Improving Information Systems Security through Procedural and Technical Countermeasures

John D'Arcy
Irwin L. Gross eBusiness Institute
Email: jdarcy@temple.edu

Improving Information Systems Security through Procedural and Technical Countermeasures

July 2005

John D'Arcy, Temple University

Executive Summary
On average, respondents reported a low likelihood that they would intentionally misuse organizational IS resources. However, having employees with even a low likelihood of IS misuse suggests that organizations are still vulnerable to insider security problems. Security policies, security awareness education/training, computer monitoring, and preventative security software are each effective mechanisms for deterring employee misuse of IS resources. It appears that many organizations are not devoting extensive efforts to educate and train users on information security issues. Employees in seven of the eight organizations studied perceived lower levels of security awareness education/training compared to the levels of security policies, computer monitoring, and preventative security software. Finally, the level of security countermeasures employed varies by industry.

Introduction
The number and seriousness of information security problems over the past couple of years indicates that organizations are more vulnerable than ever. Although public attention is quickly focused on viruses and incidents of hacking, leading research groups contend that the more likely and most lethal threats are those originating from legitimate network users. Indeed, employee misuse of information systems (referred to as "IS misuse" in this document for shorthand) represents a very real and costly threat to organizations. The 2004 CSI/FBI Computer Crime and Security Survey[1] reported that 53% of industry and government respondents faced IS security incidents due to the actions of legitimate users, with estimated losses as high as $100,000 per incident. In addition, 59% of respondents detected insider abuse of network access (such as downloading pornography, pirating software, and inappropriate use of e-mail) within their organizations, totaling almost $11 million in losses. Further, the percentage of respondents reporting IS security incidents originating from within the organization has risen steadily from 37% in 1999 to 52% in 2004. The frequency of IS misuse and the amount of losses associated with it are expected to continue in the future due to increasing computer user sophistication and the availability of advanced software tools.

Information security best practice advocates recommend that organizations implement security countermeasures as a strategy for managing and controlling IS misuse. These countermeasures should consist of a combination of procedural controls, such as security policies, acceptable usage guidelines, security awareness education/training, and technical controls, such as access

[1] This is a joint survey conducted by the Computer Security Institute and the Federal Bureau of Investigation's Computer Intrusion Squad. The 2004 survey results are based on the responses of 494 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities.

control devices (for example, userID/password authentication) and other more specialized security software.

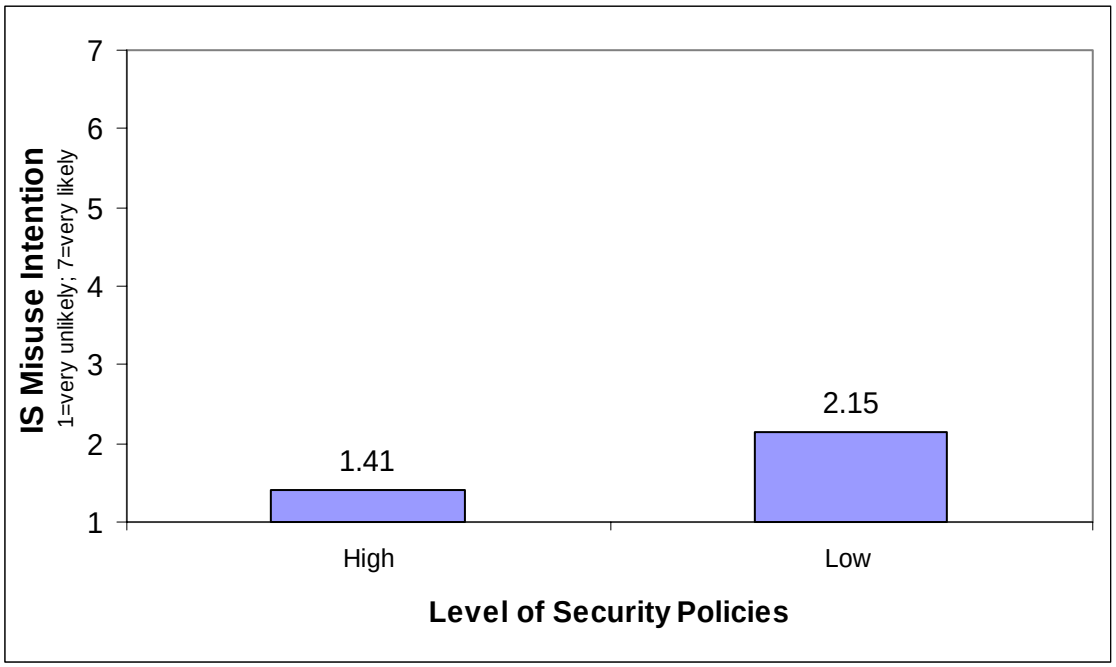
This study examines whether the existence of security polices, security awareness education/training, computer monitoring, and preventative security software are effective in deterring IS misuse. Considering that the success of IS security depends in large part on the actions of system users, the existence of these countermeasures is assessed from the employee, or end user perspective. Also examined are employee perceptions of the levels of security policies, security awareness education/training, computer monitoring, and preventative security software within their organizations. These results are compared across the eight organizations that participated in the study.

An online survey was used to conduct the study (see the Appendix for a detailed description of the survey methodology). A total of 474 employed professionals completed the survey. The following sections detail the study's findings.

Results

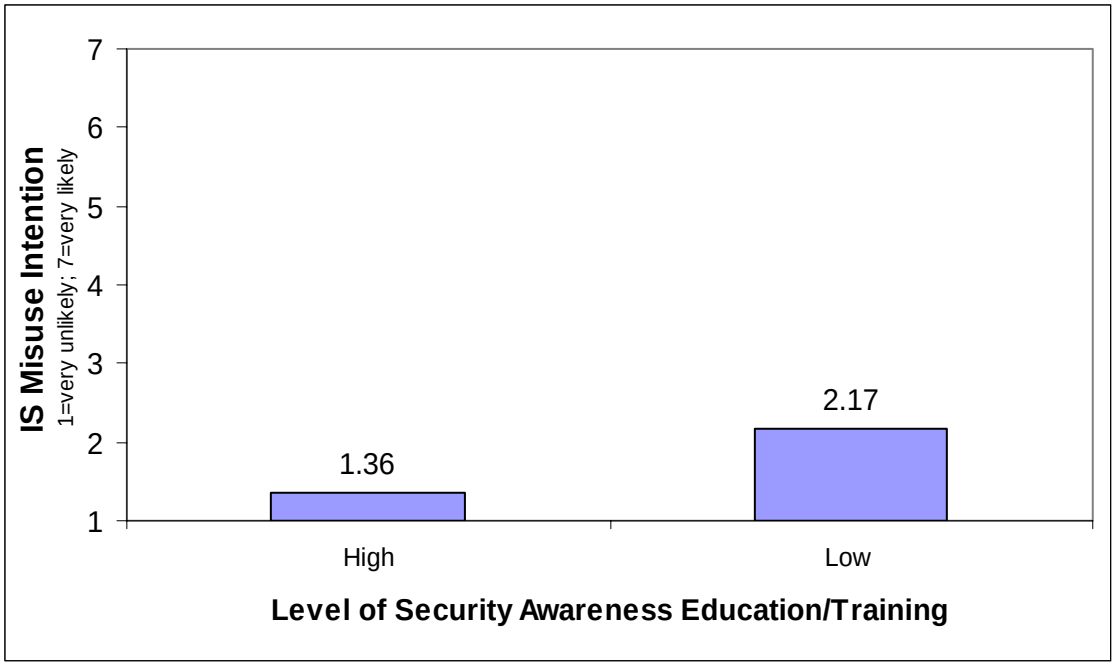
The results provide evidence that security policies help to deter IS misuse. Employees that perceived higher levels of security policies indicated that they were less likely to engage in IS misuse (see Figure 1). Average IS misuse intention was 1.41 (on a scale of 1 'very unlikely' to 7 'very likely') for those that perceived "high" levels of security policies versus 2.15 for those that perceived "low" levels.

Figure 1. Difference in IS Misuse Intention: High vs. Low Levels of Security Policies



The results also provide evidence that security awareness education/training helps to deter IS misuse. Employees that perceived higher levels of security awareness education/training indicated that they were less likely to engage in IS misuse (see Figure 2). Average IS misuse intention was 1.36 for those that perceived "high" levels of security awareness education/training versus 2.17 for those that perceived "low" levels.

Figure 2. Difference in IS Misuse Intention: High vs. Low Levels of Security Awareness Education/Training



In terms of computer monitoring, the results provide evidence that monitoring of employee computing activities helps to deter IS misuse, assuming employees are aware of such monitoring practices. Employees that perceived higher levels of computer monitoring indicated that they were less likely to engage in IS misuse (see Figure 3). Average IS misuse intention was 1.51 for those that perceived "high" levels of computer monitoring versus 2.03 for those that perceived "low" levels.

Finally, the results provide evidence that the existence of preventative security software helps to deter IS misuse. Employees that perceived higher levels of preventative security software indicated that they were less likely to engage in IS misuse (see Figure 4). Average IS misuse intention was 1.42 for those that perceived "high" levels of preventative security software versus 2.14 for those that perceived "low" levels.

Figure 3. Difference in IS Misuse Intention: High vs. Low Levels of Computer Monitoring

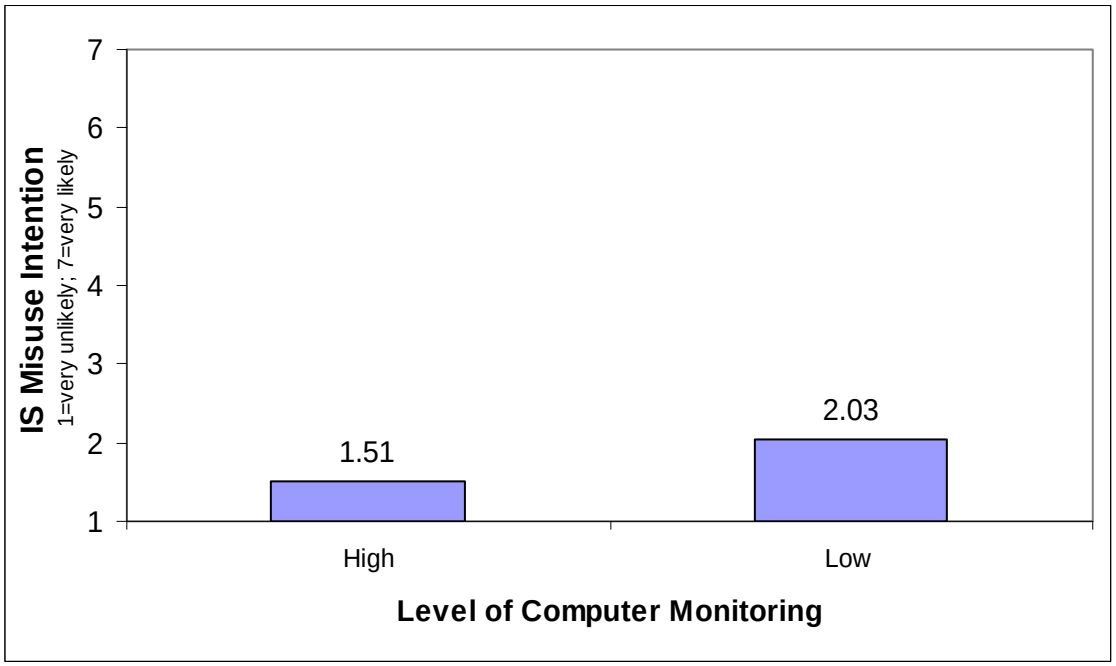
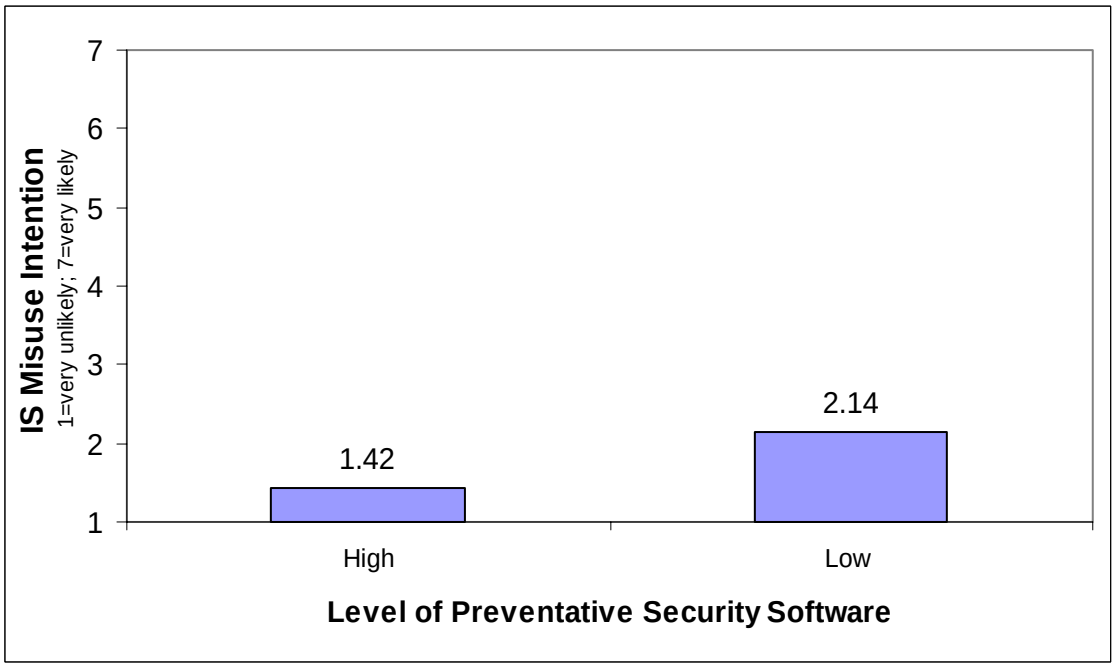


Figure 4. Difference in IS Misuse Intention: High vs. Low Levels of Preventative Security Software



The results displayed in Figures 1 – 4 point to the importance of employee perceptions of security countermeasures as a factor in predicting whether or not they would commit IS misuse. Therefore, to gauge the effectiveness of each organization's security efforts from the end user perspective, we examined respondents' perceived levels of security policies, security awareness education/training, computer monitoring, and preventative security software within their organizations. These results are displayed in Figure 5. Note: In the survey, respondents rated the level of each of the security countermeasures on a scale of 1 (strongly disagree) to 7 (strongly agree), so that higher scores indicate higher perceived levels of the particular countermeasure in Figure 5.

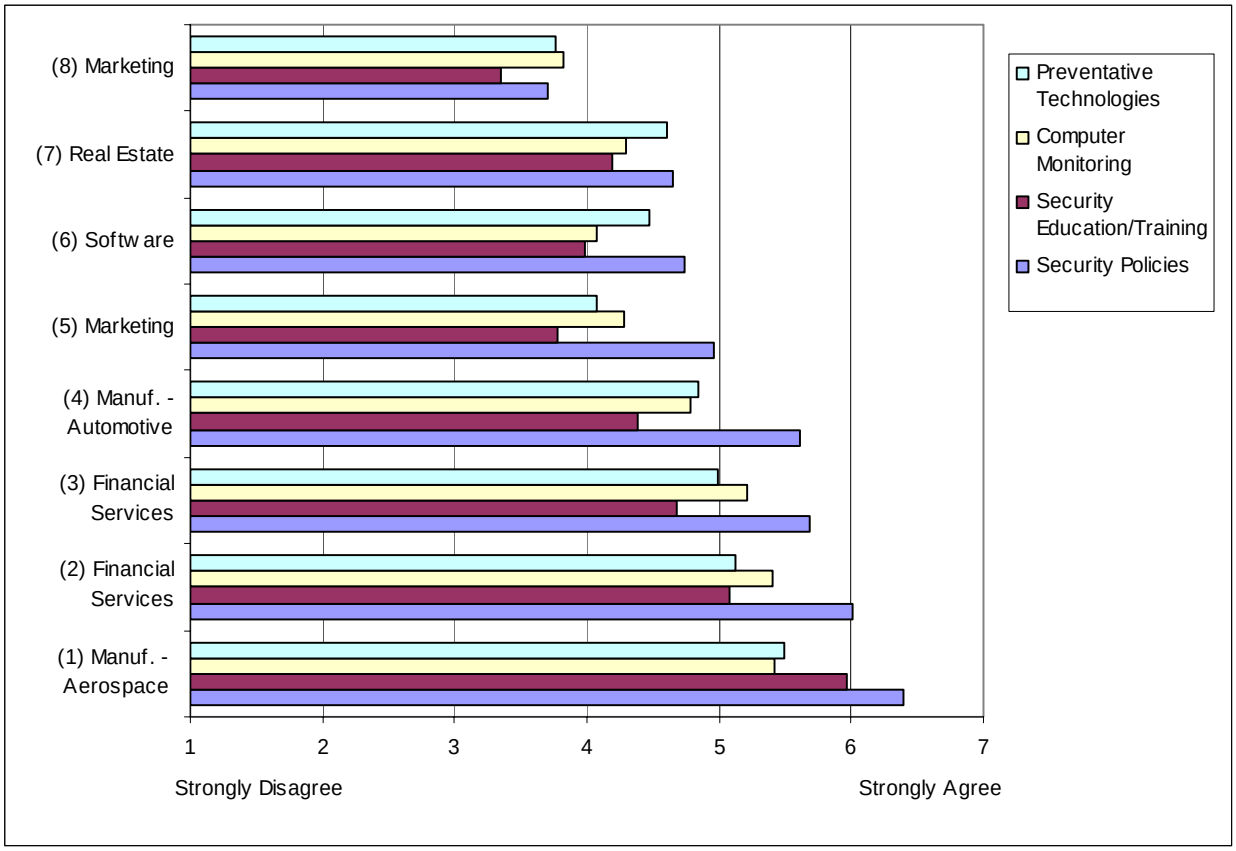
There are several interesting findings that are shown in Figure 5. First, the manufacturing (1 and 4) and financial services organizations (2 and 3) have relatively high levels of security countermeasures compared to most of the other organizations. In terms of the financial services organizations, this is probably due to the sensitivity of information that exists in this industry, which, if compromised, can lead to large potential losses (financially and in reputation). Moreover, the financial services organizations that participated in the study are large organizations that likely have more resources to devote to advanced security efforts. The same could be same for the two manufacturing organizations. Second, the two marketing organizations (5 and 8) have relatively low levels of security countermeasures compared to the other organizations. This is somewhat alarming, considering that marketing professionals often deal with consumer information that is highly sensitive. However, it should be pointed out that the two marketing companies that participated in the study are relatively small organizations that likely have little resources to devote to IS security. Hence, the findings in this study may be the result of small IS security budgets and not a reflection of the marketing industry as a whole. Finally, with the exception of those from organization 1, respondents from each of the organizations perceived lower levels of security awareness education/training compared to the other three countermeasures (security policies, computer monitoring, and preventative security software). Thus, it appears that many organizations are not devoting extensive efforts to educate users on the importance of information security.

Implications for IS Security Management

The results of this study have several important implications for the practice of IS security management. First, most respondents indicated that they are not likely to engage in IS misuse, as evidenced by the low IS misuse intention scores shown in Figures 1 – 4. This is good news for IS managers since it suggests that most employees are unlikely to cause problems for security. However, having employees with even a low likelihood of IS misuse suggests that organizations are still vulnerable to insider security problems since even a single security breach can have serious financial consequences.

In terms of the impact of security countermeasures, the results provide evidence that security policies, security awareness education/training, computer monitoring, and preventative security software are each effective in deterring IS misuse. As such, each of these countermeasures should be included as part of the organization's security management program.

Figure 5. Perceived Levels of Security Countermeasures by Organization



These findings are significant because prior research found that managers were not convinced that security efforts could deter IS misuse[2]. Instead, they considered IS security a preventative function – procedures designed to restrict abusive activities. The results of this study suggest, to the contrary, that organizations can help deter IS misuse by:

- Developing policy statements and guidelines for appropriate use of IS resources.
- Informing and educating users on what constitutes legitimate use of IS resources and what are the consequences of illegitimate use.
- Conducting ongoing surveillance of employees' computing activities and carrying out periodic audits on the use of IS assets.
- Implementing preventative security technologies that control access to IS resources.

These countermeasures should be considered as a group in order to be effective. Security awareness programs, for example, build upon a clear set of security policies and procedures that have been put in place. Employees must also be made aware of security countermeasures for them to be effective. Security policies can be introduced during employee orientation sessions

[2] Straub and Welke, "Coping With Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly, Vol. 22 No. 4/ December 1998.

and employees should be required to sign an acknowledgement indicating that they have read and understand the policy. The security policy should also be prominently displayed on the company website. In terms of monitoring practices, the security policy should specifically state that the organization reserves the right to monitor employee computing activities. Other techniques for increasing awareness of monitoring practices include reminders on screen savers, announcements of upcoming audits on the use of IS assets, and footer messages on company e-mails. Employees should also be kept abreast of the latest technological solutions being used to prevent unauthorized use of the organization's IS resources.

The study's findings also have implications for the allocation of IS security budgets. In a recent survey, 83 percent of organizations indicated that technology is their top information security spending area while only 35 percent indicated that they have security awareness programs in place[3]. The results of this study suggest that organizations should consider allocating a greater portion of their IS security budgets to the development of security policies and ongoing security awareness education and training efforts.

Concluding Comments

Many researchers and practitioners now agree that the success of IS security depends in part on the effective behavior of the individuals involved in its use. This study empirically examined employee perceptions of security policies, security awareness education/training, computer monitoring, and preventative security software, and their impacts on IS misuse intention. The results provide evidence that each of the aforementioned security countermeasures is effective in deterring IS misuse. In addition, there is evidence that the level of security countermeasures employed varies by industry. An interesting finding is the relatively low level of security awareness education/training within most of the organizations compared to the levels of security policies, computer monitoring, and preventative security software. In light of this study's findings on the apparent effectiveness of security awareness education/training in deterring IS misuse, IS managers should consider devoting more of their resources to educating users on the importance of information security issues.

[3] "Global Information Security Survey 2003," Ernst & Young.

Appendix: Survey Methodology

An online survey was completed by a total of 474 employees from eight organizations located across the U.S. The sample included employees from various departments/business units within their respective organizations that held a variety of positions including managerial, technical, professional staff, and administrative. All survey participants indicated that they used a computer as part of their job.

The survey contained five short scenarios that depicted the following IS misuse behaviors: sending an inappropriate e-mail to a co-worker, accessing confidential company information in an unauthorized manner, modifying company data in an unauthorized manner, installing unlicensed software on a company computer, and sharing a password with a co-worker. Following each scenario, respondents indicated the likelihood that they would engage in the behavior depicted in the scenario on a scale of 1 (very unlikely) to 7 (very likely). Responses to the five scenarios were averaged to form a single score, which we call "IS misuse intention."

The survey also contained a series of questions that assessed respondents' perceptions of the level of security policies, security awareness education/training, computer monitoring, and preventative security software within their organizations. Scores on the individual items for each of these variables were averaged, and then separated into high and low groups based on their medians.

