2010

Securing the IT acquisition security chain: Security concerns and human factors in IT acquisition

Eric Goldman

Securing the IT Acquisition Security Chain: Security Concerns and Human Factors in IT Acquisition

By

Eric Goldman

Thesis submitted in partial fulfillment of the requirements for the
degree of Master of Science in
Networking and Systems Administration

Rochester Institute of Technology
B. Thomas Golisano College
of
Computing and Information Sciences

Date Approved:
1 April 2010

Thesis Committee Members:
Yin Pan
Esa M. Rantanen
A. James Baroody

1 Abstract

This thesis research evaluates the extent to which IT decision makers consider security concerns and requirements while performing technology acquisition in small-to-medium sized organizations. The research sought to understand what factors influence decision maker attitudes on the role of security during acquisition and how these attitudes and decision strategies affect security throughout the system lifecycle. Through an interview based study with fifteen IT decision makers from small-to-medium sized organizations, decision maker attitudes and organizational practices were evaluated. The findings suggest that security is not often considered during the acquisition process and is not a crucial element of acquisition decision and selections strategies for a majority of the sample. There is, however, a significant relationship between acquisition and security throughout the system lifecycle and the findings further suggest that end-user consideration and involvement are crucial elements for both acquisition and security. The relative importance of security consideration by decision makers is discussed herein and suggestions are provided for steps organizations may undertake to improve their acquisition decision strategies and to better align and address security concerns and requirements.

2 Contents

3 Tables

This page intentionally left blank.

4 Introduction

This research investigated attitudes and behaviors related to the role of security in IT component acquisition. The study identified decision making strategies used by IT decision makers in selecting new components (e.g., software, hardware, or external services) and systems for internal usage. The identified strategies were evaluated and analyzed to determine to what extent, if any, IT security (risk) is considered by the IT decision maker during the acquisition phase. In addition, IT decision makers' strategies were juxtaposed with other core factors, such as end-user involvement, to determine if they had any relevant impact on the decision makers' ability to perceive and plan for future risk.

The population of interest in this study consisted of small- to medium-sized enterprises. The appropriate IT decision maker for each organization was identified by each participating organization and one-on-one in-person interviews were conducted with each participant. Previous research studies, guidelines, and recommendations have tended to focus on large enterprises. However, smaller organizations often do not have similar resources or circumstances. In order to expand the body of research, this study elected to focus exclusively on small- to medium-sized organizations.

4.1 Scope & Significance

While contemporary society has recognized the importance of IT security management at the larger enterprise level, there are still many smaller organizations that do not understand how to address these concerns. In general, it is very difficult and time intensive for any organization to exactly quantify the possible loss resulting from a security incident or to predict the likelihood of an attack on any given IT environment. Due to the complexity and cost of planning, many organizations upfront investments in security are minimal. This often leads to reactive, "fire-fighting" approaches to security. However, such an approach may lead to extended downtime, loss of reputation, and financial loss when an attack actually occurs.

One of the more popular paths in the current body of literature seeks to address this security dilemma by improving the behavior of the end-users who interact with an organization’s IT systems. In these studies, it is understood that users tend to have a low technical-competency and are prone to either abuse or misuse IT systems. By way of metaphor, it has been suggested that each individual user represents the link in a chain and that an IT system is only as secure as the weakest link. This research does not seek to disprove the previous research, but suggests that the root cause of poor IT security practices should not be attributed to the end-users. This philosophy makes the often-flawed assumption that the IT staff and relevant decision makers sufficiently understand their own security concerns and have done their due diligence to create a secure environment. In this study I sought to expand the existing metaphor to better address the role of the IT staff: While the users continue to form the links in the chain, their individual weakness become irrelevant if the lock (represented by the IT staff and relevant decision makers) holding the chain together is not fastened securely. This study sought to evaluate this theory by investigating what beliefs, practices, and contributing factors enable the creation of a strong lock, which I defined as an IT decision maker who has done her due diligence to proactively address and mitigate potential IT threats for her organization.

This study does not attempt to suggest that there is a simple formula or standard that can be applied to better predict the threat to a given IT system nor does it attempt to create some universal criteria for effective decision making (e.g., a checklist) as it is related to information security. Instead, in this study I argue that IT decision makers' acquisition decision strategies may either positively or adversely affect their ability to discover, understand, and plan for potential risk. Furthermore, this study also suggests that an individual's security assessment strategy is influenced by experience and environmental factors which may lead to an unrealistic assessment of an organization's security requirements or may lead to a security evaluation which is supported by non-truths and misperceptions.

The research focused primarily on the acquisition phase of the system lifecycle. The acquisition phase occurs after a need has been identified and the decision has been made to purchase or otherwise acquire a solution rather than to build the component internally. Thus, it is most vital to evaluate a component's fitness and security implications during this phase, before the component has been introduced into the system and other components or business processes have become dependent upon it. After a component has been selected and implemented, it is often very difficult or in some cases impossible to remove it from the overall IT system. Therefore, it is critical that IT decision makers are aware of security requirements during this phase in order to reduce reactive security management. In addition, when security is considered in this early stage it can help increase security awareness and ease security management in later stages of the system lifecycle. If a product is known to have good security support or integration with security reporting or monitoring systems, this is one less patch or concern that must later be addressed or that may only become apparent after a security incident has already occurred.

This research investigated and analyzed examples of strategies, attitudes, and external factors which improve security consciousness and awareness during the acquisition phase of the system lifecycle. Through this analysis other IT practitioners and decision makers can learn how to modify their own behavior and environment in order to increase the security of their IT systems. Furthermore, this study will help decision makers avoid common pitfalls, which may lead to a false perceptions of a security, foundationless trust, misinformed decisions, and/or selections made with insufficient qualification.

4.2 Research Questions

At the highest level, this research study sought to discover the human factors and decision making processes involved in application and system acquisition in small-to-medium sized corporate IT environments, and to what extent, if any, during this process security concerns are addressed. In order to address this greater concern, this study evaluated the following more specific questions:

Q1: To what extent, if any, is security considered during the acquisition process?

Q2: To what extent, if any, is security considered by the participants and their corresponding organization throughout the system lifecycle? What is the extent of security awareness and understanding?

Q3: Does the relative performance of decision makers (and their organizations) in the areas of experience, management attitudes, and user interaction significantly predict quality of decision making?

Q4: Does the relative quality of decision makers' decision strategies significantly predict the level of security awareness and understanding demonstrated by the participants and their organization?

4.3 Literature review

4.3.1 Relationship to Current Body of Literature

While the body of research is limited in terms of case studies evaluating deployment procedures, there is a growing interest in human factors and its relationship to security. In addition, previous findings from the field of psychology in decision theory and science contribute to the foundation of this research. Besnard and Arief note that "computer security is an area that cognitive scientists have not investigated as deeply as human computer interaction or problem solving" [1]. Generally, as will be outlined below, previous research has focused on end-users with limited analysis of IT practitioners. I believe a bias exists where it is assume that IT professionals have a higher degree of security education and understanding. However, there are surely many decision makers who have no background, understanding, or concerns about security. Decision makers may have specialized knowledge and a more technical understanding of a problem, but generally they can fall prey to the same traps as end-users. This is especially true of general psychological principles on human rationality and decision making, which are mostly independent of technical domain. The literature that approaches security from a human factors perspective goes to great lengths to explain that security and usability are often in confrontation; users will ignore security concerns when there is pressure to perform or simply when security rules present undesired hurdles to achievement of goals. One of the key findings emerging in the body of literature is the general lack of awareness and understanding of security concerns. Also noteworthy is that organizational cultures tend not to put a strong enough emphasis on security. Many papers have commented on users as "the weakest link" [2][3][4][5], that a failure of an individual in terms of security can cause breaks throughout an organization. While it is presumed that IT professionals should be the strongest link, I would say that the IT staff metaphorically represents a lock. That is to say that if they are not securing the chain and holding it together, there is no defense whatsoever.

4.3.2 Organization of this Review

This review of literature will cover major themes spanning from decision making and psychology based concepts to the role of security in software design and organizational practices. Among these are social and psychological aspects dealing with the nature of human thinking and decision making and issues of trust relationships. I then move into an overview on how individuals react to security situations and how humans effect security situations. Next, I provide a brief examination of the effects of software design and development on security and relate some of the proposed techniques for increasing software security situations. Drawing from the above, I relate the ideas and studies in the body of research to IT acquisition decision makers and other IT professionals. Finally, an analysis of the research methodology and analyses in the body of literature is presented.

4.3.3 Human Psychology and Decision Making

Before conducting an analysis of how individuals think about security and deal with security related topics, a general understanding of human thought process is necessary. Sasse et al. provide some basic

insight into the way humans evaluate a given situation [5]. Building upon previous research in psychology they relate that individuals are inclined to take the easiest route rather than evaluating a situation and appreciating all possible consequences. Various factors such as internal and external pressures can make decisions difficult; as the level of stress increases for a given decision an individual is less likely to consider consequences in order to solve the solution expediently. Besnard & Arief also supported this view, noting specifically that human reasoning is not based on achieving perfection [1]. Rather the authors' research indicated that cognitive acts involve an analysis of tradeoffs, which results in the individual choosing some perceived optimal path. This introduces new risks since the individual may not consider all consequences. In their analysis Besnard & Arief evaluated a case study covering an accident on December 30, 1999 at the JCO nuclear fuel processing plant in Japan. Workers at the plant broke with the normal processing procedures and used an illegal and dangerous procedure to expedite their tasks in order to make it easier to perform their jobs. As a result, two workers died when the process triggered a critical accident. Upon further review of the incident, it was determined that management's drive for productivity and relatively low concern for safety significantly contributed to the incident. It seems that humans are preprogrammed to make convenience decisions, and furthermore that irrational decision making increases with the amount of stress the individual is under at any given point. Risk (the potential for some action or decision to result in harm or loss, now or in the future) and stress seem directly proportional; however, individuals seem less likely to *consider* risk as the stress increases.

4.3.4 Issues of Trust

To a great extent the level of trust in a particular situation will affect how willing a user is to consider risk. Mayer et al. examined research and definitions of trust from multiple disciplines [6]. Trust can be understood as a reduction in the perception of risk, which may be the result of a relationship, analysis, or other factors which may lead one to believe that there is some manner of reducing risk. Herein I will define trust as the level to which an individual feels safe and is confident in the accuracy of his beliefs about people or things. Trust should not be confused with reliance, which may often be substituted for trust. Reliance is a mechanism whereby one believes that the partner in a trust relationship can resolve a problem or conflict which may arise even when there is insufficient proof that risk has been reduced [7]. Trust relationships exist between individuals and other individuals, as well as between individuals and organizations or institutions. An individual may also have a level of trust in his own abilities or knowledge. Chu et al. evaluated the dangers of trust in their design for creating a secure application framework [8]. In their evaluation, they defined trust as follows: "Trust is to undertake a potentially dangerous operation knowing that it is potentially dangerous" [8]. They then proceeded to look at trust from an end-user's vantage point, noting that in general a user will prefer to have some proof of harmlessness; however, they often accept weak forms of evidence in establishing trust. For example, they noted that if a piece of software is recommended by a friend whom they trust, other users are more likely to assume that software is safe even without an explicit mention of the software being "virus-free" or otherwise benign. They also noted that when responsibility can be transferred to another individual, group, or institution that individuals are more likely to put trust in an otherwise risky relationship or endeavor. They provided an example of using a credit card in a potentially insecure

transaction because the credit card company will assume the liability for any fraud that could result in the future.

In Dourish(1) et al.'s investigation of trust the researchers noted that people will often put their faith and trust in technology itself to provide protection [3]. In this case, humans will take on more risky behaviors because of their confidence in technology to protect them. That is to say a user may download an attachment from an unknown sender believing that if a virus were attached his virus scanner, spyware blocker, and other technology would prevent any harm. In the case of an IT professional, this blind faith in technology could be much worse. IT professionals who understand a given technology and how it works may be more prone to believing the provided safeguards are absolute as long as they are maintained and remain functional. As a result, IT administrators may not bother to make active decisions on security issues.

The highest level of trust is often between individuals and established institutions. One may consider banks, for example, to be relatively secure because of their investments in security guards, heavy safes, and video monitoring technology. Dourish(1) et al. asserted that this trust is often transferred from the physical world to the bank's online presence [3]. While it can be argued that banks are the biggest investors in security and security technology, they still remain lucrative targets for attackers. Such awareness is necessary for making accurate security related decisions. In terms of software, many popular download website have become institutions in their own right. Due to popularity and traffic, users may assume that others also trust these web sites without any actual foundation. In 2003, popular open source project management and repository Source Forge (http://www.sourceforge.net) was successfully attacked [9]. The root FTP servers used to host many of the projects repositories were compromised in the attack. It was unknown whether any files were compromised before the attack was discovered, but there was the possibility that malicious code could have been injected into any number of project repositories. Users would typically not think twice about downloading software from Source Forge because all projects are open source and anyone *could* review the code, and then alert the community or the Source Forge administrators of any vulnerability or danger. However, there are many unmaintained and unmonitored projects which users may still use without performing their own analysis. Users implicitly may feel safe because the content is hosted on Source Forge and that the source code is open for review, but hosting via Source Forge does not present any explicit security guarantee.

4.3.5 Human Nature and Security

Considering the above human decision making processes and factors which many increase or decrease trust, the way that individuals approach security practices and security decisions will now be addressed.

Dourish(2) et al. sought to investigate how people view problems of security, with a desired outcome of discovering related mental models and conceptual arrangements [4]. According to the authors, security "rests in practice, and in the detail of what people do" [4]. Security should be viewed in the context of what is actually done on a system, not what assets should be protected. As mentioned earlier, humans make tradeoff-based decisions which often increase risk. For this reason, it becomes clear in their study that security does not exist in a Boolean context, rather security based decisions will fall somewhere on a continuum. Further findings in [4] indicate that retrospectively poor choices can be attributed to a lack

of communication that exists between developers, implementers (such as acquisition decision makers), and users. End users often do not see software applications and their related security concerns the same way as knowledgeable IT professionals. As a result, users may not understand security mechanisms or their intended purpose. For example, a user may believe that a spam filter will delete malicious attachments, when in reality the organization's spam filters only perform basic pattern matching and normally would not scan for viruses or spyware. In addition, the Dourish(2) et al. study found there was a generational difference among users: Younger individuals were much more skeptical and concerned about potential security situations, whereas older individuals displayed a higher degree of trust. More broadly, their study highlighted that users believe their efforts to be secured are futile because the hackers, spammers, and other villains will always be a step ahead of them. Users therefore prefer to delegate responsibility elsewhere and believe they themselves are incapable or are not responsible for security within organizations.

In a later article [3], Dourish(1) et al. confirmed many of their previous findings. Some new points were also raised in this study. The authors noted that as the complexity of software increases, users will tend to explore and seek to understand it less. This correlates to another finding which explains that while a user's security decision will fall somewhere on a continuum, their choice to act or to not act is often all or nothing. For example, if a typical user is prompted to update the virus definitions for his virus scanner software, he will either do it immediately or will choose not to perform the update at all because he does not understand the purpose or need, or may simply have other tasks with a higher precedence. Usually, if the user does not immediately take care of the security concern, he will forget about it or will choose rather to just accept the security violation (e.g. spyware pop-up every few minutes) as part of normal computing operations. The authors also shared a novel observation that over time, security practices may become part of normal routine. While initially this would appear to be a positive gain, user complacency will lead to less conscious thinking of security and may also result in the users forgetting how or why a particular security task should be tackled. For example, when a new member enters a group the current group members are unable to explain the security procedures, practices, and principles to the new member. This may result in a decay of security over time as old members leave and new members join the group.

Gross & Rosson provided an overview of their interview study which assessed user security practices [2]. The authors' research indicated that there is increasing concern among users about security. However, in line with other studies [3][4], they noted that users are unable to understand and effectively implement security practices. An important concept raised in their research is that security in an ongoing process; there is no terminal goal or end point at which security can be ignored. Most users only concern themselves with security when it is obvious or a message pops up informing them of some security concern. Such intrusions result in users viewing security as a functional barrier; if a security breach occurred and prevented a user from using her systems, productivity would be stopped. This finding demonstrates that users do not typically concern themselves with security for security's sake, but rather only consider it in correlation to achieving their normal tasks. Also, Gross & Rosson observed the effect of interaction with IT staff on end-user security awareness and practice. When there is a high level of interaction among users and the IT staff, trust is increased and users are more likely to

understand and respect the need for security practices. This finding does not address if the relationship varies if the IT services are outsourced as opposed to being provided in-house.

4.3.6 The Weakest Link

Much of the literature has identified humans as the cause of most security related issues, instead of poorly written software or inadequate procedures. This section will review some of the ways that humans defeat or limit security measures.

As Sasse et al. discussed [5], regardless of capital investment in technology, security mechanisms are easily defeated (whether intentionally or not) due to human error or incompetence. In their study Sasse and her associates examined the effectiveness and success of password and authentication usage among end users. Their paper detailed that users often have great trouble remembering their many passwords due to factors such as complexity and frequency of usage. The results of their survey and in-depth interviews further indicated that in general users did not display sufficient understanding of security practices or the importance of compliance. Through their study they hypothesize that users are typically not well educated about security and do not concern themselves with security for a number of reasons, such as those mentioned above. Most alarming is that participants indicated they did not believe they would be the target of an attack; some participants explained that they did not believe they had any sensitive information or that a security compromise on their system or account would not result in any further harm to the organization. However, from practical experience I argue that most attacks on a network or vital systems do in fact begin by compromising a poorly secured user system or account since they are often not as closely monitored as servers or administrator accounts.

Users typically do not believe they have any responsibility for security. They choose to delegate the responsibility or trust in some external person, group, institution, or technology. Within an organization, users do not feel in direct danger. They choose to believe that the organization is the target; however, users seem unaware that the organization may store personal data in payroll and human resources databases. Should an attacker compromise these systems, the user could potentially be directly affected by the attack. Besnard & Arief observed that this mentality leads to activities such as writing down passwords or other convenience mechanism for circumventing security procedures [1]. It is unlikely that users seek to defeat security mechanisms for the sake of limiting security, but rather it is the result of convenience. As Besnard & Arief noted, there is a cost associated with any task and security measures often make the costs higher; by circumventing security users make their tasks less expensive either in terms of complexity or time.

4.3.7 Software is Inherently Insecure

Most software developers do not intentionally create faulty or insecure software. However, as noted in earlier sections, security adds additional costs and must always be ongoing. As a result, there is the inevitability that software will arrive for deployment with problems or security flaws, and furthermore that the initial authors were more concerned with efficiency and algorithmic elegance than with writing tight and secure code.

In a paper Collins et al. examined the consequences of poorly designed and insecure software construction on end users [10]. They note there are many reasons that software can prove defective.

While the software may be written to match specifications, that does not guarantee that specifications themselves are correct. Software may also be used in unintentional ways or combined with other applications in such a way that new security concerns are created that were not previously known. Collins and his associates recount a case study where an unknown bug existed in switches used by AT&T. The logical error was not detected in testing and the condition which triggered the failure was not common. In another case, the authors examined the implementation of electronic management system for hospital pharmacy. This case was interesting because apparent bugs were found, not by a programmer, but by a member of the hospital staff. This particular individual was highly skeptical of the system, and while she was not intentionally trying to break the system she was on high alert. Clearly, security must not only be evaluated during the initial purchasing procedure, but before and after deployment has occurred. It is also important to remember that responsibility for security or privacy concerns fall on the organization deploying the software, not the software developer in almost all cases. While lawsuits can often be brought forward for contract software that does not meet standards, most commercial and open source software authors are not accountable. The text of most open source licenses or end user license agreements specifically indemnifies the author of legal responsibility.

Sasse and her associates also noted that the design of security has an effect on security. Based on their findings [5], they noted that security increases when the application better matches the user's workflow. This logically follows findings presented earlier because the cost of a particular task is not greatly increased by following a procedure that is well designed to accompany the task. As an example, consider a user work group where users work collaboratively on reports. A role-based, collaborative document management system would allow all users to have appropriate access to a file without the burden of managing access in a more traditional method such as controlled directories in a file system. Because the processes has become more easier and less costly than typical file management, the users would likely have no qualms about the added security.

Shimeall & McDermott [11] examined Internet usage and related security concerns. They noted that software is becoming more complex, while at the same time application efficiency has taken precedence over security. As a result, there are complex systems with many points of failure, which are widely distributed and deployed, often with minimal security testing. Furthermore, they concluded that vulnerabilities will increase as programmers become more comfortable with sloppy coding procedures and usage of languages which require greater security considerations by the programmer. Take for example the PHP programming language. Because PHP is loosely-typed, data validation becomes extremely important when dealing with user input. However, it is not unlikely to find a piece of PHP code that expects an integer, accepts a string, and allows for a malicious code injection. For this reason, the authors stressed the importance of constantly reevaluating software through its lifecycle. Security or operational flaws may be discovered and patched, however, that does not guarantee that such patches will be applied or that the modification will not result in further vulnerabilities.

4.3.8 What can be done to improve security?

The most important conclusion brought about in the body of research, is that users are not well informed about security. To this end, Besnard & Arief provided recommendations and considerations for educating users about security. Note, education will not prevent all problems, but it will increase

awareness among users and administrators. Combined with the more frequent interaction proposed by Gross & Rosson [2], this will facilitate communication and trust between users and administrators. Such interaction will increase the likelihood that a user will seek guidance on a security concern, rather than simply dismissing the concern and continuing on with his work. Secondly, users must be protected from themselves. The software should be selected or written to streamline the user's workflow. Users should be presented with a minimal number of choices (e.g., menu-driven interface as opposed to a graphical interface). Specifically for security concerns, users should be given explanations in simple language and all security information should be automatically forwarded to the IT staff. In this way, the administrators will be aware of security concerns and can seek out the individual even if the user does not come forward or later ask about the security incident. Lastly, it is important to remember that users are typically not technically proficient with computers nor are they performing IT work. Security must be analyzed beyond technological concerns; this would include creating a security culture where actions such as writing down passwords are discouraged. As noted by Dourish(2) et al. [3], security should not be "transparent", but rather it should be highly visible. By providing people with the means to understand security and the consequences of their actions, there is a higher probability of users complying with security measures and rules.

4.3.9 The Administrators

Since the research findings do indicate that users are truly the weakest link, one would hope that the IT professionals or decision makers would display a greater security understanding. One might also assume that they also take strong steps to insure security in an IT environment, and thus would reduce the impact of the weak links. The literature to this point does not have significant findings or studies on the security awareness of IT professionals. In my study I propose that often there is no lock at all due to poor security practices by the IT staff, and that IT professionals are susceptible to flawed and illogical conclusions and cost-based tradeoffs in the same ways as end-users.

Findings by Dourish(1) et al. indicated that non-technical users do not perceive security in the same way as IT professionals [4]. For instance, the authors noted that often users group security and privacy concerns together, and place prime importance on issues of privacy over those of a more security nature. Since users are typically incapable of understanding security concerns the IT staff is always responsible. In a section labeled "Responsibilities of the software buyer", Collins et al. asserted that the buyer is "most responsible for the intended use of the software" [10]. The buyer, who is typically also the decision maker, is responsible for learning the software or system's capabilities and limits. If users will be interacting directly with a program, then they must also be considered so that the decision is user-centric and takes into consideration workflows. Since the buyer is the one who is making the commitment to the software, the responsibility for usage and security lies with them and not the end users. Besnard & Arief commented that "security is not the end-user's task" because security depends on where security lies on an organization's list of priorities [1]. "Good security" should be an organizational goal, not simply a goal of the IT staff. The concern for security must be important to the senior staff as well [2]. Logically, this should be the case since a system failure or security breach would result in loss of reputation and/or a stoppage of productivity. However, executives are faced with the same cost decisions that arise when considering security versus productivity.

Issues of trust can also greatly affect the perceptions and decisions related to security by IT professionals. Based on findings by Besnard & Arief [1], users were found to be susceptible to misplacing their trusts. However, misplaced trust by decision makers could be much more costly to the organization. A decision maker that is under pressure or that simply trusts vendors or other non-knowledgeable sources increases security risks for the entire organization. An individual may be swayed by commercial reviews, biased whitepapers, or online forums where the security of the application is not even discussed. Based on these positives, and lack of any known negative aspects, the IT professional may assume a higher level of trust than she should. Without furtherer research or testing, the organization may never learn they have insecure software. Besnard & Arief discussed the implication for users becoming complacent with technological protections. However, since a decision maker or other IT professional has a better understanding of the technology and what it does, the level of trust could be much higher, to the point where responsibility is transferred to the technology. For example, a System Administrator may setup software to use an automatic updating mechanism. His belief in the strength of the system may result in log files or actual systems never be audited for successful updates. However, it is imperative for the IT staff to be diligent about security, because the impetus for creating a culture of security will almost certainly not come from the users.

As mentioned throughout the literature, the concern for security was minimal in the early days of organizational computing. This raises an additional problem that IT professionals may not be security conscious. In fact, as Besnard & Arief demonstrated [1], a low level of understanding or knowledge can lead to users choosing more convenient paths. An IT professional without significant training or knowledge in IT security may choose to focus on his conventional IT tasks with minimal concern for security. However, this is unacceptable as there is likely no other source in the group who will understand or take responsibility for security.

4.3.10 Research and Analysis Methodology

Research in this domain lends itself to a qualitative approach, though other researchers chose a mixed method approach to compliment their qualitative data. The main methods used in previous research studies have been interviews and case studies. This study addresses a technical problem as well as a management problem, with a strong foundation based on general psychological ideas. Previous research has shown that security is simply not a purely technical problem; by understanding the human motivations for security decisions we can better align business practices as well as technical specifications to increase security. Many existing studies have been undertaken by computer scientists who adopted a more psychological and behavioral science approach.

In a study by Sasse et al. the authors examined how users deal with passwords and other authentication methods [5]. Their paper details four studies. In the first study they provided a questionnaire which gauged concerns such as how many passwords a given users typically maintains and asked participants to described recent security problems. The second study involved an analysis of how often users had their password reset. This data was useful in generalizing the frequency of issues. In the third study in-depth structured surveys were performed in order to determine user attitudes towards security and passwords. The fourth study followed 32 participants usage of the authentication mechanism for a courseware system.

Dourish(2) et al. used semi-structured interviews of end users and their usage of Internet technologies [4]. At the time of writing, they were reformulating the questions in order to perform more detailed interviews on a larger sample. The questioning was conducted with an ethnographic-style in order to focus on the social factors which affected security thinking. The results likely contributed to the interviews performed in their later work [3]. In this later set of findings, the authors explain that they used Grounded Theory to analyze the data. The Grounded Theory puts the emphasis on forming the theory based on the research process. The goal, the authors stated, was not to simply document what users do, but to characterize and "understand [the users'] experience of security at they encounter it" [3]. They argued that a quantitative approach was not appropriate at this stage since they were more concerned with what questions to ask rather than finding true and complete answers.

Gross & Rosson provided an in-depth explanation of how they setup their interview based study [2]. Pre-establish questions were the launching point and were general in nature. They looked for spontaneous thoughts, not narrow answers. The participants selected had significant work experience, access to sensitive data, and had no special training in security. There was some resistance to participate in the study by individuals. The authors noted that some were not confident in the guarantee of confidentiality and feared that their answers may result in disciplinary action from their organizations. I was surprised that no other literature indicated a resistance to participate considering that the topic could easily create feelings of uneasiness and discomfort. The authors continue to describe their approach as functionalist as opposed to interpretive. This approach influenced the current research because I was most interested in how the human factors of security play out in organizations and institutions.

4.3.11 Literature Review Conclusions

The body of research provides great insight into the many human factors which affect security. From the decisions people make, to the trust relationships individuals establish, many factors affect security in an IT environment. The current body of research holds a great wealth of insight into users. Building upon this base, I hoped to explore other factors which play into IT security in organizations. As people become increasingly dependent upon technology, there must be assurance and understanding of security. Beyond the security within the organizations, people become links in other chains of security, be it friends, families, clubs or organizations. By increasing security practices and understanding in the business world, security in less controlled environments (e.g., the home) may also be increased. Users do not operate the various aspects of their lives in vacuums. The file your brother sends to you gets forwarded as an attachment to your coworker, which ends up on the department file server, which ends up spreading a malicious virus to the entire enterprise. Therefore it becomes clear that the only way to prevent such a chain of events is to continue to conduct research and to educate users.

The study of security is an important topic not only for IT professionals and for corporations, but the findings can help build the general body of research in the psychological domains. Through studying security researches can examine areas such as trust, accountability, education, and decision science. Examining these principles in action can contribute to studies of intergroup relationships and education. Furthermore, this research can help ensure the security of both organizations and individuals because organizations maintain a large volumne of information in their IT systems. This information may include organizational trade secrets and personal information of employees. This information will become safer

and better protected by teaching IT professionals how to implement good security measures and how to relay security understanding to the non-IT members of the organizations. When security is better understood by all, the costs of security practices can decrease because administrators will choose better products and also develop clearer policies and procedures, which will lead to less confusion and stress for users. When users are educated and understand these principles they are more likely to make better decisions. Everyone's security and productivity is increased when an organization's security chain is made of strong links. Combined with a strong lock provided by the decision makers and other IT professionals, it will become harder for attackers to break the security chain.

4.4 Conceptual model

The conceptual model for this research is organized as a series of cause and effect statements:

1. A more thorough evaluation of IT components before purchase and integration into the greater IT system will reduce instances of future problems.
2. Decision makers who consider security during acquisition can increase organizational security because they are aware of security requirements and possible vulnerabilities in their environment before an attack occurs.
3. If management does not provide sufficient support and resources for IT security programs and actions then the IT decision makers will be limited in their ability to provide organizational security.
4. If end-users are not well trained or do not understand the ramifications of risky IT-related behavior then the IT decision makers will be limited in their ability to secure the organization's IT systems.
5. If an organization lacks experience and understanding of IT security it will be unable to recognize and properly address any possible security concerns which may exist.
6. The ability of IT decision makers to make an informed decision in the general context of acquisition is an indicator of their ability to plan and make informed decisions about organizational IT security concerns.

5 Methods

5.1 Study setting

This study was conducted during the summer of 2009 (June-August). All participants in this study came from organizations that operated in the Rochester, New York, metropolitan area. The selected participants for this study were identified by their organization as appropriate persons who were involved in the IT acquisition process for their organization. All participating organizations identified themselves as small-to-medium sized organizations having approximately 20-1000 employees.

5.2 Selection of study subjects

5.2.1 Source (Sample Population)

Research was constrained to the Rochester, New York metropolitan area. The organizations represented in this study, operate in various industries. The decision makers participating in the study were from various organizational ranks, dependent upon the particular organizational-structure of each organization.

5.2.2 Participant recruitment

Potential participants were identified through local area business organizations which provide support and networking services to local businesses, as well as the career services department at the Rochester Institute of Technology. After successfully engaging a representative from one of the above sources, I explained the research and provided them with a standard participation announcement in letter form (see Appendix 10.2) and asked them to forward this announcement to the appropriate organizations within their membership. In some cases, the representative instead provided me with a list of suitable participants because they preferred I contact each potential participant individually.

Some additional attempts were made to recruit participants for this study. Using a business-listing database, companies that seemed to best fit the criteria of this study and were located in the Rochester, New York metropolitan area were filtered and contacted directly using the same announcement as the previous method (see Appendix 10.2). In addition, companies that had close working relationships with the Rochester Institute of Technology were identified and also contacted directly.

5.2.3 Criteria for eligibility/exclusion

The following restrictions were placed on an organization being represented in this study:

1. The organization should define itself as small or medium sized with approximately 20-600 core employees.
2. The majority of the core employees in this organization must interact with personal computers or other IT technology in their day-to-day work.
3. The company may not be in the business of providing IT security solutions or building IT security products because they might have a skewed opinion on IT security compared to organizations that operate in other industries.

5.3 Description of intervention

In this interview-based study, there was no intervention. All participants were subject to the same set of questions and followed a similar interview process.

5.4 Data collection

5.4.1 Source

All original research in this study was obtained through in-person interviews with the individual identified by the organization as an IT decision maker involved in the acquisition process. Each interview lasted between approximately sixty and ninety minutes. The interviews were all conducted one-on-one and the participants provided informed consent. The interviews were either located on the premises of the organization where the decision maker was employed or in a private study room in the Wallace Library at the Rochester Institute of Technology. The interview questions focused first on general procedures related to acquisition and the focused narrowed specifically to IT security at the end. At the conclusion of the interview, the participant was allowed to readdress any questions or provide any additional commentary related to the subject matter covered in the interview. In general, questions were asked in the same order for each participant, except in the case where the participant had provided sufficient material relevant to the question in response to a previous question or if the question was inappropriate for the participant (e.g., asking a CEO about how his boss communicates with him). The specific interview questions that contributed to this research are provided in Section 0 of this report.

5.4.2 Protocol for typical participant

After a participant was identified as suitable for this research study, an in-person interview was scheduled at the convenience of each participant. Before beginning the actual interview, the participant was provided an informed consent form (see Appendix 10.1) and the opportunity to opt-out of the study or ask additional questions. The participant was also informed that the interview would be recorded to assist in later analysis. After confirming informed consent, I proceed with the interview. A general outline-script was prepared with section introductions and the actual questions to be asked. The questions were scripted for consistency and all attempts were made to use the simplest language possible for each question. As each question was asked, some clarification was provided as needed or requested by the participant. The participant's responses were recorded and notes were also taken for each response. After all of the planned questions were asked, the participant had the opportunity to add supplemental information or to readdress any subject material covered early in the interview. At the end of the interview, the participant was informed that the interview was over and the recording was stopped.

5.4.3 Steps taken to assess and assure data quality

To increase the probability of a truthful response from the participant, their confidentiality was ensured through the informed consent process. Moreover, the interview was structured to start with more innocuous topics gradually moving into areas where the participant may not necessarily be as comfortable. To this end, the study's main focus was on the acquisition process in general, only focusing on security issues after first collecting responses in general. It was an initial consideration that participants may not be comfortable talking about poor security choices or lack of security knowledge.

However, in the process of the interview all participants were comfortable admitting any shortcomings or lack of interest about security.

In addition to transcribing notes during the actual interview process, the interview was recorded. This allowed for review where the notes transcribed were either unclear or where further review of the interview was required to address a particular question.

5.5 Data Analyses

5.5.1 Result Preparation and Analysis

In order to address the research questions specified above several phases of analysis were conducted.

The first phase of the evaluation involved organizing the participant findings to ensure that the interview as whole is considered in each question. This was necessary because sometimes participants address the material in certain questions before they were asked. Also in this phase, some questions (or groups of questions) were assigned a score. The score is ordinal and its primary purpose was to match similar answers among participants in order to discover if any trends exist. Some questions or groups of questions may not have any score attached to them; these questions, however, were used to see if there are any similarities amongst participants with similar responses on scored questions or to draw additional conclusions. Once each participant had a complete answer set that was scored (where appropriate) the first phase was concluded.

The second phase involved evaluating all the responses for an individual participant to measure general attitudes and actions across all the questions in the survey. A summary of each participant highlighting any interesting responses, abnormalities, or other pertinent information is provided in Appendix 10.4.

The last phase involves evaluation of any trends or common practices identified. This was the core analysis to address this thesis and explored contributing factors to well-founded decision making in acquisition and consideration of security related requirements and practices. From the study's findings any available indicators or factors that affect the above can be identified and explored.

5.5.2 Sample size/power considerations

The sample of this study was 15 participants ($n = 15$). This sample size is inappropriate for most statistical methods and to make implied generalizations of the population. Population characterization was not a goal of this study; instead the study focused on analyzing the effect of certain decisions, attitudes, and behaviors on the decision makers' general and security decisions related to IT component acquisition. An attempt was made herein to identify individuals who hold common beliefs and practices and to group them together, however, there may be additional confounding variables not explicitly addressed in this study, which may become evident in larger samples.

5.5.3 Statistical methods

In this study the correlation between different factors were evaluated in order to provide possible explanations of a decision maker's ability to make a quality acquisition decision and to suggest explanations for the decision maker's level of security awareness and understanding. To accomplish this, certain questions asked of the participant were scored. Each question fell into a primary category as

explained above. Correlation tests are applied to these scores in order to see if there are any significant relationships. In addition, linear regression tests are employed to evaluate if proficiency in one area predicts or explains a proportion of the variance between the score in different categorical relationships.

Simple statistical methods were also used to evaluate and compare score quality in different categories in order to communicate to the reader the proficiency of the sampled participants.

5.6 Interview Questions

Table 1 provides a listing of the relevant questions asked during this interview and provides an identifying number which will be used throughout the remainder of this thesis report. A more in-depth explanation of each question is available in Appendix 10.3. Questions are organized by their primary section, however, please note some questions may have implications in other sections of the interview - please consult the appendix for further explanation. Also note that simpler language was used for each question during the course of the actual interview, but that the questions here are presented in a more formal matter to ensure clarity for the reader.

TABLE 1: INTERVIEW QUESTIONS

#	Question
	Section 1: Experience
01	How many years have you been employed at this organization?
02	Identify your job title and role; please describe your general day to day activities in this position.
03	What is your educational background? Please include all post-high school degrees, certifications, are other notable educational experiences.
04	Describe any ongoing professional education opportunities provided by your organization and your participation in such activities or conferences.
05	How do you stay current with your profession? What sources provide you with your information?
	Section 2: Acquisition Decision Strategy
06	To what extent are acquisition activities planned? To what extent are they reactive or "spur of the moment"?
07	Who are the people who identify the need to start acquisition activities or an acquisition project?
08	Who are the people who decide to then actual begin acquisition activities? Who are the relevant decision makers in the acquisition process?
09	How often do you do you participate in acquisition activities?
10	Please define how you start acquisition process in your organization. Identify if the process is formalized or regular in any way. Identify the activities that occur in the early stages of acquisition.
11	Define what constitutes a good (desirable) IT component in your organization.
12	Are there any constraints placed upon the IT components you consider in acquisition, either from the organization or from your own criteria.
13	Are there any common attributes in the IT components that your acquire for your organization?
14	Describe the final stages of the acquisition process within your organization. Once you have selected the IT component to acquire what else must occur before moving into implementation? Who else is involved in this stage? Are any approvals required to acquire the component?
15	During the acquisition process what factors or people inhibit the process? What, if any, are the sources for resistance of frequently occurring problems in the acquisition process?
16	Once a product has been finally selected and approved what are the final steps to close out the acquisition process or prepare/bridge to implementation?
17	Reflect upon a time when an acquisition project failed. Why do you believe the acquisition was a failure? If the IT component did not meet the specified purposes, why do you believe this occurred?

TABLE 1 CONTINUED

#	Question
18	Reflecting upon the previous acquisition failure, please explain what was done to address the situation.
19	How have (or will you) address your acquisition process in order to limit or prevent a reoccurrence of a similar incident?
20	Who, including yourself, would decide that the acquisition process failed or that an acquired IT component was not meeting its intended purpose after implementation?
	Section 3: Management Style and Organizational Factors
21	Is your organization best described as hierarchically organized or are the boundaries more blurred in your organization?
22	How strong is ownership of (information) assets in your organization? Do you believe that appropriate information generally flows easily across organizational borders?
23	Describe the quality of communication between upper management and the rest of the company.
24	Describe the quality and style of communication between yourself and upper management and/or your direct superiors.
25	Describe the quality of communication between upper level decision makers and the IT department as a whole. Expand on the general interaction with upper management and their general interest in IT matters.
26	In terms of management, who are the relevant decision makers in the IT acquisition process? What is their level of interaction with the acquisition activities?
27	In your own opinion, would you say IT is important to the core operation of your organization? Do you believe that the organization's success is directly related to the quality of the IT systems and components?
28	Does upper management understand the impact and value of IT? To what extent is upper management involved or concerned about IT?
29	Do you believe that the selection of one IT component over another has any appreciable impact on the organization if they all options meet the core needs?
	Section 4: User Interaction
30	Describe the range of end-user computer literacy within your organization (where do most users rank on a continuum from novice to expert).
31	If among the end-user population, there are IT experts power-users do they attempt to provide input into the acquisition process? Do you appreciate this input and do you ever seek input specifically from this portion of the end-user population?
32	In terms of the acquisition process, what considerations are made regarding end-users and how do you determine these considerations? What methods do you use in order to evaluate user-acceptance of IT components?
33	In terms of technical support, do you find that users are willing to ask for help? Do end-users regularly communicate system issues to the IT staff?
34	Describe the level of acceptance for new IT components and systems in your organization. Do end-users understand the benefit or do they perceive system changes negatively.

TABLE 1 CONTINUED

#	Question
35	In terms of your acquisition projects, to what extent do you gather input during the acquisition process? After the completion of the acquisition process, to what extent do you gather feedback?
36	Describe the opportunities for end-user IT training in your organization.
37	In terms of your acquisition projects, how are users prepared for the introduction of new systems. How far in advance are they notified of a system change and at what point would training (if necessary) begin?
38	Was there ever a time that a user refused to accept a new IT component? What was done to address this issue?
	Section 5: Security Considerations in the Acquisition Process
39	Please describe management's understanding of IT security concerns and their interest in this issue.
40	In your organization, is security motivated by internal factors, external factors, or a combination? Please describe any sources of motivation to be concerned with IT security.
41	Are you aware of any laws or regulations which affect the operation of your IT systems?
42	Does your organization have formal security policies? If your organization does have formal policies, do the policies address any requirements of restrictions for components that may or may not be acquired?
43	Do either formal computer usage or end-user security policies exist? If these policies exist either formally or informally, to what extent are they monitored and enforced?
44	In terms of end-users and security, what security concerns exist in your organization? What tools or restrictions are in place to control end-user usage of IT systems?
45	Do you believe that the security policies are well written and can be understood by end-users? Are the users aware of the existence of the security policies and are they conscious of the related obligations and restrictions?
46	Do you yourself have any background or understanding of IT security? Describe your level of IT security competence. Are there other individuals besides yourself who are more focused on IT security and, if so, what role do these individuals play in IT acquisition. Do you believe that your organization would benefit from an increase in IT staff security training or personnel?
47	Describe the role that IT security plays in your acquisition projects. Is security an important consideration when you are considering new IT components or systems? In your opinion, what exactly does security mean in the context of IT component acquisition?
48	What measures beyond antivirus and firewalls do you consider fundamentally important to ensuring security of your IT systems? How does this philosophy affect software or system acquisition?
49	From your acquisition experience, can you share any insight or provide any suggestions to increase total IT system security or to limit a decrease in total IT system security? In terms of security, are there any issues or concerns of which you would advise others to be weary?
	Summary Question
50	Do you have any additional comments or ideas about the role of IT security in the acquisition process that was not explicitly addressed earlier in this interview?

6 Results

6.1 Scoring Criteria

In this interview study, two types of questions were asked, scored and informational. Some questions, or groups of questions taken together, are assigned an ordinal score S out of a possible score P on that question or question group of questions, with 0 being the lowest possible value and P being the highest value. The possible scores are based upon predefined criteria that vary depending on each question or question group. For a full explanation of the scoring criteria for each question, please see Appendix 10.3.

6.2 Participant Scores

The following table provides the participant scores. Participants in this study are protected under informed consent, and will only be identified by a pseudo-random seven digit number, that was assigned randomly to each participant.

TABLE 2: PARTICIPANT SCORES ON INTERVIEW QUESTIONS

Participant Id		2237953	3103141	3235679	3524075	5254450	5350582	5566166	5758430	5890968	6527486	7008146	8486532	9315314	9892105	9988237
	Possible Score P															
Q01	3	1	1	3	3	3	2	3	3	3	3	3	1	3	1	3
Q02	3	1	3	2	3	3	3	2	2	3	2	2	2	2	3	3
Q03	3	2	3	2	3	1	3	3	3	3	3	2	2	3	2	3
Q04	3	3	2	3	2	3	2	3	3	3	3	2	3	2	2	3
Q05	3	1	2	2	2	3	3	2	2	2	3	3	1	2	2	2
Q06	3	NA	1	2	1	2	3	3	2	3	3	2	2	2	3	3
Q07	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2
Q08	2	2	3	2	2	2	2	2	2	2	1	1	2	2	2	2
Q10	3	3	1	3	3	3	3	3	3	2	3	3	3	3	3	1
Q11 Q12 Q13	2	2	0	2	2	2	2	2	2	2	2	1	1	1	2	0
Q17 Q18 Q19	3	3	3	3	3	1	3	3	3	3	2	2	3	3	NA	3
Q22	2	2	2	2	2	2	0	2	1	0	1	2	2	1	1	2
Q23	2	1	2	2	1	2	1	NA	2	2	2	2	2	2	2	2
Q24	3	2	NA	2	NA	NA	1	1	3	NA	3	1	3	3	3	2
Q25	3	0	NA	2	NA	NA	0	1	3	NA	2	2	3	3	2	1
Q26	3	1	2	3	2	3	1	1	2	3	1	3	2	2	3	2
Q28	2	2	2	2	1	2	0	2	2	2	2	2	2	2	2	2
Q29	2	1	2	1	1	2	1	2	2	1	2	1	1	2	0	2
Q31	2	0	2	2	2	1	2	2	2	2	2	0	2	2	2	2
Q33	2	2	1	2	2	NA	2	2	2	2	2	2	2	2	2	2
Q34	2	2	1	2	2	2	0	2	1	2	1	2	1	0	0	1
Q35	2	1	1	2	2	2	2	2	2	2	1	0	2	1	2	0
Q39	2	1	1	2	2	2	2	2	0	2	1	2	1	2	2	2
Q42	3	1	0	3	1	1	3	3	1	2	1	1	0	2	3	2
Q43	3	3	1	3	3	2	3	2	1	3	2	1	0	3	3	2
Q45	3	3	0	3	3	3	3	2	3	3	1	1	0	3	3	2
Q47	2	1	0	2	2	1	2	2	1	2	1	0	2	1	1	1

6.3 Answer Summaries by Participant

Please see Appendix 10.4 for summaries of the participants' responses. These responses can help the reader to understand the scoring and gives a general impression of the participant's though process and environmental factors. Specific and relevant results will be discussed in later sections, the Appendix is included for completeness or if the reader is interested in performing additional analysis on this data. Conclusions and trends will also be discussed in-depth in later sections.

6.4 Security Scoring Analysis

The following simple statistics summarize the sample population's scores on the security related questions. These tables are used in later analysis for characterizing the sample and for drawing trends. A basic explanation for each statistic will be explained at face value, more in-depth analysis follows in later sections where appropriate.

6.4.1 Scoring on All Questions in the Security Section of the Interview

TABLE 3: AVERAGES AND STANDARD DEVIATION FOR ALL QUESTIONS IN THE SECURITY SECTION

Mean Score	**0.6769**
Median Score	0.6923
Standard Deviation	0.2761

Table 3 shows simple statistics for the security related questions of the interview. The mean average score is 0.68/1.00, which is relatively low and indicates that the organizations in the sample on average have mediocre security practices and attitudes. The median approximates the mean indicating that the scores are roughly divided around the mean. The large standard deviation indicates that there was a wide range of scores for this section of the interview.

6.4.2 Scoring on Security Questions Directly Addressing Security during Acquisition

TABLE 4: AVERAGE AND STANDARD DEVIATION ADDRESSING ROLE OF SECURITY IN ACQUISTION

Mean Score	**0.5733**
Median Score	0.6000
Standard Deviation	0.3011

Table 4 shows the simple statistics for the questions which security attitudes and practices specific to acquisition activities. The mean and median were lower than in security as a whole, which suggests that security is not widely considered during acquisition, this will be discussed in much greater detail in later sections. The large standard deviation also indicates there was a wide range of scores where there were some who scored very high and many who scored extremely poor.

6.5 Correlations Analysis

6.5.1 Correlations between various sections addressed in the Interview

TABLE 5: CORRELATION STATISTICS COMPARING THE VARIOUS SECTIONS OF THE INTERVIEW

		Experience	Decision Strategy	Management	Users	Security
Pearson Correlation	Experience	1	-.202	-.008	.273	.263
Sig. (2-tailed)		.	.470	.976	.325	.344
Pearson Correlation	Decision Strategy	-.202	1	-.527(*)	.520(*)	.559(*)
Sig. (2-tailed)		.470	.	.044	.047	.030
Pearson Correlation	Management	-.008	-.527(*)	1	-.003	-.468
Sig. (2-tailed)		.976	.044	.	.991	.078
Pearson Correlation	Users	.273	.520(*)	-.003	1	.401
Sig. (2-tailed)		.325	.047	.991	.	.138
Pearson Correlation	Security	.263	.559(*)	-.468	.401	1
Sig. (2-tailed)		.344	.030	.078	.138	.

N (Sample Size) = 15

** Correlation is significant at the 0.05 level (2-tailed).*

Table 5 shows the correlation values between various sections of the interview. The correlations are calculated using the participants' sum scores in each category. Pearson's correlation test statistics were calculated using an alpha level of $\alpha = .05$. The most important relationship in the table is the significant correlation between security and decision strategy; 31% of the variance in participants' security scores can be attributed to their quality scores for decision strategy. These correlations will be analyzed in greater detail where appropriate in the later sections which address the specific research questions original presented in Section 4.2.

6.5.2 Regression Results: Decision Strategy on Security

TABLE 6: REGRESSION MODEL FOR THE EFFECT OF DECISION STRATEGY ON SECURITY (SUMMARY)

R	R Square	Adjusted R Square	Sig.
.559(a)	.313	.260	.030(a)

(a) Predictors: (Constant), Decision Strategy

Table 6 provides a summary of the statistics related to the regression calculation. Since there is only one independent variable being considered the r-Value and significance are the same as in the above correlation calculations. The relationship is significant at the $\alpha = .05$ level. 31% of the variance in scores in the security section of the interview can be explained by the participant scores in the decision strategy section.

TABLE 7: REGRESSION MODEL FOR THE EFFECT OF DECISION STRATEGY ON SECURITY (EQUATION)

	Coefficients	Sig.
(Constant)	-.563	.293
Decision Strategy	1.410	.030

(a) Dependent Variable: Security

Table 7 provides the coefficient used to create the regression model equation and each coefficient's significance. For this relationship, the following model can be used to predict a participant's score on the security section of the interview based on the corresponding participant score on the decision strategy questions:

$$Security\ Score = (Decision\ Strategy\ Score) \times 1.41\ -\ 0.56$$

6.5.3 Regression Results: {User Interaction and Involvement, Management Attitudes, and Experience of Decision Maker and Organization} on Decision Making

TABLE 8: REGRESSION MODEL FOR THE EFFECT OF PREDICOTORS ON DECISION STRATEGY (SUMMARY)

R	R Square	Adjusted R Square	Sig.
.822(a)	.676	.588	.005(a)

(a) Predictors: (Constant), Users, Management, Experience

Table 8 provides a summary of the statistics related to the regression calculation. The independent variables (predictors) are the participant's scores in the user interaction and involvement, management attitudes, and experience sections of the interview. The relationship is significant at the $\alpha = .05$ level. 68% of the variance in scores in the decision strategy section of the interview can be explained by considering the impact of user interaction, management attitudes, and experience.

TABLE 9: REGRESSION MODEL FOR THE EFFECT OF PREDICOTORS ON DECISION STRATEGY (EQUATION)

	Coefficients	Sig.
(Constant)	1.061	.000
Decision Maker and Organization Experience	-.337	.059
Management Attitudes	-.310	.011
User Interaction and Involvement	.407	.005

(a) Dependent Variable: Decision Strategy

Table 9 provides the coefficient used to create the regression model equation and each coefficient's significance. The reader should note that management attitudes and user interaction are significant at the $\alpha = .05$ level, while experience is trending towards significant. For this relationship, the following model can be used to predict a participant's score on the security section of the interview based on the corresponding participant score on the decision strategy questions:

$$Decision\ Strategy\ Score = (Experience\ Score) \times -0.34 + (Management\ Score) \times -0.31 + (Users\ Score) \times -0.40 + 1.06$$

This page intentionally left blank.

7 Interpretations & Analysis

7.1 Research Question Q1

7.1.1 Question Statement

To what extent, if any, is security considered during the acquisition process?

7.1.2 Interpretations and Analysis

In this study, the fifth section of interview questions addressed security factors. Interview questions 42 and 47 specifically address the participant's attitudes and consideration of security during the acquisition phase of the system development lifecycle (SDLC). The participants' scores on the individual questions can be found in Section 6.2 and a statistical analysis of these questions can be found in Section 6.4.2.

Overall, security consideration was not high with a mean score of 0.57/1.00. Close to half of the participants (7/15) had a score below the average, while three participants scored 1.00/1.00. The lowest two scoring participants were #3103141 and #7008146; these participants also scored within the bottom quartile for all questions in the security consideration category and they scored in the bottom quartile when all question scores in the study were summed together. Only one-third of the participants' scores were above 0.80/1.00.

In general, even when participants mentioned that management was aware of security concerns or that they were concerned about security issues, there was no immediate concern for defining security requirements or considering security issues during the acquisition process. There is a significant correlation ($r=0.70$, $p=0.004$) between participants' scores on the questions about security during acquisition and the scores on the other questions in the security section which address security more broadly, suggesting that those who are more aware of security needs during acquisition will show more concern for security throughout the SDLC.

Three participants (#3235679, #5350582, #5566166) scored 1.00/1.00 on these questions. Participant #3235679 is the IT decision maker for a financial services organization which is subject to very strict compliance requirements, and thus he identified security and compliance as a major part of his position's daily requirements. Participant #5350582 does not work in a highly regulated industry, but in a previous role he was a security auditor. This participant also noted that a large percentage of his time is devoted to acquisition activities. Participant #5566166's organization was also subject to compliance, and noteworthy from other participants, this participant was highly aware of the many laws and regulations which impact security requirements for his organization.

The two lowest scoring participants (#3103141 and #7008146) generally did not believe they were at risk and did not see the value in analyzing security concerns. For interview question 47, participant #3103141 commented that security is not often talked about or addressed. The participant also noted that he believes consultants only talk about security as a fear-based motivation to buy a product. Participant #7008146 noted that he actively tries to encourage an environment with loose security and a high degree of open access; therefore it would be counterintuitive for him to look for aspects of a component which may increase security. Furthermore, this participant stated that he believes most

acquisitions would not likely have any significant security repercussions. He further described his organization's security policies as weak and useless.

Within the general sample population over half (8/15) of the participants scored 0/3 or 1/3 on interview question 42, which indicates that they either have no security policies, the security policies are weak, or the policies, if they exist, have no impact on security and/or would not be actively considered during the acquisition process. Less than on third (4/15) had security policies or rules which influence and affect whether a component could or could not be acquired. The remainder of the participants in the sample did not have an explicit relationship between security policy and acquisition; however, they were aware of their security policies and requirement, and they noted that they do consider security during acquisition.

While interview question 42 evaluated security in regards to the acquisition procedures, interview question 47 evaluated the participants' attitude towards security outside of actual requirements or policies. In this sample, over half (9/15) of the participants indicated that security was not considered at all or that when it was considered it was not an important factor in the decision making process. The remaining participants in the sample (6/15) did indicate that security was an important consideration and that their impression of a component's security quality would actively affect their choice to acquire. For example, participant #9892105 indicated that security was only important to the acquisition decision if it was outlined in the business case provided by the business unit, and that absent of these requirements in the business case, there would be no consideration. Other participants noted that security was considered, but not important because they believed there was a low probability of attack. Common justifications cited included perceptions that they were unlikely targets or that there already existed significant technological controls (e.g., firewalls) and measures for security so that security did not need to be evaluated on a per-component basis. Those who did believe that security was an important consideration during acquisition expressed concerns for the effect new components would have on the existing security controls as well as changes to how users would interact with the system. Those who scored higher on this question generally understood that the introduction of a new component would result in other systemic changes – both to technology as well as policies, processes, and procedures.

Small businesses typically do not perceive a high level of outside threat; this perception, however, can lead to a lower consideration of security. In addition, this indicates that many small businesses have a very narrow understanding and definition of security. In this study, very few participants identified business continuity and disaster recovery related security concerns. Perimeter and boundary security, with which participants were most familiar, have little effect on protection and mitigation of threats from natural disasters. In addition, very few participants identified the possibility of insider threat and stated high skepticism about the possibility of insider attacks when directly questioned.

With a narrow understanding of threats and limited definitions of security requirements, it is easy for a decision maker to accept, and even foster, seemingly anti-security attitudes and practices. As a result, of limited consideration of security and unrealistic perceptions of risk, most decision makers did not demonstrate an appropriate, and in some cases not even minimal, interest in security and it was often a low priority during acquisition and in general throughout the system lifecycle. In reality, small businesses

are lucrative targets for external attackers because their security controls are weak and the IT staff (if any) will likely not possess the security background, time, and resources to actively stop or notice an attack. While an attack on a larger organization may have a higher possible reward, the risk of attacking a small business is much lower. In reality according to a study by Ryan [12], small businesses are not any less likely to be attacked compared to larger businesses.

Those small businesses which do not properly address security during acquisition are more likely to be successfully attacked. This applies to both internal and external attacks. Some participants described their IT environment as fairly open with minimal (if any) restrictions. As a result, it may be very difficult or impossible to trace the route of information leakage, information exposure, or system vulnerability exploitation. As security becomes a more popular industry buzz word and regulations increase companies which do not consider security during acquisition will face difficult challenges moving from an open environment to a secure environment. Because security is not considered an important feature, components may need to be replaced that fail to provide adequate data and system protection. This can result to disruption of daily business activities and processes because systems must be taken offline temporarily or replaced. In addition, the time spent on the initial acquisition will be lost since the process will need to be repeated when new security criteria are added. Because of the relative lack of interest in security, it will require a large amount of retraining or outside assistance to make these decisions and implement the required security.

Conversely, small businesses that have a higher consideration of security in the acquisition process tend to also have a better understanding of security in general. In this study those who scored highest on interview question 47 indicated that they understood the impact of their acquisition decisions on both systems and end-users. Because they are more aware of the impact of their decisions, they are less likely to choose a component which will later need to be replaced because of lack of functionality, security, or user acceptance. When an organization has formalized policies regarding acceptable security criteria for acquisition it indicates that decision makers have thoroughly considered the impact of security on the operation of its core business. By employing a proactive strategy the organization proves that it has evaluated possible threat scenarios and can also meet regulatory compliance. While not directly a security threat, insufficient compliance with regulations can result in large fines or the stoppage of business; thus, it is important to ensure that all systems meet compliance in order for a business to operate most efficiently. Formal guidelines for acquisition, security-wise and in general, can help reduce the likelihood of selecting a component which is not compatible with the company's existing infrastructure, procedures, and processes.

7.2 Research Question Q2

7.2.1 Question Statement

To what extent, if any, is security considered by the participants and their corresponding organization throughout the system lifecycle? What is the extent of security awareness and understanding?

7.2.2 Interpretations and Analysis

In this research study, interview section 5 (interview questions 39-49) addressed security practices and attitudes of the study participants and their perceptions of security attitudes throughout their organization. While the decision makers are ultimately responsible for the final component selection, their decision making processes may be impacted by the attitudes and practices of others. In this study, two other broad groups of influencers were identified. The first group was members of upper/executive management, who set organizational policy and may approve a decision maker's selection. The second group consisted of end-users because they often interact directly with IT systems and components. The participants scores on the individual questions can be found in Section 6.2 and a statistical analysis of these questions can be found in section 6.4.1.

Overall, organizational security awareness and understanding was not high in this sample with a mean score of 0.68/1.00 in this section of the interview. One third (5/15) of the participants had a score below the mean; however, almost one-third (4/15) had a score above 0.90/1.00. Two participants scored 1.000/1.000 (#3235679 and #5350582). The two lowest scoring participants (#3103141 and #8486532) also were in the lowest quartile for total interview score.

Interview question 39 asked the participant to respond on management's attitude towards security and their understanding of security concerns that may impact the business. Only one participant responded that management had no interest in security, while four indicated that management was aware of security concerns but it was not of prime importance. The remainder of the sample (10/15) did indicate that management was aware of IT security issues and gave such security consideration sufficient attention. The participant (#5758430) who responded that management does not think about security noted that management prefers as much openness as possible and that increased security restrictions and practices anger members of management. However, the participant did personally believe that security is important and therefore he limits management's involvement in security issues when possible. In this participant's organization, management's attitudes may be the cause of paltry security policies and may limit necessary funding for security related projects.

Interview questions 40 and 41 asked participants to explain internal and external motivations for security, including laws and regulations. The most common motivations identified by participants were external, specifically regulatory compliance or external-client demands. The external motivators seemed to be very strong driving factors with one participant noting that management would probably not care about IT security in the absence of compliance requirements. Interestingly, client requirements were a much stronger motivator than direct regulatory compliance. This may be because clients usually specify narrower requirements than regulatory laws. Few participants expressed internal (from within the organization) motivations for security. Internal motivators identified usually fell into the following broad

categories: due diligence or IT team pride; protecting corporate intellectual property; and protecting customers. Only 6/15 participants identified internal motivations, while all expect one participant identified external motivations.

In the United States, regulatory compliance is complicated and as evidence by this study, very few participants were certain of all laws with which they were required to comply. One participant noted that there is no clearinghouse or agent who tells an organization what regulations may affect it. Some participants did not believe any laws affected them either because of their size or their industry (e.g., not medical or financial). For example, participant #3103141 believed that his organization was too small and that because of the type of business they conducted, that no sensitive customer information was held by the organization. However, in the same statement he indicated that they do maintain customer contact and billing information, which should be considered sensitive information. When asked if the organization only performed cash transactions, the participant indicated that the organization also processed credit-card transactions. The participant was in a senior management position, but was unaware of his organization's obligations under Payment Card Industry (PCI) Compliance. Regardless of company size or number of transactions performed, all processors are required to comply [13]. Interestingly, some organizations chose to follow regulatory guidelines for regulations to which they were not required to comply; participants explained that customers associate certain regulations with them because of their industry, and thus they take measures to comply in order to increase their legitimacy with clients.

Interview questions 43-45 were concerned with the relationship between end-users and security concerns. In general, users are adverse to security policies and technical controls because they impede one's ability to complete a task in the most straightforward and simple manner. Users represent two major types of threats to IT systems. The first threat type is disruption of normal service, which means that a user's action may cause data to be lost or cause a system to fail. The second type of threat is that a user may (unintentionally or maliciously) access and expose confidential data or introduce unknown systems or components into the IT infrastructure whose affect on the system is unknown and unanticipated. As a result, it is important to take efforts to mitigate such activities through policy, technical controls, and monitoring in order to ensure that the IT systems continue to operate normally and that sensitive organization and customer information is protected.

In response to interview question 43, almost half (7/15) of the participants demonstrated that they had security policies which specifically addressed end-user usage of IT systems and that there was sufficient oversight, monitoring, and enforcement of these policies. The remainder of the participants in the sample either had weakly defined policies (4/15) or only very informal policies and ideas about end user security (3/15). Only one participant indicated that there were no end-user security policies and that end-users were simply trusted to do the right thing without guidance. Complementing question 43, interview question 45 asked participants if they felt that users understood the existing security policies and controls and additionally if they believed end-users understood their obligations in regards to IT security. The majority (9/15) of the participants believed that the users understood the policies, that they were well written, and that users tended to follow the policies. Some participants indicated that employees were required to sign agreements of understanding as a condition or employment. Only two

participants clearly indicated that users were highly aware and truly understood their needs. Some of those who indicated that users did not often follow, that users were not aware, or that any such policies were weak or non-existent (6/10) noted that they wanted to improve user training and awareness, but were limited by resources or organizational attitudes. There were some participants who believed that any such policies or user controls were unnecessary or unwanted because they trusted their users and/or they promoted a high level of open access. However, this is a flawed perspective because access-control systems and policies do not prevent information sharing, they merely control it.

Interview questions 44 and 48 address the specific controls and techniques used to monitor and control user access. In this study, the participants seemed to have a basic grasp on perimeter security controls, such as firewalls, as well as simple anti-virus protections. The next most common form of security controls employed were encryption of devices and transmissions, though this was not used by all organizations in this study. The use of granular access controls such as role-based access were the next common security practice; yet, some participants reported that they avoid such mechanisms in order to provide more open access and cross-role information sharing, with some claiming that implementation would be too difficult.

In this sample, the main focus was on protection at the system level with application level and data level protections being much less common. Some participants noted that at least some of their data did not require any protection. When participants made this assertion it often seemed to be based upon their own opinion, not that of management or the business unit which owned the data. Even if data is in the public domain it should still be controlled through role based access, but with global access. Some participants commented that it was very difficult or impossible to prevent users from accidently transmitting data in unapproved forms such as email. However, this may be limited with technical controls, policy, and reminders built into the application.

While all users identified at least some minimal level of controls, less than one-third (4/15) of participants identified using accounting and auditing procedures or practices. Auditing, whether internal or external, was not very common in the sample nor was review of logs or system reports. Some participants had managed (outsourced) security solutions and were not aware of any details about the protections and how they functioned; one participant noted that the company provides reports, but that he does not regularly review or monitor these status updates. It was assumed that the provider would take appropriate action. In general, it was clear that these organizations had varying levels of control and protections; however, it is not prudent to score them on the level or types of controls for two reasons. First, every organization has different needs and levels of acceptable risk. Furthermore, without the proper internal background or understanding it is not guaranteed that the organization properly configured and continues to maintain these controls or that they could sufficiently comprehend or evaluate managed provider reports.

While the above questions have addressed influence and attitudes, it is also important to evaluate the experience level specific to IT security concepts. It is not requisite that the decision maker is an expert per se; however, there must be an internal resource or accessible and security-minded consultant who can provide qualified input from the security perspective. In interview question 45 the participant was

asked to explain their own security education and experience as well other sources of security information from within the organization or through consultants.

Almost half (7/15) of the participants indicated that they did not have any significant training or background in security and that they did not retain anyone internally or externally whose job role had a significant focus on security. Many of the participants in this grouping did not believe that they needed to increase their security background or training. Furthermore, they did not believe that it was necessary to devote their own time or anyone else's time to IT security related activities for any significant amount of time. There were a few individuals who had a background in security or had a previous role in the IT security field. While those individuals with experience demonstrated a greater understanding of security, prior experience was not an indicator of increased security consciousness and consideration. Participant #8486532 has a previous role as a security administrator, yet he actively encouraged an open environment and had only minimal concerns related to IT security overall. Those participants which indicated they frequently relied upon external consultants for their IT needs noted that their consultants did not often offer security solutions, with one participant, #3103141 expressing that he believed his consultants only mentioned security solutions as a scare tactic to make a sale.

For the most part the participants in this study demonstrated that there was some level of security consideration in place. However, security measures were often limited to perimeter protection and system level access controls. In the sample population, very few participants gave the impression that they had truly thought about their organization's specific security needs as opposed to providing "standard" security controls. This was apparent by the frequent anti-security attitudes demonstrated that included blindly trusting users and encouraging an open-access environment. While security was on most participants' radars, most organizations did not devote significant time or resources to security. This cannot be attributed to the size of the company as there was no trend correlating company size to security awareness and understanding. Rather it seems that most organizations do not have an objective view of their security needs that includes identification of possible threats and their relative cost of exploitation versus cost to mitigate or prevent. Without an understanding or background of IT security needs and objectives it is impossible to objectively or empirical claim that an organization's level of security is sufficient. Simply, an organization is only secure if it is prepared to accept the exploit of all vulnerabilities it has not already mitigated. The above findings suggest that the average small business is ill-prepared to face security challenges.

7.3 Research Question Q4

7.3.1 Question Statement

Does the relative quality of decision makers' decision strategies significantly predict the level of security awareness and understanding demonstrated by the participants and their organization?

7.3.2 Interpretations and Analysis

In this study the interviews questions in section 2 addressed the quality of the decision makers' decision strategy and the questions in section 5 addressed the level of security awareness and understanding. Each participant received a score out of all applicable questions for each section. The results of each scored question or question group can be found in Section 6.2. These scores were then statistically analyzed using regression testing and correlation studies to investigate the relationships between participants' performance in each category. The results of these statistical analyses can be found in Section 6.5.1 and Section 6.5.2.

The results of this study suggest that there is a significant predictive relationship ($Security\ Score = (Decision\ Strategy\ Score) \times 1.41\ -\ 0.56$) between a decision maker's decision strategy quality and her level of security awareness and understanding. In addition, there is a significant correlation between participants' scores in these two sections of the interviews (r=0.56, p=0.03).

In Section 7.1 and Section 7.2, it was shown that the results of this study suggest that small businesses do not invest significant time or resources into security during acquisition or security more broadly throughout the SDLC. This research question therefore evaluates a possible explanation for the low level of security consideration and awareness in the small businesses. By increasing proactive consideration of security factors a decision maker can mitigate or prepare to accept a security violation in the future. The costs to make changes to an information system after acquisition are high because once a component is implemented other components and processes may have already become dependent. Therefore, effective acquisition decision strategy must necessarily entail an evaluation of future needs and requirements. As organizations become more aware of security issues and place an increased emphasis on increasing security measures, they are apt to investigate what changes can be made in order to reach this goal. Because of the correlation between security awareness and decision strategy quality, organizations wishing to improve or establish their security programs should start be evaluating and improving their acquisition decision strategies.

In this study, some participants could not adequately define how they go about their acquisition process or what qualities and characteristics are desired in a component. Without some common criteria, decisions are less likely to consider the impact on the total system or on the business case in question. While a formal plan or worksheet is not required, one should strive to use consistent, objective criteria. An acquisition decision strategy should include an appropriate research effort using qualified and objective sources, where the information comes from a qualified professional or technical researcher. A solution or set of options should then be evaluated for functionality, effect on organizational processes, and effect on other IT systems. This may include internal validation and testing as well case study analysis and proof of concept from the solution provider. Lastly, beyond the component itself it is necessary to evaluate the solution provider, solution vendor, and all human resources to ensure that

problems will be addressed in a satisfactory manner during implementation and for long-term support if desired.

In addition, the acquisition phase is the least costly place to introduce new security measures because changes to systems and processes are already imminent. Security is often difficult or impossible to implement after a component has been integrated into an organization's IT infrastructure. As a result, even if an organization desires to improve security the possible options may be limited especially if the acquisition decision was made hastily and was not performed with proper evaluation and forward-thinking consideration. A proactive approach to security begins in the acquisition phase. If a decision maker is not considering more mundane details during acquisition, it is very unlikely that they would consider more complex criteria such as security considerations. It is therefore not surprising to see the significant positive correlation between participants' decision making quality and their level of security awareness and understanding.

7.4 Research Question Q3

7.4.1 Question Statement

Does the relative performance of decision makers (and their organizations) in the areas of experience, management attitudes, and user interaction significantly predict quality of decision making?

7.4.2 Interpretations and Analysis

In this study the questions in interview Sections 1, 3, and 4 addressed the relative experience, management attitudes, and user interaction levels of the participants and their corresponding organizations. Section 2 of the interview addressed the quality of the participants' decision making in regards to acquisition. Each participant received a score out of all applicable questions for each section. The results of each scored question or question group can be found in Section 4.3. These scores were then statistically analyzed using regression testing to investigate if there was a significant relationship between experience, management attitudes, and user interaction and the participant's quality of decision making. The results of the correlation analysis can be found in Section 6.5.3.

The results of the participants scores and the regression analysis in this study suggest that a decision maker's quality of decision making can be predicted by her degree of experience, the attitudes of management within her organization, and the relationship between end-users and the members of the IT organization. The most influential category is the participant's interaction with end users (For a full breakdown and the regression equation refer to Section 6.5.3). There is also a significant correlation between participant's scores in the decision strategy section and the end-user interaction categories as calculated in Section 6.5.1, while the scores in the experience and management categories were not found to be significant in this study.

It has already been suggested above that small businesses do not demonstrate a high level of security awareness and that there is a connection between security awareness and understanding and the quality of acquisition decision making. Continuing the regress argument, in order to improve acquisition an organization may be interested in factors which will lead to more successful acquisitions and acquisitions strategies. In this study, there was found to be a significant correlation between decision strategy and the quality of end-user interaction and end-user involvement in the acquisition process. To a lesser degree management attitudes and experience also affected acquisition decision quality, which surprisingly have a negative effect on decision quality. The findings in this research study do not suggest any reasons to explain this counter-intuitive relationship.

The regression model suggests that one way to improve the quality of acquisition decision making is through increased end-user interaction and involvement. When decision makers take into account the business users of components, there will be a stronger alignment between technical needs and business objectives. Because end-users are the ones who are propelling the day-to-day operations of business, new components should best enable them to complete their tasks (where best is defined by the goals of management and possibly efficiency, creativity, or some other goal). Without user involvement, IT decision makers may not understand how certain features or processes can positively or negatively impact the end-user ability to complete tasks. In addition, it is often desirable to have a business user of

the component serve as a subject matter expert and liaison to the IT support group. The establishment of such an individual can help translate between business problems and technical solutions.

User involvement can also have an impact on security and security consideration. Security should be driven by the business case. Information or other assets have some value or legal requirement to be protected. Once a value on an asset is established an IT decision maker can decide how much effort should be invested in protecting that asset. With this knowledge, security is better aligned with strategic value as opposed to security simply for the *sake of being more secure*. While it may fall to the IT decision maker to asses this value, in most cases the IT staff are only asset custodians and not asset owners. With user involvement, asset value and related protection strategies can be assessed with a more solid foundation. By nature end-users are interested in completing tasks in the most straight forward manner. In almost all cases, security complicates any task and as a result end-user may suffer from reduced productivity or may circumvent security measures. By increasing end-user involvement, end-user are more aware of the value security brings compared to its inconvenience. Without interacting with end-users, it may be very difficult for a decision maker to determine how security controls can have the least impact on the execution of business tasks.

This page intentionally left blank.

8 Discussion

8.1 How key findings compare or contrast with previous work

In the current body of research, too great an emphasis has been placed upon poor end-user practices in regards to security. This implied that sufficient security programs existed, that they were actively enforced, and that users were aware of their security obligations. In the case of small-to-medium sized business, this research suggests that for the most part there are often no programs or policies, and in some cases very limited security controls in place. Instead, the research findings herein contain many examples demonstrating a lack of interest or an outright resistance to practical or appropriate security measures. It is highly inappropriate to place the blame for poor user behavior on the users themselves when those who are responsible for maintaining and implementing security have put forth no effort. As the custodians of data and systems, it is the IT team and IT decision makers' responsibility to mitigate poor user behavior or to make it too costly and difficult to circumvent security mechanisms or to practice insecure data handling procedures. When an organization does not have firm security policies or does not actively enforce compliance there is a little incentive for the end-users to take security measure into their own hands.

As suggested by previous research cited in the literature review, user involvement, education, and control are key to security. Without proper policies or education users may have no interest in security. However, by involving users in the acquisition phase there is a better understanding of the business process for which the component being acquired will be utilized. As a result, IT decision makers will be more aware of how data is shared, stored, and transferred. With this knowledge, appropriate security mechanisms can be selected to facilitate proper access and auditing to ensure that the users will not circumvent security guidelines in order to complete business tasks. In addition, this research found that when users were more involved in the acquisition process there was a higher rate of communication, and in some cases there was an establishment of a subject matter expert within the business organization. This individual could act as a liaison for support and may also be the business owner of the application. Previous research had indicated that poor communication leads to confusion and decreases security. The current research suggests that increased communication between end-users, IT decision makers, and vendors increases the quality of acquisition. Increased communication and research increases one's acquisition quality score and those with a higher quality score are more likely to consider security as criteria during acquisition. As a result, the research suggests that the opposite is also true – that an increase in communication can lead to better security.

8.2 Implications of findings

The findings of this study suggest that IT decision makers are in fact the lock in the IT security chain. Businesses which have poor security practices and programs are often simply not interested in security or they have not adopted a proactive approach to security. A high level of security awareness and consideration overall is correlated with an acquisition decision strategy which is based upon thorough, objective research and systemic impact analysis. IT decision makers who understand how to evaluate a component's technical and business needs will more likely choose systems which provide the most system-wide value. Conversely, IT decision makers who do not put sufficient consideration into

acquisition have very little chance of identifying security need proactively and therefore will not be able to provide the appropriate or desired level of security for their organization.

For many years, security has had little, if any, importance in IT decision making. However, because of ever-increasing government and non-government regulation, as well as customer expectations, security is becoming hard to ignore. While many small businesses may not believe they are at risk of attack, they may lose competitive advantage or suffer regulatory punishments for failing to meet security requirements. As a result, it will become increasingly important for organizations to secure their IT security chains. To meet both internal and external security demands, it will become increasingly important for IT decision makers to make thorough analyses of components which are added to an organization's IT infrastructure. Quality decisions are not dictated by experience, as many may presume, but by perseverance and due diligence. When decision makers use objective, qualified input in their decision making process and carefully consider business objectives and needs they can ensure acquisition success. In this study, some decision makers could identify common criteria and methodologies used in their acquisition process. For these individuals, it would be simple to add in one more set of criteria or to create an appropriate policy addressing these issues. However, in other organizations there were relatively few policies or guiding criteria. As a result, such organizations carry out acquisition and security haphazardly and inconsistently.

Therefore, this research suggests that in order to meet increasing security demands and requirements it is necessary for IT decision makers to become experts in the acquisition process itself. Success in acquisition is highly dependent upon awareness, and not (as suggested by these findings) expertise or even managerial support. A decision maker must be aware of both technical and business requirements for any given component and how various solutions will impact both technical system interactions and business processes. These qualities are also paramount to any security program. In security is important to understand what constitutes an asset, what is the value of that asset, and what, if any, are the appropriate or necessary steps to mitigate that risk. During acquisition, IT decision makers who are performing a thorough analysis will be asking many of the same questions which would be of interest to a security implementer. This valuable information includes what systems exist, what data is on these systems, and which individuals or other systems interact with the data on that system.

Failure to ensure quality acquisition in an organization will not negate increasing pressure for improved security. Instead, organizations with poor acquisition practices will find themselves hastily implementing unplanned or untested solutions to provide the required level of security. In the case of regulatory noncompliance, business operations may be halted entirely until the proper changes are made. At that point, the financial costs will be very high and there may be insufficient internally understanding from a combined business and technical perspective in order to find an expedient solution to the security requirements. In addition, there is also the increased likelihood of attack. Because the acquisition efforts did not likely take into account the impact on processes or other systems, there is an increased likelihood that new vulnerabilities were created either technical or through user circumvention. If security was not considered at the time of acquisition, it would be costly and difficult, if not impossible, to introduce security controls after implementation. It is also unlikely that the motivation to address these concerns would later materialize.

8.2.1 For the theory or conceptual model described in the Introduction.

The study suggests that the conceptual model presented earlier has both strengths and weaknesses. The research suggests that there is in fact a significant correlation and relationship between the depth and quality of acquisition in an organization and the level of security awareness and understanding. In addition, those participants who made security an integral part of their acquisition activities demonstrated a higher level security awareness, were more familiar with their own organization's security needs, and better understood security technology and terminology. The results of the study did not provide sufficient input to validate or invalidate whether or not there was a relationship between the quality of acquisition and reduction in component failure or defect. However, the research does suggest that those with a more thorough and higher quality acquisition strategy used strategies to mitigate future problems whereas those with weaker strategies did not often consider the possibility of component failure or the component failing to properly provide the functionality expected. End-user interaction and involvement in the acquisition process had the greatest positive influence on the quality of acquisition whereas the data suggests that the quality of acquisition was not improved by increased technical and organization experience or by increased involvement and/or support for management. The research does not provide conclusive evidence to explain the effect of management factors or experience directly on the level of security awareness and implementation.

8.2.2 For future research

In this research, the findings suggest that there is a relationship between the quality of acquisition and the level of security awareness and understanding in an organization. The research further suggests that those who have a higher quality of acquisition in general are more apt to include security consideration in their acquisition criteria. In this research, the effect of experience, management, and end-users were used in order to address the quality of acquisition. In future research, a more comprehensive study of the effect of the above three factors directly on security and the possible relationship would enhance the ability to predict acquisition success and suggest starting points for organizations to drive improvements in their security programs. Further research efforts are also needed to explain why experience and management attitudes have a negative effect on the quality of acquisition strategy.

This page is intentionally left blank

9 Bibliography

1. *Computer security impaired by legitimate users.* **Besnard, Denis and Arief, Budi.** 3, s.l. : Elsevier Ltd., May 2004, Computers & Security, Vol. 29, pp. 253-264. Doi: 10.1016/j.cose.2003.09.002.

2. **Gross, Joshu B. and Rosson, Mary Beth.** *Looking for Trouble: Understanding End-User Security Management.* College of Information Sciences and Technology, The Pennsylvania State University. s.l. : ACM, 2007. ISBN:1-59593-635-6.

3. *Security in the wild: user strategies for managing security as an everyday, practical problem.* **Dourish, Paul, et al.** 6, November 2004, Personal and Ubiquitous Computing, Vol. 8, pp. 391-401. DOI: 10.1007/s00779-004-0308-5.

4. **Dourish, Paul, Delgado de la Flor, Jessica and Joseph, Melissa.** *Security as a Practical Problem: Some Preliminary Observations of Everyday Mental Models.* School of Information and Computer Science, University of California, Irvine. Irvine, CA : s.n., 2003.

5. *Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security.* **Sasse, M A, Brostoff, S and Weirich, D.** 3, s.l. : Springer Netherlands, July 2001, BT Technology Journal, Vol. 19, pp. 122-131. DOI: 10.1023/A:1011902718709.

6. *An Integrative Model of Organizational Trust.* **Mayer, Roger C, Davis, James H. and Schoorman, F. David.** 3, s.l. : Academy of Management, 1995, The Academy of Management Review, Vol. 20. doi:10.2307/258792.

7. **Pichler, Rufus.** *Trust And Reliance - Enforcement And Compliance: Enhancing Consumer Confidence In The Electronic Marketplace.* STANFORD PROGRAM IN INTERNATIONAL LEGAL STUDIES, Stanford University. 2000. http://www.law.stanford.edu/library/special/rufus.thesis.pdf.

8. *REFEREE: trust management for Web applications.* **Chu, Yang-Hua, et al.** 8-13, s.l. : Elsevier Science B.V., 1997, omputer Networks and ISDN Systems, Vol. 29, pp. 953-964. Doi:10.1016/S0169-7552(97)00009-3.

9. **Smith, J. Eric.** Major Open Source code repository hacked for months, says FSF. *Geek.com.* [Online] August 14, 2003. [Cited: September 29, 2008.] http://www.geek.com/articles/news/major-open-source-code-repository-hacked-for-months-says-fsf-20030814.

10. *How good is good enough?: an ethical analysis of software construction and use.* **Collins, W. Robert, et al.** 1, s.l. : ACM, January 1994, Communications of the ACM, Vol. 37, pp. 81-91. ISSN:0001-0782.

11. *Software security in an Internet world: an executive summary.* **Shimeall, Timothy J and McDermott, John J.** 4, s.l. : IEEE, July/August 1999, Software, Vol. 16, pp. 58-61. DOI: 10.1109/52.776950.

12. **Ryan, Julie J. C. H.** *Information Security Practices and Experiences in Small Businesses.* Harvard. 2001. Dissertation Incidental Paper. http://www.pirp.harvard.edu/pubs/pdf-blurb.asp?id=493.

13. **Control Scan.** PCI FAQs And MYTHS. *PCI Compliance Guide.* [Online] [Cited: December 25, 2009.] http://www.pcicomplianceguide.org/pcifaqs.php#2.

14. *Taking the Mystery out of Intuitive Decision Making.* **Burke, Lisa A. and Miller, Monica K.** 4, s.l. : Academy of Management, 1993, The Academy of Management Executive, Vol. 13, pp. 91-99. http://www.jstor.org/stable/4165589.

15. *The Expert Mind.* **Ross, Philip E.** 2, August 2006, Scientific American, Vol. 295, pp. 64-71.

16. *Taking stock of naturalistic decision making.* **Lipshitz, Raanan, et al.** 5, 20001, Journal of Behavioral Decision Making, Vol. 14, pp. 331-352. http://dx.doi.org/10.1002/bdm.381. ISSNL: 1099-0771.

17. **McKenzie, Craig R. M.** Hypothesis Testing and Evaluation. [ed.] D. K. Koehler and N Harvey. *Blackwell Handbook of Judgment and Decision Making.* s.l. : Wiley-Blackwell, 2007.

18. **Gigerenzer, Gerd.** Fast and Frugal Heuristics. [ed.] D. K. Koehler and N. Harvey. *Blackwell Handbook of Judgment and Decision Making.* s.l. : Wiley-Blackwell, 2007, 4.

19. *A Synthesis of Research on Requirements Analysis and Knowledge Acquisition Techniques.* **Byrd, Terry Anthony, Cossick, Kathy L. and Zmud, Robert W.** 1, s.l. : Management Information Systems Research Center, University of Minnesota, March 1992, MIS Quarterly, Vol. 16, pp. 117-138. http://www.jstor.org/stable/249704.

20. **Gallaher, M. P., Link, A. N. and Row, B. R.** *Cyber Security: Economic Stratagies and Public Policy Alternatives.* Northampton : Edward Elgar, 2008.

21. **Silver, Mark S., Markus, M. Lynne and Beath, Cynthia Mathis.** The IT Interaction Model: An Overview. [Online] 1995. [Cited: September 9, 2009.] http://www.bnet.fordham.edu/public/ics/msilver/itimhdo.htm.

22. **Stoneburner, Gary, Goguen, Alice and Feringa, Alexis.** *Risk Management Guide for Information Technology Systems.* National Institute of Standards and Technology, U.S. Department of Commerce. 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. SP 800-30.

23. **Novak, Mark.** Extending SDL: Documenting And Evaluating The Security Guarantees Of Your Apps. *Microsoft Developer Network.* [Online] Microsoft, November 2006. http://msdn.microsoft.com/en-us/magazine/cc163522.aspx.

24. *The psychology of security.* **West, Ryan.** 4, New York, NY, USA : ACM, 2008, Communications of the ACM, Vol. 51, pp. 34-40. http://doi.acm.org/10.1145/1330311.1330320. ISSN: 0001-0782.

25. *Aligning the information security policy with the strategic information systems plan.* **Doherty, Neil F. and Fulford, Heather.** 1, February 2006, Computers & Security, Vol. 25, pp. 55-63.

26. **Roese, Neal K.** Twisted Pair: Counterfactual Thinking and the Hindsigh Bias. [ed.] D. K. Koehler and N. Harvey. *lackwell Handbook of Judgment and Decision Making.* s.l. : Wilyey-Blackwell, 2007.

27. *Coping with Systems Risk: Security Planning Models for Management Decision Making.* **Straub, Detmar W. and Welke, Richard J.** 4, s.l. : Management Information Systems Research Center, University of Minnesota, December 1998, MIS Quarterly, Vol. 22, pp. 441-469. http://www.jstor.org/stable/249551.

28. *The effect of user involvement on system success: a contingency approach.* **Tait, Peter and Vessey, Iris.** 1, Minneapolis, MN, USA : Society for Information Management and The Management Information Systems Research Center, 1988, MIS Quarterly, Vol. 12, pp. 91-108. ISSN: 0276-7783.

29. *HUMAN-COMPUTER INTERACTION: Psychology as a Science of Design.* **Carroll, John M.** 1997, Annual Review of Psychology, Vol. 48, pp. 61-63.

30. *User Involvement and MIS Success: A Review of Research.* **Ives, Blake and Olson, Margrethe H.** 5, s.l. : INFORMS, May 1984, Management Science, Vol. 30, pp. 586-603 . http://www.jstor.org/stable/2631374.

31. **West, Ryan, et al.** The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisisons. [ed.] Manish Gupta and Raj Sharman. *Social and Human Elements of Information Security: Emerging Trends and Countermeasures.* 2008, 4.

32. **Payne, Shirley.** An Ongoing Conversation with the Boss About Security. [Presentation]. Darmouth : Securing the eCampus 2009: Building a Culture of Information Security in an Academic Institution, 2009. http://www.dartmouth.edu/comp/about/conferences/security/speaker_presentations/Payne_eCampus 2008.pdf.

33. *Information systems security issues and decisions for small businesses: An empirical examination.* **Gupta, Atul and Hammond, Rex.** 4, s.l. : Emerald Group Publishing Limited, 2008, Information Management & Computer Security, Vol. 13, pp. 297-310. ISSN: 0968-5227.

34. *A conceptual foundation for organizational information security awareness.* **Siponen, Mikko T.** 1, 2000, Information Management & Computer Security, Vol. 8, pp. 31-41.

35. *Techniques for trusted software engineering.* **Devanbu, Premkumar T., Fong, Philip W-L and Stubblebine, Stuart G.** Washington, DC, USA : IEEE Computer Society, 1998. ICSE '98: Proceedings of the 20th international conference on Software engineering. pp. 126-135. ISBN: 0-8186-8368-6.

36. *A New Paradigm for Adding Security Into IS Development Methods.* **Siponen, Mikko T. and Baskerville, Richard.** Deventer, The Netherlands, The Netherlands : Kluwer, B.V., 2001. Proceedings of the IFIP TC11 WG11.1/WG11.2 Eigth Annual Working Conference on Advances in Information Security Management & Small Systems Security. pp. 99--112. ISBN: 0-7923-7506-8.

37. **Greenemeier, Larry.** T.J. Maxx Parent Company Data Theft Is The Worst Ever. *Information Week.* [Online] March 29, 2007. [Cited: 12 25, 2009.] http://www.informationweek.com/news/security/showArticle.jhtml?articleID=198701100.

38. *Explaining the Role of User Participation in Information System Use.* **Hartwick, John and Barki, Henri.** 4, s.l. : INFORMS, April 1994, Management Science, Vol. 40, pp. 440-465 . http://www.jstor.org/stable/2632752.

39. *Restoring a Sense of Control during Implementation: How User Involvement Leads to System Acceptance.* **Baronas, Ann-Marie K. and Louis, Meryl Reis.** 1, 1998 : Management Information Systems Research Center, University of Minnesota, March, MIS Quarterly, Vol. 12, pp. 111-124 . http://www.jstor.org/stable/248811.

40. *Expert Pilot's Perceptions of Problem Situations.* **Fischer, Ute, Orasanu, Judith and Wich, Mike.** [ed.] R. Jensen. 1995. Proceedings of the 8th International Symposium on Aviation Psychology. pp. 777-872.

41. *User acceptance of information technology: system characteristics, user perceptions and behavioral impacts.* **Davis, Fred D.** 3, March 1993, International Journal of Man-Machine Studies, Vol. 38, pp. 475-487. http://hdl.handle.net/2027.42/30954.

42. **Elky, Steve.** *An Introduction to Information System Risk.* SANS Institute. 2006. http://www.sans.org/reading_room/whitepapers/auditing/an_introduction_to_information_system_risk_management_1204.

10 Appendices

10.1 Participant Informed Consent Form

INFORMED CONSENT FORM FOR BEHAVIORAL RESEARCH STUDY
Rochester Institute of Technology

Title of Project:	Securing the Application Acquisition Chain: Security Concerns & Human Factors of Application and System Acquisition in the Enterprise

Investigators in Charge:

Mr. Eric Goldman
MS Candidate
Dept. of Networking, Security, and System Administration
Rochester Inst. of Technology
[redacted]

Dr. Yin Pan
Associate Professor
Dept. of Networking, Security, and System Administration
Rochester Inst. of Technology
[redacted]

A. Explanation of the Project.

1. You are being asked to participate in a research study that is investigating the procedures used for the selection of software and information technology systems used by end users for common business purposes. The results of this study will be used to determine what factors will best assist decision makers in properly assessing such software before purchasing and implementing said software.

2. The goal of this work is to evaluate decision making processes related to the software and system acquisition process in small organizations.

3. This study requires you to participate in an open ended interview. You will be responsible for answering honestly the questions asked or selecting to skip any given question. The interview study is designed to take one hour or less of your time.

4. You are not exposed to any significant risk in this study, as none of the questions address personal issues or require providing organizational confidential information. Furthermore, your name or other personal identifiable information will never be linked to any notes or results. Your answers will not be shared with your employer in any identifiable manner. All efforts will be taken to sanitize any identifying information in your interview when it is reviwed. After completing this informed consent form you will only be identified by a non-linking numeric identifier in order to protect your privacy.

5. Results of this research will be used in order to help other decision makers involved in the software and system acquisition process.

B. Your rights as a research participant

1. We will be happy to answer any questions you have about the study at any time. Mr. Goldman and Ms. Pan may be contacted at the telephone numbers and e-mail addresses shown above. If you have questions about your rights as a research subject, you can call contact the Rochester Institute of Technology Institutional Review Board at (585) 475-7673, or e-mail hmfsrs@rit.edu.

2. No subsequently published results will contain any information that could be associated with individual participants. No information identifying individual subjects will be ever associated with

the data collected. No personal information or responses will be shared with any employer, and no information will be released that could possibly link any individual with his or her responses. All data will be stored and secured only on the investigator's computer after being retrieved from the program.

3. Your participation is wholly voluntary. Your decision to participate, or to not participate, or to withdraw from the study during the experiment will in no way influence your relationship with the researcher or your organization.

4. You may refuse to participate or may discontinue participation at any time during the project without penalty or loss of benefits to which you are otherwise entitled.

5. Results of the proposed research will be used to further guide our understanding of human decision making processes in the field of information technology and related fields.

6. The results of this research will be submitted to peer-reviewed journal articles and perhaps presented at an academic conference. No information allowing for identification of individual participants will be included in these reports.

C. Statement of consent

Participant:

I agree to participate in this study, which seeks to evaluate decision making processes involved in the software and/or system acquisition process. I understand the information given to me, and I have received answers to any questions I may have had about the research procedure. I understand and agree to the conditions of this study as described on this form.

I understand that I am volunteering to participate in this study, that I will be not be compensated for participating, and that I may withdraw from this study at any time without penalty to me.

I certify that I am at least 18 years old.

I understand that I will be given a signed copy of this consent form.

_____ _____

Signature Date

Researcher:

I certify that the informed consent procedure has been followed, and that I have answered any questions from the participant above as fully as possible.

_____ _____

Signature Date

10.2 Participant Advertisement (Email)

RIT Research: Request for your participation in my graduate thesis research study

Dear Sir or Madam,

My name is Eric Goldman and I am a graduate student at RIT. I am writing to you today to ask for your company's participation in a research study I am conducting for my thesis research. The research study will evaluate factors related to application acquisition in small to medium sized organizations. The study format is an in-person interview session that should last no longer than one hour. For this study, I would like to interview any member of the IT or business staff who has a significant role in the acquisition of IT systems or software. In most organizations, such an individual may have a job title such as "System Administrator", "IT Manager", or "Chief Information Officer". The above list is only a suggestion. Acceptable participants may also have some other title. If possible, could you please put me in touch with some such individual within your organization to help assist with the research.

All participants and their answers will be kept confidential. There will be no way to match individuals or companies back to their interview responses. All measures are taken to protect all participants' individual confidentiality in this process. This study has been approved by the RIT IRB and has met institutional approval.

Thank you for your time. Please feel free to ask me any additional questions. Please forward this email to any suitable participant within your organization or feel free to forward me the contact information of any such individual. Your organization's participation is greatly appreciated in this research effort.

Sincerely,
Eric Goldman, Principal Investigator
Rochester Institute of Technology
[redacted]

10.3 Question Background & Scoring Criteria

Question	Scoring Criteria & Explanation
1	0/3 = Less than one year 1/3 = 0-3 years 2/3 = 3-5 year 3/3 = 5+ years Scoring Rationale: Increased time with a company should enable the decision maker to better understand processes and other organizational relationships. Note that this is not years of IT or other work experience, but experience within this specific organization. References: [14], [15], [16]
2	0/3 = Intern/Student 1/3 = System Administrator / IT Staff (non-management) 2/3 = Manager 3/3 = Executive Scoring Rationale: Increased rank usually indicates increased authority and therefore a greater ability to control the direction of the acquisition process. References: [14], [17]
3	0/3 = High School / GED or trade school 1/3 = Associates / 2 Year Degree 2/3 = Bachelors / 4 Year Degree or Associates + Advanced Certification or Training 3/3 = Post-Graduate Degree or Certification or Bachelors + Advanced Certification or Training Scoring Rationale: Higher levels of education expose decision makers to new perspectives and strategies which may influence their decision making. Note that this question is concerned with decision making experience and therefore the education does not necessarily need to be technical or IT oriented. References: [16]
4	0/3 = Training opportunities are not provided by the organization 1/3 = Training is only provided for participant and not other members of the IT staff 2/3 = Training opportunities exist, but the participant does not often utilize 3/3 = Participant attends at least one training or conference per year Scoring Rationale: Increased training allows a decision maker to be aware of current opportunities, methods, and concepts and provides knowledge sharing and questioning opportunities.
5	0/3 = Participant does not regularly utilize any information sources 1/3 = Participant only utilizes high level technical news sources (e.g., Slashdot, Digg, etc.) 2/3 = Participant utilizes professional, industry, or other higher level periodical and resources 3/3 = Participant participates in interactive forums or networking groups on a regular basis Scoring Rationale: Indicates to what extent the participant attempts to stay current with technology and business challenges. References: [14], [16], [18]
6	0/3 = Acquisition is never a planned or budgeted activity and is almost always reactive to immediate needs 1/3 = Acquisition is not planned for in advance, but budget resource are set aside 2/3 = Acquisition is mostly planned, but is sometimes reactive to immediate needs when it could have been planned for instead.

	3/3 = Acquisition is almost always a planned activity Scoring Rationale: A reactive approach is often rushed and may not consider sufficient criteria to choose an effective solution because of time constraints.
7	0/3 = Initiation for acquisition only happens when there is a technological failure 1/3 = Projects are "sacred cows" and are only initiated as personal interest of a high level decision maker or member of management 2/3 = The decision to initiate an acquisition project can only come from within the IT department 3/3 = Any member of the organization can suggest that an acquisition project should be initiated Scoring Rationale: The need for an IT acquisition project may not be solely technical and instead should be driven by business needs. If business users or management have the ability to suggest acquisition projects there will be a strong alignment between IT and business strategy. References: [19]
8	0/2 = Individuals who are inappropriate decision contributors are frequently involved in the decision to begin an acquisition project 1/2 = There is an inappropriate number of individuals who are involved in the initiation phase of an acquisition project 2/2 = There is an appropriate number of individuals who are qualified involved in the decision to move forward with an acquisition project Scoring Rationale: When under-qualified or inappropriate people become involved in the decision to begin an acquisition project the project may be stalled or terminated when in the absence of those persons the project would move forward as decided by qualified and appropriate individuals. References: [20]
9	Not Scored Question Background: Individuals that are involved in acquisition activities more frequently may have more experience and will have greater opportunities to review and improve their strategies. References: [21], [15]
10	0/3 = The participant cannot define the acquisition process at all and does not provide any information about the steps or activities done in order to select a component 1/3 = The participant performs minimal research and review or is locked into solutions from preferred vendors and does perform objective assessment of such solutions 2/3 = The participant is not active in the process and only evaluates or approves the results of another individuals decision. 3/3 = The participant has a good understanding of the acquisition process, even if not formalized; the participant consults resources and makes a qualified evaluation of options Scoring Rationale: If a decision maker does not fully evaluate the choices it may be difficult or impossible to ensure that the component is good fit for the complete IT infrastructure and business needs. References: [22], [18], [21], [14], [23], [24]
11,12,13	0/2 = The participant provides almost no criteria or qualities to compare components 1/2 = The participant only provides limited definitions and criteria for comparison 2/2 = The participant provides a thorough definition and demonstrates a justification for the criteria used for comparing and defining possible component selections

	Scoring Rationale: Participants that do not have definitions for what they are looking or not looking for in a product are less inclined to objectively compare options. References: [17], [21], [23], [25]
14	Not Scored Question Background: Interesting to consider if the quality of acquisition is related to approval processes and if the approval process limits or effects acquisition activities either positively or adversely.
15	Not Scored Question Background: Interesting to consider possible trends and if certain types of resistance or lack of resistance have an effect on acquisition. References: [22], [21]
16	Not Scored Question Background: Investigates efforts that are taken to prepare for implementation after a component has been selected.
17,18,19	0/3 = Participant externalizes blame and/or does not believe any measures could have been taken to prevent the failure 1/3 = Participant was slow to diagnose or recognize problem or was slow to act on a solution to the problem 2/3 = Participant can identify the root cause of the problem 3/3 = Participant has identified the cause of the failure and has adjusted her strategy for future acquisition projects Scoring Rationale: Measures whether or not the participant uses previous acquisition project failures to learn a lesson or if the participant does not seek to improve future acquisition efforts References: [26], [16]
20	Not Scored Question Background: Investigates non-IT involvement in evaluating the success and failure of an acquisition project. While a project may succeed from an IT perspective, it may be a failure from a business or management perspective. Outside validation is important aspect of communication and can help improve the process in the future. References: [21]
21	Not Scored Question Background: Interesting to see how organizational structure effects the acquisition process and information sharing, which is a component of communication.
22	0/2 = In the participant's organization there is tight control over assets and limited information flow 1/2 = There is a some degree of information flow, but boundaries still exist for cross-organizational communication 2/2 = There is a high degree of information flow and/or channels exist to facilitate cross-organizational communication Scoring Rationale: With a limited degree of communication it may be more difficult for the IT staff to get the necessary information and interaction for higher quality acquisition. References: [17], [21]
23	0/2 = Management does a poor job of communication with the company or communication is highly restrictive 1/2 = There is only a limited degree of communication from management 2/2 = Management provides a high degree of communication

	Scoring Rationale: Management communication style with the company can influence open communication throughout the organization.
24	0/3 = Management provides minimal direction and interaction opportunities 1/3 = Management provides limited one-way communication 2/3 = Management provides regular communication and is open to interaction 3/3 = Management is open and accessible and encourages two-way communication Scoring Rationale: IT decision makers may require input and support from management in order to push forward IT initiatives and acquisition projects. Management communication style may affect the ability for IT decision makers to acquire resources or move forward initiatives
25	0/3 = Management demonstrates a low level of concern and interaction for the IT department 1/3 = Management provides objectives and direction to the IT department, but is not interested in the IT department providing input or discussing the directions 2/3 = Management is open to two-way communication with the IT department and its staff 3/3 = Management is interested in IT direction being primarily driven by the IT staff and encourages two-way discussion of IT direction Scoring Rationale: Management's involvement and willingness to discuss IT objectives with the IT staff may affect the IT decision maker's ability to perform quality acquisition.
26	0/3 = There is no management intervention or important management decision makers are not involved 1/3 = Management's involvement is superficial or inappropriate people are involved 2/3 = Management is only concerned from a financial standpoint 3/3 = Management provides visibility and an appropriate level of involvement Scoring Rationale: An organization's management has a primary focus on ensuring that business continues to operate in the desired direction. Without involvement or transparency into IT acquisition decisions there may be no oversight to ensure that the acquisition is appropriate to the organization's business needs. References: [27]
27	Not Scored Question Background: Indicates whether or not the participant considers the full system lifecycle during acquisition and if IT has a strong influence on business operations and processes.
28	0/2 = Management only considers IT a financial cost center 1/2 = Management consider IT to be an important part of the organization's operations 2/2 = Management recognizes IT as important and provides the proper consideration, resources, etc. Scoring Rationale: If management does not perceive the value of IT they may resources which may be necessary in order for an acquisition maker to perform higher quality acquisition
29	0/2 = The participant does not believe that the exact selection matters 1/2 = The participant believes there is only a limited impact from her choices 2/2 = The participant believes there is a significant impact on the organization Scoring Rationale: Indicates whether the decision maker considers business rationale as well as user requirements and user behavior in their decisions. If a decision maker does not think that a decision can have a significant impact they may not perform as thorough an investigation during the acquisition.

	References: [28]
30	Not Scored Question Background: Question is intended to see if there is a trend or relationship between end-user computer literacy and the acquisition or security.
31	0/2 = Participant does not seek end-user input and disregards any input given 1/2 = Participant will listen to use input, but does not actively solicit user for input 2/2 = Participant values and seeks input from end-users Scoring Rationale: Users interact with many systems and are most familiar with business processes. Even for systems which are not user-facing there is still likely the need to provide support for some business function. Therefore, user input can be a valuable factor in making an informed decision. References: [28]
32	Not Scored Question Background: This question further investigates the user attitudes and may be helpful at identifying practices and trends compared to a participants acquisition quality score. References: [22], [29], [30]
33	0/2 = Users do not report problems when they occur and the IT staff is dependent upon technical or their own investigation to discover problems 1/2 = Users will sometimes seek assistance, but the participant believes there is need from improvement 2/2 = Communication about system and software issues is sufficient and appropriate Scoring Rationale: This question serves as a measure of communication between end-users and the IT staff. In addition, it indicates whether or not end-users are comfortable bringing issues and desires to the IT staff. References: [31]
34	0/2 = Users demonstrate a high level of resistance 1/2 = Within the user group there are laggards or there is only reluctance instead of resistance 2/2 = Most users are accepting of change and there are few, if any, laggards Scoring Rationale: If users do not accept a new system they may rely upon old systems or shortcuts, which defeat the purpose of acquiring a new system or component.
35	0/2 = There is no end-user involvement before or after the acquisition process 1/2 = There is only user involvement before or only involvement after the acquisition 2/2 = There is user involvement both before and after the acquisition Scoring Rationale: Increased user involvement can help to ensure that new technical components fit with business needs and business processes. References: [31], [28]
36	Not Scored Question Background: Indicates if the organization or IT staff understands the relationship between business process and technology. Further indicates that the IT staff has trained employees to be aware of policies and proper usage of systems and components. References: [17], [31]
37	Not Scored Question Background: Indicates the extent to which the acquisition project is planned. Also serves as a measure between IT staff and end-user interaction.
38	Not Scored

	Question Background: Provides insight into the relationships between the IT staff and end-users, as well as policy enforcement. User acceptance is also a factor in long-term acquisition success. References: [28]
39	0/2 = Management is not concerned to any extent about IT security requirements or issues 1/2 = Management recognizes security issues, but it is only of minimal importance to them 2/2 = Management is aware of security concerns and displays appropriate concern Scoring Rationale: If management is not concerned about IT security they may not provide adequate resources for the IT team to address security needs. References: [32], [31], [33], [27], [25], [12]
40	Not Scored Question Background: Intended to understand what motivates individuals to be concerned with security. May result in trends which correlate to the level of security awareness. References: [32]
41	Not Scored Question Background: Intended to see if security exists for the sake of securing the organization or simply meeting compliance. May also display a trend between level of regulation and level of security awareness.
42	0/3 = The organization has no security policies or principles which may affect acquisition 1/3 = Security policies exist but have no impact on acquisition 2/3 = Policies do not directly address security and acquisition, but the policies influence the decision maker's selections 3/3 = Explicit policies exist in regards to the role of security in an acquisition project. Scoring Rationale: This question measures the decision maker and the organization's concern for security. Also indicates to what extent, if any, security is factored into the decision strategy. References: [22], [33], [25], [12], [24]
43	0/3 = There are no formal or informal policies and/or participant indicates "complete trust" in the end-users 1/3 = There exist informal policies to address security and end-user usage of systems 2/3 = There exist formal policies, however, these policies are either not comprehensive or are not enforced 3/3 = End-user related security policies exist which are enforced and comprehensive Scoring Rationale: If end-users are not aware of the proper usage they cannot be expected to act with security in mind. Policies which are unclear or are not enforced provide little incentive for users to comply.
44	Not Scored Question Background: Investigates methodologies and controls which are used. This may be useful to establish trends. References: [22], [33], [27], [34], [24]
45	0/3 = There are no security policies in place to evaluate 1/3 = The policies that exist are poorly written and/or the users are unaware of their obligations under these policies 2/3 = The users are aware of the policies but they generally do not comply and follow them 3/3 = The users are aware of the policies and understand the consequences; for the most part users comply with these policies Scoring Rationale: The mere existence of policies is insufficient if they are unclear and the

	end-users are not aware of the policies and their obligations under those policies. References: [17], [32], [27]
46	Not Scored Question Background: Intended to see if the organization has any internal knowledge and understanding of IT security and if this affects the level of security awareness and implementation. References: [22], [17], [33], [27], [24], [35]
47	0/2 = Security is not considered at all as a component of the participant's decision strategy 1/2 = Security is considered, but is not an important factor in the decision strategy 2/2 = Security is considered an important aspect of acquisition decision strategy Scoring Rationale: This addresses one of the main questions of this research and directly asks the participant for the extent to which they consider security during acquisition. References: [20], [36], [25]
48	Not Scored Question Background: Intended to see what controls and measures are used to establish security. In addition, evaluates whether the participant considers existing security components when new components are introduced into an IT system. References: [22]
49	Not Scored Question Background: Used to explore the participant's attitudes towards security in the acquisition process.
50	Not Scored Question Background: At this point the primary purpose of this research has been explained to the participant and this question provides the opportunity to directly address this topic and to clarify or readdress any topics discussed earlier.

10.4 Result Summaries by Participant

Participant #2237953	
Q#	Response
5	He is a system administrator and relies upon peers and vendor newsletter for his sources of information.
8	At the lower levels they do much more research and bring the options to those at the higher level who are more concerned with financial matters.
9	IT is seen as overhead expense of customer projects; hard for IT team to drive IT spending because most spending is customer driven.
10	Look for the most popular options. Popularity was defined as order in page ranking, which is not an objective or measure of any quality.
18	No plans to replace faulty system because too much is already invested into this system and the impact on the total IT infrastructure would be too great.
19	Analyzing the ease of use and management would improve acquisition because we cannot be experts in everything.
23	Downward information flow is too slow, we find out about information too late and we therefore must work and make decisions under compressed schedule.
29	Common end-users do not care about the systems they use.
31	The users that are highly computer literate do not usually provide anything useful and their input is seen as an annoyance.
32	Training is very important. If the training will be too complex we will not select.
34	Normal end-users are receptive to change; developers are a point of resistance.
36	There is no mandated user training. There are supposed to be user SMEs, but most of the time they are not knowledgeable in the areas where they claim to have expertise.
39	Management understands security concerns for company. However, self-enforcement is poor at the higher level. For example, top-people would print customer data against policy.
40	We would like to have more internal focus on security, but management will not provide the resources to extend security efforts.
50	Products with frequent updates that are easy to roll out are more secure. Security is a managed process, not a reaction to bugs or incidents.
	Participant Summary: Much greater depth of research is conducted at lower level and upper level IT personnel make the final decision. Management believes in security, but does not provide adequate funding and resources. Lack of communication and greater organizational understanding of IT needs outside of the customer requirements can reduce the ability to make an informed decision and consider more appropriate possibilities.

Participant #3103141	
5	Reads traditional business sources such as Baron's, Business Week, etc and some industry specific publications. Participant notes that he takes note of the IT articles, but doesn't really understand them. Should be noted that there is no internal IT personnel in the company and that he is the primary decision maker related to IT concerns.
6	High amount of reactive acquisition that is not preplanned in advance.
10	IT is outsourced to consultants. The consultants are active and on the premises regularly during normal operations. Consultants do the bulk the research and decision making, but they have reviewed multiple consultants with references before choosing a particular consultant.
15	(Specific Instance) While the consultant came highly recommended, he was unable to work well with the internal end-users. The system selected was more confusing and less user friendly. It does not seem as if the consultant made a decision based on the internal needs of the organization.
17	Two reputable vendor/consultants from different organizations could not work together. Were not prepared or knowledgeable to mediate between the two.
19	Must evaluate consultant and make sure they not only have experience in the field, but experience within the specific industry and with company size. Participant notes that consultants who usually deal with large companies perform poorly at smaller companies. Must be prepared to do own self-evaluation and remove poor consultants if they do not live up to their reputation.
23	They are a small company (≈40 employees); has regular conference call where all employees at all levels can participate. Executive management has strong communication with managers.
28	Participant claims IT assessment is critical to planning, however see responses to question 5, 6, & 10 above. All decision input comes from outsiders who may not truly understand company's goals.
33	Believes that proactive technology is sufficient to alert them of problems before users. This attitude assumes that all problems are performance or feature related.
36	Currently insufficient, takes a very long time for users to be productive on new systems. Believes an increase in end-user IT training would be beneficial. Again, this points to the externalization of IT and the affect on internal understanding. Since IT is identified as important and a driving factor and that the choices greatly affect the user's productivity, it would make sense to have someone internally vested in making good IT decisions.
38	Do to the lack of training above, users would often continue working on legacy system negating the possible benefit of the new system and requiring maintenance and training on two systems, increase confusion and costs.
39	Believes security is important and that it is being taken care of by managed services. Reports are available, but no one internally has reviewed these security reports. Reliant upon consultants, however, participant notes that he is not aware of consultant having any specific security background and the consultants have never mentioned security.
44	Participant is unaware of the regulations they are governed under and believes that the size of the company affects obligation under regulations. Does not believe the company maintains what is commonly considered sensitive or personal information.
46,47, 48	Reliant upon the consultant for security input. Assumes the consultant is offering such services or solutions. Assumes if the consultant suggests something is may often be a scare tactic and that the size and profile of the company and the types of systems used limit possible exposure. Because there is no history of attack, does see any reason to devote more attention.
49	Secure knowledgeable people to make good decision who understand your business size, and

	needs, that you can trust over time. Like systems, test and evaluate people over time.
50	Participant does not appreciate the need for security or understand what constitutes sensitive data: Identifies that company stores billing and contact information, but does not believe this needs protection. Participant compares business to TJX claiming they don't have sensitive information that could be attacked. When further questioned, participant identifies that the company processes credit card transactions, but believes that firewalls and monitoring are sufficient. Is unaware of obligations under PCI rules. In reality, the size compared to TJX does not limit obligations or targeting.
	Participant Summary: This organization has no internal IT reference or anyone specifically concerned with IT. However, the company understands the importance of IT, how it drives business, and how it can affect user productivity. Heavily reliant upon external consultants and managed services. Consultant action and managed service reports are not critiqued unless there are big obvious problems. Strong misconception that size and business lead to security by obscurity. Internal access restrictions and information privacy are not well understood. Questionable motivation and inputs for both acquisition and security based decisions.

Participant #3235679	
3	No formal IT training or certifications.
10	Very few vendors due to the nature of the business. Primary concern is total system integration. Important to consider similar businesses.
11	Low level of internal knowledge, therefore highly dependent upon good vendor relationship, training, and straightforward system.
15	Resistance comes because users do not want to take extra steps. Cites examples of requiring second login on encrypted systems.
17	Focused on the core modules of the system, but did not fully evaluate other features that were included and eventually used. These secondary modules did not function properly – our evaluation was not extensive enough.
19	The process needs to be better defined to ensure all criteria are satisfied and all features are evaluated. Must perform the greatest extent of due diligence with references, dig into their experience.
29	Small changes are not really important, only if the core system changed since that may affect multiple processes. However, at mentioned above the introduction of extra steps greatly affects productivity and user acceptance.
36	Training is very important. "Train the trainer" to establish SMEs and internal knowledge. Need to do granular evaluation of training needs not just blanket program.
39,40, 41	In a highly regulated industry (financial) therefore the external pressures are very real and the core guidelines and requirements are well known. However, the participant note that there is no "clearing house" that informs you of your compliance and other legal requirements. Interestingly, the participant notes that the best indicator for an important compliance issue is the number of people trying to sell the company solutions to meet that regulation.
45	Extremely high level of training, education, and reeducation. Posters are printed, emails are sent out, and annual sign off is required.
49	Be concerned for the accidental information exposure and curious user. People tend to snoop around, to combat this they need a lot of training on security awareness. Security training is an ongoing process.
50	Security must be a component of acquisition – should be considered in tandem with the data stored/accessed by the product to determine the importance, value, and the data's security values. Participant understands security is important because of trickledown effects: Business and customers coexist in a financial ecosystem. Fraud and security failures that are not anticipated can lead to costs which affect everyone in the ecosystem. Important for the other businesses and customers to interact with to be secure as well.
	Participant Summary: The participant does not have any formal IT or security background. However, the industry is highly regulated. As a result, security implications are very clear and constant through all stages of the SDLC. In turn, this necessitates considering security in acquisition because the system has a limited tolerance for insecurity. While this is true for the IT people and management, users are not as concerned with security, even in the highly regulated industry. As a result, the participant notes that there must be continual monitoring, auditing, and training to limit and control internal threats. Security is understood beyond the regulations and audits which leads to reduced firefighting.

Participant #3524075	
6	Fairly spontaneous in regards to the overall company, technological environments are often customer specific and segregated form main systems. Within the customer's need more planned, however focus is on the customer over the internal company's needs.
10	Formalized process and review materials for qualified research organizations like Gardner's. Look for long term partners, who are not necessarily big, but have received recognition (not clearly specified who they are trusting to provide the recommendation). They hire direct SMEs and consultants when necessary.
14,16	Implementation plan is laid out in a project format. This entails setting up the roll-out schedule and training before going live. There is a sandboxing period and stress testing before going live.
15	Some people have religious devotion to languages or vendors, which inhibits getting the best of breed.
17,18	Product was not fully tested and does not perform properly. They now have to use workarounds and cannot replace this component do to high integration with the rest of the system.
21	Hierarchical approach has improved communication flows and increases the line of authority which increases the chances of successfully arriving at a component to implement.
32	There is a formal project termination and project review process where owners and managers evaluate the component choice. Very important in this organization since they try to build solutions that can be redeployed to new customers with only minimal changes.
36	A lot of training is offered. The buy courseware and will help people maintain their certifications, but the participant implies this is not often utilized.
39,40	The biggest drive comes from the customers, who may have regulations or requirements. This organization holds sensitive information which the clients want protected. Aware of specific regulations that affect their industry.
42	Existence of policy is a requirement of the customers. There is strong consciousness of security concerns, but it is not necessarily spelled out.
47	There is a very high consideration of controls, access, and encryption. Multiple clients are managed on the same systems, so the highest level of isolation is importance from a business standpoint. Customers can specify employee access controls and demand auditing. {{For analysis, security is best when it is driven by business not IT}}
	Participant Summary: This organization deals with a large volume of sensitive data. All levels of the company understand the need to protect private and confidential data. While not all clients specify security requirements, the fact that some do can help create general security practices across the board. This participate had a strong focus on good support and open protocols (not necessarily FOSS), however software must be malleable enough or allow integration to make sure it can suit both general and security needs.

Participant #5254450	
7	This organization relies primarily upon specific industry software with limited number of vendors. Therefore, they do not expect ideal systems and try to limit acquisitions until necessary (preferring to create hack or work around) because of the possible changes to business processes.
8	Participant is at high level and in charge of the majority of financial approvals and therefore wants other people to validate and comment on possible options before approval.
10	Share knowledge with other members of industry consortium and follow industry trends and movements to new components. Also asks vendors for input and recommendations on complimentary and products that will work with existing systems.
14	Very involved roll-out to implementation process. Roll-out to core group of testers and tweak before mass deployment. Features are evaluated before purchase, how to actually implement is a post purchase consideration.
17,18, 19	Had a previous relationship with the vendor and had developed a level of trust. Vendor did not perform all obligations. This was no apparent until the system went live. The participant believes this could not have been predicted, even though the program was tested in a sandbox.
31	Seeks user input if available. Those who are more IT-inclined will likely move into a dedicated IT position rather than remaining in a business role.
32	Service driven industry and therefore it is extremely important for end-users to have reliable systems that they like. Users are highly involved and actively encouraged to provide input. As noted in #7 above, try to maintain business process, but participant is willing to allow processes to be modified by software if there is a business case for increased productivity.
34	Participant notes that user acceptance has increased as communication efforts were increased; users are much more likely to accept new software if it is explained to them the benefit to the organization and/or to them. Note, that communication improvements are both upward and downward.
40	Participant has extremely high understanding of what constitutes sensitive information and the responsibilities of being a data custodian. This also extends to users and management. In addition, security is often specified in client RFP.
41	Participant understands that the organization is governed by PCI, but all processing takes place by a third party. Most data storage and other information assets is also stored and managed by third party.
44	Users understand security concerns, however, participant does limited security beyond what is built into existing systems because of difficulty in implementing and push-back from users. There have been no security incidents in the past to act at motivator.
46	We rely on looking at everyone else in the industry and using their solutions. Participant does not believe that they need an internal security person or increased security precautions. This is interesting considering they have a strong belief in providing security and currently weak implementation and enforcement.
47	Security is always a concern, however it is not a primary focus because participant does not believe the company will be attacked. Furthermore, we can't control the storage of the data because that is with a third party vendor. The participant believes that because they are not physically controlling the data the security burden is transferred to the third party custodian.
50	Participant believes that security needs vary depending on the particular component, its function, and the types of data it accesses. Furthermore believes that the big-name companies would not be able to stay in business if they did not prove security and that newcomers must

	first prove themselves to be trusted. Because security is a hot topic within this industry, the participant believes that this also transfers to the vendor's offerings since everyone else would not be buying it if it did not do security properly.
	Participant Summary: Participant believes that she is limited to specific vendor set and that furthermore that the big player software vendors for this industry are the best because the group uses them. Furthermore, with an expectation that software will never meet requirements the participant is lead to be more accepting of mistakes and faulty promises, which can increase the likelihood of establishing a poor trust relationship. Participant believes that outsourcing payment processing and storage is sufficient to address security. However, internal security controls are not well enforced and the motivation to increase security would likely only be motivated by the occurrence of a breech. Assumes that because the industry itself cares about security that the big player names care about security

Participant #5350582	
2	Participant mentions security tasks as one the main position responsibilities.
7	Initiation can come from IT decisions, monitoring reports, user community (specific process exists to facilitate end-user initiation of a possible IT acquisition.
9	Extremely high relative frequency of acquisition projects- many small 2 day projects and maybe around 20 capital expenditures. Participant notes that a very high percentage of his time is involved in evaluating new opportunities or solutions for existing needs.
12	Vendors must strongly built case. The company often has vendors critique competitor products to build a full matrix. May even hire a consultant to provide input in acquisition (if the technology is new to us) because they do not want to replace later and know the limits of their own knowledge and expertise. Ideally find recommendations from the most similar company.
17	VAR lead participant to believe that they had provided this solutions before; believe they did not ask specific enough questions from references. The individual components of the acquisition had good reviews, but the system as a whole had no previous case support and did not work well together.
23,24, 25	Management exists mostly in an ivory tower. Information flows to the company mostly on a need-to-know basis. Participant notes it is hard to move projects forward and that most of his communication efforts are only in passing and there is often breaks and restarts required in any project. IT is seen as a cost center to be controlled, very little management concern for IT.
28	Management sees IT as a necessary evil and does not believe in the ability of IT to drive business forward. It is very hard to convince management to back innovative or opportunistic IT projects. Management is not primarily concerned with soft (people) benefits, but would approve of IT systems that could cut costs and personnel.
31	Small number of end-users with high computer literacy. They provide ideas on a limited basis, but they are actively sought out for and are believed to be helpful in justify the business case for an IT component.
32	We establish a small pilot group during the selection phase of the acquisition process and actively solicit feedback in the formal project closing and on an ongoing basis through our support system.
34	Users are very afraid of change and new systems. While they recognize there will be new benefits, they are not highly concerned with an opportunity for increased productivity of ease of use. Interesting to note that users seem to be highly involved in the acquisition process in this organization, however, note the management attitudes on communication and towards IT.
36	High amount of training is offered and employees are regularly sent out from IT system and skills training. Training is a definite part of new systems and even small system changes.
37	Participant notes difficulty in disseminating information because IT mostly has to rely on functional managers to propagate information. Sometimes can use broadcast email or talk to affected groups in hallways conversations. However, announcing new changes has often been problematic in the past.
40	Understand regulation and possibility for personal information exposure, however, the main concern is protecting internal intellectual property.
45	Security policies are clear and often reevaluated, but participant believes employees need stronger annual review, specific IT security training, higher focus in employee on-boarding, and increased managerial awareness to integrate into business process.
46	The participant has a strong background in IT audit and there is a system administrator level individual who is in charge of security issues as part of his responsibilities.
50	The biggest challenge comes from the ever increasing number of non-uniform and poorly

	written security regulations. Furthermore, it is unclear what the implications of certain state laws (e.g., Massachusetts and Nevada) are at a national level. These laws are clearly note written with sufficient input from IT professionals and are often use ambiguous language. As a result, security policies must be reevaluated against every law that you believe affects your organization. User involvement and interaction in terms of security in important because it helps them understand requirements and sensitivity requirements of data. In addition, it is important to understand the business case that drives the need for security at the fundamental level (beyond compliance concerns) in order to determine the specific security action that data sets or processes require.
	Participant Summary: This individual has a very strong background and understanding of security concerns. The biggest limiting factor in acquisition success is this organization would seem to be top-management. Information does not flow easily through this organization, and management only sees IT as a cost center. There exists good communication and interaction with the end-users in general and in respect to acquisition, however, without management support it is hard to initiate the training and awareness which the participant would want to implement.

Participant #5566166	
10	In the past users would come with a specific product they wanted to buy, how IT works harder to discuss actual needs and does the evaluation of options with their IT background to meet business needs. To get the options, they send out RFP to the same few big vendors. They know who to contact from previous experience and because "90% of the industry" uses the same four products. This would however necessitate that in the past projects were successful, that others in the industry have very similar requirements, and that internally and externally they had performed a thorough and proper evaluation.
13	They look to select a vendor with a good reputation, which is primarily defined by the years of experience with the product. It is very easy to determine those with a bad reputation based on industry trade reviews, however, if the product is not industry specific, then the general review is more important the opinion from only inside of the industry. Next it is important that the vendor defines how they will stand behind their product through support, service, and maintenance offerings. The perception that there are only a few major players in some area can make it hard to find new offerings or unknown options which may have a "good" reputation.
15	Resistance can occur anywhere in the process. Some leaders may try to stop progress because they personally prefer an old system or want to divert funds elsewhere or the business owner of the application and the end-user either do or do not want change. Resistance also occurs in the change process, which may be attributed to the users being minimally informed about upcoming changes.
25,26	For the most part upper management leaves him alone; however, this also results in them usually providing insufficient feedback. There is a specific IT committee composed of some upper level people when it comes to making decisions and in addition some IT decisions may go to a budget committee. It is often the case that inappropriate people from upper management try to gain influence and get involved.
30,34	The users are highly literate because the workforce is young, however, even the older employees posses above-expected proficiency. The users are also fairly accepting of new changes and for the most part understand that the changes are there for their benefit.
35	There is a lot of feedback gathered through surveys, user groups. The change/implementation team continues to exist after implementation to monitor the system and provide feedback.
37	Software is deployed early outside of production for users to experiment and get familiar. Training is usually mandatory and performed in small, manageable doses. The main driving concept is to make a smooth, gradual change.
43,44, 45	Users are highly aware of the proper systems and work in a controlled environment limiting use through both controls and policy. As the primary IT decision maker he is concerned about both accidental and malicious incidents.
48	Participant notes that end user education is of primary importance. He also notes that it is important to monitor emerging threats and to stay on top of security trends.
50	The participant notes that security must go beyond the law's requirements, but does not seem to understand the importance of the individualized requirements of any acquisition case. The participant also notes that larger companies have access to more resources. As a result, he is concerned that smaller firms may lack expertise and take an attitude that if "I don't think about it, it doesn't exist". Lastly, he expanded on determining the quality of peers: Sometimes, it is not possible to tell if the person giving advice is experienced or an expert, but that you can still learn from them if they have common experience and common views. Individual credentials are not important, but the best answers come from those who can fully explain their point and reasoning and can break down a complex problem with meaningful answers. Networking and

	exchanging information is essential for success in acquisition and many other IT processes.
	Participant Summary: This participant is highly aware of the interplay and needs of the users, and in addition, the users are very aware of their obligations. There are very strong communication channels between IT and the users in this organization. Management understands the importance of IT and IT security; however, they are only minimally involved and are often the cause of problems with IT projects.

Participant #5758430	
5	This participant notes that he often will look for information out of curiosity and often utilizes interns and younger employees to bring him up to date on the latest trends. Often he is looking through trade magazines for opportunities and to see what is out there that can address problems that are currently being evaluated.
8	Try to be as collaborative as possible in decision making. There are no real boundaries of who can be involved, and in general he tries to involve those who will have the most involvement with the component.
14	After selecting a component, it is tested in a sandbox for up to six months before being put into production. During this time keep the old systems online and evaluate if this platform will meet requirements after the pre-purchase screening. User training will occur before going live as well.
15	The end-users are resistant to change and it is often difficult to bring them up to speed (thus the emphasis on training and informing above). When evaluating the product, we are evaluating how it will change our business processes – to what degree will we use the system, will we implement all aspects? Based on the component offerings we may modify our expectations for the system, which could affect processed not originally considered.
29	End-users usually do not care what system they are working on. However, it is very important to select a system that is easy to use and that they like.
32	Participant mentions that it is very difficult to push components onto users, however, if they will accept it is based upon the decision of IT and management. This is odd considering the above focus on involvement of end-users and the answers to #15. Participant also notes the he evaluate activity logs and talks with users to gather their feelings on systems. Perhaps, they do have enough understanding to make decisions on the user's behalf.
39	In terms of general IT, management allows a great deal of autonomy. In terms of security, management is not interested and does not consider it. Often, they management is actively against security because they like open access. Since it is not important to them and they are often resistant to security measures, we usually do not involve them in security related issues and try to do the most we can with our budget in this area.
40	There are no external motivations for implementing security. In the participant's previous work experience, the lack of security constantly caused problems and therefore security is considered important here because it as seen as improving the ability to focus on other tasks. There is not a large concern over protecting internal data; however, they are more concerned with the threat of data-loss or corruption. It is interesting to note that participant's correlation of security with backup and data control.
42,45	Participant wants to increase security control and security awareness, however, security is secondary as the business is rapidly growing and there is not enough support from outside of IT.
43,44	Participant does not see himself as a policeman; believes people are good and there has not been any incidents reported in the past. Would change policies and increase lock-downs if there was cause. Also, should note management's desire for openness mentioned in #40.
50	One suggestion the participant puts forward is to go for the low hanging fruit – if there is something which can easily be implemented and secured, go for it. Look for the small tasks which have the greatest chance of successfully being completed. Believes he could do more to change the culture (e.g., password sharing) if management was onboard with security.

	Summary: The participant notes that he is not a “big security guy” because he has not worked in a company where it has been important, and it is hard to convince management of the value of security. He knows the steps to take, but has not really developed them further or sought additional training because of organizational limitation. As a result, he had a misunderstanding of some security concepts discussed in the interview. In general though, they do a very thorough evaluation and the organization encourages open and rich communication channels. The acquisition process it considered in a lot of detail, however, the evaluation is mostly internally except for sales consultants with CDW or Dell.

Participant #5890968	
7	The department managers are the primary drivers of new initiatives, not IT; managers often plan and manage the initiatives. The people most involved in daily use create timeline and plan.
10	Have established relationships with consultants who give a strong amount of input and do a lot of research for them. Usually the same consultant will be used through the SDLC.
14	Training is very important. Because the company is very small everyone is cross trained so people can be shifted to priority tasks. Looks to make a smooth transition to the new systems.
15	The business of business often takes priority over initiatives and training.
20	The company is a shared environment, a total review is made and everyone communicates. When the end-users are not happy with a system, it is of prime importance.
31	The majority of the company is very highly computer literate and therefore their input is always valued and the participant always seeks their input.
34	They are excited for new technology, but at the same time they want to defend systems they believe are already good and with which they are comfortable.
39	Uptime is absolutely crucial for this business and they are a prime target for attackers, therefore security is extremely important and a constant though throughout.
42	Due to the nature of this business, products are almost all security focused and you need special licensing to even obtain these products.
43,45	Most users are aware of their obligations, but still very close monitoring and auditing of activity is performed. Users are not trusted. For example, one employee was found to have hacked the system and was fired and all system access was removed within three hours. Start monitoring employees as soon as they do anything suspicious to protect the company.
46	The Participant claims to be a businessperson and that she has little understanding of IT. However, she reads the security reports to ensure everything is functioning properly and takes action on all issues even if she does not have the technical knowhow to perform all steps.
47,49	Security evaluation is of prime importance. Furthermore, the culture of security with both employees and customers is just as important. Security must be easy or it will not be used. It is important for everyone to understand the systems and how to use the controls, otherwise you will most likely not have good security and likely also wasted time and effort selecting and implementing the product.
	Participant Summary: The main goals in acquisition are involvement and clear goal setting. However, the participant relies heavily on consultants even with internal IT staff and users with very high computer literacy. Also, throughout the interview she would make comments such as, “this is how things are done in a small business”; this line of thinking is dangerous because even within the same sector different organizations have different goals, plans, and priorities. Security is of fundamental importance in this industry and it is de facto part of the culture and decision making processes.

Participant #6527486	
8	Solutions are brought to a technology committee which consists of partners of the company; they want to provide input beyond just financial approval. The partners, however, are not necessarily technically inclined. This should lead the reader to question their suitability to make decisions.
11	A good product is one that is reliable, which the participant defines as always working on demand and doing everything that the vendor claims it should do. Before selecting the product, whether or not the component does what is purports to do is based on user input and suggestions from members of a strategic alliance which is composed of multiple similar companies within the industry. The participant notes that the members of the alliance tend to use the same products, which he attributes to the alliance itself not the quality of the products.
15	The participant notes that this organization operates in two locations and that the cultures of the two locations differ. In addition, the secondary office does not feel it gets a fair say in the decision making process. He also notes that most users do not want to learn anything new and that they are reluctant to take the time to stop their normal activities and educate themselves. It should be noted that he is placing the training onus on the end-users themselves.
18,19	The participant again mentions user acceptance as an issue and mentions that when components were introduced poorly there was a much lower rate of adoption. When he discusses ways to avoid this problem he does not address the user involvement, but instead cites that more buy-in is required for managers and partners to push forward success.
25,26	There are some members of the technical decision committee mentioned above in #8. While some are interested in IT, there are those who are not and the participant notes that this causes problems and slows down the process. In addition, the participant feels that the IT budget is set arbitrarily.
32	The users can be involved in the demo process, but their opinions are not often considered unless there are large issues or concerns. The participant also notes that if the users hated a current system that would lead to a review of the product, but most likely would not start efforts to replace the product.
34	The users are not resistant, but are reluctant to new systems “because the focus is mostly on their jobs”. He also reports that user will often try to get out of training and there is no external mechanism to force the users or reprimand them in this regard.
38	Users will sometimes bring in unsupported tools which is detrimental to the workflow, but there is no official policy preventing this.
39	Management is not very concerned or interested, however, the participant attempts to makes sure that it is put on the agenda and brought to their attention.
41	We are not formally regulated, but we follow SoX guidelines and worksheets to help make our customers happier. This motivation for security comes from “following the crowd” and in reality only amounts to “security theater”. As in question #11 above, this organization is following the crowd. In this case, the compliance is bad because they are not focusing on their real security issues and instead are focusing on a set of regulations which do not necessarily even apply to them.
45	The policies are clearly written, but we do not devote sufficient time to reviewing and making sure the users understand, as a result the users are not usually conscious of the policies in daily life. In addition, we do not have sufficiently strong internal monitoring and enforcement.
46	His consultants are not security focused, but he believes they consider security. He is too busy with day to day operations to learn about security or devote time to its practice. He has a low internal motivation for security which may affect management and the users or the relationship

	may flow in a different direction.
49	The participant notes that there is some auditing and accounting of end-user activity and believes that if the employees were more conscious that there were being watched they may improve their behavior. He also cautions about non-approved tools that users may use to store or move data which could enable policy violation or result in insecure transmission or storage.
50	The participant believes that it would benefit the acquisition process if there was a formal set of evaluation points that included common criteria, including security. He also notes that for data storage they use a third party who specializes in secure storage rather than running the chance of mis-configuration by internal staff.
	Participant Summary: There is a poor relationship between the users and the IT department. This, however, seems correlated to the nature of the organization where the company partners have a very large control and do not provide rich communication channels or support for IT. As a result, there are often inappropriate people and inappropriate motivations for acquisition choices. The organizational culture lacks support for the IT team and as a result they are often powerless to enforce policies and to provide proper training. Lastly, the participant perceives securities importance at the system level and is less concerned with component/application level concerns.

Participant #7008146	
8	Decision makers involved in the acquisition process can involve himself, the controller, and a specific partner who is in charge of technology. In some cases it may have to be approved by other partners, however, the participant is not sure exactly who else may be involved and if they are qualified to provide input on the task.
15	Participant expresses difficulty convincing management of the value of IT acquisitions and that they often try to stay with technology long after it should be replaced.
17,18, 19	Product did not work as advertised and described by the technician. The participant did not get a clear explanation and proof of concept before implementing. In this case he trusted the vendor without sufficient outside validation or referencing. Participant also note that you should try to run systems in parallel as options which require a full switch are often hard to rollback in case of implementation failure.
24,25	Management often will ignore the participant and he must make a concerted effort to bring matters to their attention. Overtime management is improving their perception of the importance of IT, however there is not champion within management to help push forward IT initiatives and facilitate communication.
29	Participant has a hard time defining criteria except in very broad terms saying that it matters of course “if it works” and that it fits within budgetary constraints.
32	There is usually minimal end-user involvement; participant and management believe they understand the users’ needs and requirements. An external auditor has come in the past to evaluate user opinion. This has been done once, but has not been repeated due to financial costs; however, participant would like to see this external review performed every 3-5 years.
34	Users are excited about new programs and often take a great interest. They are not afraid of upgrades.
40,41	Firm believes in protecting confidential user data. They understand what they are liable for protecting. The participant mentions they take actions such as archiving emails and using encryption software but claims these actions are not tied directly to any regulation. Participant further believes that if they were under any form of regulation that the industry group to which the company belongs or management would inform him; this unfortunately assumes that these people are interested or feel they are obligated to find out about such requirements.
43,44, 45	The participant only has a minimal understanding of the security technologies used. In addition, the policies are described as “sketchy”. The participant believes that the users know the correct thing to do and that if necessary he can take appropriate action before something becomes a problem. In this organization, all users have administrator access on system and they purposely try to keep data open and easily accessible because people need access to the data and the participant believes it is impossible to control data copying and inappropriate transit. There are no role based or access controls commonly used, this, however results in a lack of accountability should there be an incident. The participant claims that to implement these types of controls would be too difficult and would only inhibit productivity.
46	Security is managed through security-specific consultant. The participant has no real interest in this area or expertise and does not seem eager to develop in this area.
47, 48	Security is not really considered during acquisition and the participant does not believe most things would affect security. The participant’s view of security is limited to perimeter/firewall ideologies. The participant has mentioned that the majority of his time is spent “fire fighting”, but does not seem to realize he can take proactive action to address such issues. Participant mentions that the servers are locked down because they are obviously more sensitive and hold critical data; it should be noted that he does not recognize that information is then accessible

	and possibly stored on end-user systems.
50	The participant believes that vendors are out to make “good products” and they are looking to sell to top customers. Furthermore, he reasons that because they know they are affecting a lot of people and their reputation is at stake they will make good decision for product options and security. The participant cannot think of any reason not to trust any commercial big-ticket vendors.
	Participant Summary: The participant does not have a lot of communication with the end users. In addition, it appears that upper management and the firm’s partners get involved with and directly manage many issues, even when it may be inappropriate or detrimental. While their understanding of IT’s importance is improving over time, IT is still not sufficiently supported or funded. In addition, the firm and the participant understand that security is important but do not seem to have good internal understanding or control, noting that the security policies are weak and unenforced. In addition, security mechanisms are weak and not well understood; in fact, the organization actively tries to maintain an open environment free of security controls and restrictions, which goes against their goal of properly protecting user information mentioned in questions #40,41.

Participant #8486532	
5	The participant does not utilize trade or CIO publications because he believes they have too much propaganda. Instead the majority of his information comes from technology interest sites such as Slashdot.com and through Google searches. The sources may not direct him to the material that is important for him to carry out the more technical aspects of his position.
7, 8	There is continuous monitoring and possible acquisitions are discussed in weekly IT meetings. Often times users will come directly with needs or may even suggest a solution of their choice.
10	Participant has a consulting background and has collected several useful contacts through his previous work. He reuses the contacts who have provided the best advice in the past or who would be most familiar with the need that is being evaluated.
14,16	A staging meeting is planned to set parameters for maintenance, internal understanding, and pre-implementation testing. Small user pilot group is setup before full deployment.
17, 19	The solution was not setup and maintained internally; management brought in the component and it was completely maintained by third party vendor. The participant and his group were not kept up to date on the status of the component. The participant believes this issue could have been reduced with improved communication efforts with both users and the vendor.
23	The CEO is really focused on open communication and has an open door policy. As a result communication is very open and rich throughout organization.
25	Management gives an appropriate level of input and they are very good and identifying needs and opportunities and asking for IT's input in a timely manner.
32	There are uses selecting for testing during pre-implementation. The participant is able to solicit feedback from users effectively through managers. After an implementation an informal email request for feedback will be sent out or an anonymous survey will be created on SharePoint.
37	Participant informs users as far out as possible and training starts after the system is in place because if users are trained before the system is live there is an increased chance of them forgetting.
15,38	It is odd that he reports no problems or resistance at any time in the process. It is entirely possible given his length of time with the company, but perhaps this indicates that he is not doing a sufficient job of searching for issues or that proper channels for such reporting do not exist.
40	The focus is on protecting physical assets from theft. The motivation for security is that they have placed the expectation upon themselves, however, the participant does not elaborate on what this means. There is a lack of detail and understanding of what is important to protect or what the goals of security are in the organization; rather, security seems to mean that there is some security technology in place.
42,43	There are confidentiality agreements, but there are no formal policies. There is a very high degree of user trust and the participant believes that users need open access and this is also part of the CEO's philosophy on open communication. The open culture is very interesting consider that there are a large number of remote workers, though they connect securely and with company equipment. The participant does not believe a formal document would change anyone's attitudes or performance and that minimal perimeter and physical security measures are sufficient.
46	The participant's attitudes towards security are very interesting considering he has previous experience as security/firewall practitioner and that a member of his IT team is a computer security hobbyist/enthusiast. Perhaps management's views on openness and the organization's minimal interest in security affect his stance on IT security.
47	While there are no policies specifically addressing security, there are conscious efforts to

	evaluate security concerns during acquisition. The participant notes that when evaluating a vendor/product he looks for clients who are more likely to care about security, such as government or military customers. This is an interesting contrast to other participants who typically look at what is used in their industry.
	Participant Summary: In general this participant provided very little input and definition of the various actions taken during the acquisition process. The participant did not provide a lot of support for his statements. The way that security is viewed in this company is curious considering the participant's background. Security is recognized as something that must be addressed; however, management is not very interested and is frustrated by this. The goals and purpose of any security efforts are unclear; security seems to exist for the sake of doing something which can be called security. While the participant says that security is part of the obligation to customers, his answers do not indicate that there are any specific measures taken to address any specific concerns, even at a high level (e.g., protect personal information, prevent external intrusion). The users are given any unreasonable amount of trust and there is no policing or auditing of their actions. In terms of the participant's external decision input, he relies upon weak sources and personal connections, which may increase biased decisions.

Participant #9315314	
7	The impetus for acquisition often comes during the annual budgeting process; each business unit is interviewed to determine their needs for the upcoming year. In addition, the participant may determine a need from his own review of the current systems or it may come directly from an revenue generating opportunity proposed by an external customer.
10	The participant notes that the amount of time research and evaluation is highly correlated with the expected dollar cost of the component being acquired. Things which will use up more funding will require more backing to substantiate moving forward. In relation to security this may be a bad thing because even a low dollar cost may result in a big system impact.
14	There is a weekly meeting with the CFO where she wants a proven business case to justify the cost. To this end, everything must be evaluated and defined including user requirements, site preparation, and what people or processes are affected.
19	The vendor came highly recommended and as a result there was little consideration beyond dollar value. The participant notes that he rarely ever expects software to be good because it is not until service packs are released that decent quality assurance has been performed. He cites a major factor in favoring any particular product is often attributed to support. A clear support contract is necessary because, as he stated above, there will always be problems with any component. However, it is usually only the big ticket products which have formal support contracts specified. Smaller vendors may not see the value in providing support and documentation in comparison to the pricing they offer.
24,25	There is generally good communication in this company. The participant interacts directly with the CEO quite often. In addition, the participant and upper management discuss issues in regular one-on-one meetings which help filter information both upwards and downwards.
31	The participant highly values end-user input and believes it increases efficiency and in addition makes IT more transparent and the IT department's contributions more visible at all levels.
32	Work with users to understand the business requirements and to make sure there is a clear translation between IT systems/processes and business objectives.
34	The participant cites both active and passive resistance to the introduction of new systems. The users feel like they are being punished with a system change. It should be noted that while communication is very good and their needs are considered (see #32) there is minimal user involvement in the selection and decision process.
37	The participant provides training about a month out and informs users of selection choice very early on in the process. They have experimented with when to train users and now start efforts when the product is in the implementation/validation phase. The end users further are involved in writing custom documentation, which also helps established business user SMEs.
40	External customers have specific regulatory measures which then affect how the participant and his organization implement security protection. A large percentage of the security auditing is supported or performed by the customers or their consultants. In general the participant notes he prefers efficiency over security.
42	The participant notes that there are no specific security guidelines for the acquisition process but that the business requirements may define any security concerns, but not necessarily.
43,44	As the company grows in size there is an increased concern for end-user security and they are working to establish retraining efforts. The participant recognizes the possibility of insider threats. The users work in tightly controlled environments and efforts are made to provide read-only access whenever possible and customer data and critical information is highly segregated. At the same time, internal company data is not controlled as much and is relatively open.

46	Participant responds that he believes internal controls are sufficient and more effort would only be needed with a public presence or if there was some external portal. However, current internal production systems are not completely blocked from external access.
	Participant Summary: The participant enjoys good support from upper management in terms of acquisitions and security. There is a high level of consideration with users, but a limited amount of actual involvement in the decision making process. Security is perceived at a perimeter level and the participant operates under the assumption that compliance with broad regulations is sufficient to define an adequate level of security for the organization. Beyond compliance, security is seen as a nuisance and is not embraced; internal data that does not belong to customers is given relatively little security or protection.

Participant #9892105	
4	The participant has a relatively large IT staff and makes efforts to ensure they are going to training and conferences. He can go to training/conferences when he requests.
7	The initiator may be either a business analyst within IT or a representative of a particular business unit. Needs are then discussed and evaluated as a joint effort between the business unit and the IT group.
11	The participant primarily looks for flexibility and scalability in a product, where is the product going in the future and will it grow with our needs. Moreover, the quality of the vendor is extremely important and is the second most important factor after price. The participant looks to form partnerships with vendors. Beyond analyzing the product offerings he wants to know that the vendor is financially stable and what comprises their business vision and strategy in order to evaluate long-term value and sustainability of support over time. As a partner, the participant notes it is important to evaluate what the vendor can do for your business beyond simply selling you a product.
15	The participant notes that in general the culture of the organization is interested in maintaining the status quo. When change is needed, business units may come requesting a specific product rather than identifying core needs and requirements. It can be difficult to get the business users to sit down and discuss the requirements and details. Because the assets are ultimately implemented and maintained by the IT team, it is important for them to pick the best products for the total IT infrastructure rather than the business units preferred selection, which may not have been researched or selected through a comparative analysis.
19	The participant stresses the importance of performing sufficient due diligence to ensure that as many issues are addresses proactively as possible and that strong communication is important throughout the process with users, vendors, and within the IT team. If necessary, you must be willing to modify timelines and plans to address concerns before they become problems.
24,25, 28	Some people view IT as a cost center, while other members of management look to establish partnership relationships across the business with IT. The participant enjoys very good two-way communication with upper management, including the board of directors. While not all members of management are concerned with IT, those that do understand how IT will help drive the business forward.
29	The participant believes that the acquisition selection does not have a large impact on the company. Those who complain about a particular system or component often have a personal agenda or bias and usually do not have business rationale as their justification. Combined with the response to #15 above, it would seem that the participant uses business justification over user acceptance as the metric for measuring system success.
32	User complaints are factored into the process through reviewing support tickets. Users are then brought on early to the decision making team. However, it seems from the previous responses that their purpose is mainly for IT to understand the business requirements and they may not have limited decision influence.
34	He notes that the end-users are fairly resistant, but that this reluctance is decreasing over time. He attributes this change to policies he has enacted since joining the company. In the past acquisitions were largely decided by the business units and the IT team would simply administrate these systems and there was a general lack of internal partnering. Also, in the past a policy of using preferred vendors led to poor selections, which as a result lowered end-user confidence in the performance of new components and systems.
40	The organization has both internal and external motivations. The external motivations come

	from regulatory compliance and customer security requirements. Internally, there is a focus on both protecting customer data and on protecting the organization's proprietary information and intellectual property.
43,45	The users are consciously aware of the policies and must sign an acceptance of the policies annually. The participant notes that the language is very clear, without acronyms, and it would be very difficult to plead ignorance of the rules. Management is very tough on security and non-compliance has resulted in past terminations.
47	Security is primarily considered as business requirements, not a technical requirement. While it is good to match any IT need to a business objective, some security must exist purely technically as a type of overhead or there is a risk of having insufficient security when it is not considered in the business case.
50	The participant again notes that all decision must be logical and that emotional impact on decisions should be minimized. Even within the IT organization, is it important to remember the business requirements. In addition, whenever possible components should be commoditized; a component should plug-in easily with the system and it should be possible to replace that component with a similar option without much modification to the overall IT infrastructure?
	Participant Summary: The participant has extensive business experience and enjoys an organization with strong communication. He has a very strong business focus and works very hard to tie together IT and business objectives. The one concern is that all security concerns may not be considered in a business justification or from internal IT projects. In addition, while there is communication and involvement with the end-users, it does not appear that the participant gives sufficient consideration to the human/soft needs.

Participant #9988237	
4	Attend conferences and events regularly because the organization wants to know what is going on in the industry and what the market is looking for to better target the organization's product offerings.
7	On a monthly basis the IT team meets and any members of the IT team can make suggestions. Almost all acquisition projects are initiated by the IT team. Most projects focus on solving problems, there is very little opportunity seeking in this organization.
11	The participant defines the systems and components that he acquires as mainstream, defining the organization's IT needs as "vanilla". Preferred vendors are almost always used in the acquisition process. The mainstream is defined by the participant "as small businesses" or "common to any business". There is very little experimentation and the participant believes that by sticking the mainstream they are getting products "which are tried and true" and that users will be most comfortable with. This philosophy, however, makes assumptions that their IT needs truly are vanilla and that the masses have made an informed decision, rather than relying on the same wisdom of the crowd philosophy.
12,13	These definitions are very weak and the decision maker relies heavily upon his staff doing a thorough evaluation and research; however, there is no guarantee that they are using any common criteria or any criteria in their decisions at all as far as the decision maker is aware.
17,18, 19	On an upgrade projects there was poor communication between IT and the business unit. The business unit was heavily resistant about changing their infrastructure. As a result, there was a termination. The participant believes that in the future better communication is needed with a clearer focus on business objectives as opposed to emotional and personal biases.
25	There is limited communication and direction. Management expresses some interest, but they are not highly interested in following up
26	Management's involvement in decision making is limited; however, it does increase if they are personally interested in a particular acquisition project.
32	Users are not formally part of the acquisition process; however, the IT team monitors the helpdesk to identify user-focused issues. The participant also commented on the support system explaining that there was too much in-person support requests and they are trying to force increased usage of the helpdesk system.
37	A rollout process is defined before implementation; however, the participant explains that there is no common criteria or time frames that he can recall over time.
39	Security is of growing importance to management as they increase the amount of work where customers require certain security standards and implementations in order to compete for contracts.
41	The participant described the majority of the regulations as being non-technical dealing with export agreements and international trade agreements. The participant believes that enforcement of these policies is more casual then through any technical or internal policy means.
42	They are working on developing new policies and have plans to include security through the SDLC because having such policies specified will be a direct requirement of their external customers.
44	There are minimal concerns for internal issues such as data leakage. The participant trusts his employees "because they are an asset of the organization", which is a very weak argument that lacks any rationale. There is a culture of trust in the organization, and a minimal amount of user-control. In regards to compliance with regulations, he believes the employees are aware of their requirements, but notes that there is currently no way to enforce or monitor compliance.

50	While the participant trusts his end-users, he would like to implement some controls to prevent accidental breeches of policy or poor security actions. Security is just beginning to be important to this organization and that participant believes that awareness and controls will increase as management increases their understanding of the importance it has specifically for them to do business with their external clients. Lastly, the participant notes that being overzealous about security could be just as costly as not doing enough, however, there is no mechanism or measure in this organization to see where they are on that continuum.
	Participant Summary: While management understands the importance of IT, they are not highly concerned with its operation unless they are personally involved. There is also minimal user involvement while there is some consideration. Because the organization believes their IT needs are vanilla, they assume they already have what they need and there is very little searching for opportunities. As a result, they do not search for reasons to disprove the vanilla theory by querying more user opinion. This also has the effect that users are not expecting the systems to be customized to their needs therefore making it hard to anticipate any direct benefit to themselves as the result of new system or component. Because security is needed in order to remain competitive and there will be a very high amount of external pressure, it is very likely that security will increase over time, especially because management is beginning to understand how security is a necessary cost. However, this may not lead to the best possible security fit for this organization because there is no internal pressure or internal consideration of the realistically non-vanilla needs.