaviour; change to the passwords, unsolicited reboots; shortcuts, double folders on the drive and so on. The results showed that a small number (5 of 66) participants access work accounts using public computers and are more likely to lose their credentials or corporate data if these devices are insecure or compromised. This would also indicate the user is not aware of the potential risks of doing so. In general, the number of employees that log into work account using public computers is less, this shows that most employees are aware of the risk associated with using public

Table 4: Security awareness level rating for the security categories

Incident reporting	Data	Email security	Malware	Phishing	Password	Security policy	Physical	Internet	Desktop
84 Significant	60 Elevated	35 Low	52 Elevated	41 Elevated	74 Moderate	32 Low	40 Elevated	37 Low	36 Low

computers. The researcher recommends that employees follow the organisations policy and best practises when using public computers.

A total of 32 participants said they share passwords, 28 specified with whom the password is shared and 4 did not specify. Employees specified that they share their password with managers and colleagues when they are on leave. One respondent said they share their password with anyone, they hold higher risk than the other participants.

4. Discussions

This section discusses the findings of the quantitative and qualitative data analysis of the different security categories. The purpose of the discussion is to validate the data using the analysed data to determine the data validity. Deductions drawn from the findings about the CIA awareness level are also discussed.

Table 4 is a summary of security awareness rating for different security categories based on Bond (n.d) risk score presented in Table 3. The case site's general security risk rating using quantitative data depicted that employees are conscious of good security values and threats, have been correctly educated, and conform to all organisational security principles and policies. This was in the email security, security policy, internet and desktop categories. However, according to the organisation's IT team, no such training was conducted. For example considering a response to question 4: "how careful are you when you open an attachment in an email?"; 29% know that they should only open expected attachments from people they know. The respondents (51%) would open the attachment as long as they know the sender and 20% believe that there are no risks. The result statistic shows that there is a need for training in this category.

Data, malware, phishing and physical security categories reflect that users have already been educated on organisational security principles and policies; they can identify threats, but may not follow good security practices. When it comes to passwords, users are conscious of threats and know that they should follow good security practices and procedures, but they need training on organisational security principles and policies. They might not be able to recognise or act on a security breach.

There was no awareness of incident reporting, users were not knowledgeable of good security practices or threats, nor are they conscious of or submissive to organisational security practices and policies. But the validation of the data using both qualitative and quantitative methods for security categories proved that employees have a low risk rating of most security categories. The overall security rating was calculated at 38, which is a low level. The weakness of using one metric is a biased assessment of the outcomes of a particular method; even if many quantitative metrics are used, the result of a method lack correct measurement lacking correct of the outcome (Witty, 2013). There is thus a need for repetitive measures after intervention.

Based on the findings, the following deduction can be drawn about the CIA status:

- Confidentiality (C) - Employees are conscious of threats and acknowledge they should follow good security practices and procedures, but need training on organisational security principles and policies. They cannot identify security breaches and take appropriate action
- Integrity (I) - Employees are not conscious of good security practices, values or threats, they do not know or submit to organisational security values and policies.
- Availability (A) - Employees are not conscious of good security practices or threats, they are not knowledgeable aware of or submissive to organisational security principles and policies. This may compromise data availability as they are prone to security attacks.

4.1 Derived metrics

The security metrics for the organisation were classified according to the CIA triad goals. Generally

all the measures focus on awareness or knowledge of different security issues that are common within the organisation. Table 5 presents a summary of the deduced metrics per security objective and a corresponding calculated risk rating. In total there are 11 metrics which can safely cover the CIA security triad. The 11 metrics were derived from the security awareness level for each security category that was assessed as shown in tables 3 and 5.

Table 5: Risk rating per security objective based on the metrics

Security Objectives	Metrics	Security objectives Risk Rating
Confidentiality	Incident Reporting Data Confidentiality Email Security Malware Phishing Password Security policy Physical Security Internet Security	76
Integrity	Incident Reporting Email Security Malware Password Desktop Security Internet Security	52
Availability	Malware Security policy Physical Security Desktop Security	40

Conclusion

Based on the phase 1 findings, there was a need to develop security metrics to measure the security in the organisation. Metrics were developed and a security awareness program needs to be developed and implemented in the case site. Frequent measurements of the security status need to be implemented to keep track of the state.

Overall employees' awareness level was low and security standards and best practices are recommended. There is a need to complete the awareness program and implement it.

Security awareness shapes attitude and behaviour change. The repeated application of good behaviour develops a security skill in employees for better organisational security culture.

The security metric will assist the Information Technology department to: (1) detect security breaches early, (2) develop security awareness programs and policies and (3) encourage top management to get involved by putting security measures which will assist in cost cutting and increase revenue. Future research directions are to apply the same metrics in a similar setup and evaluate the effectiveness thereof.

Again, first introduce the work and then briefly state the major results. Then state the major points of the discussion. Finally, end with a statement of how this work contributes to the overall field of study

Acknowledgements

During the research I have received knowledge, support, encouragement and guidance from extraordinary people who made this research project possible and it's my pleasure to be grateful to them. Firstly, I would like to thank my Lord, God for all his blessings and for making Mrs. Fungai Bhunu Shava my supervisor. I would like to thank my supervisor her encouragement, guidance, support from the beginning until the end which enabled me to understand research better and her patience at all times. Thank you to the Ministry IT department for allowing me to conduct a research at their ministry and their support, and all employees who were willing to complete the survey for the project. To my husband Wilson Tjirare, thank you for your patience, love, support and encouragement. To Grace Sageus and Michael Hamatwi thank you for your support and encouragement. Finally I would offer my gratitude to all those who supported me in any way for the completion of my research project.

References

1. Hinson. G., (2014).*The true value of information security awareness, addressing the rhetorical question: Why do we need security awareness?*. Retrieved from http://www.noticebored.com/html/value_of_awareness.html. 2014
2. Alshboul, A. (2010). *Information systems security measures and countermeasures: Protecting organizational assets from malicious attacks. Communication of the IBIMA, 2010*(2010), 9. doi:486878.
3. Hubbard, W. (2002). *Methods and Techniques of Implementing a Security: GSEC Practical Assignment, version 1.3. SANS.* Retrieved from http://www.sans.org/reading-

room/whitepapers/awareness/methods-techniques-implementing-security-awareness-program-417

4. SANS Institute. (2014). *Critical Security Control: 9, Security Skills Assessment and Appropriate Training to Fill Gaps.* Retrieved from http://www.sans.org/critical-security-controls/control/9

5. Communications Security Establishment Canada (CSEC). (2012). *ITSG - IT Security Risk Management: A Lifecycle Approach - Security Control Catalogue - ITSG-33 – Annex 3.* Retrieved from http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg33-ann3-eng.html

6. Goodchild, J. (2012). *Using security metrics to measure human awareness: Free tools offer security practitioners a way to measure the effectiveness of awareness programs.* Retrieved from http://www.csoonline.com/article/2132367/metrics-budgets/using-security-metrics-to-measure-human-awareness.html

7. Navarro, L. (2007). *Train employees - your best defense - for security awareness.* Retrieved from http://www.scmagazine.com/train-employees--your-best-defense--for-security-awareness/article/34589/.

8. Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt. United States of* America *(USA):* Pearson Education, Inc. from http://it-ebooks.info/book/2612/

9. PricewaterhouseCoopers. (2013). *Raising security awareness in your employees: The human factor in information security.* Retrieved June 2, 2014, from http://www.pwc.ch/user_content/editor/files/publ_adv/pwc_raising_security_awareness_e.pdf

10. MetricStream. (2014). *ISO/IEC 27002: Adopt best practices to improve accountability and communication.* Retrieved from

11. Enterprise risk management (2007). *Security Awareness Program: Control Essentials, 2(5)*. Retrieved from http://www.emrisk.com/sites/default/files/newsletters/ERM_Newsletter_May_2007.pdf

12. Chia, T. (2012). *Confidentiality, Integrity, Availability: The three components of the CIA Triad. Retrieved* from http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

13. Rathbun, D. (2009). *SANS institute infosec reading room: Gathering security metrics and reaping the rewards.* Retrieved from http://www.sans.org/reading-room/whitepapers/leadership/gathering-security-metrics-reaping-rewards-33234

14. Abbadi, Z. (2007). *Security Metrics What Can We Measure?.* Retrieved from https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed _Abbadi.pdf

15. Vogel, V. (2014). *A guide to effective security metrics.* Retrieved from *https*://wiki.internet2.edu/confluence/display/itsg2/Effective+Security+

16. Payne, S. C. (2006). *A Guide to Security Metrics: SANS Security Essentials GSEC Practical Assignment* Version 1.2e (2007). SANS.

17. Basili, V.R., Caldiera, G., & Rombach, D.H. (nd). T*he goal question metric approach.* Retrieved from http://www.cs.umd.edu/~mvz/handouts/gqm.pdf

18. Manke, S. & Winkler, I. (2013*). The habits of highly successful security awareness programs: A Cross-Company Comparison.* Retrieved from http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf

19. Oates, B.J., (2006). *Researching information systems and computing.* Los Angeles: Sage, pp. 143

20. Onwuegbuzie, A. J., & Collins, K. M. T. (2007). *A typology of mixed methods sampling designs in social science research.* The Qualitative Report, 12(2), 281-316. Retrieved from http://www.nova.edu/ssss/QR/QR12-2/onwuegbuzie2.pdf

21. Robert Wood Johnson Foundation. (2008). *Purposeful Random Sampling.* Retrieved from http://www.qualres.org/HomeRand-3812.html

22. Bond, T. (n.d). *Employee Security Awareness Survey.* Retrieved from http://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf

23.Witty, B. (2013). *Metrics must have qualitative and quantitative components.* Retrieved from http://certspeak.com/2013/01/24/metrics-must-have-qualitative-quantitative-components/

24.Standards Consultants, (n.d). *What is the difference between 27001 and 27002?.* Retrieved from http://www.standardscons