International Journal of
Electronic Commerce Studies
Vol.1, No.1 , pp.37-50, 2010

A Laboratory Study Designed for Reducing the Gap between Information Security Knowledge and Implementation

Revital Elitzur
Loyola Marymount University, USA
Email: ysai@lmu.edu

Ying Sai
Loyola Marymount University, USA
Email: relitzur@lion.lmu.edu

ABSTRACT

Companies often have the knowledge on procedures to prevent or mitigate against information technology security risks. Yet these companies may not take adequate measures to implement these procedures, and instead, leave themselves vulnerable to security breaches. Potential reasons for this gap between information security knowledge and implementation are provided based on interviews with information technology managers at a global automobile sales and marketing company. Four mechanisms to reduce this gap are proposed, along with a new approach to conduct a laboratory experiment to evaluate the effectiveness of these mechanisms, applied independently and in combinations.

Keywords: Information Security, Business Enabler, Laboratory Experiment

1. INTRODUCTION

Over the past decade, the use of distributed, web-based information technology spread across all industries and types of business entities, from international multi-billion dollar revenue corporations, to small sole proprietorships. Advances in information technology have fueled business growth through real-time integration opportunities and increased customer reach.

As greater utilization of information technology has made distributed, web-based information systems more pervasive within business, so has the exploitation of security weaknesses in this technology. The impact of such a breach often includes both hard (measurable) and soft (not easily quantifiable) cost components, such as customer restitution costs and damage to brand image, respectively [1].

It is often cited that instead of proactively identifying vulnerabilities, enforcing security measures, and improving the information security standing for the company, management teams tend to view information security projects as pure cost rather than as a business enabler [2]. With multiple business projects and information technology

projects competing for limited budget, many information security projects with well-established technologies and procedures are not implemented until it is too late.

Companies have the knowledge, or the ability to gain the knowledge to carry out procedures to prevent or mitigate against information technology security risks [3]. Yet these companies may not take adequate measures to implement these procedures, and instead, leave themselves vulnerable to security breaches.

This exploratory paper evaluates why companies may not resolve known information technology security risks, and proposes mechanisms to reduce the gap between knowledge of information security mitigation procedures and implementation of these procedures. The paper then introduces the concept of utilizing a laboratory experiment to evaluate the effectiveness of these mechanisms.

2. BACKGROUND

In recent years, the landscape of information technology has changed. Business is becoming more global, as advances in internet technologies have enabled companies to cross international boundaries and extend beyond providing a web presence, generating new commerce, connectivity, and communication models. Likewise, business is becoming more real-time through advances in broadband and wireless technologies.

The change in the landscape of information technology has resulted in a transformation of information security, as technology breakthroughs have led to new security challenges. Examples include wireless network breaches, identity theft, the Enron scandal which contributed to the creation of the Sarbanes-Oxley Act of 2002, and the September 11, 2001 terrorist attacks which led to Congress enacting the Federal Information Security Management Act of 2002. Since January 2005, it is estimated that nearly 250 million records containing sensitive personal information have been compromised in security breaches occurring in the United States [4].

From a technical perspective, the impact of a security breach may be regarded to be the system and data recovery cost. For example, if an intruder destroyed databases stored on the server, the system engineers would need to reinstall the server and restore the databases from backup tapes. This, however, is an example of a comparatively minor impact of a security breach. Security breaches in which customer data or other sensitive information is stolen can be significantly more expensive to resolve. This is due to the downstream effect of utilizing stolen information to commit identity theft.

As an example, the information security breach discovered by TJX Companies in December 2006 is estimated to have compromised 94 million credit cards. This breach may cost upwards of $1 billion to resolve, based on estimates by Forrester Research that the average security breach can cost between $90 and $305 per compromised record [5]. This estimate includes hard costs to reissue credit cards and debit cards whose customer information was stolen, expenses relating to the fraudulent purchases committed using the stolen information, as well as litigation fees and remedies.

More recently, in early 2008, Bank of New York Mellon Corporation suffered an information security breach resulting in the loss of 12.5 million customer records. The company is offering two years of free credit monitoring and $25,000 of identity theft insurance to customers impacted by this security breach [6]. This breach may cost in the order of $1 billion to resolve, in addition to potential fines imposed by government regulatory agencies.

Some impacts from information technology security breaches, however, cannot be quantified easily. These impacts relate to brand image and company reputation. As an example, consider the database in which an automobile manufacturer stores data relating

to problems encountered by customers and dealers with vehicles produced by this manufacturer. If the contents of this database are made publicly available through unauthorized access, customers may switch to other automobile manufacturers or band together to bring forth a class action lawsuit against the company.

In the examples noted above, the company affected by the breach could have prevented it from occurring by implementing information technology security improvements which would have cost significantly less than the hard and soft costs resulting from the breach. Yet these companies did not take actions to resolve these security weaknesses prior to the breaches.

To understand why companies may not resolve known information security risks, six information technology (IT) managers at a global automobile sales and marketing company were interviewed. The objective of these interviews was to understand the challenges these managers experienced in obtaining funding for information security projects, as well as to learn which techniques have been effective in securing budget for such projects. The findings from these interviews are discussed below.

3. CHALLENGES ENCOUNTERED BY 'IT' MANAGERS

As indicated by the IT managers interviewed, current methods for obtaining funding for information security projects are inadequate, leading to a gap between knowledge of information security mitigation procedures and implementation of these procedures [7]. These IT managers expressed a number of challenges in justifying information security projects in a manner which encourages the granting of funding for these projects by business executives.

The IT managers consistently noted the *difficulty in translating information security risks to business impact*. Each potential project vying for funding requires the creation of a business case which documents the project's root cause, opportunity, benefits, strategic alignment, risks, dependencies, timeline, and budget. For the strategic alignment section, project sponsors are expected to describe how the project will enable the company to achieve one or more of its strategic initiatives, such as selling more vehicles, increasing the efficiency of vehicle parts distribution, or improving customer satisfaction. Often, IT managers are uncertain how to tie an information security project to these strategic initiatives, and instead, describe the benefits of such projects in vague terms relating to risk avoidance.

An additional challenge is the *ongoing clash for budget allocation between the Information Technology division and business units*. The annual budget process within the company allocates funding to each "vertical" business unit and each "horizontal" support division. Examples of vertical business units are Vehicle Sales and Parts Distribution, while Human Resources and Information Technology are horizontal support divisions. These support divisions are regarded as cost centers, whose budgets are limited to the bare minimum, while vertical business units are viewed as profit centers which contribute to revenue. Information security projects have historically been funded from the Information Technology budget, and not by any business units. This requires such projects to compete with limited funds needed for ongoing system maintenance and break/fix support activities.

The IT managers felt that a *lack of sufficient understanding regarding information security risks by business executives* hindered their ability to obtain funding for information security projects. To illustrate this point, one of the IT managers compared information security to insurance. The insurance industry, as he pointed out, has been in existence for hundreds of years, with business executives understanding and supporting

the need for various corporate insurance policies. Information security, on the other hand, has only recently started to gain momentum with CEOs, especially in non-government, non-financial industry sectors. This led to business executives in the company looking at information security projects as additional expenditures to correct prior implementation errors, rather than regarding these projects similar to insurance policies.

Likewise, the IT managers noted that *business executives may not regard information technology security to be a core competency of the company*, and may consequently not perceive a need to excel in this area. Instead, information security is frequently viewed with an attitude of "if it ain't broke, don't fix it." There is thus a tendency by companies to perform the minimum and focus on the low-hanging fruit, treating information security as a one-time effort instead of an ongoing maintenance activity.

Moreover, the IT managers pointed out that even if budget was not an issue, *business units often oppose implementation of information security practices* aimed at reducing the risk of security breaches, since such practices often result in new restrictions, additional tasks, and increased cost upon the business. For example, implementing separation of duties may require business units to expend additional budget on staffing multiple individuals to perform a task that was previously completed by one individual.

Another challenge expressed by the IT managers relates to the *emergence of standards*. In their company, the business case for an information technology project must document whether standards have been defined by an independent organization. It is more difficult to obtain approval for projects for which standards have not been defined, since business executives want to avoid the unnecessary cost associated with being tied to a specific vendor implementation. Yet with information security experiencing significant innovation in recent years, the definition and acceptance of formal standards often lag behind vendor implementations.

4. PROPOSED APPROACH

As noted by the IT managers, information security projects often compete for funding against business projects. Furthermore, unlike business projects which generate revenue, information security prevention and mitigation are often regarded as costs by business executives.

The approach proposed by this paper is therefore to shift from a position in which information security projects vie against business projects to one in which they are aligned with the business. Finding a way to turn an information security practice into a business enabler will therefore greatly augment the likelihood of that practice being implemented. For example, enforcement of strong passwords and periodic password changes can pave the way to implement single-sign-on in order to increase employee productivity. Likewise, security improvements in a company's information technology infrastructure and systems may enable cost reductions or efficiency increases in the company's supply chain.

4.1 Potential Gap Reduction Mechanisms

Based on the interviews with the IT managers and a review of current literature, four mechanisms for reducing the gap between information security knowledge and implementation are being recommended. These four mechanisms are aimed at increasing the alignment of an information security project with the business.

Total Return on Investment (ROI). Keeping business executives well-informed using management terminology was considered to be a key mechanism to promote the granting of funding for information security projects. IT managers must present every information security risk and project to business executives in terms that resonate with management, including return on investment and strategic alignment. Similarly, business executives need to gain an understanding about the ongoing nature of information security improvements, enabling them to regard information security as another form of insurance.

To put information security projects on the same footing as business projects, a total ROI calculation should be used instead of the classical ROI computation [8]. The difference between the two formulas is that total ROI deducts from the numerator the value of the change in risk resulting from the project. An information security project which reduces a certain risk will therefore have a higher total ROI value than the corresponding classical ROI value. Using total ROI thus enables a more accurate comparison between information security projects and business projects.

Sarbanes-Oxley Act Compliance. Another technique the IT managers indicated as being effective in increasing the likelihood of obtaining project funding has been to associate an information security project with regulatory compliance requirements such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA). Compared to other legislation, the Sarbanes-Oxley Act may have the greatest influence on reducing the gap between information security knowledge and implementation, since it places responsibility on leaders of public corporations to establish and maintain adequate internal controls [9].

News of Breaches at Other Companies. Likewise, the IT managers also noted that examples of security breaches at other companies have proven effective at helping to obtain funding for information security projects. Knowledge that a security breach has occurred at another company, along with data on the resultant costs incurred by that company, makes that security risk more "tangible" to business executives [10]. The IT managers shared examples of executives calling them to ask whether a company is at risk after security breaches at other companies were made public, offering funding and support for remediation of the vulnerability if the company is indeed at risk.

White Hat Security Testing Findings. To bolster the business case for information security projects, the CIO periodically employed the services of third-party computer security experts (white hat hackers) to conduct penetration testing and report their findings. Doing so enabled the CIO to provide business executives with independent justification for information security projects, referred to as "buying the credibility" by the IT managers. A growing number of companies are using white hat testing to identify security vulnerabilities before hackers break into their information technology infrastructure and systems [11].

Given the gap reduction mechanisms suggested above, the effectiveness of each of these mechanisms in reducing the gap between information security knowledge and implementation must be evaluated. To determine effectiveness, a new research approach is being proposed, based on the use of laboratory experiments to establish whether hypotheses on the effect of the gap reduction mechanisms should be rejected or not. This is described further in the following sections.

4.2 Management Decisions under a Single Gap Reduction Mechanism

The experiment will test four hypotheses relating to the effect of specific gap reduction mechanisms on management's decision to fund information security (IS) projects:

H_1: Total ROI does have an effect on management's decision to fund IS projects

H_2: SOX compliance does have an effect on management's decision to fund IS projects

H_3: Breach news does have an effect on management's decision to fund IS projects

H_4: White hat testing does have an effect on management's decision to fund IS projects

For each of the hypotheses, one of three outcomes is possible:

1. Do not reject the hypothesis – the gap reduction mechanism was ineffective
2. Reject the hypothesis, with a negative effect – the gap reduction mechanism decreased the likelihood of an information security project being funded
3. Reject the hypothesis, with a positive effect – the gap reduction mechanism increased the likelihood of an information security project being funded

The outcome of the experiment will be a list of gap reduction mechanisms, ranked by their likelihood of helping an information technology security project gain approval for implementation.

4.3 Management Decisions under Combined Gap Reduction Mechanisms

After conducting the experiment for the above four hypotheses, each of which represents a single gap reduction mechanism, the experiment will be re-run to test combinations of gap reduction mechanisms.

Each of the four gap reduction mechanisms will be combined with one of the other four mechanisms, resulting in six combinations of two gap reduction mechanisms, since order is not relevant. That is, combining total ROI with SOX compliance is the same as combining SOX compliance with total ROI.

The following six hypotheses, corresponding to the six combinations of two gap reduction mechanisms, will therefore be tested:

H_5: Total ROI and SOX compliance do have an effect on management's decision to fund IS projects

H_6: Total ROI and breach news do have an effect on management's decision to fund IS projects

H_7: Total ROI and white hat testing do have an effect on management's decision to fund IS projects

H_8: SOX compliance and breach news do have an effect on management's decision to fund IS projects

H_9: SOX compliance and white hat testing do have an effect on management's decision to fund IS projects

H_{10}: Breach news and white hat testing do have an effect on management's decision to fund IS projects

The experiment will not be conducted with combinations of more than two gap reduction mechanisms, because each gap reduction mechanism requires additional time and money to be expended. For the purpose of this research, it is assumed that the incremental benefit of adding a third gap reduction mechanism is outweighed by the additional expenses required to apply it.

4.4 Effect of Unexpected Events of Management Decisions

In addition to testing the effect of gap reduction mechanisms, both discretely and in combinations, the effect of unexpected events will be tested as well. For this research study, an unexpected event refers to an unanticipated incident which has the potential of affecting decisions made by business executives across multiple industries and geographies. Such incidents are likely to affect fundamental parameters and assumptions relating to how business is conducted.

Examples of unexpected events are the economic crisis of 2008, hurricane Katrina, and the September 11, 2001 terrorist attacks. The purpose of this phase of the experiment is to determine whether unexpected events impact the effectiveness of the proposed gap reduction mechanisms.

4.5 Experiment Design

This experiment will be conducted in four phases, described below and illustrated in Figure 1.

Phase 1: Baseline. Participants will be asked to perform the role of business executives evaluating information security projects independently, in order to select whether each project should be funded for implementation. Each of these projects will initially be described in terms of its implementation cost and technical description of its benefits, without application of any gap reduction mechanism. A business project with similar cost will be provided for comparison.

Each participant will be asked to decide between implementing a given information security project and implementing the equivalent cost business project, and the decision will be recorded. A value of 0 will be assigned if the business project is selected, and 1 if the information security project is selected. This process will be repeated across all information security projects, thereby forming the baseline for the experiment.

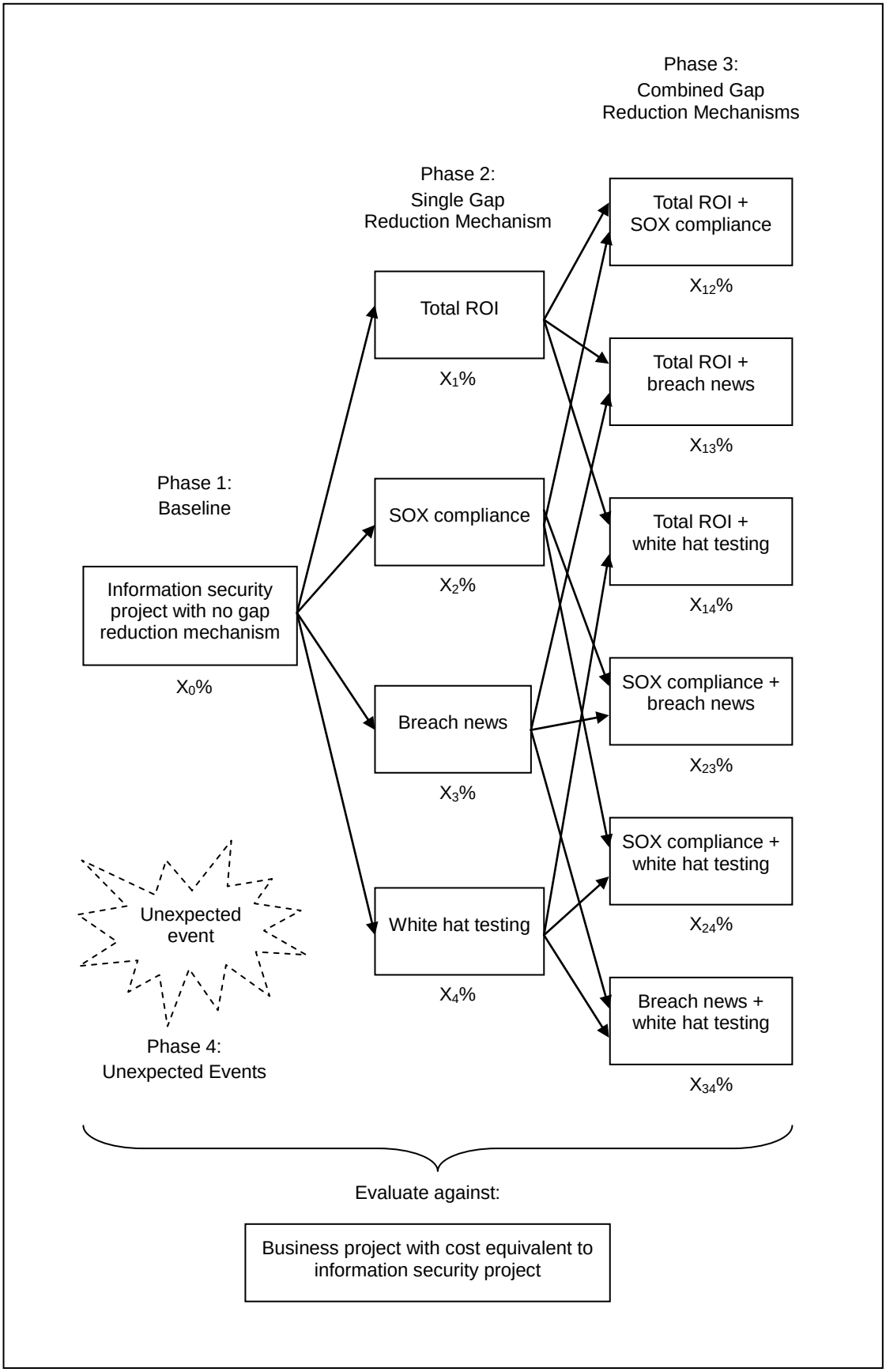

Figure 1. Experiment Design

Phase 2: Single Gap Reduction Mechanism. The sample group of participants will then be randomized into four groups. Each of these four groups will be evaluating information security projects with a specific gap reduction mechanism applied, in order to test the four hypotheses H_1, H_2, H_3, and H_4, as defined above. As a result, one fourth of the participants will be assigned to look at information security projects with total ROI quantified, one fourth to SOX compliance, one fourth to news of breaches, and the final fourth to white hat testing results.

Gap reduction mechanisms will be applied by providing additional details to the project description. For example, to apply the total ROI gap reduction mechanism, an information security project previously described as "improve wireless security to prevent a network breach" at a cost of $1,000,000 will now include an impact analysis indicating this project is expected to generate a total ROI of 300%. This value is computed based on the number of customer records at risk of being compromised, the cost to deal with each compromised record, and an estimate of likelihood of this security breach occurring. Likewise, an example of applying white hat testing would be to expand the project description to indicate that the security testing team was able to break into the network undetected, and access specific personally identifiable information within two hours.

The participants will be asked to decide between implementing a given information security project (now with a single gap reduction mechanism applied) and implementing the equivalent costing business project, and the decision will be recorded. Values of 0 and 1 will be assigned as before. This process will be repeated across all information security projects.

Phase 3: Combined Gap Reduction Mechanisms. In the next phase of the experiment, the participants in each of the four groups from Phase 2 will be further subdivided into three subgroups. These twelve subgroups will be merged into six groups, each of which will be evaluating information security projects with two gap reduction mechanisms applied, in order to test the six hypotheses H_5, H_6, H_7, H_8, H_9, and H_{10}, as defined above.

In each of the six groups, half of the participants will have previously been testing one of the two gap reduction mechanisms, and the other half will have previously tested the other group reduction mechanism. For example, in the group testing the use of total ROI and SOX compliance as combined gap reduction mechanisms, half of the group will have previously been members of the group that tested total ROI as a single gap reduction mechanism, and the other half will have previously tested SOX compliance as a single gap reduction mechanism.

The participants will be asked to decide between implementing a given information security project (now with two gap reduction mechanisms applied) and implementing the equivalent costing business project, and the decision will be recorded. Values of 0 and 1 will be assigned as before. This process will be repeated across all information security projects.

Phase 4: Unexpected Events. In the final phase of the experiment, participants will be regrouped into the original four groups corresponding to the four gap reduction mechanisms. They will then be made aware of an unexpected event with significant impact, such as a widespread financial crisis, along with consequences of the event, such as difficulty in obtaining credit.

Participants will then be asked to decide between implementing a given information security project (now with a single gap reduction mechanism applied) and implementing the equivalent costing business project, and the decision will be recorded. Values of 0 and 1 will be assigned as before. This process will be repeated across all information security projects.

4.6 Statistical Analysis

Once the experiments are conducted, the chi-square test for the difference between two proportions will be used for analyzing the data collected in each experiment [12].

The goal is to determine the impact of each gap reduction mechanism on the likelihood of business executives deciding to undertake an information security project in lieu of a similar costing business project. These likelihood values are represented in Figure 1 by the X% labels. Accordingly, X_0% represents the frequency in which the information security project was selected, absent any gap reduction mechanisms. X_1%, X_2%, X_3%, and X_4% represent the frequencies for selecting the information security project when each of the four single gap reduction mechanisms was applied. Likewise, X_{12}%, X_{13}%, X_{14}%, X_{23}%, X_{24}%, and X_{34}% represent the frequencies for selecting the information security project when each of the six combined gap reduction mechanisms was applied.

5. SIGNIFICANCE

Companies have the ability to carry out procedures to prevent or mitigate against information security risks, yet these companies often do not take adequate measures to implement these procedures, and instead, leave themselves open to security breaches. Interviews conducted at a global automobile sales and marketing company provided an understanding of challenges faced by IT managers in obtaining funding for information security projects, resulting in a gap between knowledge of information security practices and implementation of these practices.

These challenges included difficulty in translating security risks to business impact, competition between information technology projects and business projects for budget, insufficient understanding of security risks by business executives, information security not considered a core competency of the company, business units opposing information security practices, and the emergence of standards.

Based on these interviews and a review of current literature, a number of mechanisms for reducing the gap between information security knowledge and implementation have been offered, including quantification of total return on investment, alignment with Sarbanes-Oxley Act compliance, news of security breaches at other companies, and findings from white hat security testing. Laboratory experiments have been proposed to determine the effectiveness of individual gap reduction mechanisms, as well as combinations of these mechanisms, and to evaluate whether unexpected events affect the decision-making process. These lab experiments provide a new approach to answer the question on how management decides which information security projects to implement, given a limited budget.

5.1 Academic Significance

The laboratory experiment proposed in this paper is significant from an academic perspective because of its novel approach in a number of academic areas.

Based on a review of current literature, the approach proposed above is unique in that it suggests the use of a laboratory experiment to evaluate the effectiveness of mechanisms to reduce the gap between information security knowledge and implementation. This effectiveness will be measured in terms of the percent likelihood of a gap reduction mechanism resulting in an information security project being approved for funding. The findings from this experiment will therefore provide insights into the

thought process used by business executives to approve information security projects for implementation.

The experiment will be operated utilizing a computer-based interactive simulation. Initially, it will be performed using college students as a proxy for business executives in order to execute the end-to-end process and make adjustments prior to conducting the experiment with business executives. While this is a known limitation of this approach, the benefit of utilizing an interactive simulation is that later on, the experiment can be transitioned to be executed in a business setting, in order to obtain more relevant results. The simulation can be carried out in multiple types of industries and business entities in order to study potential differences in the decision-making process.

Another advantage of using a computer-based interactive simulation is that unlike a survey, a simulation enables parameters to be adjusted as the experiment is being conducted, such as the introduction of an unexpected event. The simulation can also be easily customized to reflect the unique attributes of the business environment in which it is being executed.

An additional benefit of this approach is that it will require the formulation of a consistent definition and quantification method for each gap reduction mechanism. For example, when applying news of breaches as a gap reduction mechanism, the type of information provided by the news report can vary across a wide spectrum. Similarly, the components included within the computation of ROI can vary, depending on which ROI formula is used. In order to apply the gap reduction mechanisms uniformly across the information security projects, a consistent measurement system will be defined for each gap reduction mechanism.

4.2 Business Practitioner Significance

For business practitioners, there are multiple advantages to reducing the gap between knowledge and implementation of information security practices. A key benefit is cost avoidance, since implementing preventive measures is generally less expensive than implementing reactive measures. Preventive measures enable a company to avoid the hard costs of dealing with the aftermath of a breach, including investigation, remediation, fines, and lawsuits, along with soft costs such as damage to the company reputation and brand image.

Another benefit of preventive measures is that the business is able to operate in a healthier state overall. When the company is not engrossed in dealing with the aftermath of information security breaches, its management and business units are able to spend time growing the business versus "fighting fires" relating to the breaches. Likewise, the information technology department is able to spend time implementing features to support business growth versus remediating systems and data impacted by security breaches.

Effective implementation of information security practices is not a one-time task, but an on-going activity. By creating a process by which information security knowledge is transformed into practices, the company will benefit by the cultivation of a culture of continuous improvements. Such a culture makes it easier to identify and resolve security risks *before* a breach takes place, due to the increased awareness by employees.

In cases where information security practices are required to ensure compliance with regulations or legislation, reducing the gap between knowledge and implementation of information security practices can help prevent information security breaches which may result in fines for the company, or worse, prison time for executives, as is possible with violations of the Sarbanes-Oxley Act.

5.3 Future Research

As an area of future research, an experiment can be designed and executed to evaluate which gap reduction mechanisms are likely to result in a business manager forming a portfolio of projects yielding a greater overall total return on investment compared to a portfolio created without the gap reduction mechanisms. The outcome of such an experiment will be a list of gap reduction mechanisms, ranked by the increase in total return on investment they can enable the company to achieve.

In this experiment, each participant will be asked to perform the role of a business executive forming a portfolio of projects by allocating a limited budget to those projects they consider to be the most essential for the company to undertake. The participant will be provided with a set of projects from which to make their selections, and this set of projects will include both business projects and information security projects. The portfolio of projects selected will be considered the baseline portfolio and the overall return of that portfolio will be computed and recorded.

Next, a gap reduction mechanism will be applied to each of the information security projects, and the participant will be asked to re-form the portfolio of projects. The overall return of this new portfolio will then be computed and recorded. This process will be repeated for each gap reduction mechanism. The goal of this experiment will be to determine which gap reduction mechanisms resulted in the formation of project portfolios that provided the highest return for the company compared to the baseline portfolio.

Another area of future research relates to the relative severity of the challenges listed in the "Inadequacy of Current Approach" section, as pertaining to a particular company. The approach proposed in this paper considers all the challenges to be equally weighted in terms of severity. Accordingly, the difficulty in translating information security risks to business impact is regarded as being as severe a challenge as the clash for budget allocation between information technology projects and business projects.

Yet in a particular company, certain challenges may be more severe than others. For example, business unit opposition of implementation of information security practices due to the resulting restrictions might be very intense at a given company, even if IT managers are able to translate information security risks to business impact. The experiment can therefore be modified to adjust the severity of each of the challenges according to the company being studied. The goal will be to determine whether the effectiveness of the gap reduction mechanisms varies depending on the types and severity of challenges faced by a given company.

REFERENCES

[1] *CISA Review Manual*, Information Systems Audit and Control Association, 2005.
[2] R. T. Mercuri, Analyzing security cost. *Communication of ACM*, 46(6), 2003.
[3] M. Gaulke, Risk management in IT projects. *Information Systems Control Journal*, 5, 2002.
[4] Chronology of Data Breaches, *Privacy Rights Clearinghouse*. http://www.privacyrights.org/ar/ChronDataBreaches.htm, Accessed December 1, 2008.
[5] N. Swartz, Record data breaches in 2007. *Information Management Journal*, 42(2), 2008.

[6] M. Torres, Florida attorney general warns about identity theft after Bank of New York Mellon loses data. *McClatchy - Tribune Business News*, September 10, 2008.
[7] R. Elitzur, *Automotive company information technology manager interviews*, Unpublished notes. Loyola Marymount University, California: Los Angeles, 2008.
[8] S. A. Purser, Improving the ROI of the security management process. *Journal of Computers & Security*, 23(7), 542-546, 2004.
[9] J. Allen, Governing for enterprise security. *Carnegie Mellon Software Engineering Institute*, CMU/SEI-2005-TN-023, 2005.
[10] J. B. Freedman, Information security: Is silence golden? *Americas Conference on Information Systems*, Nebraska: Omaha, 2005.
[11] B. White, Where the holes are: New tools help companies identify the real security risks in their computer systems – before the hackers. *Wall Street Journal*, June 9, R12, 2008.
[12] D. M. Levine, D. F. Stephan, T. C. Krehbiel and M. L. Berenson, *Statistics for managers* (5th edition), Pearson Prentice Hall, 2008.