Journal of Theoretical and Applied Information Technology
31st August 2016. Vol.90. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REDUCING SECURITY INCIDENTS IN A CANADIAN PHIPA REGULATED ENVIRONMENT WITH AN EMPLOYEE-BASED RISK MANAGEMENT STRATEGY

[1]EDUARDO DESOUZA, [2]RAUL VALVERDE
[1] Community Care Access Centre, Toronto, Canada
[2]Department of Supply Chain and Business Technology Management,
Concordia University, Montreal, Canada
[2]CONAIC AC, Mexico City, Mexico
E-mail: manneiro@hotmail.com, rvalverde@jmsb.concordia.ca

ABSTRACT

The paper uses a case study research approach in defining how an employee based risk management strategy such as employee information security training, employee motivation, and quality assurance can be used to reduce security incidents in a Canadian PHIPA regulated environment. During the research, information security professionals and employees were asked direct questions aimed at understanding the reasons why internal data breaches are recurrent, and what are users' perception and understanding of existing security policies, processes, and their role in protecting information in their work environment. By using a qualitative case study research design method, data was collect from a small but targeted group of information security professionals and employees within healthcare organization in Ontario. The gathered data was analyzed to identify what are the main causes of security incidents, and what organizations, in the healthcare field can do to better involve their employees for the reduction of breaches and incidents. The recommendations made by this research paper have the potential of influencing an organization's organizational culture and employee behavior. The main goal of this paper was to develop an employee based risk management strategy for enterprise level risk management focused on positively influencing employee behaviour.

Keywords: *Risk Management, Incident Management, Risk Reduction, PHIPA, Training Programs, Health Care Information Security.*

1. INTRODUCTION

It is continuously emphasized in the information security landscape that most information security incidents are committed by insiders, either by malicious or disgruntled employees, pointing out that employees are the weakest link in most information security programs. Information security professionals and information security vendors, such as Information Security Networks, do believe that "An organization's first line of defense for strengthening security is its users" [1]. Our very first line of defense, our employees, is also the weakest point in information security. Employee training is a necessity for an information systems to operate smoothly as employees clearly see this activity as a long-term investment, which will ultimately benefit both the firm and its employees [2]. Lack of training also increases the risk of system implementation failure [3].

Security awareness focuses in changing behavior and provides users with enough information so that they can recognize security concerns and act upon it as instructed [4]. A security awareness program targets a broader audience with broader topics such as password management, spam, social engineering, and others. A security training program targets a specific group of users and aims at teaching skill sets and developing competencies. Education aims at forming a body of knowledge and further study concepts and principals [4]. The majority of security incidents are caused by trusted employees within the organization, and in most instances, these incidents are a result of human error [5], this justifies the need to put emphasis in training to reduce security incidents.

This research paper used a case study research approach in defining how employee information security awareness and training, and employee motivation can be used to reduce security incidents in their work environment. This paper is intended to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

generate recommendations grounded in the data collected and analyzed during the research period.

2. PROBLEM DEFINITION AND SCOPE

Electronic Health Recording systems and patient assessment tools, hosting and making use of Personal Health Information, have become a major government point of focus in the last decades, as an example, the province of Ontario has recently allocated $72 million for an electronic health recording system that will be completed by 2015 which will involve 43 Toronto-area hospitals and 201 long-term care facilities [6]. In Ontario, Personal Health Information (PHI) refers to the collected identifiable information about an individual [7]. As individuals, our Personal Health Information is of great importance and sensitivity, hence why health care providers and healthcare institutions must abide to statutes that govern the collection, use, and disclosure of such information. Organizations spend large sums of money on state-of-the-art safeguard technologies (devices and software) in order to protect this Hosting Personal Health Information from internal and external threats. The costs involved in achieving compliance and securing data is high, but what can healthcare organizations do to influence employee behavior in order to reduce information security incidents? Answering this question will be the main focus of this research paper. Information security relies on the interaction of people and technology.

The reality is that the consequences of information security breaches to an organization can be catastrophic, and organization users are a major contributing factor: Examples of potential losses include:

- Financial loss: Large organizations, public or not, will pay a high price in dealing with data security problems. It has been estimated that large organizations, in the UK for example, will most likely spend from £280,000 to £690,000 in dealing with data security problems alone [8].
- Company image and reputation degradation: in Ontario, organizations hosting PHI are required to promptly notify individuals if the security of their information has been breached. By word of mouth, or by the media, data breach news can quickly spread and negatively impact an organization's image, suggesting it to be a bad business partner[7].
- Client dissatisfaction: Organizations that experience data breach may also receive legal actions pressed by affected individuals.
- Business disruptions: Lack of training can lead to business disruptions in the supply chain that can cause losses [2].
- Other risks: Once the Personal Health Information of an individual or individuals is breached, the disclosed information can be used by others for malicious purposes, such as blackmailing and impersonation. Other family members may also be at risk since an individual's PHI may reference health history information of other family members.

The main goal of this research is to produce an employee based risk management strategy that will touch every department within the organization. The data collected and analyzed from participating information security professionals and users was the foundation to build and shape this study's deliverable.

3. LITERATURE REVIEW

Organizations can use awareness and training programs as vital vehicles for disseminating information that employees, at all levels, need to know in order to effectively do their jobs [9].

In their paper, entitled "The insider threat to information systems and the effectiveness of ISO17799", Theoharidou et. al. [10] mention that information system security was perceived, in the past, as a technical issue, but in recent years information system security has become a people issue, regardless of computer technology advancements today.

With the rapid development and innovations of technology, it is imperative to employees and organizations to have the ability to learn and continue to learn at a fast pace. This brings us to the interaction between users and technology. The majority of security incidents are caused by trusted employees within the organization, and in most instances, these incidents are a result of human error. Burke and Christiansen [11] pointed out that the 56%, of the 400 participating organizations, classified their internal security incidents as human error (accidental). Employees have become one of the most serious threats to their organizations with contractors and temporary employees being the greatest security risk.

The risk increases exponentially for organizations that do not have a mature and efficient information security program implemented. Risk management and compliance are a good start but with so many evolving threats, organizational changes, and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

computer technology advancements, there is no single solution to mitigate them all [12][13][14].

Information Technology has evolved exponentially, but there is very little focus of the IT industry in informing users of new vulnerabilities and threats associated with emerging technology [15].
Employees are the most important factor in ensuring the security of the IT systems they interact with, and the security of the information that they process [15].
NSTISS (National Security Telecommunications and Information Systems Security) re-leased a paper in 1994, entitled "National Training and Standard for Information Systems Security (INFOSEC) Professionals", where NSTISS acknowledges that technology, poli-cies and staff members within organizations must rely heavily on information security training, and that upcoming professionals, in the IT field, must understand information security principals in order to consider the protection of information as one of the core requirements of systems design. NSTISS's training guide also mentions that awareness, training, and education must be the last layer, the foundation, in an information security program since this last layer must translate technology and policies to the proper audience [16].
People are the most important aspect of information security. Bogart [17] refers to the 90/10 rule in her presentation, entitled "Information Security Liaison: Awareness Training", where she explains that information security is only 10% technology, and 90% are people and processes.

Additionally, Schneier [18] also refers to technology as being a small portion of information security while people is the main point of focus. The biggest challenge is with the interaction of people and technology; many times resulting in good people doing bad things, in most cases unintentionally.

This paper recommends the use of both methods, behavior modification and socialization, in order to influence employee behavior, good behavior, as a supporting pillar of the proposed employee focused risk management strategy.

4. RESEARCH METHODOLOGY

This study used a case study research method, where data was collected from primary and secondary data sources. A case study "involves the investigation of a particular situation, problem, company or group of companies" [19]. Secondary data, or supporting data, was collected from related books, journals, on-line articles, vendors' websites, technology news websites, and Canadian government and regulatory websites. Canadian government and regulatory websites were a vital source of information in assessing provincial and federal regulations that provides guidance to healthcare organizations in securing and protecting Personal Health Information in Ontario.
The main source of data collection chosen for this study was primary data. Primary data may be gathered by means of observation, surveys, and experiments [20]. Primary data was collected in the following manner:

- Research approach: survey and observation
- Contact methods: personal (interview) and online (survey)
- Research instruments: formal discussion on challenges faced in protecting information in the healthcare industry and online questionnaire survey

Primary data was collected from a targeted group of professionals, and given its direct approach; it was believed that primary data would provide this study with accurate and high quality data. The online survey was answered by information security professionals from the following organizations: Ontario Associated of Community Care Access Centres, Cancer Care Ontario, Canadian Institute for Health Information (CIHI), Ontario TeleHealth Network (OTN), Sick Kid's, eHealth Ontario, Sunnybrook, North East Community Care Access Centre, and Champlain Community Care Access Centre. One-on-one interviews were performed with information security experts from Cancer Care Ontario (CCO), and Ontario Community Care Access Centres (OACCAC). One-on-one interviews were performed with the Business Technology Solutions (BTS) - User Training and Education professional from OACCAC [34] [35].
A total of six one-on-one interview sessions were conducted with information security processionals from OACCAC and CCO organizations. Session one was in the form of open discussion about the challenges faced by healthcare organizations in protecting and securing their information. Two one-on-one interview sessions were also conducted with BTS - User Training and Education professional at OACCAC. Session one was also in the form of open discussion on what trainers can do to assist employees with retaining information from awareness and training sessions. The online survey questions were created based on the knowledge

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

gained from the interview sessions (session one). An on-line survey, with 32 questions, was used to reach a broader group of information security professionals. Employees at all levels (IT Director, CIO, department managers, and other users) were observed during this study at OACCAC. During the observation period, attention was focused on how staff members at different levels dealt with and made decisions that affect the security of PHI in their work environment.

Research results were compared against credited awareness and training guidelines, credited awareness and training approaches and methodologies from the National Training Standard for Information Systems Security (INFOSEC) Professionals in order to identify awareness and training program gaps and to recommend improvements. Guidelines and recommendations from the Federal Information Security Management Act of 2002 (FISMA) were also studied during this research.

The interviews were one-on-one sessions, 60 minutes in length each session.

- Interviewee 1: Manager of the Enterprise Information Security Office at Cancer Care Ontario.
- Interviewee 2: Information Security Architect at the Ontario Association of Community Care Access Centres.
- Interviewee 3: Business Technology Solutions (BTS) - User Training and Education professional at the Ontario Association of Community

Candidates were selected based on their skill set and knowledge level on information security and privacy, and their knowledge on employee training and skill set development. Participates spent 15 to 20 minutes to complete the online survey. The intension of the online survey was to gather primary data and quality data on some of the challenges currently faced by healthcare organizations in securing and protecting Personal Health Information. One of the important aspects of online survey is its flexibility, which helped to alleviate the geographical distance issue and the busy schedule of the participants. The participants of the study were selected via convenience sampling. This sampling technique refers to obtaining sample units or people who are available. This method is justified since the participation in the study was voluntary and it is difficult to anticipate the number of participants in the sample. Out of nine organizations invited to participate in the on-line survey, seven of them completed the online survey. The survey was distributed to participating organizations via the web-based survey services provided by Survey Monkey as recommended in [20].

5. DATA ANALYSIS

Data collected from the online survey will be interpreted through data analysis and changed into information. This study will interpret the findings, draw conclusions and report them in this section. The data analysis technique adopted by this study is statistical analysis, which is an analytical tool provided by the online survey website utilized by this research (Monkey Survey).

The analysis phase of the paper focused in further studying the following research topics (qualitative risk analyzes scenarios):

- What can organizations do to involve employees for the reduction of security incidents for their work environment in a regulated PHIPA environment?
- Identification of organization's information security program maturity
- Understand the baseline characteristics of information security and privacy training programs in Ontario's health care sector
- Understand what technologies are currently covered by the organization's awareness programs
- Awareness and training program effectiveness - PHIPA compliance and organization level understanding
- Understand how employee focused organizations are in supporting its information security awareness and training program
- Understand overall security incidents and breaches' causes and processes handling at a high level

The data collected during this research indicates that in 83% of the participating organization, employees receive information security and information privacy material within the very same awareness and training session, which could result in a lack of clear distinction between security and privacy concepts. Six of the participating organizations were asked to identify the main causes of security incidents in their regulated environment. A Human error came up with the highest score of 83%, chosen by five of the six participating organizations. Malicious internal activity also scored high, four out the six

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

organization identified malicious internal activity as a threat. When questioned about the main cause of privacy breaches, all six organizations pointed out human error as also the main cause. Social engineering attacks and malicious internal activity also scored high.

Five of the participating organizations did have policies and procedures in place including privacy policies. Even though these organizations have defined policies and procedures in place, they lacked information security professionals to further develop and update their information security programs against new compliance requirements and new threats. Four of the seven participating organizations answered that they assume that all employees have the same information security knowledge level, prior to training them.

These organizations also rated the overall level of information security understanding of their organization as moderate, which could be misleading since their training material may not target to correct audience. Five out of the seven participating organizations admitted that their security training program does not identify employee information security knowledge gaps. The collected data indicates that employee feedback is not accounted in the information security training program lifecycle of these organizations.

All participating organizations make use of computer based training to deliver their information security training. When asked what could be the possible causes of employees failing to apply what was taught during their security training, 66% of the participating organization answered that information security is not a priority to their users. This was a surprising finding since these organizations deal with PHI (Personal Health Information), and therefore, information security must be one of their top priorities in order to comply with provincial and federal regulations. 83% of these organizations provide their users with a communication channel so that they can anonymously report security violations.

Since most of these users may not have been provided with a clear distinction between security and privacy by their organizations, it would be difficult for these users to be able to accurately and efficiently report security incidents. There is no regulatory body, standard, or guidelines that provide healthcare organizations with recommendations on how often they should train their employees in information security. Therefore, when asked how often these organizations provide security training to their employees, their answers showed a wide range of periods. One organization answered that training is provided to employees once a month, two other organizations answered once a year, two more answered twice a year. There were also two organizations that answered that training is provided after major business or organization changes. Proper use of email seems to be a big concern to organizations since email is a common medium of data leakage. There is the potential threat of users sending work related data to their personal email accounts which breaches company's policies. Internet security also scored high in the survey. Internet security is concerned with website content that users may be able to access such as phishing sites and sites with infected contents. Physical access concerned to the protection of organizations' physical assets that could host PHI or other confidential information.

The majority of the participating organizations omitted database security, Web 2.0 technology, removable media and mobile device technologies as being part of their security awareness and training material. This is an indication that these organization's security awareness and training content may not be up-to-date with the current technologies being used in their environment.

PHIPA provides basic guidelines for protecting personal health information (privacy) in Ontario, and it is not primarily concerned with data security as an element of privacy. Some privacy elements rely on security mechanism. Information security awareness and training falls under security controls, and as a result, there is no standard, or regulation, in Ontario that directs organizations in the healthcare industry to implement effective information security awareness training programs, this makes hard for information security professionals to identify information security awareness and training deficiencies and gaps. The Federal Information Security Management Act of 2002 (FISMA), demands federal agencies in the USA to implement defined security controls. FISMA's categorizes awareness and training as operational and under security controls. FISMA further provides guidelines on how federal agencies can define, develop, deploy, and maintain their security awareness and training policy and procedures [21].

Even though all participant organizations acknowledged having an understanding of PHIPA standards, their security incident numbers from 2011 show only a slight improvement compared to 2010. This could be an indication that their existing security awareness and training programs

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

may not be contributing to employee information security awareness development and skill set learning. PHIPA compliance does not have a direct affect in security controls since it does not rule the way information security is conducted.

Only one of the six participating organizations has a system in place that tracks who has read company policies. In order to ensure that policies have been fully read and understood by employees, organizations could make use of frequent internal surveys and questionnaires to develop a sense of how well employees understand existing and new polices. Employees may not support policies that they do not understand, or are not aware of. 50% of the participating organizations do not request employee feedback on their security measures; they only do so after major business changes. This gap in communication, between information security professionals and employees, could lead to user resistance in using new security measures and supporting technology.

All participants agreed that organizations would learn from each other's' mistakes and challenges by sharing incident occurrence information, but 50% of the organizations confirmed that their reluctance in sharing PHI incident information is due to protecting company image. The seven participating organizations were inquired if they monitor and analyze employee behavior in order to identify unexpected patterns, and five out of the seven organizations answered that they do monitor and analyze employee behavior. When asked about what employee motivation approach they use, only 50% of the organizations motivate their employees to follow company policies and processes. Without incentive from organizations, employees may not have a consistent behavior in putting these policies and processes into practice. This misalignment, high expectation without incentive, could be one of the root causes of most insider security incidents..

Table 1 Summarizes The Research Findings

Research Question	Findings
Overall maturity rating of organization's information security programs	71% answered that they have "defined policies, procedures, and dedicated security resources"
Dedicated security personnel	There was no consistency in the answers provided by the participating organizations
Does your training program assume that all users have the same knowledge level, prior to training them?	57% of the participating organizations answered "Yes"
How would you rate the overall level of information security understanding of your organization?	57% of the participating organizations acknowledged that they have moderate understanding of information security
Does your security training program identify knowledge gaps?	71% of the participants answered "No", that they are not concerned with identifying users' knowledge gaps
What training delivery methods does your training program make use of?	All participants (100%) make use of computer based training
What security or privacy program elements does your training cover?	All organizations (100%) cover "Acceptable use". "Social Engineering" came up with the lowest score
The reason why employees fail to apply what was taught during their security training could be attributed to:	"Information security is not a priority to our users" came up with the highest score of 66%
What tools does your security program provide your users with in order to report security violations?	83% answered that "Users are provided with a communication channel so that they can anonymously report such violations"
How often does your organization offer security training to its employees?	There was no consistency in the answers provided by the participating organizations
What technologies are covered by your security training program?	eMail (data leakage) with 100.0%, Internet security and proper use with 83%, and Operating system security with 33%
What is the level of understanding on PHIPA standards in the organization as a whole?	Overall, there was no consistency in the answers provided by the participating organizations
How does your organization security training program cover Information Security and Information Privacy training	83% of the participants acknowledged that "Information Security and Information Privacy training are bundled into the same training session to make better use of allocated employee's time"
How does compliance affect employees' behavior?	Out of 6 participants, 4 acknowledged "Reduced occurrences of incidents and breaches" as a result of compliance
Does your organization monitor employee behavior to detect incidents?	83% of the participants answered "Yes"
Which employee motivation rewarding approach does your organization make use of to motivate employees to follow policies and processes	Overall, there was no consistency in the answers provided by the participating organizations
How does your organization introduce new security policies	5 out of the 6 participants acknowledged that they make

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to your employees?	use of "Company Portal"
How does your organization make its employees more acceptable of technology changes?	"Through training (classroom or virtual classroom)" had the highest score, 83%
How often does your organization request employee feedback on the security measures it has in place?	There was no consistency in the answers provided by the participating organizations
Users are most compliant when they perceive communicated risks as high. How does your organization sustain an appropriate level of risk perception?	There was no consistency in the answers provided by the participating organizations
What is your current level of security incidents related to PHI data, compared to the previous year?	83% of the participants answered 1 to 5 incidents
Why would organizations be reluctant to share PHI incident information?	There was no consistency in the answers provided by the participating organizations, but 50% of the participants selected "Damage company image"
What would be the benefit in sharing incident occurrence information with partners and other organizations in the same industry?	All participants answered "Great benefit since organizations would learn from each other's' mistakes"
Does your organization keep track, or logs, of incidents and human errors?	All participants answered "Yes" to this question
In general, what were the main causes of security incidents and privacy breaches? Please enumerate (1 being the main cause). Security Incidents	"Human error" had the highest score, 83%
In general, what were the main causes of security incidents and privacy breaches? Please enumerate (1 being the main cause). Privacy breaches	"Human error" had the highest score, 100%

6. PROPOSED EMPLOYEE FOCUSED RISK MANAGEMENT STRATEGY

Based on the information gathered and analyzed by this research, this paper has identified shortcomings in the existing management of human-factor risks by the participating healthcare organizations:

- There is a risk of security awareness and security training materials being delivered to the wrong audiences within the participating organizations.
- There may be a lack of clear understanding of information security and information privacy concepts within these organizations, which could result in poor reporting of privacy breaches and security incidents.
- Security policies, procedures, and security awareness and training material may not be up-to-date with current technologies being used within the participating organizations, which could result in employees' lack of security awareness and knowledge on currently used technologies.
- Likelihood of communication gap between information security professionals and employees possibly leading to user resistance in using and complying with new security measures and supporting technology.

The proposal being presented makes recommendations to modifying existing assessment approaches in order to create a systematic approach to identify, assess, and mitigate risks related to people and processes. Threat and Risk Assessment (TRA) and Privacy Impact Assessment (PIA) are current tools in the enterprise for identifying security and privacy risks. However, PIA's tend to be legally (compliance) focused (e.g. authority to use information) and TRA's tend to be focused on the technical aspect (technology) of security controls, thus, both of these assessment tools can gloss over, or not accurately, capture the associated human-factor risks. Since employees are the weakest link in the information security chain, TRA and PIA could be assessing the wrong risks in healthcare organizations [22].

TRA and PIA assessments use distinct methodologies to assess risks associated with existing, or emerging, technologies and information systems in an organization:

- A TRA assesses risks to an organization's information technology assets
- A PIA assesses risks to the privacy of information (an individual's privacy)

The safeguards (mitigation) recommended by both TRA and PIA assessments are usually technical safeguards for technology risks [23]. This research recommends these mitigations to also consider risks related to people and processes. Employees are the weakest link in the information security chain [22], and 48.8% of all malware attacks rely on user interaction [24].

People need to be influenced to effectively follow and commit to organization's policies, processes, rules, and standards. This paper has generated information that leads to believe that employee misbehavior to be a vital cause of the majority of internal security incidents and privacy breaches. TRA and PIA assessments would avoid repetition and silos during their respective assessment process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

if both tools used a common repository for identified threats and risks information.

A well-established information security culture within the organization where employees see themselves as group members with a sense of collective effort (behavior) in protecting organization assets and private information is essential. Possible employee mitigation methods (behavior change):

- Stimulate employees' inner responsibility (commitment). Inner responsibility is automatically exercised by people as long as they are provided with the reasoning behind a request or requirement [25].
- Behavior trigger. Instructive information is made clear, short, and most importantly suggestive to motivate users to comply with requests and requirements [25].
- Use of consistency and established patterns. The tendency of groups is to stick to established patterns even as new needs arise. Once a practice has become established, it is likely to be perpetuated" [26].
- Social Proof. Development of an organization security conscious by clearly communicating the impact of compliance and non-compliance of rules, policies, and procedures.
  - User empowerment through user knowledge development by providing users with clear, well communicated, engaging, enforceable, and up to date security policies and procedures [27].
  - Organizational culture focused on information security. Organizational culture must rely on senior management governance to serve as role model for employees to observe, learn, and practice information security policies, rules, and procedures [15].
- Positive reinforcement. "Encourage desired behavior by introducing positive consequences when the desired behavior occurs" [28].
- Employee participation and feedback. People are more inclined to accepting changes if they have a participative role in the decision making process [28].
- Security and privacy integration into organization cultural changes, where security and privacy are transparent (integrated) into everyone's job and responsibility. Compliance by default
- The use of Emotional Intelligence. Organization and employee relationship development and strengthening. Emotional Intelligence "describes an ability, capacity, or skill to perceive, assess, and manage the emotions of one's self, of others, and of groups" [29].

The implementation method of the recommended risk management strategy is to use existing risk assessment tools, such as TRA and PIA, since they are well accepted and extensively used in the healthcare industry. TRA and PIA assessment tools can be adapted with the right inputs to better reflect human factors by expanding the Administrative Control sections of the TRA. A TRA Administrative Controls has the potential of influencing employee behavior and experience (human factors), since they are actual people controls such as security policies, administrative directives, organizational structures, responsibilities definition, and procedural safeguards. Also, the data collection phase of a TRA involves collecting all policies and procedure currently in place, identifying gaps and undocumented policies and procedures. The threat analysis phase of the TRA looks at every threat (element of risk), human and non-human, which could impact (tamper, destruct, interrupt) an organization asset [21].

The data collection and threat analysis phases of the TRA must be expanded to better focus on user feedback in regards to their current level of understanding and commitment to security policies, rules, and procedures. A risk management process encompasses both TRA and PIA assessment tools and can be implemented at any levels within the organization (enterprise level), tactical or operational levels. The results of this research paper leads to believe that the participating healthcare organizations do not make a clear distinction of awareness, training, and education programs and use these terms interchangeably.

TRA and PIA assessments could be modified to properly identify differences amongst awareness, training, and education program requirements and to also define their objects and audiences.

The proposed employee based systems approach risk management is included in Fig. 1 and detailed as follows:

Information security risk management system interacts with the organizational culture and with all departments within the organization. The red arrows indicate the inputs in the form of active support and governance of Senior Executives and Board of Directors throughout all phases of the risk management approach.

1. Senior Executives and Board of Directors: Senior Executive and Board of Directors are ultimately responsible for the governance and success of the risk management and provide input to the risk management approach.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. Employee Based Risk Management Strategy: This layer ensures that the risk management approach focuses on employee behavior and their relationship with corporate assets and processes
3. Human Factor: Threat & Risk Register (logging & tracking): This is the risk assessment layer, and it uses both TRA and PIA to assess the impact of employee behavior to the security of information within the organization. Threats and risks, related to employee behavior, are identified and logged as outputs of this layer (repository).
4. TRA Administrative Controls / Risk Mitigation: Employee risk factors identified in the previous layer is passed onto the TRA Administrative Control layer as inputs, the output of this layer is the proper risk mitigation controls.
5. Awareness and Training Programs / Clear Distinction and Objectives: The input is the risk mitigation controls that are integrated into awareness and training programs (output). Awareness and training programs' audience and objectives are defined. The ultimate goal of the awareness and training programs is to influence employee behavior (motivate acceptable behavior)
6. Employee Behavior and Employee Feedback: Due to the dynamic nature of the systems approach to risk management, employee information security awareness and knowledge are constantly updated. Expected behavior observed (compliance with company's policies and guidelines). Employees become resilient to common threats (social engineering, web phishing, data leakage …). Employee feedback is collected and supplied to the Employee Based Risk Management Strategy layer for periodic updates, further development and improvement of the risk management approach.
7. Proper Information Handling / Improved Information Security: The ultimate goal of the risk management approach is the reduction of internal security incidents and privacy breaches.

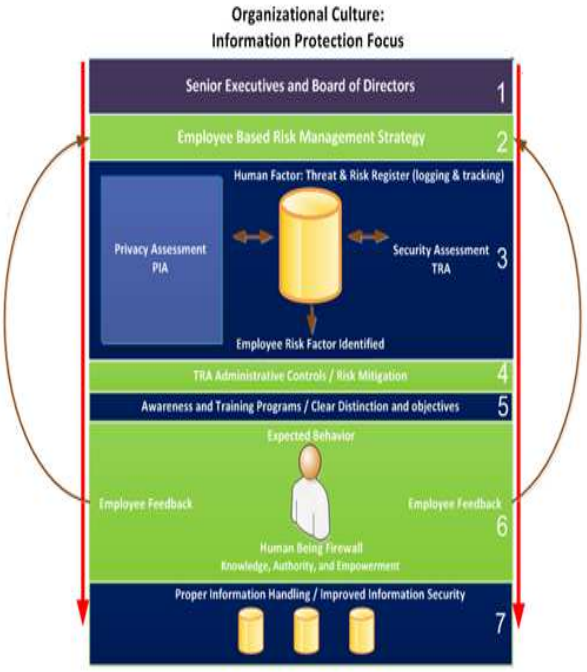

Figure 1 Proposed Employee Focused Risk Management Strategy

7. CONCLUSIONS

The employee based risk management strategy developed by this study highlights that TRA and PIA assessment tools, currently used by healthcare organizations, could be successfully modified to assess risks associated with people and processes in any type of organizations. As a result of the modified TRA and PIA assessment tools, effective mitigation methods that influence employee behavior may be successfully identified and integrated into the organization's awareness and training programs.

This research generated the following findings, which if addressed appropriately, may contribute to the overall improvement of the information security programs of the participating organizations:

- Unclear distinction between information security and information privacy by the participating organizations, which could lead to the inaccurate reporting of incidents and breaches by employees.
- Employees are pointed out as the main cause of both security incidents and privacy breaches.
- Policies, procedures, and guidelines are only useful if they are kept current..
- The knowledge level of information security and information privacy of staff members must be

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

identified and training material must be developed to targeted audiences.

- The responses provided by the participating organization indicated that their policies and procedures are not kept current with the technologies used by their employees in the workplace.
- PHIPA is concerned with data privacy. ISO standards, COBIT, Sarbanes-Oxley Act are some of the international information security standards that could be used by healthcare organizations to further improve their information security programs
- The participating healthcare organizations acknowledged that sharing security incidents and privacy breach information would be beneficial since they could learn from each other mistakes, but are highly concerned on how this information would affect their organizations' image and reputation.

The key deliverable of this research paper was to provide recommendations on how internal security incidents and privacy breaches can be mitigated through changes in employee behavior through awareness (development of basic information security knowledge) and training (development of information security skill set) programs.

This research proposed an employee based risk management strategy that mitigates internal incidents, based on employee involvement. Organizations in the private and public sectors could benefit from the proposed strategy since the proposed strategy provides recommendations in enhancing organizations' security awareness and training programs, and as a result, organizations may benefit from the proposed solution in the following aspects:

- Minimize financial impact and business disruptions related to data breach
- Improve company image and reputation by being a data security oriented organization
- Improve client dissatisfaction and confidence by taking a companywide approach in data security.

One limitation of this study is its lack of generalizability since it involved only one case study[32], however, there is evidence of good results for information systems research with a single study as indicate by [30] [31]. [33] insists that "the reliability of a case study is more important than its generalizability" since it presented an evidence and the findings can be very useful in mitigating internal incidents, based on employee involvement. Another limitation of this case study includes the sample size since we are using convenience sampling and this can compromise the accuracy of the results. This research also opened the doors for future research investigation on why organizations perceive technology as the most important element of information security, while employees and processes are perceived as secondary elements.

The provincial government of Ontario regulates the collection, use, and distribution of private information; it could also regulate the security aspect of private information. Healthcare organizations are in need of common guidelines (standard) for information security.

Information security training must follow the same training methods that other training subjects follow, with qualified training professionals.

Although not covered by this research, the creation of a healthcare security incident portal for the healthcare community in Ontario could also be further studied and considered. Information security professionals could comment and exchange information on security incidents and effective mitigation methods. Such tool could allow for information security professions to identify incidents and mitigation strategies that are common to their region and industry. Emotional Intelligence has been briefly mentioned on this paper but was not covered in this research due to lack of time and resources.

REFERENCES:

[1] Infosec (2011) Proactive controls to mitigate IT security risk (Online), http://www.infosec.co.uk/ExhibitorLibrary/992/CZ_Corporate_Brochure_A4_Web_23.pdf (Accessed on: 10 July, 2011).

[2] Valverde, Raul, Saadé, Raafat G (2015) The Effect of E-Supply Chain Management Systems in the North American Electronic Manufacturing Services Industry. Journal of Theoretical and Applied Electronic Commerce Research, 10 (1). pp. 79-98.

[3] Hubbard Derek and Valverde Raul (2014), Reducing Systems Implementation Failure: A conceptual Framework for the Improvement of Financial Systems Implementations within the Financial Services Industries: In: Silhavy, R., Senkerik, R., Oplatkova, Z.K., Silhavy, P., Prokopova, Z. (eds) Modern Trends and Techniques in Computer Science, Advances in Intelligent Systems and Computing, vol 285, Springer.

[4] Wilson, M., & Hash, J. (2003). Building an information technology security awareness and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

training program. *NIST Special publication*, *800*, 50.

[5] Stephens, Juliette and Valverde, Raul (2013) Security of E-Procurement Transactions in Supply Chain Reengineering. Computer and Information Science, 6 (3). pp 1 to 20

[6] CTV (2011) Toronto Electronic health records a step closer for all in Ontario (Online), Available from: http://toronto.ctv.ca/servlet/an/local/CTVNews/20110511/ehealth-records-electronic-ontario-health-110511/20110511?hub=TorontoNewHome (Accessed on: 24 May, 2011)

[7] PHIPA (2004) Ontario's Personal Health Information Protection Act - PHIPA (Online) Available on-line: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm (accessed on: 17 October, 2011)

[8] Espiner, T. (2010) Businesses struggling with data breaches (Online), from: http://www.zdnet.co.uk/news/security-threats/2010/04/28/businesses-struggling-with-data-breaches-40088793/ (Accessed on: 11 June, 2011)

[9] Wilson, M., and Hash, J. (2003) Building an Information Technology Security Awareness and Training Program (Online), Available from: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (Accessed on: 10 November 2011)

[10] Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005) The insider threat to information systems and the effectiveness of ISO17799 (Online), Athens University of Economics and Business, Available from: ftp://163.25.117.117/gyliao/TODylan/The%20insider%20threat%20to%20information%20systems%20and%20the%20effectiveness%20of%20ISO17799.pdf(Accessed on 21 October, 2011)

[11] Burke, B. and Christiansen, C. (2009) WHITE PAPER - Insider Risk Management: A Framework Approach to Internal Security (Online), Sponsored by: RSA, The Security Division of EMC, Available from: http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf(Accessed on 21 October, 2011)

[12] Almadhoob, A., & Valverde, R. (2014). Cybercrime Prevention in The Kingdom of Bahrain via IT Security Audit Plans. Journal of Theoretical and Applied Information Technology, 65(1), 274-292.4

[13] Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System. IFAC-PapersOnLine, 48(3), 1846-1852.

[14] Stephens, J., & Valverde, R. (2013). Security of e-procurement transactions in supply chain reengineering. Computer and Information Science, 6(3), 1.

[15] Tipton, H. and Krause, M. (2004) 'Information Security Management Handbook. Fifth Edition'. CRC Press LLC, Florida. ISBN 0-8493-1997-8.

[16] NSTISS (1994) NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS (Online), Available from: http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf (Accessed on: 22 October, 2011)

[17] Bogart, K. (2003) Information Security Liaison: Awareness Training (Online), Available from: security.arizona.edu/files/ISL%20Awareness%20Training.ppt (Accessed on: 09 November, 2011)

[18] Schneier, B. (2000) 'Secrets and Lies: Digital Security in a Networked World'. John Wiley & Sons, Inc., New York. ISBN 0-471-25311-1

[19] Dawson, C. (2009) 'Project in Computing and Information Systems: A Student's Guide Second Edition'. Pierson Education Limited. Essex. ISBN 978-0-273-72131-4

[20] Kotler, P. and Armstrong, G. (2010) 'Principles of Marketing: see how good it is for you… Thirteenth Edition'. Pearson Prentice Hall. London. ISBN-13:978-0-13-607941-5

[21] Bayne, J. (2002) SANS Institute InfoSec Reading Room. An Overview of Threat and Risk Assessment (Online), Available from: http://www.sans.org/reading_room/whitepapers/auditing/overview-threat-risk-assessment_76 (Accessed on: 15 November, 2011)

[22] RCMP (2007) Royal Canadian Mounted Police: Technical Security Branch. Harmonized Threat and Risk Assessment (TRA) Methodology (Online), Available from: http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf (Accessed on: 16 November, 2011)

[23] Dubeau, L. (2008) 'A Plan for Privacy and Security Risk Management within Ontario's Community Care Access Centres'. M.Sc Information Security Degree dissertation, University of London, England. Available by

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

request to the author, lyndon.dubeau@gmail.com

[24] Microsoft (2011) An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in the first half of 2011 (Online), Available from: http://www.microsoft.com/security/sir/default.aspx (Accessed on 16 November, 2011)

[25] Cialdini, R. (2001) Influence: 'Science and Practice. Fourth Edition'. Allyn and Bacon, Massachusett. ISBN 0-321-01147-3

[26] Thaler, R. and Sunstein, C. (2008) 'Nudge: Improving Decisions About Health, Wealth, and Happiness'. Penguin Books Ltd. New York. ISBNS 987-0-300-12223-7

[27] Tanner, J. (2010) The Human Firewall (Online), Available from: http://www.issa.org/Library/Journals/2010/January/ Tanner-The%20Human%20Firewall.pdf (Accessed on: 16 November, 2011)

[28] Huczynski, A. and Buchanan, D. (2007) 'Organizational Behaviour. Sixth Edition'. Prentice Hall, Milan, Italy. ISBN 978-0-273-70835-3

[29] Orr, R. and Sherlock, J. (2006) Emotional Intelligence (EI): Implications for Information Technology (Online), Available from: www.ecu.edu/cause06/presentations/EI_EDUCAUSE_11.6.ppt (Accessed on: 18 November, 2011)

[30] Valverde, R. Toleman, Mark and Cater-Steel, A. (2011) A method for comparing traditional and component-based models in information systems re-engineering. Information Systems and e-Business Management, 9 (1). pp. 89-107.

[31] Valverde, R. (2008). The ontological evaluation of the requirements model when shifting from a traditional to a component-based paradigm in information systems re-engineering. DBA Thesis, Univ. of Southern Queensland.

[32] Bell, J. (1992). "Doing your research project", Milton Keynes: Open University Press.

[33] Bassey, M. (1981), "Pedagogic research: on the relative merits of search for generalization and study of single events", Oxford Review of Education, 71, 73-79.

[34] OACCAC (2007) Main Page (Online), Available from: http://www.ccac-ont.ca/Content.aspx?EnterpriseID=15&LanguageID=1&MenuID=68 (Accessed on 24 May, 2011)

[35] OACCAC (2008) Ontario Associated of Community Care Access Centres.OACCAC Mission and Vision (Online), Available from: http://www.ccac-ont.ca/Content.aspx?EnterpriseID=15&LanguageID=1&MenuID=1030 (Accessed on: 20 October, 2011)