Metrics for Smart Security Awareness

William Aubrey Labuschagne, CSIR, Pretoria, South Africa [1]
Namosha Veerasamy, CSIR, Pretoria, South Africa [2]

[1] wlabuschagne@csir.co.za
[2] nveerasamy@csir.co.za

Abstract: Technology has integrated with society resulting in the dependence of its availability to conduct daily activities. In the corporate domain the availability of information is critical to decision making as it affects the bottom line of the business. Also, the compromise of information could have detrimental effects on the organization as investors and customers could lose confidence. Information Communication Technology (ICT) users need to made aware of their responsibilities for protecting data and assets. Security awareness can help enable users with the necessary knowledge to operate in the ICT domain more safely. Smart security awareness will consist of proactive measures and mechanisms in systems that will automatically detect when users are moving away from safe practices. This paper will discuss the practical implementation of metrics within a smart security awareness system to promote safe security practices. The application of proactive mechanisms will help reduce security breaches. This paper introduces the concept of smart security awareness. However, measuring the effectiveness of smart security awareness can be challenging. This research proposes customised smart security awareness metrics that can help assess smart security awareness more effectively. In this paper, a more proactive smart security awareness system and metrics are proposed, which integrates various measurement tools. Overall, the research aims to provide a more practical approach for establishing and assessing smart security awareness in an organization. In general, the proposed metrics can serve as an important tool to improving security in an organization. The use of more innovative metrics can help assess security awareness more effectively.

Keywords: smart security awareness, security awareness, metrics, situational awareness, Smart Security Awareness System

1. Introduction

Technology has integrated with society resulting in the dependence of its availability to conduct daily activities. In the corporate domain the availability of information is critical to decision making as it affects the bottom line of the business. Also, the compromise of information could have detrimental effects on the organization as investors and customers could lose confidence. Goel and Shawky (2009) reported a 1% negative impact on market value once a breach has been disclosed. Security breaches have been reported by Adobe (Zorz 2013) and American Express (Buffington 2014) whereby infiltration by cyber criminals resulted in the loss of client information and intellectual property. Organizations are required to comply with standards defined within the business domain. For example, within the credit card industry the Payment Card Industry Security Standards Council developed a standard to protect clients (Shaw 2009). Security awareness forms part of such standards as in the case of PCI DSS Requirements 12.6 (LLC 2010) and ISO/IEC 27002 Paragraph 8.2.2 (International Standards Organisation (ISO) 2012) that focus on securing the human element. Wilson and Hash (2003) define security awareness as "*Efforts designed to change behavior or reinforce good security practices*". In other words, the effectiveness of a security awareness program can be measured by the change in behavior related to information security, for example the adoption of strong passwords after attending a awareness program that addressed password management.

Security awareness programs should address a specific need and not merely to inform participants but also change behaviour. Parsons, McCormac, Butavicius, Pattinson and Jerram (2014) showed the security awareness programs are more effective once the training is focused on addressing a specific need that the participants can relate to and how the issue affects them. Kruger and Kearney (2006) conducted a study by developing a prototype model to assess awareness levels within a company and concluded that knowledge (what you know), attitude (what you think) and behavior (what you do) should be considered when measuring effectiveness. Behavior is a key indicator of effectiveness as it

was also noted by Wilson and Hash (2003). Success of security awareness programs have been reported by Eminağaoğlua, Uçarb and Erenc (2009) who conducted a 12 month study on a company with 2900 employees. They focused on password usage and with the use of password audits measured the effectiveness of the implemented security awareness program.

Schneier (2013) states that security awareness training is currently not working. If security training is merely carried out to meet compliance requirements, its effectiveness will never be measured or even considered as an essential requirement to the organisation. Higgins (2013) states that security awareness should be seen as a developing culture which focuses on security. Making security awareness a priority demonstrates that an organisation is serious about information security. Furthermore, security awareness training that is focused on the skillset of the employee promotes the actual development of the employee and not just a compliance measurement for the organisation. However, to be truly effective security awareness metrics need to take into account customised solutions that can offer greater insights. Khan, Alghathbar, Nabi and Khan (2011) identified methods to deliver security awareness topics to the target group. These include posters, email, newsletters, in person training, computer based training**.** Kajzer, D'Arcy, Crowell , Striegel and Van Bruggen (2014) explored whether the personality of a participant would improve the retention of transferred knowledge. They concluded personality does play an effect. Various issues can therefore affect security awareness. It is therefore critical to measure the effectiveness of all these methods in real time as a proactive measure to address gaps in the security awareness program before a breach occurs.

The authors proposes the deployment and rollout of automated security awareness based on current events and threats originating from the environment resulting in proactive adaption of security measures limiting human intervention.

With the advances in machines learning the capability to automate cyber attacks can be developed as demonstrated by Lauinger, Pankakoski, Balzarotti, and Kirda (2010) by automating social engineering attacks. Yuri (2017) also reported that the automation of creating phishing emails is becoming prevalent and more effective. This is due to the collection of personal data from various online sources which include social networking sites and the use of machine learning to automatically develop personalised social engineering attacks based on the collected data. Dietterich (2010) developed a capability using machines learning to perform cyber situation awareness. However, the proposed smart security awareness concept would include other aspects which include the human behaviour and more importantly the evolving threat landscape originating from the external environment. Barford (2010) demonstrated the use of Honeypots to create a network situational awareness. Vast sets of data would be generated and stored. The use of Big Data analyses would be required to create insight and actionable responses as seen by the development of the Cyber Situational Awareness Analytic Capabilities (CSAAC). Bart (2016) developed a framework to create cyber situational awareness using big data to collect, analyze, visualize and share information pertaining to Cyber Threat Analysis.

Smart cities are built around the concept of collecting data from several sensors to create situational awareness by analysing the big data collected and using machine learning to make sense of the data and react if required. This can be demonstrated by having sensors measuring traffic flow of the highways and automatically reporting if an accident occurs and dispatch traffic control units to the scene of the incident. Another example is the use of sensors to detect water leakage and automatically informing the response teams for reparations. These capabilities are possible by collecting data from the environment and ensuring intelligence is developed to react automatically without human intervention. The concept of smart cities has also been transitioned into other domains like agriculture which has become known as smart farming. In this case, sensors would inform the farmer about the current situation and could automatically make decisions. Take the example of tractors with sensors detecting the fuel available and other sensors reading the fuel levels at the fuel depot located on the farm. If the fuel levels are low on the tractor and the depot, then the fuel supplier will be automatically contacted to replenish the fuel on the farm. The concept of ‘smart’ can also been seen in tourism and health. Taking these cases into consideration the concept of ‘smart’ could be loosely defined as collecting data to create situational awareness and automatically respond to a specified condition. This concept can be extended to information security awareness resulting in the concept of smart security awareness. This paper will discuss the practical application of smart security

awareness where sensors would provide a digital situational awareness and automatically respond to potential internal and external threats.

2. Smart Security Awareness

The concept of smart security awareness is the creation of a capability to automatically sense a threat within and external to the organization resulting in an automated proactive response to mitigate and secure the organization. This paper discusses two components of such a capability which include the system and the metrics used to create smart security awareness.

2.1 Smart Security Awareness System

The proposed establishment of smart security awareness would replicate the implementations of smart cities utilizing technology which include Big Data and the Internet of Things. The use of these two technologies creates an eco system for situational awareness and automated proactive responses limiting human intervention and reducing errors prone to humans like fatigue and stress.

The high level design of the Smart Security Awareness System is depicted in Figure 1. Overall, the Smart Security Awareness System would require capabilities to sense events and determine a response affecting each of the domains.

The conventional distribution of information is initiated by a source and then follows a network path until the destination is reached. However, within the internetworked environment, whereby devices are connected to the Internet, four domains are identified which affects cyber security. These four domains consist of the environment (also known as the threat landscape), the network, the host and finally the end user. All communications within cyberspace would traverse through these four domains. The environment is seen as the external threat landscape whereby new attacks are developed to target assets. Due to the high interconnectivity, the spreading of information/ events takes place at a rapid rate. Therefore, awareness of new information/events is also occurring rapidly. For example, the release of source code of exploiting tools is reported and discussed online. Using this information is critical as end users might not have an interest or access to that information which affects the security of the user in the long run. The use of smart security awareness would use the information about releasing source code to the public and create awareness internally to the organization.

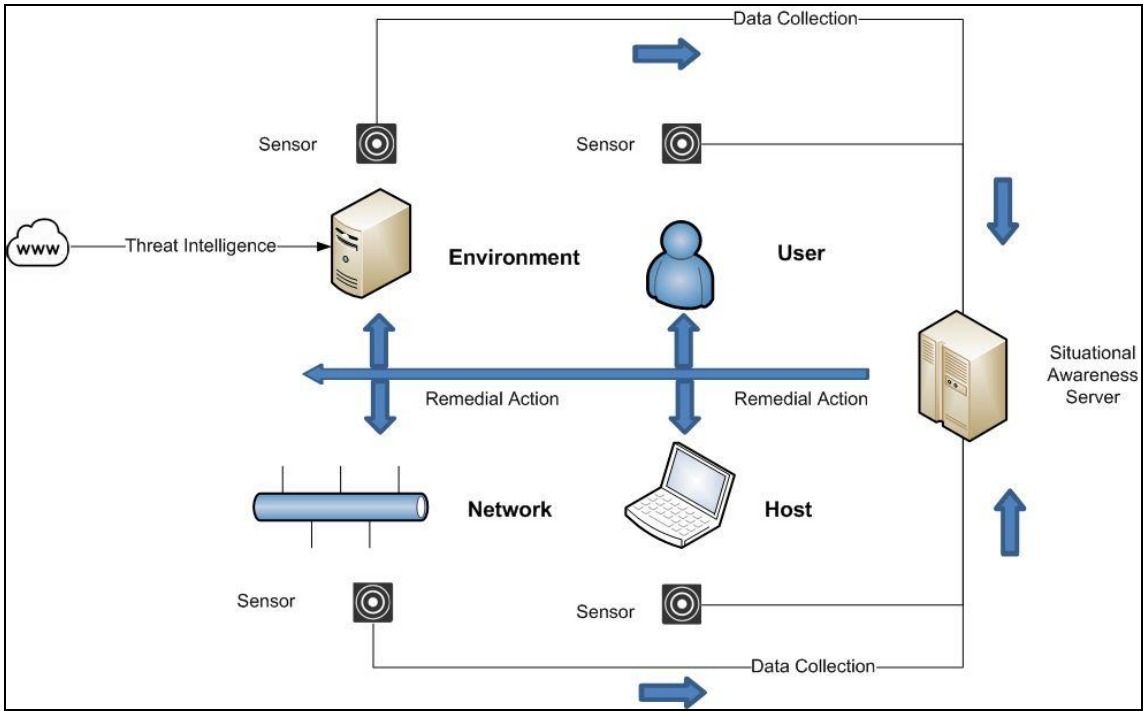

Figure 1: Smart Security Awareness System High Level Design (Source: Own)

Each domain which forms part of the Smart Security Awareness System would have sensors deployed to collect data. The data would be transported to a centralized situational awareness capability for analyses and create the appropriate response in the form of remedial action. The use of threat intelligence feeds could automatically sense the existence of a new threat and automatically update sensors within the organization. For example, if a new threat is identified whereby Microsoft Word is targeted to carry exploits, automated emails could inform users within the organization of Microsoft Word documents infected with potential malware. The organization could also automatically quarantine Microsoft Word files before releasing them to the users and lastly ensure that the system security solutions have been updated. These updates could automatically be rolled out to end users devices. The role of intelligence and situational awareness using reliable data is critical in an automated environment reacting to a legitimate threat.

Any solution utilizing situational awareness is affected by changes. In other words, the positive and negative effects of a Smart Security Awareness System need to be taken into consideration. The system would defensively put measures in place to mitigate the threat but cyber criminals could craft events to artificially control the Smart Security Awareness System. The sensors defined within the design of the Smart Security Awareness System would collect data from each domain and be utilized within metrics forming part of smart security awareness.

Kotenko, Novikova (2014) and Erbacher (2012) proposed the use of a dial based graphs to represent metrics. The use of rings and colours would enable users to quickly obtain cues from the metric. Their implementations were adapted for smart security awareness providing users with a mechanism for situational awareness. Four quadrants were created to represent awareness domains (as depicted in Figure 2) and cover the current threat landscape, network, host and the user. Both the threat landscape and the network are external to the organization and the device of the user, while the host and user behaviour is considered internal to the user as they have a level of control.

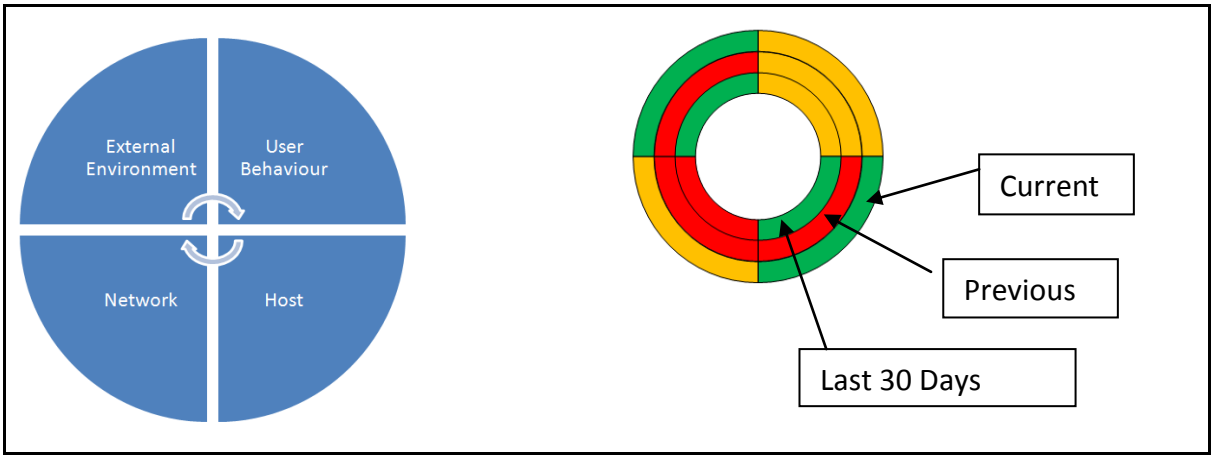

Figure 2: Smart Security Awareness Domains and Indicator

The four quadrants are then divided into three layers. The outer layer represents the current status, the inner layer is the previous status and the inner layer is an average status for the last 30 days. Status is defined as level of risk whereby red is a high risk status, for example disabling a firewall. Amber represents medium risk and green is low risk. In the event that a new exploit is identified within the external environment, upon classification the smart security awareness system would obtain the necessary information about the exploit and trigger the required actions. In this case the exploit targets Microsoft documents, the dial would be updated to indicate a high risk event has been identified in the threat landscape. The host quadrant would be updated to red as the host device is vulnerable. In the backend of the organization's system, all Microsoft files entering would be vetted before delivering to the recipient. Mitigation and awareness information would then be also sent to the end user and updates to the system needs to automatically applied to secure against the possible threat. Another example is if the user installs software and opens a port. This action is seen as creating a vulnerability and violating a policy. Therefore, the user would the labelled red (high risk). The host and network would then be either amber or red based on the type of port opened. The

environment external would remain green as the threat does not originate from that domain. In this case, the system would inform the end user via email and provide remediation action, the network configuration might be updated to prevent data to be directed to the opened port and automatically remove the software from the host. This dial could be installed as a widget on the device and be always visible to the end user to provide situational awareness.

The next section discusses an abridged list of proposed metrics associated with smart security awareness.

2.2 Smart Security Awareness Metrics

The Merriam-Webster dictionary defines metrics as a system of standard measurement (2014). In business terms, it refers to a type of measurement that is used to gauge a quantifiable component of performance (Rouse 2007). Metrics can help assess value outputs (like checking for correct behavior) and also to improve processes. Process improvement metrics can help increase effectiveness. Value checking metrics can influence critical business indicators like costs, revenue, productivity and even risk. Metrics provide for data quantification in the following ways:

- Analysis of field
- Identification of key characteristics in a field
- Help with the creation of scenarios (before- and-after, what-if, why-why-not)

Savola (2007) explains that measurements can be obtained from counting metrics generated from analysis. Furthermore, Savola points out that metrics are derived by comparing two or more measurements. Overall security metrics help to assess the behavior and performance in a field. In order to propose effective metrics, it is important to define proper measurement criteria. According to Jaquith, good metrics should (2007):

- Be understandable across the organization and the industry- Employees and industry members should have a shared comprehension of the indicators. A shared understanding helps create a uniform system of measurement that can be used for measurements. The use of simple and standardized terminology can aid with the comprehension of concepts.
- Be calculated mechanically- The use of automated calculations ensures that the numbers are collected systematically. Manual collection of data can be labour intensive. By using mechanical methods, data can be collected seamlessly.
- Be clear and ambiguous- Using clear language can reduce ambiguity and confusion.
- Consistently measured- If the data collection is repeated, the same values should be obtained. To maintain credibility, there should be no subjective influence.
- Cheap to compute- keeping the costs low makes the metric collection more affordable.
- Expressed as number or percentage- the use of a number or percentage makes the measurement value much easier to read. The use of subjective ratings or ordinal scales do not provide for uniform measurements. Numbers and percentages are more objective and provide for better context of the values.

Overall, metrics should aim to be simple, consistent, automated, affordable and understandable. This will help provide for better measurement and assessment of the values.
The PCI Security Standards Council created best practices for implementing a security awareness program that provides a comprehensive list of metrics to be applied (Security Awareness Program Special Interest Group PCI Security Standards Council 2014). For example, "*Vulnerability scans are active and detect high or critical vulnerabilities*", "*Updates and changes implemented successfully with minimal disruptions*" and "*Malware infections reduced over time*" are considered metrics as they can be measured and provide relevant information. It is important to note that metrics specific to behaviour change is critical in assessing if an information security awareness campaign or program is successful. Winkler (2013) highlighted that merely attending an information security awareness course due to compliance would not be effective. Mandatory training without understanding the need would not encourage participants to change behaviour and in most cases the content will be forgotten.

Table 1 consists of metrics to be used within smart security awareness to establish the capability. Future work within the domain of smart security awareness would expand on a comprehensive list. It should be noted that metrics needs to be applied to each unique circumstance and base on the specific needs of the organization.

Table 1: Smart Security Awareness Metrics

Environment	Network	Host	User
Disclosure Time	% of Attachments Vetted (Deploy in Sandbox Environment)	% of Unknown Services / Applications	Security awareness level
Reliability of Threat Intelligence Feed	% Deviation from Baseline	Time to Update Operating System	Number of Policy Violations
Time to Release Mitigation Response	% of Unauthorized Network Traffic (FTP)	Time to Update 3rd Tools (Java and Acrobat Reader)	% of Web Traffic for Personal
Incident Response Time	% of Unauthorized Network Devices	Device Encryption (Hard Drive and External)	Time to open Emails with Attachments
Vendor Response Time	Time to Recover from replacing physical network device (Router)	% of Malware Infections Reported	Password Strength
Technology security maturity	Time to Respond to Incident	% Host Intrusion Detection Alerts	% Remote Access to Organization Network
Compliance to Government Policies	Time to Identify Network Topology Changes	Time to Update Anti Virus	Number of Lost Devices (Property)
Vulnerability index	Time to Identify Unauthorized Network Service (Database Server deployed on User Device)	% Security Controls Deployed (Operating System Hardened)	Number of non role defined applications installed by User

The “Security awareness level” metrics listed in the Smart Security Awareness Metrics table is measured in the following ways:

- **Personal interviews**- are viewed to be one of the best methods to assess awareness levels and also teach people about security awareness topics. However, the time to interview each employee in an organization is not feasible. A trained interviewer would also be required which would introduce additional costs. Furthermore, employee responses from an interview could be negative. Employees might deem the interviews as being invasive, unnecessary or not useful. This could detract from the purpose for the interview. Moreover, the scheduling of an interview would need to take into consider productivity and availability constraints.
- **Surveys**- using surveys, an organization could gain a high-level view of the security awareness levels of its employees. A survey could also function as a type of early warning system so as to identify potential issues. Technological solutions for surveys now provide for automated deployment and analysis methods.
- **Quizzes**- provide another form of in-depth identification of problem areas or individuals who may require more intense training or remediation. By using surveys and quizzes, an organization can identify security awareness topics that require deeper attention. The use of scripts can automate the process of deploying and analyzing quizzes and surveys. Automated techniques can also help reduce interferences with employee productivity as they may complete these assessment measurements at their own convenience.
- **Forums** – can provide employees with the opportunity to discuss security topics. Forums can replace interviews which focus on direct outputs from the employees. Instead forums provide a more interactive environment for information sharing. As part of the analysis, the nature of the discussion and topics can be used to help determine retention rate of topics and which areas are of concern. Forums provide a medium for knowledge capture which can help create better security awareness.

It should be noted that each of these methods does have disadvantages which should be considered if it will be utilised to determine the security awareness levels. For example, the data may not truly reflect the situation. Couper (2000) explains that measurement errors is the deviation of the respondents answers from their true values. This may stem from personal issues of the respondent like motivation, deliberate distortions, inability to understand or from the actual instrument of the

survey like poor wording, bad design or technical issues. Overall, the measurement of the security awareness metrics should be designed to prevent bias from filtering through. The alternative methods discussed provide different ways of capturing the metrics that may provide more impartial results.

This section looked at metrics that can be utilised as part of smart security awareness. The goal of the paper was to propose how smart techniques can be used part of security awareness and how metrics can contribute to the field.

3. Conclusion

Security awareness can be further improved by focusing developing capabilities that are situational awareness and automate the process to spread awareness of imminent threats and proactively adapt systems to prevent exploitation. With the current advances in technology which include machine learning and development of Big Data and Smart Cities a more effective capability based on automation and intelligence is possible to improve security awareness.

This paper introduces the concept of smart security awareness and proposes a system and supporting metrics in developing such a capability. Overall, metrics provide a means of measurement that can be used for performance assessment and situational awareness. Actual behaviour together with effectiveness can be assessed. Good metrics should strive for understandability, automatic computation, unambiguity, consistent measurement, affordability and simple expression like a number or percentage. If these principles are applied, metrics can be more effective.

Metrics can be used in a proactive or reactive manner. Proactive measures can be used to educate or warn users about potential dangers, for example a security awareness training session focusing on phishing. Reactive measures assess behaviour changes like passwords patterns and operating system updates based on reliable threats intelligence. This paper proposes a high-level smart security awareness metric system that incorporates novel proactive and reactive components. Overall, the proposed metrics can serve as an important tool to improving security in an organization. The use of more innovative metrics can help assess security awareness more effectively.

4. REFERENCES

Barford, P., Chen, Y., Goyal, A., Li, Z., Paxson, V. & Yegneswaran, V. (eds) (2010) *Employing Honeynets For Network Situational Awareness*, Springer US, Boston, MA.

Bart, D. (2016), *Big Data Platform (BDP) and Cyber Situational Awareness Analytic Capabilities (CSAAC)*, Defence Information System Agency.

Buffington, A. 2014, 5 June 2014,-last update*, American Express credit card data exposed* [Homepage of Net-security.com], [Online]. Available: http://www.net-security.org/article.php?id=2034 [2014, 0611] .

Couper, M.P. (2000) Review: Web surveys: A review of issues and approaches, *Public opinion quarterly,* : 464-494.

Dietterich, T.G., Bao, X., Keiser, V. & Shen, J. (eds) (2010) *Machine Learning Methods for High Level Cyber Situation Awareness*, Springer US, Boston, MA.

Eminagaoglu, M., UÃƒÂ§ar, E. & Eren, S. (2009) The positive outcomes of information security awareness training in companies-A case study, *Information Security Technical Report,* **14**(4): 223-229.

Erbacher, R.F. (2012), "Visualization Design for Immediate High-level Situational Assessment", *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*ACM New York, NY, USA, : 17.

Goel, S. & Shawky, H.A. (2009) Estimating the market impact of security breach announcements on firm values, *Information & Management,* **46**(7): 404-410.

Higgins, K.J. 2013, 4 April-last update*, Hacking The User Security Awareness And Training Debate* [Homepage of Dark Reading], [Online]. Available: http://www.darkreading.com/end-user/hacking-the-user-security-awareness-and/240152288 [2014, 0210] .

International Standards Organisation (ISO) (2012), *Information technology — Security techniques — Guidelines for cybersecurity*, ISO/IEC JTC 1/SC 27/WG4, Geneva.

Jaquith, A. (2007) *Security metrics: replacing fear, uncertainty, and doubt,* Addison-Wesley Professional.

Kajzer, M., D'Arcy, J., Crowell, C.R., Striegel, A. & Bruggen, D.V. (2014) An exploratory investigation of message-person congruence in information security awareness campaigns, *Computers & Security,* **43**(0): 64-76.

Khan, B., Alghathbar, K.S., Nabi, S.I. & Khan, M.K. (2011) Effectiveness of information security awareness methods based on psychological theories, *African Journal of Business Management,* **5**(26): 10862-10868.

Kotenko, I. & Novikova, E. (2014), "Visualization of Security Metrics for Cyber Situation Awareness", *2014 Ninth International Conference on Availability, Reliability and Security*IEEE , : 506.

Kruger, H.A. & Kearney, W.D. (2006) A prototype for assessing information security awareness, *Computers & Security,* **25**(4): 289-296.

Lauinger, T., Pankakoski, V., Balzarotti, D. & Kirda, E. (2010), "Honeybot, Your Man in the Middle for Automated Social Engineering", *Proceedings of the 3rd USENIX Conference on Large-scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More*USENIX Association Berkeley, CA, USA, : 11.

LLC, P.S.S.C. (2010), *PCI DSS Requirements and Security Assessment Procedures*, Payment Card Industry Data Security Standard.

Merriam-Webster 2014, *, Metric*. Available: http://www.merriam-webster.com/dictionary/metric [2014, 0311] .

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. (2014) Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), *Computers & Security,* **42**(0): 165-176.

Rouse, M. 2007, *Definition Business Metric*. Available: http://searchcrm.techtarget.com/definition/business-metric [2014, 0311] .

Savola, R. (2007), "Towards a security metrics taxonomy for the information and communication technology industry", *International Conference on Software Engineering Advances (ICSEA)*IEEE , : 60.

Schneier, B. 2013, *Definition Business Metric* [Homepage of Schneier on Security], [Online]. Available: https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html [2014, 0214] .

Security Awareness Program Special Interest Group PCI Security Standards Council (2014), *Best Practices for Implementing a Security Awareness Program*, PCI Security Standards Council.

Shaw, A. (2009) Data breach: from notification to prevention using PCI DSS, *Colum.JL & Soc.Probs.,* **43**: 517.

Shoshan, Y. (2017) *Automation in Phishing: Fighting One Automated Industry with Another*.

Wilson, M. & Hash, J. (2003), *Building an information technology security awareness and training program (NIST SP 800-50)*, National Institute of Standards and Technology (NIST), Washington, United States of America.

Winkler, I. & Manke, S. (2013) *4 Ways Metrics Can Improve Security Awareness Programs*.

Zorz, Z. 2013, 4 October 2013,-last update*, Adobe breached, customer info and source code compromised* [Homepage of Net-security.org], [Online]. Available: http://www.net-security.org/secworld.php?id=15711 [2014, 0510] .