A Comprehensive Framework for a Risk and Role Based Enterprise Security Awareness, Training and Education Program for ISO/IEC 27002 Compliance

Author: Allen M.-K. Nip, April 2011

Research Advisors (Dr. Pavol Zavarsky, Ron Ruhl and Dr. Dale Lindskog)

Information Systems Security Department
Concordia University College of Alberta
7128 Ada Boulevard, Edmonton, AB T5B 4E4, Canada
Phone: 1.866.479.5200

allen.mk.nip@gmail.com, {pavol.zavarsky, ron.ruhl, dale.lindskog}@concordia.ab.ca

***Abstract*— Organizations are faced with a variety of ever changing information security risks. This study examines the state of information security, user groups and user roles responsible for and ISO/IEC domains required for risk mitigation in a large public organization in Canada. The objective is to develop a comprehensive risk and role based framework for an enterprise security awareness, training and education (SATE) program for ISO/IEC 27002 compliance with the intent to improve an existing SATE program in a large public organization. This paper discusses the results of an information security survey conducted in 2010 and describes the framework and its components and interactions.**

Significant findings of this study include: (1) a new and more comprehensive set of user roles within a user group for a SATE program not previously identified by the SANS Institute, (2) a significant number of new threats and vulnerabilities not previously identified in global and national information security surveys, (3) the use of a risk factor to prioritize what information security risks should be addressed in a SATE program, (4) the rationalization for the subject content in an enterprise SATE program and (5) a framework for a risk and role based enterprise SATE program for ISO/IEC 27002 compliance.

Keywords-component; user role; role based; risk based; ISO/IEC 27002 compliance; security awareness; security training; security education; threats; vulnerabilities

I. INTRODUCTION

How people perform their tasks in a secure manner is critical for maintaining information security within an organization. It is often said that "*people are the weakest link in information security*" [1, 2, 3, 4 and 5]. The question here is to determine who should be made aware, trained or educated to mitigate the information security risks identified within an organization, what information, knowledge or insight does a user require to fulfill their information security role and responsibilities [3] and why is it important for a user to fulfill their role and responsibilities with respect to information security. The intent of this research is to develop a risk and role based framework to help refine an existing SATE program in a large public organization.

This study examines the state of information security in a large public organization to develop a risk and role based framework for an enterprise SATE program for ISO/IEC 27002 compliance. This study surveys the following areas: (1) user participation in a SATE program, (2) existence of user groups and user roles within a large public organization, (3) importance, source and occurrence of pre-defined and open-ended threats and vulnerabilities and its impact and risk to a large public organization and (4) user groups and user roles that should be targeted to mitigate the information security risks identified. In addition, this study (1) uses a risk factor to assist in the prioritization of risks to be addressed in a SATE program, (2) determines what ISO/IEC 27002 domains should be required for risk mitigation and (3) provides the rationalization for the particular subject content a user should be made aware of, be knowledgeable or understand to mitigate the information security risks identified. A survey questionnaire is used to provide empirical data for the development of the framework. This paper discusses the results of the survey questionnaire and the framework with its components and interactions.

II. LITERATURE REVIEW

Organizations invest in technologies such as anti-virus solutions, virtual private networks and encryption to secure their information technology assets, however, "*investments in technology are of little value unless people are trained on what to do and how to do it*" [6, p.16]. Many of these investments appear to be primarily focused on outsider threats, however, insider threats also need to be considered [7, 8] and mitigated as well. CompTIA Research [9] reported that more than half the information security breaches were caused by the failure of staff to follow information security procedures. Computer Security Institute (CSI) [10] found that the top 5 attacks (viruses, insider abuse of network access, laptop and mobile device thefts, unauthorized access to information and denial of services), between 1999 and 2008, were ranked similarly with respect to occurrences. Of these top 5 attacks, insider abuse of network access, laptop and mobile device thefts and unauthorized access to information were user related. With this in mind, information security is everyone's responsibility [11].

ISO/IEC 27002 [12], Control Objectives for Information and related Technology (COBIT) [13], the Information Security Forum [14] and the National Institute of Standards and Technology (NIST) [15] viewed information security awareness and training as a best practice for information security while Ross et al. [16] viewed it as an operational control to mitigate information security risks. Ernst & Young [6] pointed out that developing an appropriate information security awareness program is a challenge while Deloitte Touch Tohmatsu [17] emphasized that a one size fits all approach does not work as they were found to be too high level and generic to have any impact [18]. With this in mind, how can an organization develop a tailored SATE program?

Information security crosses all levels within an organization; vertically, horizontally and cross-functionally [19]. All users have a role to play with respect to information security within their organization. These roles may differ vertically, horizontally as well as cross-functionality between organizations. Rotvold [20, p. 33] emphasized that "*all users should be aware of not only what their roles and responsibilities are in protecting information resources, but also of how they can protect information and respond to any potential security threat or issue*".

To develop a tailored SATE program for an organization, the following three basic questions should be answered:

1) Who needs to be made aware, trained or educated (i.e. identify target user groups based on user roles) in information security? A user role is a person(s) with a set of roles and responsibilities with respect to mitigating an information security risk. A user group consists of a group of user roles with a similar business function (e.g. System Developer user group are responsible for the system development life cycle). Note the use of the term user groups and user roles in this paper is not related and should not be confused with operating system (e.g. Active Directory Services) security classes, nor database and application related user groups, roles and permissions,
2) What information, knowledge or insight does a user require to fulfill their information security role and responsibilities [3]? and,
3) Why is it important for a user to fulfill their role and responsibilities with respect to information security?

This is further supported by the SANS Institute [21] where an Instructional Systems Design (ISD) was combined with the NIST SP 800-16 model [22] to integrate security awareness and education. The ISD processes defined "w*ho needs to be trained in what content areas and why*" [21, p. 2]. The SANS Institute recommended the following basic steps for developing a security awareness training program:

1) *"Apply ISD processes to security topics,*
2) *Apply NIST SP 800-16 to provide the right content for the right people. Identify target audience for security training,*
3) *Map out the core body of knowledge to identify the appropriate level of training and,*
4) *Design and develop the security awareness training program to support role and performance based security needs"* [21, p. 2].

The European National Information Security Agency (ENISA) [23] outlined a similar set of steps in developing a security awareness training program:

1) Develop a matrix identifying target user groups, what type of awareness, training and education is required and how it should be delivered and,
2) Develop a second matrix mapping the user target group and information security subject content to be covered.

NIST [22] recommended the following assessments to be conducted for determining the requirements of a security awareness and training program:

1) Assessment of the current delivery of a security awareness and training program,
2) Materials, subject and percentage of users enrolled,
3) Review of audit findings, threat risk assessments or security program reviews,
4) Surveys and interviews with key personnel such as business application owners and management,
5) Review and analysis of information security events that have recently occurred and,
6) Review of global surveys, findings and trends.

By identifying the target user groups based on user roles [23, 24 and 25], the first question "*who needs to be trained*"

component of a SATE program is answered. Various studies [21, 22, 26 and 27] have outlined various user roles, some of which were similar as well as different.

The next step is to determine the subject content to be delivered by the SATE program. The subject content, which is the information, knowledge or insight required by a user to fulfill a particular role, answers the "*what content is required*" component of a SATE program. The SANS Institute [21] has defined a set of topics for specific user roles.

In a risk based approach to a SATE program, an organization should undertake an information security threat risk assessment to determine what the organization's perceived and actual threats are [11, 28, 29 and 30]. Nellis [24] recommended interviewing senior management to identify their information security concerns as well as using the results from threat risk assessments when developing a SATE program for senior managers. By identifying the organization's information security risks, users can be made aware of them through a SATE program [26].

Specific and detailed subject content, generally intended for IT professionals who have information security related responsibilities but are not information security professionals, can be delivered through information security related training [3]. Training may vary from beginner to advanced levels. The subject content should be tailored to fit the user's role and their information security related responsibilities. Training requirements have been well documented for a Senior Systems Manager [31], System Administrator [31], and Systems Certifier [33] and Systems Developer [34 and 35]. In addition, Hansche [11] has outlined the topics and provided descriptions for training courses as well as their intended audiences.

Information security education provides the insight for understanding why a particular subject matter is important and is aimed at information security professionals [22]. Education may consist of specific courses towards a degree or certificate in information security. Various United States (U.S.) federal publications [25, 36 and 37] have documented educational requirements for information security professionals.

"W*hy a user should be aware of, have knowledge or insight into various information security topics*" is not well reported in the literature. NIST [16] and Information Systems Audit and Control Association (ISACA) have documented various mappings between different security control standards and frameworks such as COBIT, National Institute of Standards and Technology (NIST) SP 800-53 and SP 800-26, and ISO/IEC 17799.

III. RESEARCH OBJECTIVES

The research objectives of this study are to:

1) Provide insight into the state of information security for a large public organization in Canada,
2) Identify user groups and user roles and their prevalence in a large public organization,
3) Identify user groups and user roles responsible for mitigating information security risks,
4) Identify appropriate subject content for a SATE program by user group,
5) Identify why is it important for the user group to be aware of, knowledgeable or understand the subject content presented in a SATE program and,
6) Develop a role and risk based framework for an enterprise SATE program for ISO/IEC 27002 compliance.

IV. METHODOLOGY

This research focuses solely on an enterprise approach to SATE, similar to those outlined by Westby and Allen [19, p. 5] where they viewed information security, as "*managed as an enterprise issue, horizontally, vertically, and cross-functional throughout the organization*".

A. Study Design

A paper survey questionnaire is developed to collect empirical data for the development of a comprehensive risk and role based framework for an enterprise SATE program for ISO/IEC 27002 compliance. The survey questionnaire consists of three major parts: Part 1 examines user participation in a SATE program (refer to Section V. *User Participation in a SATE Program* for analysis of survey questionnaire results); Part 2 determines user groups and user roles within a large public organization (refer to Section V. *User Groups and User Roles* for analysis of survey questionnaire results) and; Part 3 examines the importance, source and likelihood of occurrences of pre-defined and open-ended threats and vulnerabilities and its impact and risk to a large public organization and lastly, user groups and user roles that should be targeted to mitigate the information security risks identified (refer to Section V. *Threats, Vulnerabilities, Risks and User Mitigation* for analysis of survey questionnaire results).

In 2010, data are collected over a period of two months from survey participants who are members of an Enterprise Information Security Forum (EISF) in a large public organization in Canada. These members are designated as Information Security Officers (ISO) responsible for information security for their respective departments, agencies and boards and their positions vary from Executive Directors, Senior Managers to Senior Security Analysts.

Upon completion of all the interviews, the final phase of the study encompasses the author identifying what particular ISO/IEC 27002 domains are required to mitigate each of the information security risks identified.

B. Administering the Survey Questionaire

A survey questionnaire is administered by the author in an interview with the survey participants. Each interview is conducted in a private office to ensure the privacy of results. Prior to the start of the interview, the role that survey participants play in completing the survey questionnaire is explained to them. Survey participants are also told that they may choose to withdraw from the survey questionnaire at any time or not answer any of the survey questionnaire questions without prejudice and the results would remain anonymous and only be reported as an aggregate. Survey participants are asked to sign an Informed Consent Form, indicating their consent to participate in the survey questionnaire.

Definitions, used for ranking various survey questionnaire variables, are provided to the survey participant prior to the start of the interview to ensure consistency in the survey questionnaire responses. Each survey questionnaire is assigned a survey number to ensure anonymity. All the data is captured and transcribed on to the survey questionnaire as the interview is being conducted. A date and time stamp is placed on the survey questionnaire at the end of the interview. Each interview takes between ninety to one hundred and twenty minutes to complete.

V. SURVEY QUESTIONAIRE ANALYSIS

A total of twenty-two EISF members, representing twenty-one out of twenty-two departments and one of two select agencies and boards, have completed the interviews. Responses are varied in terms of the level of detail provided and completeness. User groups, user roles as well as threats and vulnerabilities not previously identified on the survey questionnaire and identified by the survey participant are captured during the interview. Newly identified information is not carried forward to subsequent interviews to eliminate the need to resurvey indefinitely. All data are transcribed onto a spreadsheet for data analysis.

A. User Participation in a SATE Program

Table I shows an estimate of the percentage of users participating in a SATE program for a large public organization. Participation rates vary considerably.

The data collected for the Awareness program type are a true estimate of participation rates, considering all users within an organization should be participating in an Awareness program. However, the results for the Training and Education program types should not be interpreted as is. Normally, users participating in such programs are a subset of the total number of users within an organization.

TABLE I. PARTICIPATION IN AN INFORMATION SECURITY AWARENESS, TRAINING AND EDUCATION PROGRAM

SATE Program Type	**Survey Participant Reported Estimate of User Participation (% of Total User Population)**		
	Mean	***Range***	***Standard Deviation***
Awareness	49.7	2-100	34.3
Training	8.3	0-95	21.2
Education	0.4	0-1	0.2

The study is unable to take into consideration the total number of users that make up the subset of either the Training or Education program. Security training and education programs are generally targeted for technical administrators and information security professionals respectively. These users make up a small percentage of the total staff count within an organization, with technical administrators generally having a higher staff count than those of information security professionals.

Table II shows the user groups and user roles found and their prevalence within a large public organization.

TABLE II. IDENTIFICATION AND PREVALENCE OF USER GROUPS AND USER ROLES

User Groups (bolded and italicized) and User Roles *** New User Groups and User Roles**	**Percentage of Survey Participants Indicating the Presence of the User Roles Within Their Own Organization**
****Management***	
*Executive (Minister, Deputy Minister, Assistant Minister)	100
*Senior Management	100
*Program Manager	100
*Chief Information Officer	100
*Senior Financial Officer	100
****Information Owner***	
*Data	100
*Application	100
****Systems Developer***	
Programmer	91
*Change Manage Officer	59
*Quality Assurance Staff	62
*Enterprise/ Data/ Business / Technical/Application Architect	77
*Business Analyst	80
*Project Management Office	50
*Geo-spatial Analyst	12
****Technical Administrator***	
System (server)	100
Network	100
Database	100
*Database Security	36
E-mail/Blackberry	100
*Data Center Manager	91

User Groups (bolded and italicized) and User Roles * New User Groups and User Roles	Percentage of Survey Participants Indicating the Presence of the User Roles Within Their Own Organization
*Web/SharePoint	100
*Storage Area Network	42
*Desktop Support	100
*Service Desk	95
*Security Operations	13
*Domain Administration	30
*Mainframe Administration	30
*Application Administrator	60
*Production Support	40
Information Security	
Information Security Officer	100
Information Security Manager	73
*Disaster Recovery Coordinator	100
*Business Continuity Coordinator	100
*Business Area Security Analyst	16
*Physical Security Unit	18
*Technical Security Committee	18
Non-Technical	
General Users	100
Legal Affairs	68
Contracting Officer	76
* Internal Audit	91
Human Resources	59
*Enterprise Risk Management	91
*Records Management Staff	95
*Freedom of Information and Protection of Privacy	95
*Web Coordinator	95
*Contractor	90
*Volunteer	1
*Business Partnership	62
*Facilities Manager	95
*Service Request Coordinator	94
*Financial Controller	100
*Communications Staff	100
*Business Intelligence Analyst	14
*Enforcement Staff including Special Investigator	30
Procurement	1
*Administrative	100

The user groups identified in the study are similar in description and function to those reported by the SANS Institute [21], however, the user roles do differ significantly. New user roles and user groups not previously reported by the SANS Institute are marked by an asterisk in Table II. The majority of the user roles and user groups identified in this study are new. Note in some cases, the percentage of respondents is extremely low. In these cases, it is important to note their presence as their prevalence may vary between organizations.

In this study, the number of user roles identified within a particular user group is significantly greater than those reported by the SANS Institute [21] with the exception of *Information Owner* user group. It is critically important to identify as many user roles as possible to ensure that all users and their particular role they play to mitigate information security risks within the organization are accounted for.

B. Threats, Vulnerabilities, Risks and User Mitigation

The threats and vulnerabilities listed on the survey questionnaire are identified from a combination of sources: annual global surveys conducted by the Computer Security Institute (CSI) [10], Deloitte Touche Tohmatsu [7 and 18] and from the experiences of the author. A total of forty-three threats and vulnerabilities are listed on the survey questionnaire with another seven added through the course of the survey. These seven are not carried through the course of the interviews to prevent the research from running indefinitely.

The number of threats and vulnerabilities that are identified and surveyed in this study is significantly greater than those found in some global and national surveys, twice the number in the case of CSI [10]. It is critical that there be a comprehensive identification of known or perceived threats and vulnerabilities types to ensure that potential or known ones are not missed.

The importance, source and likelihood of occurrence of threats and vulnerabilities and its impact to the organization are collected during the interviews. Table III lists the top twenty-five information security risks and their source(s) found in this study.

TABLE III. RANKING AND SOURCE OF TOP 25 INFORMATION SECURITY RISKS

Importance of Risk	Internal	External	Both
1. E-mail attacks		X	
2. Inappropriate Internet use	X		
3. Inadequate classification of information	X		
4. Malware (e.g. viruses, Trojans)			X
5. Inadequate software testing procedures	X		
6. Web site vulnerabilities			X
7. Inadequate audit practices	X		
8. Poor security software coding practices	X		
9. Phishing		X	
10. Inadequate server / network redundancy	X		
11. Inadequate protection of sensitive / confidential information	X		
12. Misuse of corporate storage	X		
13. Theft / loss / disclosure of personal information			X
14. Theft / loss / disclosure of corporate data			X
15. Laptop and other hardware theft			X
16. Inadequate business continuity plan	X		
17. Misuse of corporate bandwidth	X		
18. Inadequate threat and	X		

	vulnerability testing			
19.	Poor or inadequate user access controls	X		
20.	Physical security breach			X
21.	Lack of security considerations in systems development life cycle	X		
22.	Inadequate physical security controls			X
23.	Inadequate environmental controls	X		
24.	Bot attack		X	
25.	Inadequate disaster recovery plan	X		

Clearly, the source of majority of the threats and vulnerabilities surveyed are internal rather than external. CSI [10] reported that forty-three percent of their respondents attributed their security breaches to malicious insiders with non-malicious insiders being a greater problem as compared to malicious insiders.

The likelihood of a threat and vulnerability occurrence combined with the level of impact to the organization is used to calculate a risk factor for each threat and vulnerability. This risk factor could be used to help prioritize what information security risks and subsequently driving what subject content should be addressed in an organization's SATE program.

The final phase of the study determines what primary, secondary and tertiary ISO/IEC 27002 domains should be implemented and form the subject content for a SATE program to mitigate the information security risks identified. This requires a thorough understanding of the ISO/IEC 27002 standard. In addition, the author's knowledge and experiences in the large public organization has helped facilitate the identification of recommended domains.

Table IV is an example of the outcome of the results from Part 3 of the survey questionnaire and the final phase of this study. In this case, the specific information security risk identified is an e-mail attack; the user groups responsible for risk mitigation are: *Non-Technical, Technical Administrator* and *Information Security;* the user roles responsible for risk mitigation are: All Users, System, Network and E-mail, Information Security Officer and Information Security Manager and; the recommended ISO/IEC 27002 domains to mitigate an e-mail attack are domains 6, 8, 10, and 13.

Table V summarizes what ISO/IEC 27002 primary and secondary domains should user groups be aware of, be knowledgeable or have an understanding of, for the all information security risks identified in this study. To create such a table, an organization should identify the following:

1) Information security risks it faces,
2) User groups and user roles that are responsible for mitigating the information security risks identified,
3) ISO/IEC 27002 domain(s), similar to Table IV, to mitigate each individual information security risk identified;
4) Ranking of the information security risks identified,
5) Set of information security risks that an organization

TABLE IV. IDENTIFICATION OF USER GROUPS AND USER ROLES AND RECOMMENDED ISO/IEC 27002 DOMAINS FOR MITIGATING AN E-MAIL ATTACK

Risk	**User Group (bolded and italicized) / User Roles**	***Recommended ISO/IEC 27002 Domains**
E-mail attacks	***Non-Technical*** • All Users ***Technical Administrator*** • System • Network • E-mail ***Information Security*** • Information Security Officer • Information Security Manager	**6. Organization of information security** 6.1 INTERNAL ORGANIZATION 6.1.2 Information security co-ordination 6.1.3 Allocation of information security responsibilities **8. Human Resources Security** 8.1 PRIOR TO EMPLOYMENT 8.1.1 Roles and responsibilities 8.2 DURING EMPLOYMENT 8.2.1 Management responsibilities 8.2.2 Information security awareness, education, and training **10. Communications and Operations Management** 10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT 10.2.1 Service delivery 10.2.2 Monitoring and review of third party services 10.2.3 Managing changes to third party services 10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE 10.4.1 Controls against malicious code 10.4.2 Controls against mobile code 10.8 EXCHANGE OF INFORMATION 10.8.4 Electronic messaging **13. Information Security Incident Management** 13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES 13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses 13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 13.2.1 Responsibilities and procedures 13.2.2 Learning from information security incidents 13.2.3 Collection of evidence

* Primary (Bolded), Secondary (Upper Case) and Tertiary (Mixed Case) Domain Requirements

wishes to focus on in a SATE program.

Upon completion of steps 1 through 5, an organization can create a consolidated table similar to Table V, listing all the user groups and the recommended ISO/IEC 27002 domains for compliance for the set of information security risks that it wishes to focus on.

TABLE V. SUMMARY OF USER GROUPS AND RECOMMENDED ISO/IEC 27002 PRIMARY AND SECONDARY DOMAINS REQUIRED FOR COMPLIANCE FOR ALL THE INFORMATION SECURITY RISKS IDENTIFIED IN THIS STUDY

User Group	Recommended ISO/IEC 27002 Primary and Secondary Domains
Non-Technical	**6. Organization of Information Security** 6.1 INTERNAL ORGANIZATION 6.2 EXTERNAL PARTIES **7. Asset Management** 7.1 RESPONSIBILITY FOR ASSETS 7.2 INFORMATION CLASSIFICATION **8. Human Resources Security** 8.1 PRIOR TO EMPLOYMENT 8.2 DURING EMPLOYMENT 8.3 TERMINATION OR CHANGE OF EMPLOYMENT **9. Physical and Environmental Security** 9.1 SECURE AREAS 9.2 EQUIPMENT SECURITY **10. Communications and Operations Management** 10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT 10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE 10.5 BACK-UP 10.6 NETWORK SECURITY MANAGEMENT 10.7 MEDIA HANDLING 10.8 EXCHANGE OF INFORMATION 10.9 ELECTRONIC COMMERCE SERVICES 10.10 MONITORING **11. Access Control** 11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 11.2 USER ACCESS MANAGEMENT 11.3 USER RESPONSIBILITIES 11.4 NETWORK ACCESS CONTROL 11.5 OPERATING SYSTEM ACCESS CONTROL 11.6 APPLICATION AND INFORMATION ACCESS CONTROL 11.7 MOBILE COMPUTING AND TELEWORKING **12. Information Systems Acquisition, Development and Maintenance** 12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 12.2 CORRECT PROCESSING IN APPLICATIONS 12.3 CRYPTOGRAPHIC CONTROLS 12.4 SECURITY OF SYSTEM FILES 12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES **13. Information Security Incident Management** 13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES 13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS **15. Compliance** 15.1 COMPLIANCE WITH LEGAL REQUIREMENTS 15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE 15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS
Management	In addition to those domains identified for Non-Technical user group: **14. Business Continuity Management** 14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
Information Owner	In addition to those domains identified for Non-Technical user group: **14. Business Continuity** 14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
System Developer	In addition to those domains identified for Non-Technical user group: **10. Communications and Operations Management** 10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 10.3 SYSTEM PLANNING AND ACCEPTANCE
Technical Administrator	In addition to those domains identified for Non-Technical user group: **12. Information Systems Acquisition, Development and Maintenance** 12.6 TECHNICAL VULNERABILITY MANAGEMENT
Information Security	All domains (6-15)

***** Primary (Bolded) and Secondary Domains (Upper Case)

In order to compare the results between user groups, a minimum baseline set of recommended domains requirements for compliance is established. Given that the "All Users" user role within the "*Non-Technical*" user group

encompasses all users, this is the obvious choice for establishing the baseline. Table V also outlines the additional domain requirements above the recommended baseline for all the other user groups.

Given the roles that the Information Security Officer and Information Security Manager within the "*Information Security*" user group play, for those organizations that have adopted the ISO/IEC 27002 standard, it is recommended that both user roles should have a thorough understanding of all ISO/IEC 27002 domains (6 through 15).

In addition to the primary and secondary ISO/IEC 27002 domain requirements identified in Table V, tertiary domain requirements are also identified by the author. An example is the "Disaster Recovery and Business Continuity Coordinator" user roles that should be knowledgeable in tertiary domain 14.1.

VI. FINDINGS AND INTERPRETATION OF RESULTS

A. Findings Related to User Groups and User Roles

The SANS Institute [21] identified six major user groups. Table II, earlier in this paper, identifies six similarly equivalent user groups. Table VI compares the user groups between the two studies.

TABLE VI. COMPARISON OF USER GROUPS

User Groups	
***SANS Institute**	***EISF members***
Managers	*Management*
Other Personnel	*Non-Technical*
System Owners	*Information Owner*
Administrators	*Technical Administrator*
Programmers	*Systems Developer*
Security Professionals	*Information Security*

*SANS Institute [21]

The user groups are similar in some instances while different in other instances. The labeling of user groups by the SANS Institute [21] appeared to focus on the type of users within the user group. In contrast, the labeling of the user groups in this study is primarily based on the function that the user group performs. The *Technical Administrator* and *Systems Developer* user groups would have been better named as *Technical Administration* and *Systems Development* respectively. The overall function of each of the user groups is similar. Where differences exist, this study identifies a broader scope of user roles within a particular user group than those identified by the SANS Institute [21]. With a broader scope of user roles defined, it enables the development of custom tailored SATE programs for select user roles.

The SANS Institute [21] identified the *Managers* user group as users in a management role, from C-level to program managers, whereas the *Management* user group in this study encompasses the equivalency of C-level personnel (Minister, Deputy Minister and Assistant Deputy Minister) to program managers.

In the *System Owners* user group, the SANS Institute [21] recognized Network, Application and Database user roles. In comparison, the *Information Owner* user group in this study focuses primarily on the function of being an owner of information, identifying the Data (mainly unstructured) and Application (structured data) and excludes the Network user role. From an *Information Owner's* functional perspective, the Network user role is likely of no concern; however, from an Information Security Officer or Information Security Manager's functional perspective, the Network user role is critical in securing the network.

In the *Administrators* user group, the SANS Institute [21] identified technical user roles that were responsible for managing the network, operating systems, e-mail, and the database. In this study, the equivalent *Technical Administrator* user group has a wider scope of user roles, adding the Service (Help) Desk, Desktop Support, Web and SharePoint Administrator, Domain Administration and other user roles. Each of these user roles identified has a security role to play; an example is the Service Desk that is responsible for resetting a user's password or Domain Administration that is responsible for managing user accounts.

The SANS Institute [21] only identified the System and Application user roles within the *Programmers* user group. In comparison, the equivalent *Systems Developer* user group expands the scope to include other user roles involved with the systems development life cycle. These include the Enterprise / Data / Business / Technical and Application Architect, Change Management Officer, Project Management Office, Business Analyst, Quality Assurance and Geo-Spatial Analyst user roles.

In the *Security Professional* user group, the SANS Institute [21] identified only the Information Systems Security Officer, Information Systems Security Manager and Security Engineer user roles. In this study, the Security Engineer user role does not exist in the equivalent *Information Security* user group; however, this role may be filled by a Systems and/or Network user role within the *Technical Administrator* user group. For the *Information Security* user group, this study identifies additional user roles involved with information security such as the Business Continuity and Disaster Recovery Coordinator, Business Area Security Analyst, Physical Security Unit and Technical Security Committee.

Another significant difference between the two studies is the identification of external user roles (i.e. Volunteers and Business Partnership) in this study. The SANS Institute [21] solely focused on internal user roles. By identifying external user roles, the organization can take into consideration the type of impact these users may have on information security. For an organization that has a value chain that extends to external users from other organizations, a threat risk assessment should be completed with recommendations provided to deal with these particular user roles.

Overall, the six user groups and various user roles identified in this study appear to adequately represent all users within a large public organization.

B. Findings Related to Occurrences of Security Breaches.

The joint Rotman-TELUS study [38, 39 and 40] surveyed Canadian government, public and private institutions between 2008 and 2010. The following discussion solely focuses on comparing security breaches pertaining to Canadian government institutions from its full report in 2009 [39] with the results from this study. In the Rotman-TELUS study, eighteen types of information security breaches were surveyed. In comparison, forty-three types of information security breaches are surveyed, making this study wider in scope and more comprehensive. Both studies found malware and spam to be the most prevalent type of information security breach with bots and phishing attacks ranking similarly within the top six. The areas of significant differences are found in the following areas: the Rotman-TELUS study found laptop or mobile hardware theft to be the second most prevalent type of information security breach versus thirteenth in this study while unauthorized access to information by employees was ranked third in the Rotman-TELUS study and twenty-eighth in this study. This study lists inappropriate Internet use and misuse of corporate storage rounding out the top five types of information security breaches.

In 2009, CSI/FBI [10] reported malware and laptop/mobile device thefts as the top and second most prevalent type of information security breach respectively thus similar to the Rotman-TELUS study. CSI/FBI also reported insider abuse of the network and e-mail to be the third most prevalent type of information security breach. In comparison, this study separates insider abuse of the network and e-mail into (1) inappropriate Internet use (ranked third), (2) misuse of corporate storage (ranked fourth) and (3) misuse of corporate network bandwidth (ranked ninth).

C. Findings Related to Risks

Table VII compares the rankings of security issues of concern those found in government institutions in the Rothman-TELUS [39] study with the ranking of risk types discovered in this study. The only similarity between the 2 studies is the accountability of user access. Otherwise, the ranking differs significantly due to the difference in the number of security issues of concern or risks identified in each study thus making comparisons difficult. The use of wireless networks, storing data in the cloud and need for compliance with USA or other foreign regulations and legislation is virtually non-existent and does not appear as a risk in this study.

TABLE VII. RANKING OF SECURITY ISSUES OF CONCERN / RISKS

Ranking	**Security Issues of Concern by Government Respondents**	**Ranking of Risk**
	****2009 Rotman-TELUS***	***EISF members***
1	Disclosure / loss of confidential customer data	E-mail attacks
2	Business continuity / disaster recovery	Inappropriate Internet use
3	Compliance with Canadian regulations and legislation	Inadequate classification of information
4	Managing security of wireless and mobile devices	Malware (viruses, Trojans)
5	Employees understanding and complying with security policies	Inadequate software testing
6	Loss of strategic corporate information	Web site vulnerabilities
7	Accountability of user actions and access	Inadequate audit practices
8	Managing risks from third-parties, i.e. business partners, suppliers and collaborators	Poor security software coding practices
9	Managing data in the cloud (cloud computing)	Phishing
10	Compliance with USA or other foreign regulations and legislation	Inadequate server / network redundancy

*Rotman-TELUS [39]

D. Findings Related to ISO/IEC 27002 Compliance

One of the key research objectives of this study is to answer the question of "*why is it important for the user to be aware, knowledgeable or understand a particular subject matter pertaining to information security*". The answer is that the ISO/IEC 27002 standard, for those organizations that have adopted it, provides the controls that should be implemented in order to mitigate the information security risks identified within an organization. A thorough understanding of the standard is necessary in order to determine what controls (i.e. domains) at the primary, secondary and tertiary level should be implemented for the information security risks identified. By identifying these domains, the information can used to develop subject content for an enterprise SATE program.

E. Findings Related to Security Awareness, Training and and Education Programs

Requirements for a SATE program should be tailored to the information security risks identified within the

organization, starting with the most important information security risks (i.e. highest risk factor). It is critical for a SATE program to thoroughly identify both the risks and those who may be responsible for mitigating them as both may differ between organizations. One should determine the information security risk to the organization, not merely threats and vulnerabilities as the likelihood of occurrence and the impact of the threat and vulnerability to an organization may differ. Specific SATE programs should be tailored to each user group and each user role that are responsible for mitigating the information security risk identified. The subject content and the level of detail should be dependent on the user groups and the user roles identified and the type of SATE program to be delivered.

Security awareness programs should focus on general information security concepts and mitigation strategies for the information security risks identified; deriving the subject content primarily from the primary and secondary domains of the ISO/IEC 27002 standard for mitigating the risk identified. The targeted audiences for a security awareness program are as follows: the *Management*, *Non-Technical* and *Information Owner* users groups.

In contrast, a security training program should promote specific user groups and user roles to be highly knowledgeable in specific areas of information security related to their user role. The subject content tends to be highly technical, deriving the content from the primary, secondary and tertiary domains of the ISO/IEC 27002 standard for the information security risks they are responsible for mitigating. The recommended targeted audiences include select user roles from the *Systems Developer* and *Technical Administrator* user groups. These user groups would benefit from formal training courses. An example of such courses for a Programmer user role within the *Systems Developer* user group may include secure coding practices or mitigating web based attacks. A System user role within the *Technical Administrator* may benefit from a course in securing a virtual infrastructure environment, enterprise backup strategies or system hardening.

Security education programs are intended to promote the understanding of information security theory and concepts. These technical and management programs are generally at the university or college degree level. The targeted audiences for such programs are the Information Security Officer and Information Security Manager. For organizations that have adopted the ISO/IEC 27002 standard, both user roles should have a thorough understanding of all the domains, from primary through to the tertiary level.

F. Findings Related to a Role and Risk Based Framework for Enterprise Information Security Awareness, Training and Education Requirements and ISO/IEC 27002 Compliance

This study combines information security risks identified by an organization with user groups and roles responsible for mitigating them to develop a framework for an enterprise SATE program for ISO/IEC 27002 compliance. This is consistent with the literature [11, 21, 26, 28, 29, 30 and 39]. Figure 1 proposes a comprehensive framework for a risk and role based enterprise SATE program for ISO/IEC 27002 compliance.

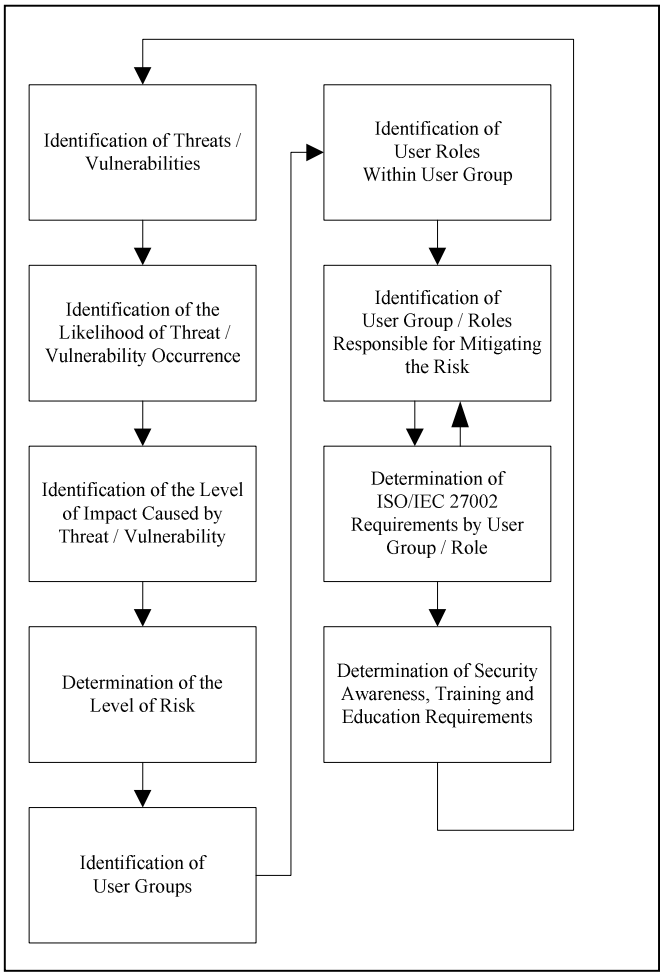

Figure 1. Framework for a Risk and Role Based Enterprise Security Awareness, Training and Education Program for ISO/IEC 27002 compliance.

The proposed framework consists of the following steps:

1) Identification of threats and vulnerabilities. This should be as comprehensive as possible to capture as complete a set where possible. They should be as specific as possible. Sources of potential threats and vulnerabilities that could be considered include threat risk assessments (i.e. security breaches, security event logs, and audit findings),

work experience, business areas, management, technical administrators, and global and national surveys,

2) Identification of the likelihood of threats and vulnerabilities occurring. Sources of information may include security breaches that have occurred as well as security event logs,
3) Identification of the level of impact caused by the threat and vulnerability,
4) Determination of the level of risk to the organization. Use steps 2 and 3 to calculate a risk factor (i.e. determine the level of risk). Once the risk factor is determined, rank the risk factor,
5) Identification of user groups within an organization,
6) Identification of user roles within a user group,
7) Identification of user groups and user roles responsible for mitigating the information risk. The importance of identifying as many user roles as possible is critical to ensure that all users and their particular role they play to mitigate the information security risks within the organization are identified,
8) Based on the user group and user roles responsible for mitigating the information security risk identified in step 7, determine the ISO/IEC 27002 domains required by user group and user roles. Note steps 7 and 8 may be an iterative process to refine which user group and user role are actually responsible for mitigating the information security risk and,
9) Based on the ISO/IEC 27002 domain requirements by user group and user roles in step 8 and the ranking of the risks (i.e. risk factor) identified in step 4, determine the SATE requirements for each user group and user role, starting with those with the highest risk factor. Should new threats and vulnerabilities be identified, proceed back to steps 1 through 8.

For organizations that have adopted the ISO/IEC 27002 standard as a best practice for information security, identifying the domains within the standard required to mitigate an identified risk answers the question why the user roles should either be aware, knowledgeable or understand the subject content delivered by a SATE program.

VII. CONCLUSION AND DISCUSSION

This research study expands on the existing literature on security awareness training, and education by NIST, SANS Institute and others by providing empirical data from a large public organization in Canada. The results can be considered representative of the large public organization in this study with that the vast majority of the departments and select agencies and boards participating in the survey questionnaire.

This study takes an enterprise approach in developing a risk and role based framework for an enterprise SATE program for ISO/IEC 27002 compliance. By identifying various different user groups and user roles from the various departments and select agencies and boards of a large public organization, this study is able to ensure a comprehensive coverage of the organization, vertically from executive to the general user, horizontally within a particular business function such as information technology and cross-functionally from different functional areas such as finance to legal.

User groups in this study are generally similar in description to those described in the literature. The labeling of the user groups in this study focuses more on function rather than the type of users within a user group thus appears to be more suited as a user group label. The most significant difference is the number of user roles identified within each user group, far outnumbering those reported in the literature. A significant number of new user roles are identified, providing a broader coverage of the enterprise vertically, horizontally and cross-functionally.

Information security breaches found in this study are similar yet different to other recent global and national surveys. Malware infection is the top information security breach in this study as well as many of the global and national surveys. For other security breaches, the rankings differed. The differences may be attributed to the large number of risks identified in this study as compared to other studies, making comparison of results difficult. In one national study, some security issues such as use of wireless networks and storing data in the cloud are not applicable as they are virtually non-existent in this study.

The current literature supports using a role or risk based approach in developing an enterprise information SATE program. This study combines both approaches to provide a more holistic view for developing a risk and role based framework for an enterprise SATE program for ISO/IEC compliance. By linking the information security risk identified within an organization to the user role(s) that are responsible for mitigating it, an organization can better tailor its enterprise SATE program to be risk and user role specific. By identifying the ISO/IEC 27002 domains required for compliance to mitigate the information security risk identified provides the justification for a particular subject content that should be included in an enterprise SATE program. This, in turn, reinforces compliance with the ISO/IEC 27002 standard to mitigate the risk identified.

With this study's large public organization adopting the ISO/IEC 27002 standard as its best practices for information security, it provides an opportunity to refine its current information security awareness program and develop new education and training programs. In addition, by adopting a

particular SATE approach in one organization, it provides an opportunity to share the results with other public organizations across Canada and elsewhere.

VIII. LIMITATIONS AND FUTURE RESEARCH WORK

This research study is solely based on one large public organization in Canada. Further empirical evidence from other large public organizations in Canada and elsewhere as well as private enterprise organizations would help confirm the proposed framework.

Interviews conducted in this study are limited to EISF members. Given the role of EISF members play in their organization, the assumption is that they are the most knowledgeable people in the field of information security for their department or select agency or board. Surveying other senior personnel such as the Chief Information Officer and other C-level people within an organization for their views on the state of information security would provide a different perspective.

The identification of ISO/IEC 27002 domains that should be implemented is solely the view of the author. A peer review of these would help confirm the results. Further identification of tertiary domain requirements by user roles would provide additional subject content for specific training courses.

ACKNOWLEDGMENT

I would like to express my appreciation to the Graduate Advisory Committee: Dr. Pavol Zavarsky, Ron Ruhl and Dr. Dale Lindskog for their support and guidance throughout this research. I would also like to express my sincere thanks to the senior management of the Corporate Information Security Office, all EISF participants and author's work place for the support of this project. Without this support, this research would have not been possible. Finally, special thanks to my family, classmates and friends for their encouragement, support and advice.

REFERENCES

[1] Guyot, L. (2003). Essential Information Security for Corporate Employees. SANS Institute Infosec Reading Room. 21 pp.

[2] Beishon, M. (ed.) (2005). A Director's Guide: Information Security: Best Practice Measures for Protecting your Business. Department of Trade and Industry, Government of United Kingdom. 82 pp.

[3] Johnson, E.C. (2006). Security Awareness: Switch to a better program. Network Security. February 2006. pp. 15-18.

[4] Ali Pabrai, U.O. (2005). Security Awareness Training: Strengthen Your Weakest Link. Certificate Magazine. August pp. 28-29.

[5] Ernst & Young (2006). 2006 Global Information Security Survey: Achieving Success in a Globalized World: Is Your Way Secure? 37 pp.

[6] Ernst & Young (2008) Moving beyond Compliance: Ernst & Young 2008 Global Information Security Survey. 33 pp.

[7] Deloitte Touche Tohmatsu (2007). 2007 Global Security Survey: The Shifting Security Paradigm. Deloitte Touche Tohmatsu. 44 pp.

[8] R. Richardson (2008). 2008 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. 30 pp.

[9] CompTIA Research (2007). Summary of "Information Security: A CompTIA Analysis of IT Security and the Workforce". Computing Technology Industry Association (CompTIA). http://www.comptia.org/sections/research/reports/200704-ITSecurity.aspx

[10] CSI (2009). 14th Annual CSI Computer Crime and Security Survey Executive Summary. 17 pp.

[11] Hansche, S. (2001). Information System Security Training: Making it Happen, Part 2. Security Management Practices. Information Systems Security. Vol. 10, No. 3. pp. 51-70.

[12] ISO/IEC 27002. (2005). Information technology — Security techniques — Code of practice for information security management. First Edition 2005-6-15. ISO/IEC. 136 pp.

[13] COBIT 4.1 (2007). IT Governance Institute. 195 pp.

[14] Information Security Forum (2007**).** The Standard of Good Practice for Information Security. 372 pp.

[15] Brown, P., J. Hash and M. Wilson. (2006). Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology (NIST) Special Publication 800-100. 137 pp.

[16] Ross, R. S. Katzke, A. Johnson, M. Swanson, G. Stoneburner and G. Rogers (2007). Recommended Security Controls for Federal Information Systems. National Institute of Standards and Technology, NIST Special Publications 800-53 Revision 2. December 2007. 188 pp.

[17] Valentine, J.A. (2006). Enhancing the Employee Awareness Model. Computer Fraud & Security. June 2006. pp. 17-19.

[18] Deloitte Touche Tohmatsu (2009). Protecting What Matters: The 6th Annual Global Security Survey. Deloitte Touche Tohmatsu. 56 pp.

[19] Westby, J.R and J.H. Allen (2007). Governing for Enterprise Security (GES) Implementation Guide. TECHNICAL NOTE

#CMU/SEI-2007-TN-020. Software Engineering Institute, Carnegie Mellon University. 116 pp.

[20] Rotvold, G. (2008). How to Create a Security Culture in Your Organization. The Information Management Journal. September/October 2008. Association of Records Managers & Administrators (AMRA) International. pp. 33-38.

[21] Gilbert, C. (2003). Developing an Integrated Security Training, Awareness and Education Program: The Most Essential Best Practices". SANS Institute Infosec Reading Room. 12 pp.

[22] Wilson, M. (ed.), D.E. de Zafra, S.I. Pitcher, J.D. Tressler and J.B. Ippolito. (1998). Information Technology Security Training Requirements: A Role and Performance-based Model. National Institute of Standards and Technology (NIST) Special Publication 800-16. 188 pp.

[23] European Network and Information Security Agency (ENISA) (2008). Information Security Awareness in Financial Organizations. November 2008. 48 pp.

[24] Nellis, R. (2003). Creating an IT Security Awareness Program for Senior Management. SANS Institute. Version 1.4b, March 24, 2003 15 pp.

[25] United States Department of Homeland Security, Office of Cybersecurity and Communications, National Cyber Security Division. (2008). Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. September 2008. 48 pp.

[26] Wilson, M. and J. Hash (2003). Building an Information Technology Awareness and Training Program. National Institute of Standards and Technology (NIST) Special Publications 800-50. 70 pp.

[27] Kritzinger, E. and E. Smith (2008). Information Security Management: An Information Security Retrieval and Awareness Model for Industry. Computers & Security 27 (2008). pp. 224-231.

[28] Kark, K. (2005). Five Steps to Effective Security Awareness. Forrester Research. December 23, 2005. 9 pp.

[29] Iqbal, S. and U. Tahir (2008). The Security of the Organizational Knowledge: The Organizational Perspective. Masters dissertation, Computer and Systems Sciences, Lulea University of Technology. ISSN 1402-1552. 52 pp.

[30] von Solms, B. and R. von Solms (2004). The 10 deadly sins of information security management. Computers & Security (2005) 23. pp. 371-376.

[31] Committee on National Security Systems (2004). National Information Assurance Training Standard for Senior Systems Managers. CNSS Instruction 4012. June 2004

[32] Committee on National Security Systems (2004). National Information Assurance Training Standard for System Administrators (SA). CNSS Instruction 4013. April 2004

[33] National Security Telecommunications and Information Systems Security (NSTISS) (2000). National Training Standards for Systems Certifiers. NSTISSI 4015. December 2000.

[34] McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley Software Security Series by Cigital. PowerPoint Presentation - 59 slides.

[35] Heffner, R. (2007). SOA Competency Planning and Educational Resources. Forrester June 26, 2007 17 pp.

[36] National Security Telecommunications and Information Systems Security (NSTISS) (1994). National Training Standards for Information Systems Security (INFOSEC) Professionals. NSTISSI 4011. June 20, 1994

[37] Committee on National Security Systems (2004). National Information Assurance Training Standard for Information Systems Security Officers. CNSS Instruction 4014. April 2004

[38] Hejazi, W. and A. Lefort (2008). 2008 Rotman-TELUS Joint Study on Canadian IT Security Practices. 65 pp.

[39] Hejazi, W. and A. Lefort (2009). 2008 Rotman-TELUS Joint Study on Canadian IT Security Practices. 79 pp.

[40] Hejazi, W. and A. Lefort (2010). 2010 Executive Briefing: Rotman-TELUS Joint Study on Canadian IT Security Practices. 34 pp.