Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Information Security Awareness: Issues and Proposed Solutions

by

IDDRISU, Fuad

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: March 2008

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Andy Igonor, Associate Professor, MISSM

Information Security Awareness: Issues and Proposed Solutions

by

IDDRISU, Fuad

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Andy Igonor, Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Date: March 2008

Concordia University College of Alberta
Information Systems Security Management
7128 Ada Boulevard, Edmonton, AB T5B 4E4

Information Security Awareness
Issues and Proposed Solutions

By

Fuad Iddrisu

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

March 31, 2008

Research Advisors:

Pavol Zavarsky
Associate Professor and Director of Research, Information Systems Security Management
Concordia University College of Alberta

Andy Igonor
Assistant Professor, Information Systems Security Management
Concordia University College of Alberta

TABLE OF FIGURES

Abstract

This research paper investigated what eleven organizations from the private and public sectors in Edmonton are doing to promote information security awareness training, how these organizations measure the level of information security awareness, and how often the organizations promote information security awareness training. In an effort to measure the level of awareness, this research paper tested the applicability of the Security Awareness Index (SAI). A qualitative approach using survey method of data collection supplemented by interviews with Chief Information Officers/security managers was used to answer the research questions. Secondary data in the form of reports also served as additional evidence.

The survey results indicated that there is an increasing focus on information security awareness in Edmonton. Interview feedback revealed that organizations who participated in the survey, measure the level of security awareness through various methods such as surveys, quizzes, spot checks, number of security incidents, auditing and so on. It was also noted that majority of the participated organizations promote on-going security awareness as a result of policy compliance. Lastly the Security Awareness Index (SAI) was found to be applicable in practical work because it focuses on general employee awareness and addresses common security issues in organizations today.

1.0 Introduction

1.1 Problem Description

Information security awareness training has become a very important issue for most organizations today. Organizations have come to realize that protecting sensitive information from risks such as accidental disclosure and social engineering attacks cannot be achieved by employing technical solutions. The human factor plays a very significant role in the protection of information assets and resources. It is in view of this fact that organizations are expected to introduce security awareness programs with the goal of creating a culture through which individuals in the organization become conscious of the need for security.

A 2007 research brief by NACIO entitled "Insider Security Threats" highlighted the fact that cultural change involves changing the way employees perceive IT security, consistency and patience are necessary ingredients [1]. "Managing change is the component of the security program designed to ensure that training/awareness/education deployments do not become stagnant and therefore irrelevant to real emerging issues faced by organizations" [2]. Information Security Forum (ISF) through surveys and research, have defined information security awareness as: "an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organization from lasting behavioural change" [3].

Information security awareness programs must be continually measured and tested to determine the effectiveness of the program. "You can't manage what you can't measure" [4]. It is important to measure the effectiveness of the awareness program to check for compliance and understand the security posture of your organization.

1.2 Motivation for Research

In today's business world, the operations of organizations are dependent on information assets and resources, some of which are very vital. Most organizations process a lot of sensitive information, such as personal data, financial information and documents of various organizations. Information assets are continually at risk, vulnerable to accidental and malicious events attributable to internal and external threat agents. Such events have the potential to cause significant harm to organizations.

A 2007 survey conducted by Computer Security Institute (CSI) shows that 61 percent of organizations spend 5 percent or less of their overall IT budget on information security and about 50 percent of the organizations spend less than 1 percent of their information security budget on awareness training [5]. Yet research conducted by Mr. Gullik Wold points out that "organizations that do not promote information security awareness are more likely to experience a major security incident than those that do promote awareness." [6].

1.3 Research Questions

In 2002, PentaSafe Security Technologies conducted a worldwide survey to measure how organizations improve security awareness and understanding, and how well employees understand and act upon their organizations information security policies, threats and issues [7]. The objective of this research paper is to test the applicability of the Security Awareness Index and also answer the following research questions:

- What are private and public organizations in Edmonton doing to promote information security awareness?
- How are these organizations measuring the level of information security awareness?
- How often do organizations promote security awareness training?

2.0 Method and Procedure Used to Answer Research Questions

To test the applicability of the Security Awareness Index (SAI), a practical test of the SAI questionnaire was used on a sample of 11 organizations from the private and public sectors in Edmonton. The survey questionnaire to be filled was in two parts. Part one was aimed at Chief Information Officers/security managers, and focuses on the following three research questions:

- How do you promote information security awareness?
- How do you measure the level of security awareness among employees?
- How often does your organization promote security awareness training?

Part two, which is a small paper based questionnaire, was aimed at end users and covers topics discussed in Section 4 of this document. A small paper based questionnaire was used on end users because interviewing all participants is time consuming and also provides for more honest answers rather than in an interview. Part one of the survey questionnaire was interview based because it provides for clarification when the need arises and also due to the small number of respondents.

PentaSafe Security Technologies SAI scoring methodology was used on the end user questionnaire to measure information security awareness levels. The scoring methodology was also relied on to determine how often employees receive awareness training. The SAI scoring methodology is determined by evaluating the answers of each respondent. Some answers receive a score, from 1 to 10, while other answers do not receive a score. The score is weighted according to how much PentaSafe Security Technologies felt the answer reflected security awareness [7]. By way of an example, consider the question how long has it been since you read any of your organization's security policies?

Answer	**Scoring Answer**	**Score**
Less than 6 months ago	Yes	10
Between 6 months and 1 year ago	Yes	9
From 1 to 2 years ago	Yes	5
Between 2 and 5 years ago	Yes	3

More than 5 years ago	Yes	1
I have never read any security policies	N/A	0
The organization does not have security policies	N/A	0
Unknown	N/A	0

Attending/receiving security awareness training in less than six months is the most satisfactory and therefore awarded the most points. Attending security awareness training bi-annually is a security best practice and also a proactive approach taken to update employees on new policies, procedures and threats. Security awareness training offered five year ago is awarded a score of one point because security risks are continuously changing and the need for employees to stay up to date is essential. The questions with zero points are seen to be ineffective security best practice. It must be noted that information security best practice exists to help organizations assess their security risks and implement appropriate security controls. Best practices are the most efficient and direct means of achieving a standard of due diligence.

The SAI benchmarking score is from 0 to 100 whereby a score of 90 - 100 is an "A", 80 - 89 is a "B", 70 - 79 is a "C",   60 - 69 is a "D", and below 60 is an "F" [7]. Scores from the survey are graphed by percentages and compared to SAI results to determine if there is an improvement in employee attitudes, knowledge, and behavior as well as cooperate culture.

It must be emphasised that this research paper does not look at how organizations support an on-going security training program nor does it look at the success factors for improving information security awareness.

The survey results are based on responses from 165 participants randomly selected from 11 organizations in Edmonton. The organizations are grouped by industries to see if the work with information security awareness is industry specific.

Figure 1: Number of Contacted Organizations

Industry	Survey Participants	Number of Organizations Contacted	Number of Organizations Interviewed	Interview Groups
Finance	40	7	3	A-B-C
Telecommunication	30	5	2	D-E
Automotive	15	3	1	F
Health	20	5	1	G
Public	60	15	4	H-I-J-K
Total	165	35	11	

3.0 Analysis of Feedback from Interviews

Below is the feedback collected from interviewing Chief Information Officers/security managers from the various organizations that participated in the survey. It must be noted that any information collected during the interview is handled with extra care to ensure full anonymity of the respondent. To achieve this, the participant’s personal information such as names and workplace has been excluded in this report.

Private Organization A

This is a financial organization that has established and implemented an overarching information security policy to ensure all relevant individuals understand the key elements of information security and the need for its practice. The policy defines and ensures that employees understand their personal information security responsibilities.

Organization A has specific activities designed to promote information security awareness. Some of which include a process to ensure that information security education and training is promoted among business managers, end users, IT staff and internal and external stakeholders.

Specialized information security awareness material, such as brochures, posters and intranet-based electronic documents are also used to promote security awareness.

Attendance to information security awareness sessions is mandatory as defined in the organizations security policy. In addition, organization A links information security to personal performance objectives/appraisals. Information security successes are also publicized throughout the organization.

This organization arranges awareness programs yearly with three awareness sessions targeted at top management, IT staff and end users. Organization A measures the level of awareness by implementing a process to monitor compliance to security policies. In addition, an automated tracking system has been designed to capture key information regarding program activity.

Lastly, if an awareness briefing is conducted, a survey or questionnaire is distributed seeking input from employees. A follow process is then initiated to determine how the briefing was perceived.

Private Organization B

This respondent is also a financial institution in the private sector with over 800 employees in various locations within the province. Organization B has a security department and an IT steering committee which oversees IT operations and ensures that IT security strategy aligns with business objectives and goals.

Organization B has a formal e-learning program that was designed by an outsourced vendor. Employees are encouraged to participate in the e-learning course. The focal point of the course is to inform employees that security is not an individual issue but a corporate wide problem that needs to be addressed.

Organization B uses the intranet and printed policy manuals to communicate security policies. Employees from this organization are required to read and sign policy compliance forms. The organization also promotes information security by using security alerts, posters, in-house security articles and information security training during new hire to raise information security awareness.

All employees, service providers, consultants and vendors are required to read security policies that apply to them. Also organization B tracks and follows up to ensure that the employees have complied with the organizations security policies, and participated in the e-learning course.

The security department holds ongoing 'Lunch & Learn' sessions regularly. The objective of the sessions is to have an informal get-together during lunch hour and cover a variety of security-oriented issues some of which include secure disposal of assets and acceptable use of portable devices.

Organization B’s security policy states that security awareness training and education must be provided to all employees annually.

The method used in measuring the effectiveness of the security awareness program is through employee performance. This is done “before” and “after” completing the e-learning course. The CIO also conducts “spot checks” of user behavior. This includes walking through the office checking if sensitive information is not adequately protected.

Private Organization C

This organization is from the financial sector. The Chief Information Officer is responsible for developing policies and security best practices. This private organization has an Information Management Branch that arranges special security awareness programs for every fiscal year.

Senior managers in the organization are made aware of the security challenges in the organization. ISO/IEC 27002:2005 best practices are adopted for implementing security controls.

Specific awareness sessions are often initiated as a result of an internal or external security incident. These specific awareness sessions are not part of the recurrent or continuous programs. These awareness sessions target a security topic that requires special attention. Some topics of concern include potable device security and social engineering attacks. The Information Management Branch is currently planning an awareness session on social engineering to address recent security breaches caused by social engineering attacks. Organization C has been promoting security awareness training for the past 2 years and plans to be consistent in its implementation.

Information about internal security incidents are made public for all employees in the organization. Organization C has a stringent penalty for internal security breaches to the organizations security policy. All new employees annually as well as the start of special projects have to sign a declaration of confidentiality and compliance to all policies standards and guidelines.

Organization C measures the level of awareness by tracking the number and type of security incidents that occur before and after an awareness session. The indicator used to determine the effectiveness of the program is based on the number of reported incidents.

In addition, this organization also conducts “spot checks” of user behavior and is in the process of designing an approach to measure how easy it is to gather sensitive information through social engineering attacks. The output from such tests will indicate how employees’ attitudes are towards social engineering threats.

Private Organization D

This organization is from the telecommunication industry. Organization D has designed an information security awareness questionnaire seeking input from employees. These questionnaires are given to new hires during orientation. The organization has a follow up process where after three to six months new hires are again asked the same questions to find out what they remember from the orientation and what areas they require more information on.

Organization D conducts regular spot checks of employee behavior to ensure a clear desk policy is enforced. This organization also tracks the number of security incidents and is in the process of educating employees on how to report security incidents or breaches.

Each operational division has a documented security policy and operations procedure. Roles and responsibilities have been clearly defined and communicated to staff. All employees are required to sign a form to confirm that they understand their roles and responsibility in regards to internal security. Organization D is also implementing an in house information security awareness training session which focuses on job roles.
Organization D arranges information security awareness training quarterly. Organization D uses user satisfaction with information security efforts as part of an effectiveness measurement process. A short survey is sent to end users asking questions like:

- How satisfied were you with the training you received?
- What impact did it have on your ability to do your job? etc.

The satisfaction results are calculated to determine the level of information security training provided to the organization.

Private Organization E

This organization is also from the telecommunication industry. Organization E's staff are educated and trained on how to run systems correctly and how to develop and apply security controls. The idea is to provide staff with the skills required to run systems correctly and fulfill their information security responsibilities.

This organization has a Chief Information Officer who is accountable for assessing security requirements, recommending security controls and ensuring that security controls function effectively in the environments in which they are applied.

In support of the organization's continuing effort to raise information security awareness among employees, this organization has established an information security awareness week and a conceptual online security course. The information security awareness week consists of a series of free events designed to educate participants on how to protect information assets and resources.

This organization is in the process of documenting a security policy that will define how often to arrange awareness programs. However, organization E is in the process of planning a second information security session that will focus on employee attitudes and behaviour. The organization plans to incorporate give away in the session to encourage employee participation. A CD containing basic security steps for protecting home computers is an example of some of the give away to be considered for the information security session.

Organization E intends to use short survey questions and face to face interviews to measure the success of the second awareness session. The results of the measurements will be evaluated and taken into account for future security awareness programs.

Private Organization F

Organization F is from the health sector and manages sensitive information on a daily basis. This organization promotes security awareness refresher training to personnel annually at a minimum.

Early this year, employees were given a security handbook at an initial security awareness briefing. The security awareness handbook describes the security awareness program and provides information on security procedures and resources.

Organization F maintains a highly visible security environment that provides for the safety of the organizations assets, resources and employees. All employees have been made aware of procedures for reporting security incidents. In some cases, an actual security breach that compromised the security systems in the organization is used as an example in the weekly security tip on the intranet without pointing out the source.

All new hires who use information assets/resources or who have access to areas where critical information resources reside, are required to attend formal security awareness training as designed by the organization within 30 calendar days of their start date. Receipt of security awareness training is documented in the employee's personnel file with employee's acknowledgement of receipt and understanding.

Organization F ensures that its employees receive security awareness training every year. This organization also performs a lot of information security awareness measurements some of which include:

- Sending out questionnaire every month seeking information security input from employees;
- Arranging information security quizzes;
- Measuring awareness before and after an awareness training through surveys;
- Logging of internal network traffic;
- Tracking the number and type of security incidents;
- Monitoring compliance to policies and procedures.

Private Organization G

This is a small business from the automotive industry. Organization G tasked a security firm to develop security policies that reflects business needs. This organization has no security department or security officer. There is also no formal information security program in place but the Network Administrator points out some activities that promote or raise awareness which include, new employees are required to undergo a security clearance and must read and sign an acceptable use policy, a declaration of confidentiality, and lastly the corporate security policy before they can start working.

Organization G uses the Intranet to communicate information security messages. Employees are also given a CD with anti-virus software for use on their private computers.

Information asset and resource users are informed of their information security responsibilities through performance evaluation and new employee orientation. In addition to the activities mentioned above, the Network Administrator is accountable for monitoring, reviewing, and updating technical controls.

Organization G has not established an information security awareness program and has also not attempted to measure the level of awareness among employees.

Public Organization H

Organization H is a public organization. This organization has established and maintains information security awareness programs to ensure that all individuals are aware of their security responsibilities and know how to comply with them. In 2005, the Information Security Officer with the support of the information security team developed and delivered the first information security awareness training of its kind in the organization. The initial information security awareness training was delivered to all staff. The organization had about four large-scale training sessions offered. The training included the following:

- Viewing a video on information security;
- Viewing PowerPoint presentations on information security with a focus statement that security is everyone's business;
- Distribution of an information security awareness brochure.

Employees are also encouraged to participate on an online e-learning course sponsored by Service Alberta. Organization H uses a data classification scheme to categorize and prioritize information. Resource/information asset owners have been identified and are required to review user access privilege on an ongoing basis. This organization is also required to arrange annual security awareness programs as defined in the Government of Alberta security policy. Organization H also relies on annual audit results to determine the effectiveness of their awareness programs.

Public Organization I

This organization is part of the public sector and promotes information security awareness by ensuring that all relevant individuals understand the key elements of information security, its importance and understand their roles and responsibilities in terms of internal security. As a public organization they follow Government security standards and policies. Management is responsible for the security of all information and supporting systems within their business unit. This organization ensures that information systems have adequate management control and accountability, balanced with the business requirements of the organization.

This organization encourages employees to visit the Government e-learning site to participate in the on-line e-course. Organization I paste security posters in elevators and hallways as another form of promoting information security awareness.

This organization has defined mandatory FOIPPA training in their security policy and occasionally some bulletin on information security awareness is e-mailed to all staff.

New employees are required to attend an information security awareness orientation on acceptable use policy and ethical conduct.

Organization I uses a service desk function as the single point of contact which tracks all problems and incidents. Management has defined and implemented an incident and problem management system to report and resolve issues in a timely manner. There is a process in place to ensure that senior management receive all incident statistics and status reports on a regular basis and ensures that problems and incidents are resolved in a satisfactory and timely manner.

Organization I is mandated by the Government of Alberta security policy to develop and implement a Ministry-wide information security awareness program on an annual basis to provide information security for the operations and assets of the Ministry. The program is to include information security awareness training and education to inform personnel of information security risks associated with the activities of personnel, and responsibilities of personnel in complying with Ministry policies and procedures. Organization I relies on annual audit results for measuring the effectiveness of their awareness program.

Public Organization J

This is a public organization that is required to promote security awareness education and training at least on an annual basis as documented in the Government of Alberta security policy. This year, this organization has delivered 1.5 hour sessions to all staff and distributed a handout which contains information on privacy and security best practices.

Earlier this year, this organization started emailing staff relevant security news. Power point presentation slides are uploaded onto the local intranet where staff are encouraged to read. Other methods used to promote information security awareness are through e-learning course and new staff orientation where the presenter speaks for 25 minutes on privacy and security risks. Information security awareness material, such as brochures, posters and intranet-based electronic documents are also used to promote security awareness.

Last year, there was a poster event on security awareness. There are two computer security days, open to all staff, scheduled for twice per year, given by the Information Security Office. Organization J measures awareness from audit results and through evaluation forms.

Public Organization K

This organization is required to comply with the Government of Alberta security policy. The Chief Information Officer of this organization emphasizes on the need for continuous education and training on information security risk in order to change employee behavior.

All new employees are required to attend a security course. In addition an awareness-training course is mandatory for all employees every year as stated in their security policy.

This organization ensures that a clear desk policy is implemented. The organization's Intranet is used actively as a communication channel for information security issues. Policies, standards, user guidelines etc. are available for all employees on the local network.

Risk assessments are performed internally using local resources which intern promotes security. Random spot checks are regularly enforced to ensure if documented routines and procedures are being followed.

Audits, evaluation and feedback mechanisms are used to measure awareness among employees. The Government of Alberta IT division also has an e-learning course where employees are encouraged to participate. Results obtained from the e-learning course are used as some form of measurement of employee awareness.

Conclusion

Based on the inputs from the interviews, it can be stated that the financial institutions, take a proactive approach to information security. According to the feedback, 10 out of the 11 organizations consider information security training very important and promote information security through awareness programs. Responses from the interview reveal several probable reasons. Some reasons include adopting security best practices, complying with security policies, demonstrating commitment to secure information resources, protecting company image/reputation and reducing security cost. Analysis of the interview feedback reveals that there is a significant amount of work done in the area of reporting, preventing or reducing the number and extent of information security incidents. It was also noted that clarification of job roles and responsibilities is also an area of focus. In addition, social engineering, portable device use, clear desk and secure disposal of assets are other areas where these organizations show security concern. A striking finding from the analysis of the interview feedback is that e-learning is the most popular method used to promote security awareness. Another striking finding is that the public organizations who participated in the survey rely on annual audits as the most favorable technique used to measure the effectiveness of their security efforts.

It must be emphasized that while these organizations are doing a good job of safeguarding information assets and resources through the promotion of information security awareness programs, there is still plenty of room for growth and improvement. Additional training and ongoing updating should be enforced to ensure employee's keep pace with rapidly evolving security issues and challenges. More work is also required in the area of measuring the effectiveness of security efforts. Lastly, particular emphasis should be placed on changing organizational culture to a more security conscious environment. That is to say more policies, procedures, and standards should be developed, communicated and enforced.

4.0 Reviewing SAI Topic Areas

The SAI covers topics such as security policies, education and training, compliance procedures, security threats, acceptable behavior and security awareness training. The scope of security threats identified by PentaSafe Security Technologies research paper is limited to e-mail usage, password management and construction. The granularity of acceptable behavior questions revolves around security incident reporting. This research paper is limited to the SAI scope.

As an information security professional, it is clear to me that most organizations do not have documented policies or procedures in place, and even if policies and procedures do exist, there is no formal process for communicating the documented policy or procedure. The purpose of a security policy is to enable the development of detailed standards and guidelines for specific systems, issues and an organizational unit representing a discipline. A security policy identifies the requirements and responsibilities covering the security management of the Information Technology systems within organizations. Organizations concerned with securing their critical information assets at a minimum should consider documenting security policies and procedures.

Information security awareness, awareness training, and education are all critical requirements for the successful implementation of any information security program [8]. These three elements are related, but involve distinctly different levels of learning. Information security awareness provides a baseline of security knowledge for all users, regardless of job duties or position. The base level of information security awareness required of end users is the same as that needed by senior managers. It is important that information security awareness programs are tied directly to security policy development. While an information security awareness training and education program is no guarantee that your organization will be protected from malicious attacks, the program can surely decrease the impact an attack will have on your organization [9].

Education differs from training. NIST Special Publication 800-16 defines education as, a “level which integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technology and social)” [10] whereas “training strives to produce relevant and needed security skills and competencies” [10]. Awareness is defined in as follows: “Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.” [10]

Majority of organizations are required by law or policy to comply with industry-specific regulations designed to safeguard the Confidentiality, Integrity, and Availability of information assets and resources. Organizations that do not comply with security regulations face serious consequences including heavy fines and legal action. Compliance means "adhering to the requirements of laws, industry and organizational standards and codes, principles of good governance and accepted community and ethical standards" [11]. The objective of the question from this section is to determine if employees know the consequences of failing to comply with their organizations security policy which in other words is a security violation.

E-mails are an effective means for communicating information. However, if not used appropriately it exposes you organization to malicious attacks such as viruses, phishing and hoaxing. To improve efficiency and productivity in organizations, employees should be made aware of their responsibilities when using e-mail to ensure that an effective, professional, ethical and lawful attitude is displayed in accordance with their organizations acceptable use policy. Questions from this section will help determine whether employees are made aware of e-mail acceptable use.

Passwords are an important aspect of computer security and the most popular form of user authentication. Password protected employee accounts are very common and widely used in most organizations today. Given the sensitivity of the information within these accounts and the potential for abuse and misuse of the information by others, one might think that users that have authorized access to sensitive information would create very secure passwords. This has not proven to be the case as Shannon Riley investigated what practices users employ in creating and storing passwords. Shannon Riley determined that the majority of participants reported weak practices in password generation. Common practices reported include using lowercase letters, numbers or digits, personally meaningful words and numbers i.e. dates [12].

A security incident is an activity or event that has the potential to compromise the security of organizations, and which could result in negative impacts to the Confidentiality, Integrity or Availability of organization’s information assets. All suspected and actual security incidents must be detected, identified, assessed, responded to, and recovered from in the most timely, efficient and effective manner. Questions from this section will help understand whether employees know what a security incident is, and the importance of reporting security incidents.

5.0 Comparing Survey Results with Security Awareness Index Survey

An analysis of the results obtained from the survey reveals that there is a significant improvement in information security awareness when compared to results obtained from PentaSafe security technologies six years ago.

SAI measures security awareness levels by assessing 3 aspects of security awareness i.e. Education and training, knowledge and perception and attitude. Graphical representations of survey results as compared to PentaSafe SAI research results are depicted below:

EDUCATION AND TRAINING

Figure 2 (PentaSafe results): How long has it been since you read any (all) of your organization's security policies (that apply to you)?

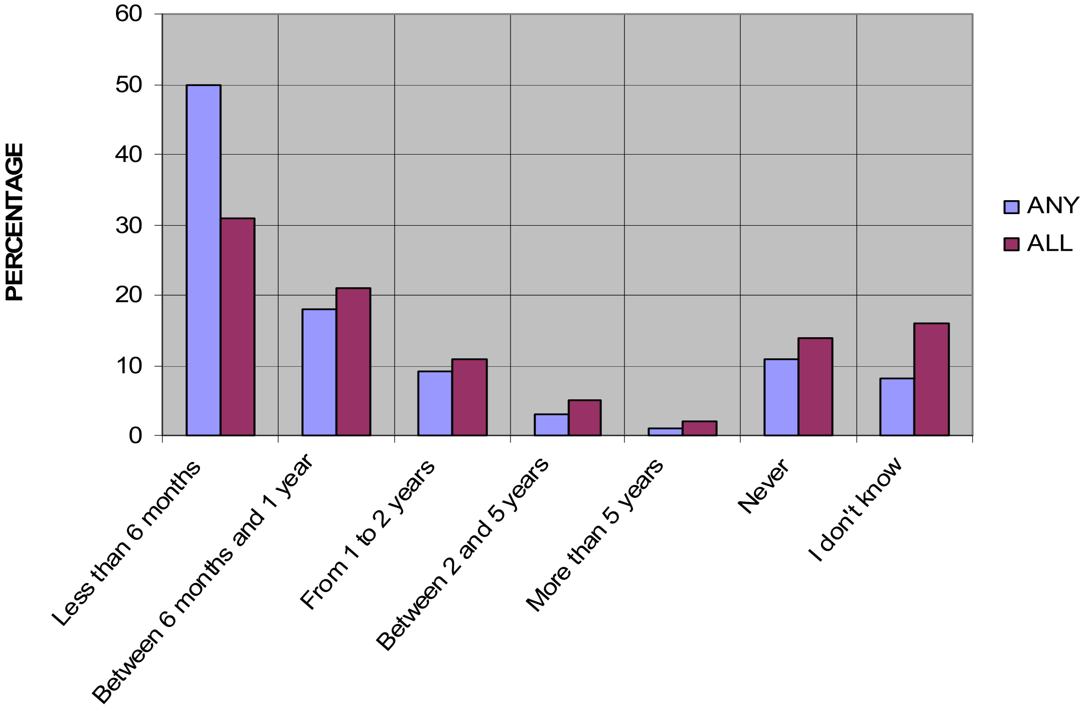
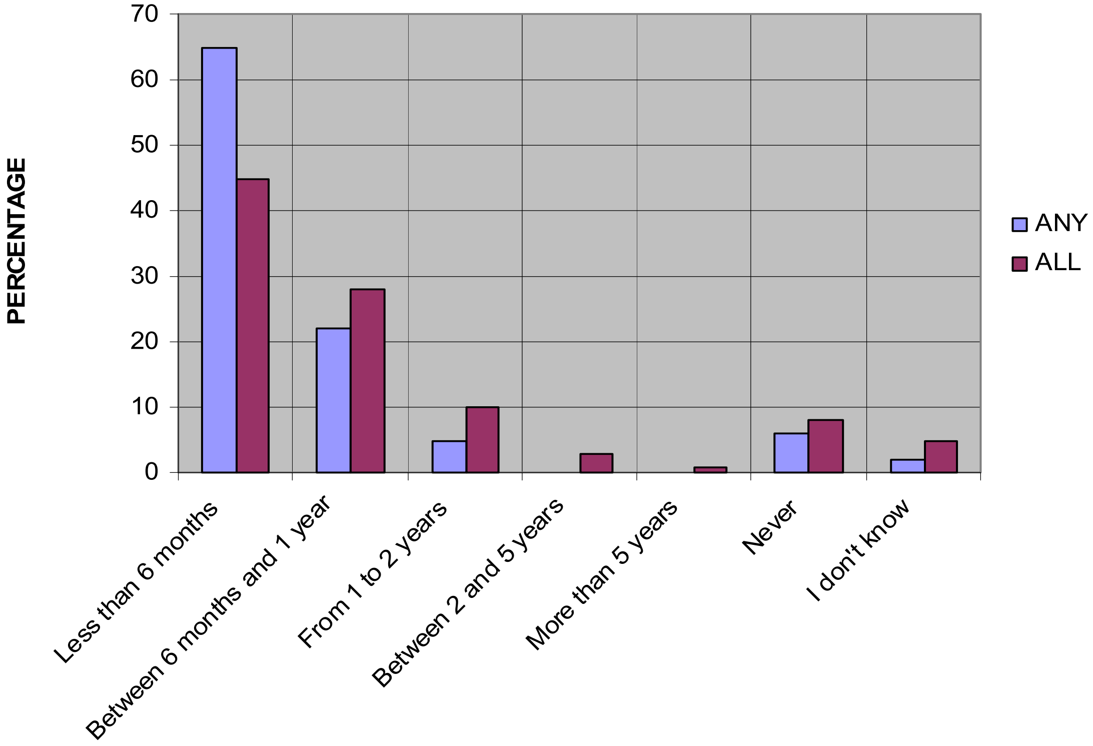


Figure 3 (Survey results): How long has it been since you read any (all) of your organization's security policies (that apply to you)?



Comparing figure 1 and figure 2, you can observe an improvement in the number of employees reading security policies. This change may suggest that organizations have come to realize the importance of security policies and the benefits of documenting and communicating a comprehensive security policy. Security policies support business objectives by safeguarding employees and assets and assuring the continued delivery of services. It should be noted that security policies should only serve as a minimum requirement for improving information security. Additional training on various security topics should be emphasized on.

Figure 4 (PentaSafe results): How long has it been since you have received formal security awareness training from your organization?

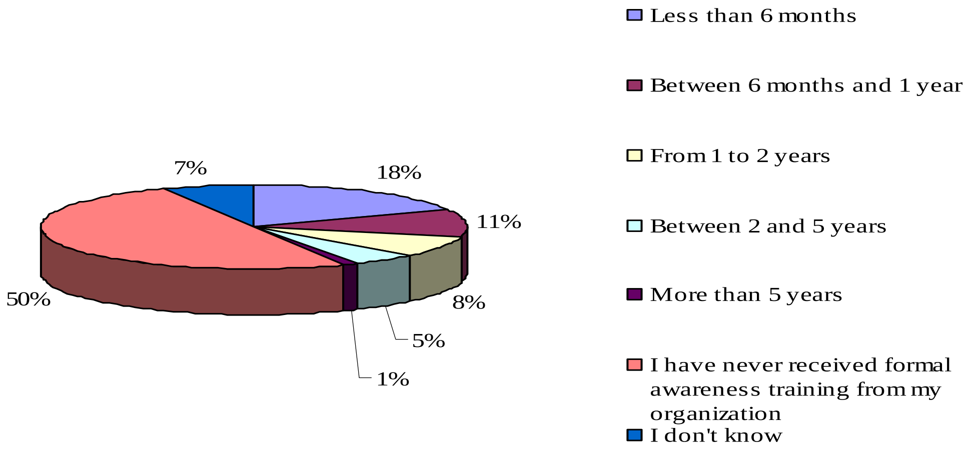
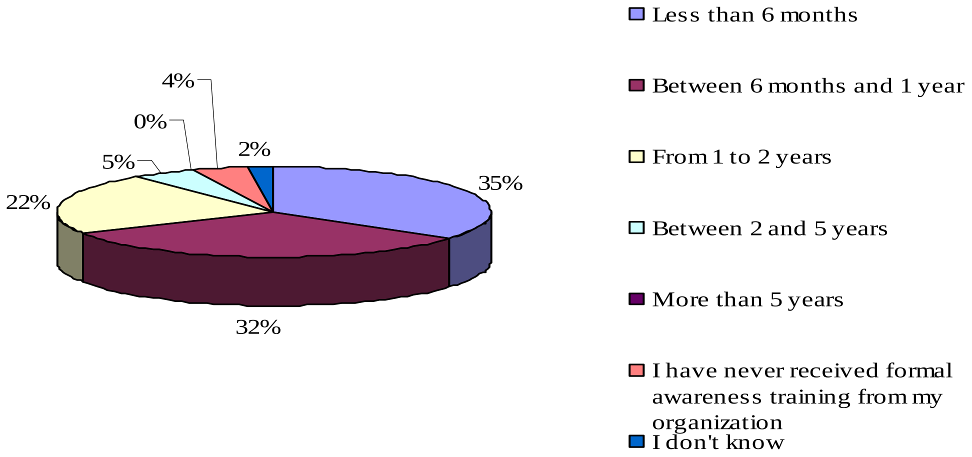


Figure 5 (Survey results): How long has it been since you have received formal security awareness training from your organization?



From the 2 graphs above, it can be clearly stated that more employees are receiving security awareness training within a reasonable time frame. Figure 4 shows that 35% of employees have received formal security awareness training in less than 6 months, showing an increase of 17% from the PentaSafe SAI research results. This improvement suggests that the organizations who participated in the survey realize the importance of security awareness and the need to keep abreast with security issues. Ninety four percent (94%) of the organizations who participated in the survey are trying to adopt into their organizations culture a process of promoting ongoing security awareness programs to change the behavior and attitudes of employees as well as increase both security and employee productivity. It must be noted here that selecting the options "more than 5 years", "I have never received formal security awareness training from my organization" and "I don't know" receive zero points from the SAI scoring methodology. All other options are seen as an effort and are awarded points according to effectiveness.

KNOWLEDGE

Figure 6 (PentaSafe results): "I feel empowered to make informed decisions about the security of information and technology."

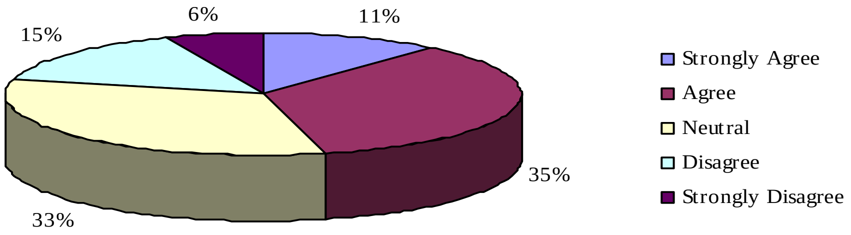
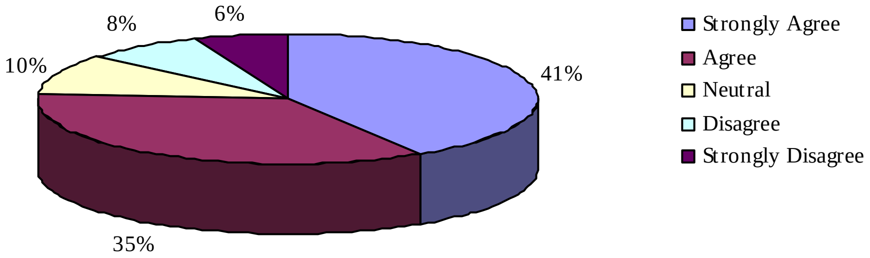


Figure 7 (Survey results): "I feel empowered to make informed decisions about the security of information and technology."



Survey results indicate that employees are becoming more knowledgeable in information security and are making conscious decisions to protect their information assets. Figure 6 shows a 30% increase in the number of employees who selected the 'strongly agree' option. Figure 6 also shows a decrease in the number of employees that selected 'neutral' or 'disagree'.

EMAIL ATTACHMENTS

Figure 8 (PentaSafe results): Assume you receive an e-mail from someone you know but you have not spoken to that person about it. If the e-mail contained a file with any of the following extensions, which would you feel are safe to execute by double-clicking on it?

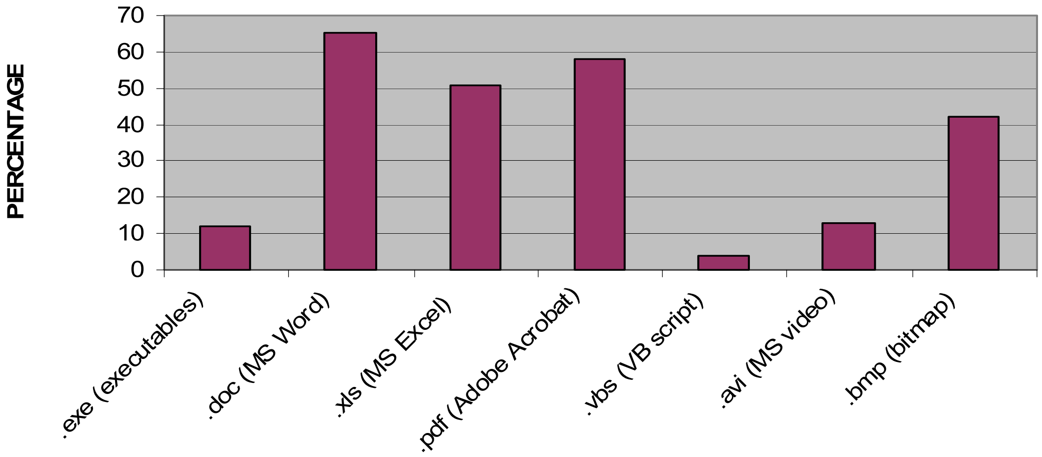
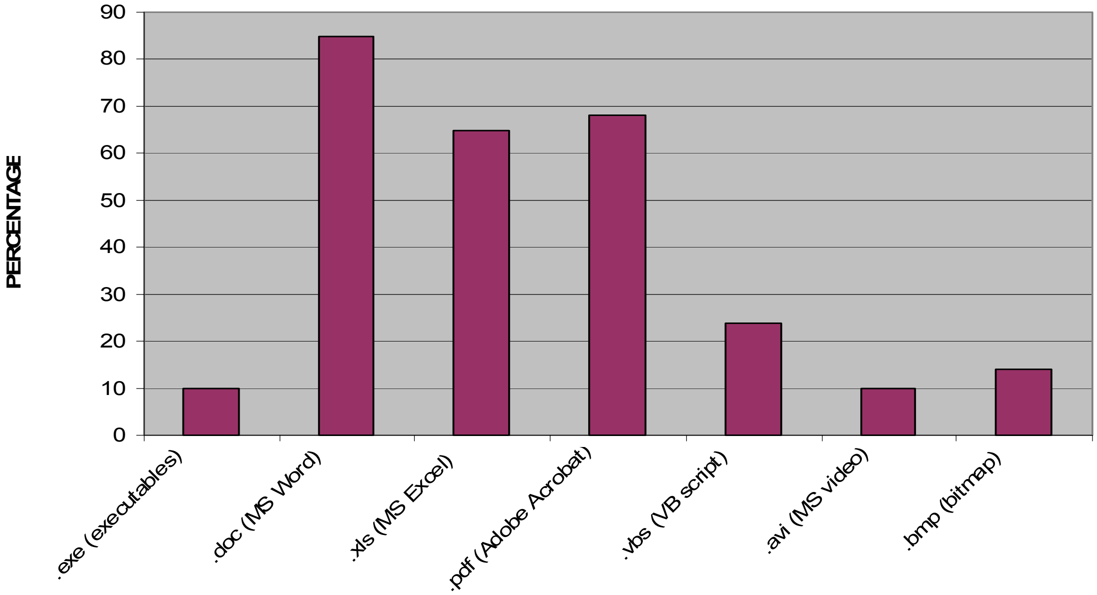


Figure 9 (Survey results): Assume you receive an e-mail from someone you know but you have not spoken to that person about it. If the e-mail contained a file with any of the following extensions, which would you feel are safe to execute by double-clicking on it?



Comparing the 2 graphs reveals an unsatisfactory score in the area of execution (opening) of dangerous file types. From the graph in figure 8, it can be observed that there is an increase in the number of employees opening the VB script. The VB script is one of the most dangerous file types that employees should not open if there are unsure of the sender. Organizations should focus on training users on the potential risk of executing files that are unknown.

PASSWORD SECURITY

Figure 10 (PentaSafe results): To which of the following employees in your organization would you tell your network (e.g., windows, netware) password if that person requested it?

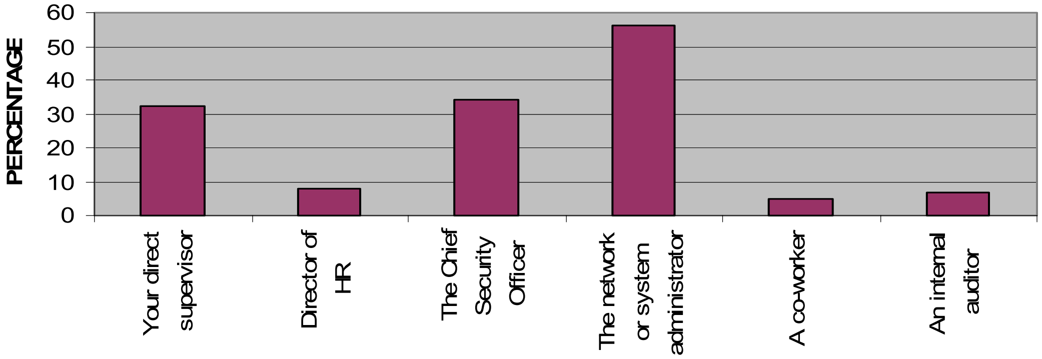
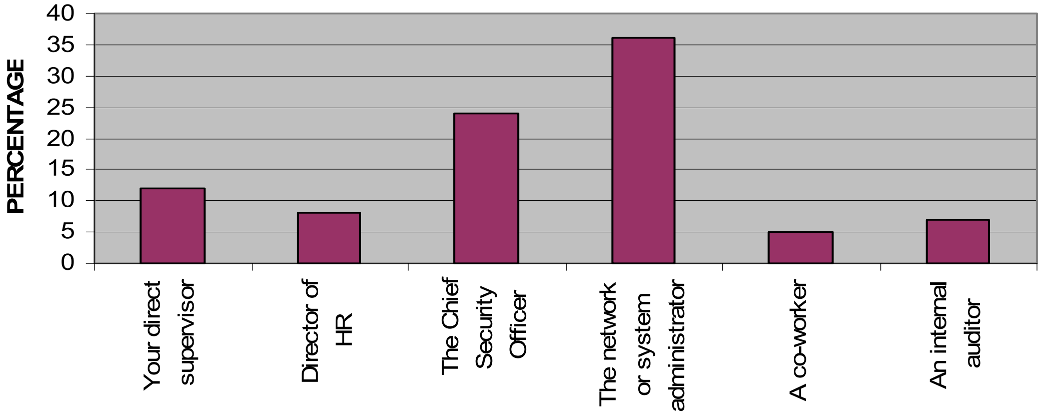


Figure 11 (Survey results): To which of the following employees in your organization would you tell your network (e.g., windows, netware) password if that person requested it?



A recent survey conducted by Infosecurity Europe shows that almost two thirds of office workers and IT professionals give a stranger their work passwords [13]. The survey also found that workers were more trusting of the IT department than of their boss [13]. Figure 10 and 11 show a high number of employees that would give their password to the network or system administrators. This observation supports the results obtained by Infosecurity Europe. Comparing the 2 graphs reveals that there is a decrease in the number of employees that will disclose their passwords to someone else in their organization.

Figure 12 (PentaSafe results): Which of the following passwords would you feel are acceptable and safe to choose as your network password?

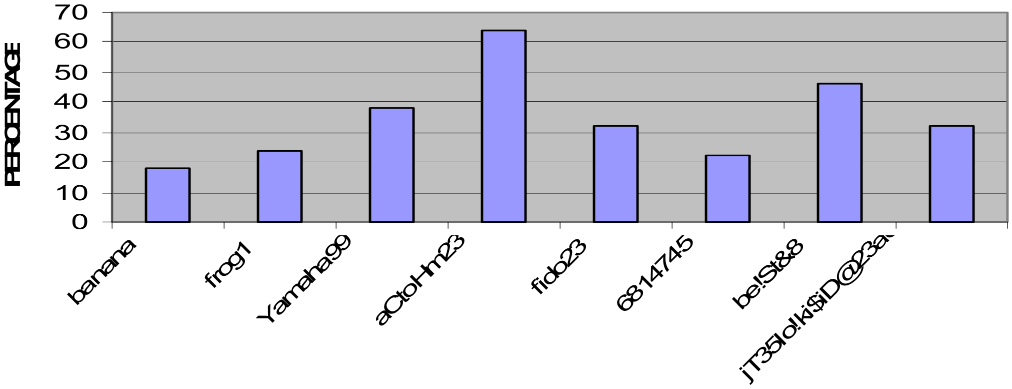
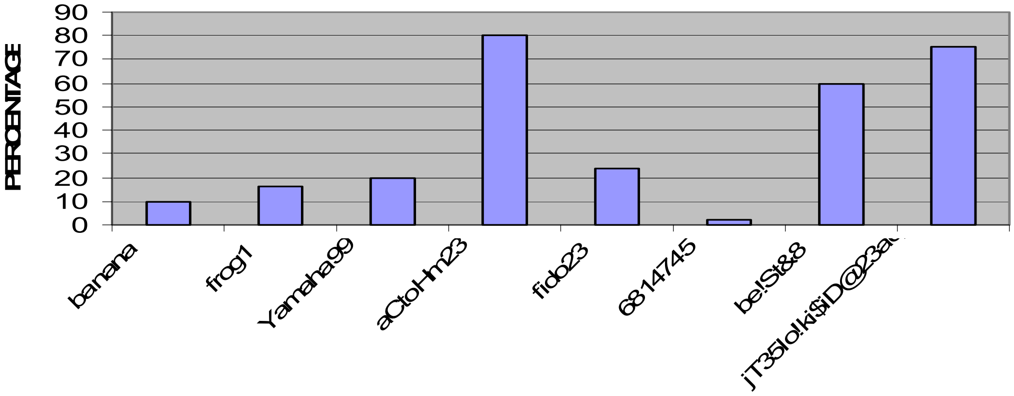


Figure 13 (Survey results): Which of the following passwords would you feel are acceptable and safe to choose as your network password?



Passwords are the key to many systems and applications. Compromised passwords are one of the means by which unauthorized people gain access to a system. These days there are many password-cracking programs that will crack week passwords within a short period. From figure 11 and 12 the 2 most selected passwords are so complex that they are most likely to be forgotten. To protect passwords from being compromised, employees should be educated or trained on good password construction. Organizations should also consider establishing a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

HANDLING POLICY VIOLATIONS

Figure 14 (PentaSafe results): “I am confident that I would know a security policy violation if I saw one.”

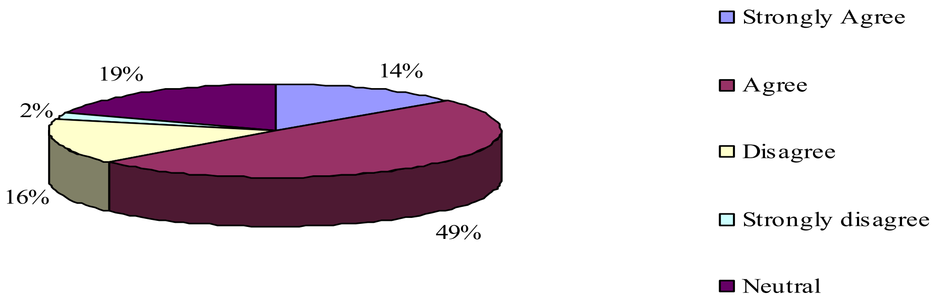


Figure 15 (Survey results): “I am confident that I would know a security policy violation if I saw one.”

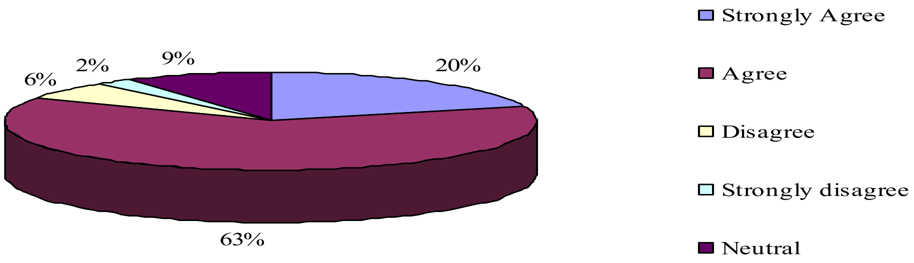


Figure 14 shows that 83% of respondents either strongly agree or agree with the statement. Comparing the two survey results reveals that there is a 20% increase in the number of employee’s that will know a security policy violation. There is also a 10% decrease in number of respondents that selected disagree or strongly disagree. This improvement can be related to the training provided around security incident reporting from the interview feedback.

Figure 16 (PentaSafe results): "I would know how to report a security incident or breach."

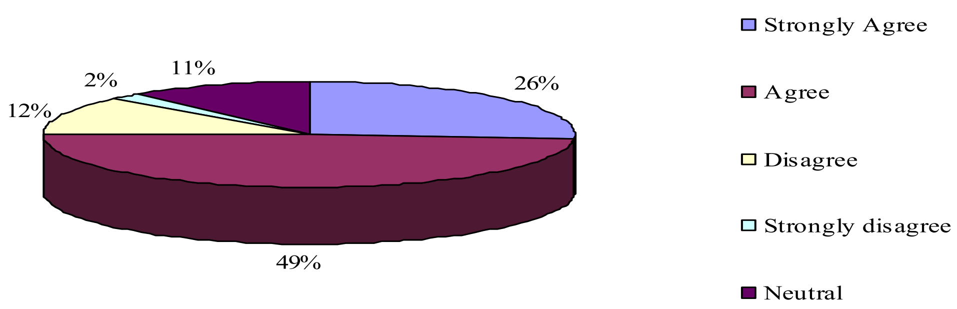
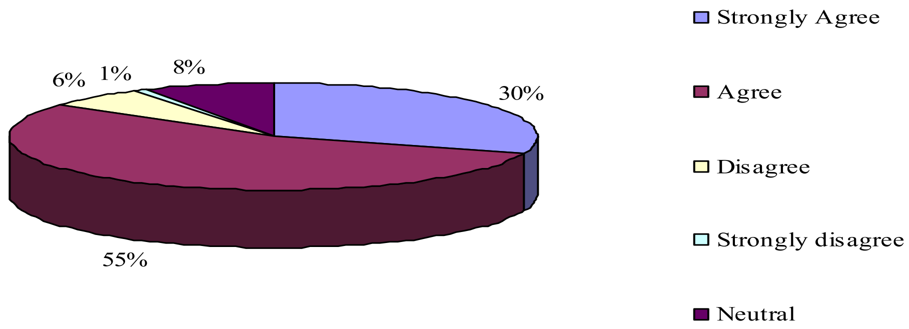


Figure 17 (Survey results): "I would know how to report a security incident or breach."



The first action following the detection of a security incident or breach is to notify the appropriate authority. Figure 16 shows that 85% of respondents would know how to report a security incident or breach. 7% of respondents would not know how to report a security incident. These numbers indicate that organizations who participated in the survey are doing a good job in the area of reporting security incidents.

Figure 18 (PentaSafe results): “Do you know the consequences of failing to comply with your organizations security policy”

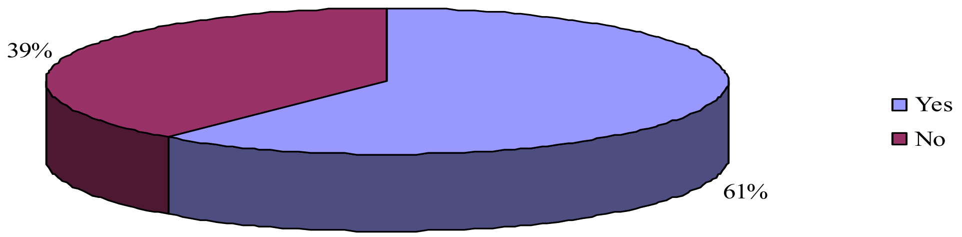
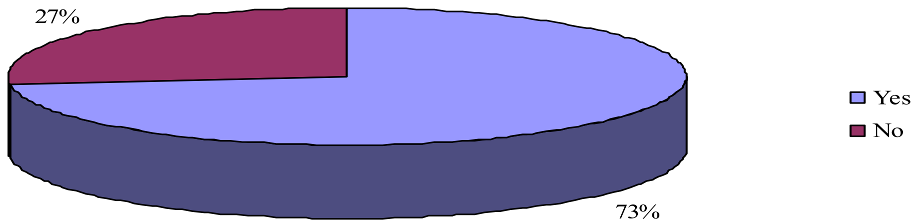


Figure 19 (Survey results): “Do you know the consequences of failing to comply with your organizations security policy”



By analyzing figure 18 and 19, it can be observed that there is an improvement in compliance results. The graphs show a 12% increase in the number of respondents that believe they know the consequences of failing to comply with their organizations security policies which is an indication that if compliance practices are implemented correctly, they could significantly reduce the frequency and impact of security violations.

PERCEPTION AND ATTITUDE

Figure 20 (PentaSafe results): Agreement with statements about security perceptions and attitude

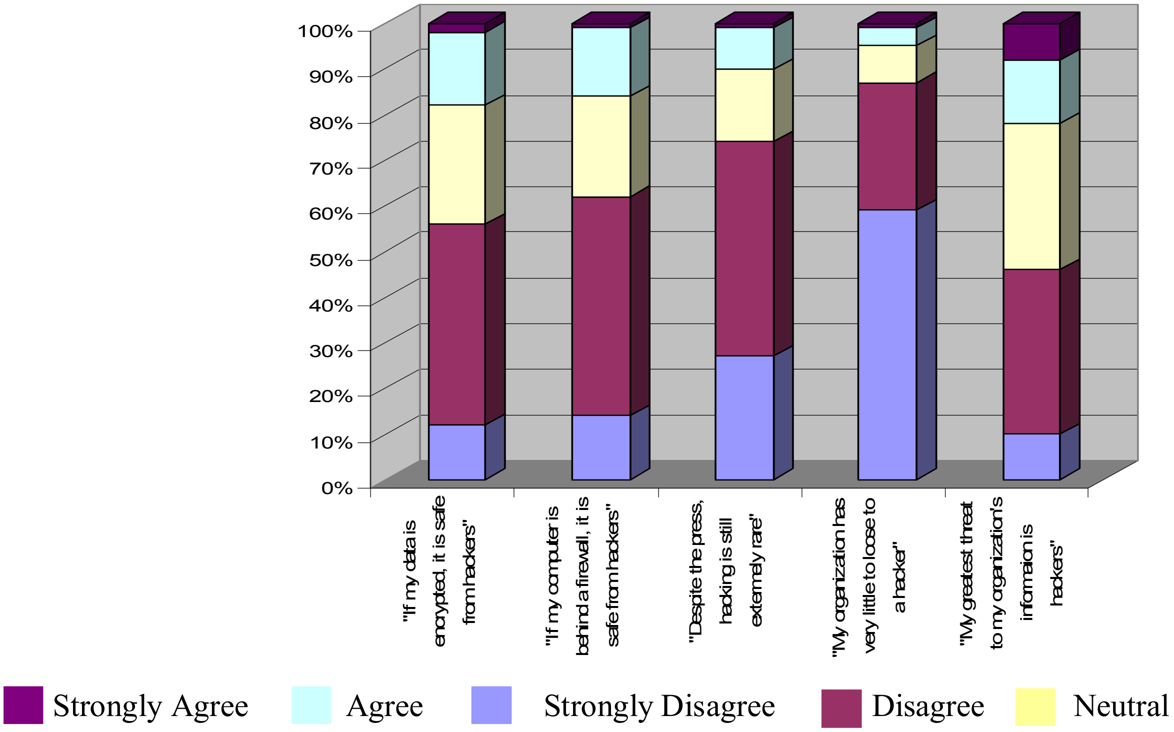
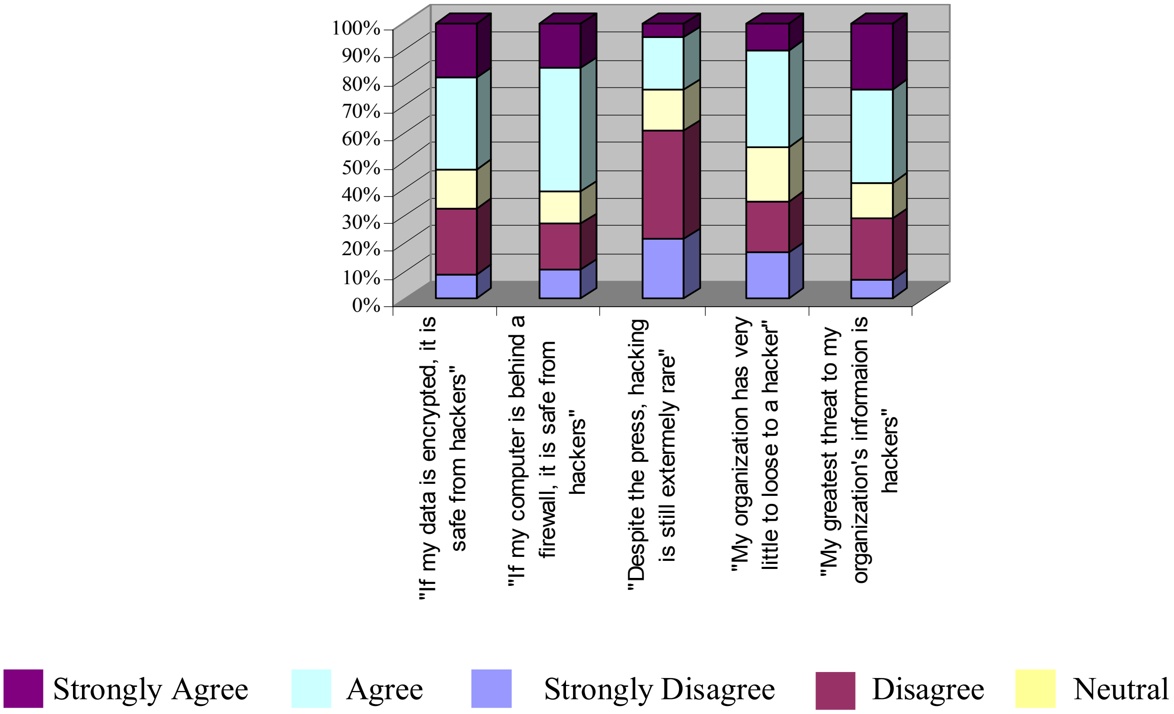


Figure 21 (Survey results): Agreement with statements about security perceptions and attitude



The attitude and perception of employees are very important for the information security of organizations today. Attitude is a way of thinking, feeling or behaving. Perception is the way in which individuals analyze and interpret incoming information and make sense of it. Employee attitudes mean more to information security than technical solutions. Most secure systems will not give organizations any security if the people operating it have the wrong attitudes. Good attitudes are something that must be built. From the perception and attitudes graph results, there is an overall positive response to the questions asked when compared to SAI results. However, there might be a possibility that some employees might not state the truth about their own attitudes or perception. Therefore, the focus should not be on what an employee knows but on what he or she does with this knowledge.

6.0 Security Threats to Consider When Using SAI Questionnaire

The security awareness index covers interesting security topics that require general employee awareness. However, interview feedback suggests that the organizations who participated in the survey have an interest in the following areas.

- **Portable Devices:** Portable data devices such as USB drives, laptops, personal digital assistants and blackberries are a common source of data breach. While the small size of these portable devices can be an advantage, it also can be a disadvantage since portable devices can be easy to steal. Portable devices theft has become a major issue as the thieves are in for financial gain and are therefore interested in the information that is contained on these devices. Portable devices are usually given to employees where it is necessary for the effective performance of an employee's duties. These services should only be used in a manner which protects system resources and the information stored. Users who rely on hand held devices should be educated on portable devices security best practices or acceptable use.

- **Secure Disposal:** The data stored on hard disks and other storage media such as tape must be protected when these media, or equipment containing them, are no longer required or do not function. With the advent of new and additional laws surrounding the protection of personal data, organizations should consider educating users in this area to protect sensitive information from being accidentally disclosed to unauthorized persons.

- **Clear Desk:** Let's consider a common security mistake in almost all organizations worldwide which is, writing employee names and passwords on Post-it notes stuck to their computers. Desks should be cleared of all documents and papers to ensure that sensitive papers and documents are not exposed to unauthorized persons. To ensure employee compliance with data protection regulations, protection from identity theft etc, organization should implement a clear desk policy and communicate the policy through awareness training or some other method.

- **Social Engineering:** Social Engineering is a threat, often overlooked but regularly exploited. In information security, social engineering is a term that describes a non-technical kind of attack that relies heavily on human interaction and often involves deceiving other people to destroy the integrity of normal security procedures. Karen J Bannan defines a social engineer as "a hacker who uses brains instead of computer brawn" [13]. Hackers call data centers and pretend to be customers who have lost their password or show up at a site and simply wait for someone to hold a door open for them. Other forms of social engineering are not so obvious. The victims of social engineering are deceived into releasing information that they do not realize could be used to attack their organizations computer networks. A real life example of social engineering is as follows: "In 1994, a French hacker named Anthony Zboralski called the FBI office in Washington, pretending to be an FBI representative working at the U.S. embassy in Paris. He persuaded the person at the other end of the phone to explain how to connect to the FBI's phone conferencing system. Then he ran up a $250,000 phone bill in seven months" [14]

  Social engineering can not be stopped fully no matter what logical or physical controls are put in place. The reason for this is because there is always the possibility of the 'human factor' being influenced by an event. To minimize social engineering attacks, it is important to understand the significance of the threats involved and adopting controls that can be implemented to protect against such attacks.

- **Roles and Responsibilities:** The need for clarification about the roles and responsibilities in information security is very important. In any organizational environment, who does what, is a fundamental part of people working together. We all have a responsibility for maintaining the security and confidentiality of information assets. Employees are ultimately responsible for protecting their organizations information assets and resources. Therefore, it is imperative that all personnel, including vendors and contractors, be aware of their security responsibilities.

Employees are the first line of defense for security in every organization, as they will be the first to identify unusual activities or behaviors. If employees do not know or understand their security responsibilities, they will be unable to enforce and comply with them. Without this, security in organizations would fail and expose information assets to unacceptable and unnecessary risk. Therefore, continuous awareness of employee’s responsibilities should be emphasized.

7.0 Conclusion

This research paper investigated the applicability of the SAI and determined that the SAI can be used in practical work because it addresses common security issues in organizations today. The SAI was found to be applicable on large, medium and small organizations because it focuses on general employee awareness. Even though the questionnaire can be improved on, the SAI metrics can serve as a benchmark to measure information security awareness levels.

This research paper also investigated what private and public organizations in Edmonton are doing to promote information security awareness and found out that there are various initiatives undertaken by the organizations who participated in the survey to raise information security awareness. Some of the initiatives include a poster awareness program, incident reporting procedures, education and training, security awareness videos and security awareness day or week.

In addition to investigating what private and public organizations in Edmonton are doing to promote information security awareness, this research paper also investigated how these organizations measure the level of awareness and the consistency of the awareness program. Interview feedback indicated that majority of the organizations measure the level of information security awareness through various methods such as surveys, quizzes, spot checks, number of security incidents, auditing and so on. Lastly, the organizations do a good job in trying to be consistent with their awareness programs. However, this is because most of the organizations are mandated by policy to promote on-going security awareness training.

8.0 Appendix A

Security Awareness Index Questionnaire and Scoring Methodology

Please circle the appropriate answer(s)

1) How long has it been since you read any of your organization's security policies?
(Select one)

Answer	**Scoring Answer**	**Score**
Less than 6 months ago	Yes	10
Between 6 months and 1 year ago	Yes	9
From 1 to 2 years ago	Yes	5
Between 2 and 5 years ago	Yes	3
More than 5 years ago	Yes	1
I have never read any security policies	N/A	0
The organization does not have security policies	N/A	0
Unknown	N/A	0

2) How long has it been since you read all of your organization's security policies that apply to you?
(Select one)

Answer	**Scoring Answer**	**Score**
Less than 6 months ago	Yes	10
Between 6 months and 1 year ago	Yes	9
From 1 to 2 years ago	Yes	5
Between 2 and 5 years ago	Yes	3
More than 5 years ago	Yes	1
Never read all security policies	N/A	0
The organization does not have security policies	N/A	0
I do not know which policies apply to me.	N/A	0
Unknown	N/A	0

3) Are your organization's security policies easily available to you?
(Select one)

Answer	Scoring Answer	Score
Easily available	N/A	0
Not easily available	N/A	0
My organization does not have policies	N/A	0

4) How long has it been since you have received formal security awareness training from your organization?
(Select one):

Answer	Scoring Answer	Score
Less than 6 months ago	Yes	10
Between 6 months and 1 year ago	Yes	9
From 1 to 2 years ago	Yes	5
Between 2 and 5 years ago	Yes	3
More than 5 years ago	N/A	0
I have never received formal awareness training from my organization	N/A	0
Unknown	N/A	0

5) Do you feel your organization's security policies are too restrictive?
(Select one)

Answer	Scoring Answer	Score
Too restrictive	N/A	0
Not too restrictive	N/A	0
My organization does not have policies	N/A	0

6) Do you know the consequences of failing to comply with your organization's security policies?

(Select one):

Answer	**Scoring Answer**	**Score**
Yes	Yes	10
No	N/A	0
My organization does not have policies	N/A	0

7) Assume you receive an e-mail from someone you know but you have not spoken to that person about it. If the e-mail contained a file with any of the following extensions, which would you feel are safe to execute by double-clicking on it?

(Multiple select)

Answer	**Scoring Answer**	**Score**
.exe	No	3.75
.doc	No	3.75
.xls	No	3.75
.pdf	N/A	0
.vbs	No	3.75
.bmp	N/A	0

8) To which of the following employees in your organization would you tell your network (e.g., Windows, NetWare) password if that person requested it?

(Multiple select)

Answer	**Scoring Answer**	**Score**
Workers direct supervisor	No	2.5
Director of HR	No	2.5
The chief security officer	No	2.5
The network or system administrator	No	2.5
A co-worker	No	2.5
An internal auditor	No	2.5

9) Which of the following passwords would you feel are acceptable and safe to choose as your network password?
(Multiple select)

Answer	Scoring Answer	Score
banana	No	1.875
frog1	No	1.875
Yamaha99	No	1.875
aCtoHm23	Yes	1.875
fido23	No	1.875
6814745	No	1.875
be!St&8	Yes	1.875
jT35Io!ki$iD@23aq	No	1.875

10) Please rate your level of agreement with the following statements.
(Select one for each)
Statement: "I feel empowered to make informed decisions about the security of information and technology."

Answer	Scoring Answer	Score
Strongly Agree	Yes	1.5
Agree	Yes	1.25
Neutral	Yes	.75
Disagree	N/A	0
Strongly Disagree	N/A	0

Statement: "I am confident that I would know a security policy violation if I saw one."

Answer	Scoring Answer	Score
Strongly Agree	Yes	1.5
Agree	Yes	1.25
Neutral	Yes	.75
Disagree	N/A	0
Strongly Disagree	N/A	0

Statement: "I would know how to report a security incident or breach."

Answer	**Scoring Answer**	**Score**
Strongly Agree	Yes	1.5
Agree	Yes	1.25
Neutral	Yes	.75
Disagree	N/A	0
Strongly Disagree	N/A	0

Statement: "I would like to receive more training on information security from my organization."

Answer	**Scoring Answer**	**Score**
Strongly Agree	N/A	0
Agree	N/A	0
Neutral	N/A	0
Disagree	N/A	0
Strongly Disagree	N/A	0

Statement: "If my data is encrypted, it is safe from hackers."

Answer	**Scoring Answer**	**Score**
Strongly Agree	N/A	0
Agree	N/A	0
Neutral	Yes	1.5
Disagree	Yes	1.5
Strongly Disagree	Yes	1.5

Statement: "If my computer is behind a firewall, it is safe from hackers."

Answer	**Scoring Answer**	**Score**
Strongly Agree	N/A	0
Agree	N/A	0
Neutral	Yes	1.5
Disagree	Yes	1.5
Strongly Disagree	Yes	1.5

Statement: "Despite the press, hacking is still extremely rare."

Answer	**Scoring Answer**	**Score**
Strongly Agree	N/A	0
Agree	N/A	0
Neutral	Yes	.75
Disagree	Yes	1.25
Strongly Disagree	Yes	1.5

Statement: "My organization has very little to lose to a hacker."

Answer	**Scoring Answer**	**Score**
Strongly Agree	N/A	0
Agree	N/A	0
Neutral	Yes	0
Disagree	Yes	1.25
Strongly Disagree	Yes	1.5

Statement: "The greatest threat to my organization's information is hackers."

Answer	**Scoring Answer**	**Score**
Strongly Agree	N/A	0
Agree	N/A	0
Neutral	N/A	0
Disagree	Yes	1.25
Strongly Disagree	Yes	1.5

11) Please fill in the blank with one of the following choices:

"Security is _________________".

Answer	Scoring Answer	Score
100% technology, 0% people	N/A	0
75% technology, 25% people	N/A	0
50% technology, 50% people	Yes	2.5
25% technology, 75% people	Yes	2.75
0% technology, 100% people	Yes	3

9.0 Appendix B

Letter Sent Out to Organizations

Dear Sir/Madame:
My name is Fuad Iddrisu. I am a student at Concordia University College enrolled in a Master's program in Information Systems Security Management. I am currently working on my thesis which focuses on information security awareness in Edmonton.

The purpose of this thesis is to determine what organizations in Edmonton are doing to promote information security awareness in their workplace. Along with this, I will explore whether or not there is a security program within the organization, how often the program runs and whether or not the organization has attempted to measure the level of information security awareness amongst its employees.

The survey I wish you to fill out will be in two parts. Part one will be an interview with information security managers/ Chief Information Officers and Part Two will be a set of questions given to the employees to complete. Both the questionnaires and interview should take about 15 -20 minutes to complete.

Thank you for your time and consideration and I look forward to your organizations participation in this project. I believe that participation in this research will also assist your organization in identifying your security practices, establishing your organizations security benchmark and the benefits and shortfalls of your current security practice.

I can be reached at (250) 507-7207 to arrange a time to meet to provide you with further detail and to give you the questionnaires. I can also email the questionnaires to you if you would like. Again, I thank you for your time and consideration and I look forward to your quick response.
Sincerely

Fuad Iddrisu

10.0 Appendix C

Bibliography

1 NACIO *"Insider Security Threats"* (2007)

2 Mark Wilson and Joan Hash (NIST 800-50) *"Building an Information Technology Security Awareness and Training Program"* (2003)

3 ENISA *"Current practice and the measurement of success"* (2007)

4 K Rudolph *"Measure What Matters"* (2007)

5 Robert Richardson "Computer Crime and Security Survey" (2007)

6 Mr. Gullik Wold *"Key factors in making ICT Security Policies effective"* (2004)

7 PentaSafe Security awareness index report "*State of security awareness among organizations worldwide*" (2002).

8 University of Georgia (SATE): http://www.infosec.uga.edu/sate/index.php

9 Laura Taylor *"Security awareness and Training 101"* (2004)

10 NIST Special Publications 800-16 "*Information Technology Security Training Requirements"*

11 Australia Standard *"Compliance Programs AS 3806"* (2006)

12 Shannon Riley *"What users know and what they actually do"* (2006)

13 Infosecurity Europe conference: http://www.out-law.com/page-7961

14 Karen J Bannan "*who is spying now"* (1994)

15 Bruce Schneier "*Secret and lies*" (2000)