12-3-2012

An Information Security Awareness Capability Model (ISACM)

Robert Poepjes
University of Southern Queensland

Michael Lane
University of Southern Queensland

DOI: 10.4225/75/57b55238cd8d2
10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

AN INFORMATION SECURITY AWARENESS CAPABILITY MODEL (ISACM)

Robert Poepjes[1] and Michael Lane[2]
[1, 2]School of Information Systems, University of Southern Queensland
Queensland, Australia
[1]rpoepjes@gmail.com, [2]lanem@usq.edu.au

Abstract
A lack of information security awareness within some parts of society as well as some organisations continues to exist today. Whilst we have emerged from the threats of late 1990s of viruses such as Code Red and Melissa, through to the phishing emails of the mid 2000's and the financial damage some such as the Nigerian scam caused, we continue to react poorly to new threats such as demanding money via SMS with a promise of death to those who won't pay. So is this lack of awareness translating into problems within the workforce? There is often a lack of knowledge as to what is an appropriate level of awareness for information security controls across an organisation. This paper presents the development of a theoretical framework and model that combines aspects of information security best practice standards as presented in ISO/IEC 27002 with theories of Situation Awareness. The resultant model is an information security awareness capability model (ISACM). A preliminary survey is being used to develop the Awareness Importance element of the model and will leverage the opinions of information security professionals. A subsequent survey is also being developed to measure the Awareness Capability element of the model. This will present scenarios that test Level 1 situation awareness (perception), Level 2 situation awareness (comprehension) and finally Level 3 situation awareness (projection). Is it time for awareness of information security to now hit the mainstream of society, governments and organisations?

Keywords
IT Security, awareness, situation awareness, ISO27000, awareness importance, awareness capability, awareness risk.

INTRODUCTION

The need for improved information security received attention in the late 1990s when substantial disruption to computing services was caused by computer viruses such as Code Red and Melissa. Since then there has been a never-ending flow of new viruses and information security threats such as spam emails (Erado, 2003), identity theft (Butler, 2007), data leakage (Lew, 2010) and we continue to see computers impacted by these and other threats. A report on email security awareness found that 'three in five users (58%) on average say that their computer has been affected by a virus' (Ipsos, 2010). Information security threats continue to evolve. Old style threats that first emerged via emails are in 2012 arriving via mobile phones with the threat of death (News.Com.au) for anyone not paying the stated ransom. These threats continue to manifest themselves in many different ways, including phishing emails requesting "customers" to provide passwords to bank accounts, or to advance money in order to gain greater returns such as the Nigerian scam (Australian Securities & Investments Commission, 2008).

The Computer Security Institute (Richardson, 2007) reported that 'financial fraud overtook virus attacks as the source of the greatest financial losses, and also that the average annual loss reported in the survey has risen to $350,424 from $168,000 the previous year'-yet we still find people falling victim to what is essentially still the same technique applied many years ago. Poor management of computer access within organisations leaves these organisations vulnerable to employees and ex-employees having more access than is required. The Access Governance Trends survey (Ponemon Institute, 2010) found that eighty-seven percent of respondents believe 'that individuals have too much access' that is not pertinent to their job. Aspects of data leakage have been communicated through the trials and tribulations of Wikileaks (Parkinson, 2011). Facebook now has a dedicated web page focusing on information security (Facebook, 2012). Perhaps awareness of information security has now hit the mainstream of society, governments and organisations.

The emergence of identity theft and financial fraud from phishing (Butler, 2007) began causing similar problems to those experienced during the early years of viruses in the late 1990s and early 2000s. The results of a 2007 Australian Bureau of Statistics survey on personal fraud (Australian Bureau of Statistics, p. 11) reported 124,000

victims of identity theft (0.6% of the Australian population), with 'the 25 to 34 years age group having the highest number of victims (34,400 or 28%)'. Of these victims, 20,100 suffered a financial loss. This age group also represents those that have largely grown up during the computer age. Society's reliance on information technology for Internet banking, share trading, instant messaging, blogging and social networking, as well as critical infrastructure's use of information technology, provides a perfect attack vector.

Awareness of information security controls

Information security controls are the rules and regulations, that when fully understood and correctly deployed are capable of preventing or minimising the impact of cyber attacks ((Tsohou et al., 2010), (Butler, 2007), (Australian Government, 2010)). Knowledge (information security awareness) of these controls can provide a strong level of defence for organisations (Lindstrom and Hagerfors, 2009; Johnson and Goetz, 2007). Awareness of a new virus or phishing attack, awareness of identity theft, and what controls can minimise the likelihood and impact of these threats and understanding how awareness influences the importance, capability and effectiveness of information security controls is important. It provides insight and a challenge for the development of models incorporating measures of importance and capability by linking information security control methodologies with human awareness. The Inquiry into Cyber Crime (Australian Government, 2010) took submissions from the Australian Computer Society who argued 'Australians seem to be aware of, and are taking precautions against, old cyber crime threats but are not aware of, or taking steps against, new and emerging cyber crime threats'. As technology permeates more aspects of our lives, daily activities contribute to both the reporting of another information security breach as well as to the growing knowledge of the subject.

Increasing use of social media, growth of data and the risk of data leakage, technology improvements putting significant computing power on smart phones and iPad-like devices, increased online purchasing, and more critical infrastructure relying on computer automation leads to all of us needing to become more technology risk aware. Whilst there is a large body of literature that describes what to include in an information security awareness program, there is however little information on how awareness influences the effectiveness of the information security controls and little is documented about how capable or effective these awareness programs are, and whether they raise the perception, comprehension and decision making of individuals and organisations in relation to potential threats. This paper describes the research undertaken to developing an information security awareness capability model (ISACM) that can be used to identify awareness gaps and associated risks to organisations in relation to specific information security controls.

RESEARCH METHODOLOGY

The following steps were undertaken as part of the research and design of the ISACM.

Literature review

A literature review was undertaken to discover the current state of information security and in particular information security awareness, with a focus on discovering what if any methodologies and tools were available to measure awareness. The science of Situation Awareness was also researched to see whether it could provide an approach for measuring awareness capability.

Design of an overall ISACM

The ISACM focuses on 3 key elements. The foundation for these elements is based upon the controls contained within the ISO/IEC 27002. These elements are **Awareness Importance**, which refers to how important awareness is, or how influential awareness is in the success of the correct functioning of a process or control. In simple terms, for example crossing a busy street, it is important to be aware of oncoming traffic before crossing. Awareness Importance would be high. Compared to driving a car, knowing how fuel enters the cylinders is not important in order to drive the car. Awareness Importance of engine function in this case would be low. The next element is **Awareness Capability**, which refers to how capable a person is when faced with a decision. Extending the previous example, before the person crosses the street, are they capable of comprehending the situation of the oncoming traffic? This capability will influence how successful the street crossing would be. The final element is **Awareness Risk**, which is the gap that results from the required amount of awareness (Awareness Importance) being greater than that actually being displayed (Awareness Capability).

Surveys will be used to help build the ISACM. A preliminary survey of information security professionals will assist with determining the Awareness Importance measure, and a subsequent survey will be used to develop the Awareness Capability measure.

Developing the measures and validating the model

The main objectives of each of the 39 security controls for the ISO/IEC 27002 standard were used to construct questions to assess an information security professional's view of the importance of the controls for three key stakeholder perspectives (IT staff, senior management and end users). These have been developed into a preliminary survey, which will be presented to information security industry experts and practitioners. A subsequent survey (based on Situation Awareness principles) will be used to measure awareness capability in a specific organisation.

Background

The literature review conducted as part of this research considered the current state of information security, with a focus on the role that awareness plays in achieving security objectives. It then looked at how Situation Awareness provides a possible way of measuring capability. This research was then used to develop an initial model. Details of the contributions of existing literature to this development of the ISACM are described below.

ISO27000 Series of information security management standards

Considerable time was spent looking at the ISO27000 series of standards and how they could assist with improving information security. The ISO 27002 standard in particular covers a code of practice for information security management. It provides a detailed level of best practices that organisations should at least consider in managing information security. Not all will be applicable for every organisation, but the detailed guidance not only provides what should be considered, but it also describes why. In information security practices it is often the "why" that is missing.

Too often a policy will state, "don't do this" or "you must comply with this", but the reasoning behind these rules is often missing. ISO 27002 can help address this information gap. Literature also suggests that it was also important to realise that there are different stakeholder requiring different levels of awareness in relation to information security controls (National Institute of Standards and Technology, 2003; Choi et al., 2008). For example, an end user does not need to understand the detailed technicalities of how encryption software handles messages in a secure way. Generally all they need to know is how to use it and under what circumstances. The ISACM needed to distinguish between various stakeholders. The three stakeholder groups' chosen where IT staff (including the information security professionals), senior management (decision makers) and the end user.

Situation Awareness (SA)

With the major focus of this paper being on awareness, it was important to look at theories of how humans acquire and manage awareness. Many of these theories stem from human factor and cognitive theories. Some authors (Curts et al., 2002) suggest that the OODA (observe, orient, decide and act) loop, and cognitive hierarchy may be relevant in understanding how humans acquire knowledge and then act. Another theory is the Shewhart or Deming Cycle of Plan-Do-Check-Act (PDCA) that describes a cyclical approach to undertaking tasks. A relatively new field is Situation Awareness (SA). Endsley and Garland (2000) relate a general definition of SA as '... the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future'. In simple terms it is about being aware of information or cues in your environment, and then determining what might happen next, or what will happen if you take a certain course of action.

Much of the early focus of SA was on pilots. Problems with SA are quoted (Endsley and Robertson, 2001) as having been accountable for 88% of pilot errors that involved human error. SA therefore provides a theoretical framework that could be applicable to information security awareness, as many information security incidents or events are the result of human errors. For example, people are aware of computer viruses, but still many people readily click on unknown links and attachments due to a lack of awareness of the risks associated with do so. Figure 1 provides an adapted model of Situation Awareness, showing how the measures of Awareness Importance, Awareness Capability and Awareness Risk can map to the SA model.

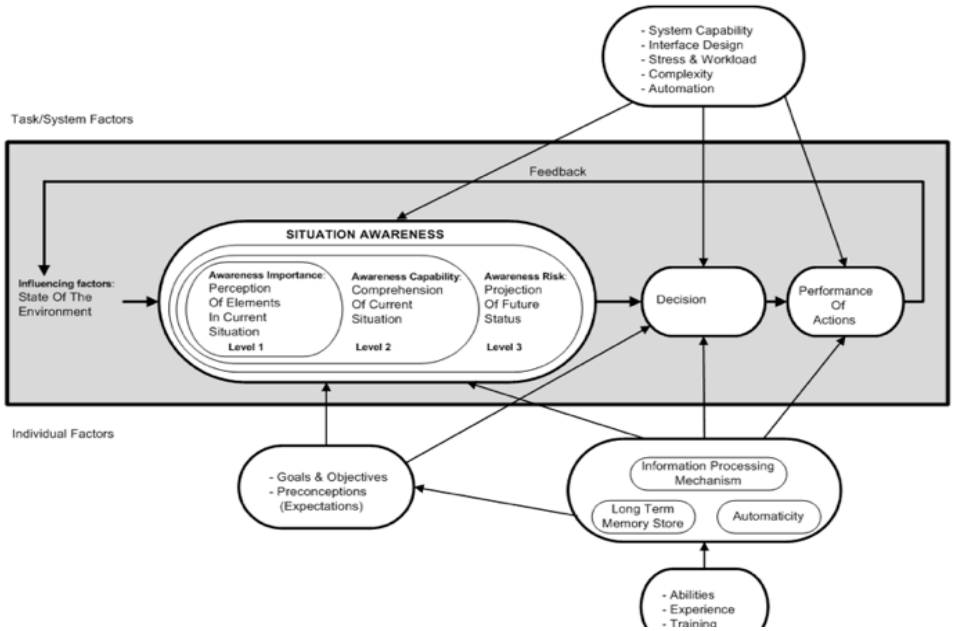

Figure 1. Situation Awareness in dynamic decision-making (Adapted from Endsley and Garland, 2000)

DEVELOPMENT OF THE ISACM

Awareness Importance element

Below is a detailed description of how the Awareness Importance element of the ISACM was developed.

Step 1: Determine a solid foundation of knowledge

AS/NZS ISO/IEC 27002:2006 provides a code of practice for information security management and contains 11 security control clauses, which contain 39 main security categories. Each of these contains a control objective as well as one or more controls that can be used to help achieve the control objective. This standard includes a significant amount of information as part of the implementation guidance. At its extreme, if you were fully aware of all of the guidance, and were able to implement each of these, the level of information security would be high. The guidance is in the form of “the following should be considered”, or “the following should take place”. So awareness of what should be considered, or take place becomes important for the success of the control. This becomes the foundation on which the awareness importance measure has been developed.

Step 2: Identify the detailed awareness points that could be rated

Using a spreadsheet the guidance provided by the ISO/IEC 27002 standard in relation to 11 information clauses was broken down into a series of questions awareness-like questions. This provided me 788 awareness-focused questions, spread across the 39 main security categories and a basis for asking, "how aware does one need to be of the point listed, in order for that point/control to be effective"? Within the 39 main security categories a weighting factor has been applied in terms of the impact it has on that main security category. Figure 2 shows this level of detail through an example **7.2 Information classification** that represents one of the 39 main security categories. The standard further breaks this down into controls that can be applied to achieve the control objective of the main security categories. In this example it is **7.2.1 Classification guidelines** and **7.2.2 Information labelling and handling**. The guidance points become the final capture point. So within 7.2.1 there are 4 main guidance points (the Control has been included for reference). They have been weighted at 50%, 20%, 20% and 10% respectively. These weights are opinion based on the first author’s industry experience and these results will be replaced based on the results that will be obtained in the preliminary survey.

CONTROL STATEMENT	Weight	AWARENESS IMPORTANCE				Calculated scores		
		IT Staff	End User	Senior Management	Overall Weight	IT Staff	End User	Senior Management
7.2 Information classification	**100.0%**	**2.96**	**3.06**	**3.88**	**100%**			
7.2.1 Classification guidelines	**100.0%**	**2.10**	**3.10**	**4.60**	**55%**	2.100	3.100	4.600
Control Control Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. Implementation guidance								
Classifications and associated protective controls for information should take account of business needs for sharing or restricting information and the business impacts associated with such needs.	50%	2	3	5		1.000	1.500	2.500
Classification guidelines should include conventions for initial classification and reclassification over time; in accordance with some predetermined access control policy (see 11.1.1).	20%	2	3	5		0.400	0.600	1.000
It should be the responsibility of the asset owner (see 7.1.2) to define the classification of an asset, periodically review it, and ensure it is kept up to date and at the appropriate level. The classification should take account of the aggregation effect mentioned in 10.7.2.	20%	2	4	4		0.400	0.800	0.800
Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations, which may have different definitions for the same or similarly named labels.	10%	3	2	3		0.300	0.200	0.300
7.2.2 Information labeling and handling	**100.0%**	**4.00**	**3.00**	**3.00**	**45%**	4.000	3.000	3.000
Control An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. Implementation guidance								
Procedures for information labeling need to cover information assets in physical and electronic formats.	35%	4	3	3		1.400	1.050	1.050
Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label (in the output). The labeling should reflect the classification according to the rules established in 7.2.1. Items for consideration include printed reports, screen displays, recorded media (e.g. tapes, disks, CDs), electronic messages, and file transfers.	25%	4	3	3		1.000	0.750	0.750
For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction should be defined. This should also include the procedures for chain of custody and logging of any security relevant event.	25%	4	3	3		1.000	0.750	0.750
Agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other								

Figure 2. Analysis of detailed Awareness Importance factors

Although this provided the greatest granularity possible in terms of specific awareness, the practicalities of verifying this level of detail may be difficult. Each of these 788 points were rated to arrive at initial awareness importance ratings. In terms of scoring each of questions, a weighting factor was developed for each of the points. Percentage of importance was multiplied by the rating for each control. That was then added up for each of the sub-controls (i.e. 7.2.1), and that is then multiplied by that sub-controls weighting (i.e. 55% importance of 7.2). It could be that this sub-control weighting (i.e. 7.2.1) may vary from industry to industry. This could allow the model to be adjustable per industry sector, however this has been excluded from this current research.

Step 3: Modifying the detailed awareness points to a practical level

For practical purposes, the level of detail shown by the 39 main security groups has been used. However the awareness importance rating calculated using the more detailed model above will be used to compare with the results obtained through the preliminary survey. This survey will capture the level of detail below for all 39 main security groups.

ISO/IEC 27002 Controls Standard	Information Security Awareness - Awareness Importance						
	Importance (influence) that awareness provides to the controls. How aware should they be?						
ISO/IEC 27002 list of controls	Not at all	Slightly	Moderate		Very aware		Extremely
5 Security policy							
5.1 Information security policy	1	2	3	4	5	6	7
6 Organization of information security							
6.1 Internal organization	1	2	3	4	5	6	7
6.2 External parties	1	2	3	4	5	6	7
7 Asset management							
7.1 Responsibility for assets	1	2	3	4	5	6	7
7.2 Information classification	1	2	3	4	5	6	7
8 Human resources security							
8.1 Prior to employment	1	2	3	4	5	6	7
8.2 During employment	1	2	3	4	5	6	7
8.3 Termination or change of employment	1	2	3	4	5	6	7

Figure 3. Part of the Awareness Importance element of the ISACM

Step 4: Developing the survey instrument to gather awareness importance ratings

Obtaining some key attribute data was the first task the survey needed to achieve. The preliminary Survey is aimed at information security professionals, so it is important to see how "expert" these people are. It was important to see how much information security experience the survey participants had. It was also important to see which stakeholder group the survey participant belonged to. Although the definition of IT staff specifically included information security staff, it was important to check with the survey participant.

Designing the 39 main questions was the next task. Initially reference was made to the work done with the spreadsheet that deconstructed the guidance material for each of the 39 main security categories. By looking at the overall objective stated within the standard for each of these 39 categories, this provided a balanced point of questioning without losing the overall context. Below an example of one of the original objective as stated within the standard has been outlined, followed by the survey question that has been constructed to measure awareness importance. It was important to develop concise and clear questions.

Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operations of all information-processing facilities should be established. This includes the development of appropriate operating procedures. Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

The question that was developed for the preceding objective is

How aware of formalising operational procedures and responsibilities, do the stakeholder groups need to be, so that the correct and secure operation of information processing facilities is managed?

Step 5: Developing the rest of the model

Although the final two elements of the model have yet to be fully developed, they consist of two separate measures. The **Awareness Capability** element is a measure of how much capability is being displayed. Situation Awareness theory is being used to frame this measure and it will be assessed through a subsequent survey. A number of scenarios will be presented and questions posed. These will be a series of cascading questions that firstly test Level 1 situation awareness (perception) and if correctly answered will lead to a test of Level 2 situation awareness (comprehension) and if correctly answered will lead to a test of Level 3 situation awareness (projection). The final result will be a measure of how much capability (or situation awareness) is being displayed by survey respondent. The final element is a simple comparison between the desired awareness (Awareness Importance) and that being displayed (Awareness Capability). This is the **Awareness Risk** element of the ISACM.

Information Security Awareness Capability Model (ISACM) – an example of three clauses

The ISACM contains each of the 39 base controls as described by ISO/IEC 27002, grouped into the 11 security control clauses. The extract from the model shown below in Figure 4 is a data collection view of the ISACM and shows the combination of the various elements described above. This will be populated once the preliminary and subsequent surveys have been conducted. This ISACM will have strong practical application for organisations wishing to improve information security through improved awareness by identifying gaps (awareness risk) in current levels of information security awareness.

Information Security Awareness Capability Model																
ISO/IEC 27002 Controls Standard	**Stakeholder Group**	**Awareness Importance**							**Awareness Capability**							**Awareness Risk**
		Importance (influence) that awareness provides to the controls for each stakeholder group. How much awareness is required?							Level of Awareness being displayed by each Stakeholder category.							Highlights gap in required awareness - Interface with Risk Assessment matrix
ISO/IEC 27002 list of controls		None		Slightly	Moderate	Very		Extremely	None		Slightly	Moderate		High Expert		Overall Rating
5 Security policy																
5.1 Information security policy	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.															
	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
6 Organization of information security																
6.1 Internal organization	Objective: To manage information security within the organization.															
	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
6.2 External parties	Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.															
	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
7 Asset management																
7.1 Responsibility for assets	Objective: To achieve and maintain appropriate protection of organizational assets.															
	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
7.2 Information classification	Objective: To ensure that information receives an appropriate level of protection.															
	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None

Figure 4. The Information Security Awareness Capability Model (ISACM)

FUTURE WORK

The next step in this research project is to conduct the preliminary survey to obtain the Awareness Importance ratings. This information will be analysed and reported upon separately. The consensus score for the awareness importance obtained from this survey will form the basis of the awareness importance rating within the ISACM model.

The precise mechanism for querying Awareness Capability still needs to be developed and tested in a specific organisational setting. Situation Awareness theory will provide guidance for development of instrument to measure awareness capability. A subsequent survey will be developed and used within an organisation to measure the awareness capability. This will then allow for the Awareness Risk measurement to be derived by comparing Awareness importance rating scores with the Awareness capability scores. This will point to areas of risk for organisations in terms of a lack of awareness in a particular stakeholder group for a particular security control. Targeted rectification can then be applied to instances in an organisation where there is a less than desirable level of Awareness capability in relation to specific information security controls.

CONCLUSION

Without measuring the effectiveness of any awareness program in relation to information security in an organisation, it is likely that money and time will be wasted and the desired improvements may not be achieved. This is particularly so within information security. We continue to see “old threats” appearing in the new technologies to which we are exposed. A greater focus on knowing what is important could be the key and could allow greater focus within awareness programs. The ISACM could aid organisations with this goal. As the model is used within organisations it will no doubt continue to be fine-tuned. It is also something that other research can contribute to and build upon. Awareness continues to be a difficult topic for society to crack. Like obesity awareness campaigns and anti-smoking campaign, often the messages can be quite obvious yet the messages do not seem to get through, or at least the perception that the problems continue to exist or get worse. Hopefully that won’t be the same with information security awareness if an effective mechanism such as ISACM is used to identify the information security risks that exist in an organisation in relation to specific security controls in rigorous manner.

REFERENCES

Australian Bureau of Statistics. (2008). *Personal fraud*. Retrieved from http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/4528.02007?OpenDocument.

Australian Securities & Investments Commission. (2008). *Nigerian scams* [Online]. Retrieved from http://www.fido.asic.gov.au/fido/fido.nsf/byheadline/Nigerian+scams?openDocument

Australian Government. (2010). Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. In: *COMMUNICATIONS, H. O. R. S. C. O*. (ed.). Canberra.

Butler, R. 2007. A framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library, 25*, 517-533.

Choi, N., Kim, D., Goo, J. & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*, 484-501.

Curts, R. J., Campbell, D. & Macarthur, J. E. (2002). *Building A Global Assurance Program*. CRC Press.

Endsley, M. R. & Garland, D. J. (2000). *Situation Awareness Analysis and Measurement*, Mahwah, New Jersey, Lawrence Erlbaum Associates.

Endsley, M. R. & Robertson, M. M. (2001). *Building A Framework For Situation Awareness*. Retrieved from http://www.satechnologies.com/Papers/pdf/SATrainingchapter.pd

Erado. (2003). Erado reports 36% increase in Spam messages [Online]. Retrieved from http://www.prweb.com/releases/2003/09/prweb82272.htm.

Facebook. 2012. *Facebook Security* [Online]. Retrieved from http://www.facebook.com/security

Ipsos. (2010). 2010 MAAWG Email Security Awareness and Usage Report. Retrieved from http://www.MAAWG.org.

ISO/IEC. (2005b). ISO/IEC 27002:2005 [Online]. International Organization for Standardization. Retrieved from http://www.iso.org/iso/home.htm.

Johnson, M. E. & Goetz, E. (2007). Embedding Information Security into the Organization. *IEEE Computer Society*, 16-24.

Lew, J. J. (2010). WikiLeaks - Mishandling of Classified Information. In: *PRESIDENT, E. O. O. T*. (ed.). Washington, D.C.

Lindstrom, J. & Hagerfors, A. (2009). A Model for explaining Strategic IT and Information Security to Senior Management. *International Journal of Public Information Systems,1*, 13.

News.com.au. (2012). Police call for calm on hoax text and email that threatens recipients with death [Online]. Retrieved from http://www.news.com.au/money/money-matters/police-warn-on-hoax-text-and-email-that-threatens-recipient-with-death/story-e6frfmd9-1226432660084

National Institute of Standards and Technology (2003). Building an Information Technology Security Awareness and Training Program. In*: COMMERCE, U. D. O.* (ed.). US Government Printing Office.

Ponemon Institute (2010). *Ponemon Institute 2010 Access Governance Trends Survey*.

Parkinson, D. 2011. Life after WikiLeaks. *SC Magazines:* For IT Security Professionals. Haymarket Business Publications Ltd.Richardson, R. 2007. CSI Survey 2007: The 12th Annual Computer Crime and Security Survey. Retrieved from http://www.gocsi.com/

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security, 18*, 350-365.