An Exploratory Study on Managerial Security Concerns in Technology Start-ups

Boon Yuen Ng
Department of Information Systems
National University of Singapore
ngby@comp.nus.edu.sg

Anqiang Eric Feng
Department of Information Systems
National University of Singapore
fenganqi@comp.nus.edu.sg

Abstract

Studies have shown that smaller businesses are less likely to have extensive security in place because of the false sense of safety being small. What is more worrying is that small businesses are being attacked more frequently in today’s environment. Since protective measures often require significant managerial vigilance, an appropriate level of awareness and concern among managers may be a prerequisite for adequate security protection. Given its importance, there is a need to understand the factors that influence managers’ security concerns. Using the Model for Managerial Perceptions of Security Risk as a framework, we explore the factors that influence security concerns of small businesses. Ten technology start-ups in Singapore participated in this study. Findings provide an in-depth understanding of the factors – Organizational Environment, IS Environment and Individual Characteristics. Two new factors that significantly influence managers’ concern are identified – Trust between Managers and Employee, and Alignment to Business Needs. With a better understanding of these factors, more effective security management can be designed to heighten security consciousness of managers in start-ups. Findings also provide an impetus for researchers to conduct future studies in this domain.

Keywords: Information Security, Security Risk, Small Business, Technology Start-ups

1. Introduction

Information security refers to the protection of information and its critical elements, including systems that use, store and transmit that information (Whitman 2004a). Management of information security is increasingly gaining importance as our dependence on information and communication technologies grows. However, managers seem to have a low regard for security (Straub 1990). Many organizations feel that information security has no value when there is no visible attack and this perception remained unchanged over a decade (Ernst and Young 2004). It is therefore appropriate that research efforts reveal the circumstances in which low security consciousness is likely to occur (Goodhue and Straub 1991). With this knowledge, more effective security management can be designed to heighten security consciousness of managers and even employees.

Small businesses have a different environment compared to bigger organizations. A recent study has discovered that many managers of small businesses have little understanding of information security threats, risks and the associated business implications that might result (Kotulic and Jan 2004). Smaller businesses are also less
likely to have extensive security in place because of the false sense of safety being small (Kotulic and Jan 2004). What is more worrying is that small businesses are being attacked more frequently in today’s environment (Kankanhalli et al. 2003). Given its importance, there is a need for better understanding of the factors that influence managers’ security concerns in small businesses.

As such, this study aims to contribute to the security literature by exploring the factors that influence managers’ security concerns in small businesses. In particular, we have chosen to study technology start-ups, as such small businesses are typically dependent on the Internet which exposes them to online security threats. Our research question is, "What are the factors that influence managers’ security concerns in technology start-ups?" Through this study, we aim to contribute to the better understanding of managerial concerns and perception of security in the context of small businesses, so that security in small businesses can be improved.

2. Literature Review

A number of studies have examined computer usage in small businesses but do not specifically address security issues underlying computer usage (Nazem 1987; Delone 1988). Other studies have researched security issues but these studies were conducted in relatively large organizations (Straub 1990; Straub and Nance 1990; Loch and Carr 1992; Straub and Welke 1998). A number of researchers have suggested that organizational size is a significant variable and thus it was hypothesized that the IS concerns of small businesses are different (Alpar and Ein-Dor 1991).

Results of a study conducted on 1200 small businesses suggested that small business owners and managers do take some steps to secure their computer systems. However, in specific areas such as physical security and managerial control, serious problems were found (Pendegraft et al. 1987). Findings from another study showed that there was a moderate level of security awareness but low level of security implementation in small businesses (Bradbard et al. 1990). Results from a recent study showed that small businesses have a “low-risk” attitude regarding external threats (Keller and Powell 2005). The “small is safe” fallacy was also consistent with other studies done on small businesses (Herbert 2003; Kotulic and Jan 2004). Small business managers felt that they were at a low risk from Internet threats as they were too small to be of any interest to the hackers (Herbert 2003). It was noted that smaller businesses were also less likely to have extensive security in place (Kotulic and Jan 2004). All these studies emphasize the need to explore the security environment of small businesses in particular. There are few such studies and this will be considered of value to the security literature considering the significant number of small businesses connected to the Internet.

3. Research Model

Figure 1 presents our research model, which is based on the Model for Managerial Perceptions of Security Risk (Straub and Welke 1998). This model argues that a manager’s concern about security in the organization depends on the potential of abuse in a given industry, company-specific action that has been taken to maintain security, and
individual factors such as computer literacy and managerial role (Goodhue 1986; Goodhue and Straub 1991; Straub and Welke 1998).

**Managerial Perceptions** – This reflects the manager’s concern about security or systems risk in the organization. Systems risk is defined as the likelihood that an organization’s information systems are inadequately protected against damages (Straub and Welke 1998).

**Organizational Environment** – This refers to the external environment (industry) of the organization. It reflects the level of risk that is inherent in the industry. Managers in industries with a high level of risk would be more concerned about security.

**IS Environment** – This reflects managers’ basic understanding of technical and managerial security controls, as well as company-specific actions that have been taken to control systems risk. In organizations that allocate significant resources to providing security, managers would be less concerned about security.

**Individual Characteristics** – This reflects how well informed managers are to local incidence of computer abuse and susceptibility to damage, such as awareness of system violations and background in systems work. Greater awareness would bring about greater concern.

![Figure 1 – Model for Managerial Perceptions of Security Risk (Straub and Welke 1998)](image)

### 4. Research Methodology

It has been suggested that when doing research on topics as highly sensitive as IT security, mass mailings of surveys may not be appropriate (Kotulic and Jan 2004), because companies are less likely to divulge highly sensitive data in survey. For this reason, information is gathered from the start-ups through one-on-one interviews, in a semi-formal manner. Such interviews can be conducted in a sensitive manner such that start-ups will feel more at ease. Hence, more insights can be generated, providing a rich source of data and content for analysis (Yin 1994).

Ten technology start-ups from Singapore participated in this research. For all ten companies, the Chief Executive Officer (CEO) represented the company for the interview. All ten companies are operating for less than three years. Nine out of ten companies have less than ten employees and most of them are part-time employees. Only one company has 12 employees. CEOs have also requested anonymity for this study to protect their companies’ interests.

Each interview session took about 45 to 60 minutes. During the start of every interview
session, the objectives of the research study were read out and any doubts were cleared
before proceeding with the interview. Pre-determined questions were asked and
participants also expressed their views in addition to the questions, thus adding richness
to our findings.

5. Results and Analysis

5.1 Key Findings
The key findings gathered from the interviews will be organized using the Model of
Managerial Perceptions of Security Risk (Straub and Welke 1998).

5.1.1 Managerial Perceptions
CEO’s views of security indicate low concern for system risk. All ten companies – in one
way or another – feel that security should not be the main focus at this point of time.
“Security to us is done in bare necessity. The main thing is still the service that we
generate revenue from and whatever it takes to maintain that service. We won’t go all out
to plan our security.”

Risk is a function of two main factors – risk impact and likelihood of security breach
(Stoneburner et al. 2002). In the findings, start-ups perceived both risk impact and
likelihood of security breach to be low due to the availability of contingency plans and
the company’s small size respectively. Most start-ups feel that the risk impact is low as
they have nothing much to lose in the first place. Being start-ups, many of them feel that
they are too small to catch attention of the attackers. Hence the likelihood of getting
attacked is also low. However, the CEOs view that if the start-ups increase in size, the
value of their assets will increase too and they will then begin to focus on protecting their
assets since there will be “more to lose”.

5.1.2 Organizational Environment
All ten companies interviewed agreed that risk is inherent in their industry and they are
constantly faced with threats such as the emergence of viruses and worms or hackers
stealing data. However, as discussed earlier, the companies felt that their small size
reduces the likelihood of attacks despite the inherent risk in the industry.

5.1.3 IS Environment
During the interview, CEOs were asked to list the security controls that were
implemented in their companies. All the controls that were listed were either technical
controls, such as encryption of data, or operational controls, such as regular back up of
data. However, there seems to be a lack of management controls. For example, all start-
ups admitted that they do not have any security policies written in black and white. Most
of the policies, such as regular reminders to change passwords or patch their software, are
communicated verbally. One company echoed the views of other companies on why
there is no need for security policies at this point of time:
“Our company is relatively small. All the employees are in one office...When our
company expands, say more than 20 people, that’s when we will need to sit down and talk
about the policies to implement.”
Interestingly, like other bigger companies, start-ups tend to overlook the insider threat even though many studies have shown that the greatest threat of computer abuse comes from within the organization itself – its employees and contractors (Whitman 2004b). Most of the controls implemented deal with threats from outside the organization.

One start-up raised an important point on expertise. Even if start-ups are given a whole list of security threats that might affect them, expertise and resources would still be a significant determining factor, as start-ups do not have the “liberty to hire security experts”.

5.1.4 Individual Characteristics
During the interview, the CEOs were asked to self-assess their level of security knowledge and computer literacy. Only two CEOs rated their security knowledge and computer literacy below average. Interestingly, both CEOs outsourced their security function to a third party for that reason, that is, the lack of security expertise and knowledge.

One of the start-ups described a recent security incident which made him more alert to the possible consequences of a security breach. Another start-up also experienced a similar security breach. As this start-up summarized:
“Once bitten, twice shy. You need a security breach before any security measures come up. So if nothing happen, we would not do anything.”

5.2 Other Findings
Beside the earlier points, two important themes were raised which have a significant influence to the managers’ concerns of information security.

5.2.1 Strong Trust between Managers and Employees
Most of the CEOs reasoned that trust is a major factor for the lack of security controls in the company. One of the reasons that they can operate by trust is due to the size of the company. On top of that, most of the employees hired are friends of the CEOs. Being small indicates a stronger cohesive bond among the employees and management. As such, perceived threats come from external instead of internal. Thus, most of the security measures are for protection against external threats. Some of the CEOs felt that trust is more reliable than security controls. However, they admitted that trust cannot replace security measures and policies when the company starts growing.
“Right now, we have a core group of people whom we trust. When we hire more programmers, we will put a few security policies in place as we do not know them personally.”

5.2.2 Alignment to Business Needs
For most CEOs, security becomes a liability when it does not provide any business value. They would rather concentrate on “coming up with the product, marketing and sales” which bring direct value to the business. Most of the CEOs also concur that security is not of a high priority at the beginning stage of business development, mainly due to
limited time and resources. Unlike larger organizations which may have the money and human resources to invest in security, start-ups have to allocate their resources at the right places to ensure success of business. If precious resources are to be allocated to security, it must have high business value, either expressed by customer needs or reflected as a cost saving initiative.

A few companies stated that before they plan for security or invest in any security products, they would first carry out a cost-benefit analysis as security is a form of cost. There are a few start-ups that outsource their security function to third parties as a form of cost saving. In this way, they do not need to spend their effort on implementing and maintaining security which they perceive as non-critical and does not add business value.

6. Discussion and Implications

6.1 Discussion

Our findings have shown that start-ups perceive their risk level as low, even though they agreed that risk is inherent in their industry. One of the key reasons for the “low risk” attitude is due to the perception of “small means safe” fallacy. Small business managers often feel that they are at a low risk from security threats as they view themselves as too small to be of any interest to hackers (Herbert 2003). It may take a security incident for them to be concerned about security. This is consistent with another study which pointed out that investing in information security is something that all too often does not occur until after a system has been compromised, a computer has been attacked or a federal mandate requires it (Keller and Powell 2005).

As the perceived risk level is low, protection measures tend to be less than adequate too. As observed from our findings, the companies focus mainly on technical and operational controls. Management controls is definitely lacking, as we see that the companies do not plan for security because of their small size. Another common observation is the lack of resources and security expertise. Outsourcing becomes an attractive option, as start-ups do not have the resources to hire security personnel.

An important factor that influences managers’ perception of security risk is the high level of trust among employees and manager and this seems unique to start-ups. Because of the high level of trust, there is less concern and need for security measures, especially for protection against insider threats. Managers have also pointed out that alignment to business needs is a pre-requisite for security implementation. Unlike larger organizations, start-ups are limited by their resources such as time and money, as well as the need to concentrate on their core business. Security naturally becomes secondary.

6.2 Implications for Practice

The findings provide an in-depth understanding of the factors that influences managers’ perceptions of system risk in small organizations, in particular, technology start-ups. From this study, a stronger managerial case can be built to educate managers of small businesses about security threats and protective measures. A customized set of security measures and policies that will be applicable and useful to small businesses can be
created to better suit the context and environment. With a better understanding of the factors influencing security concerns of managers, we would also be able to craft out more appropriate security awareness programs that will effectively raise security concerns of these managers. Small businesses should also be educated that security can be more integral to their strategic initiatives (Ernst & Young 2005) as alignment to business needs is an important factor that we have uncovered. As small businesses tend to consider outsourcing, they should also be educated that outsourcing itself is also a security threat if inadequate attention is paid to vendor risk management (Ernst & Young 2005).

7. Limitations and Future Research
In this study, only one interview session was conducted with each start-up. There can be additional ways of collecting data from each company, adding to the richness of the data. A longitudinal study can be conducted to investigate security concerns of managers over time as the company grows in size and assets. Valuable insights generated from such studies will be useful for both business practitioners and researchers. Another limitation is that all companies are based in Singapore, which has an established legal framework in electronic transactions and computer crime. This may explain why inherent risk in the industry does not seem to be a significant factor among the companies we interviewed.

Studies can be carried out to test the new factors that we proposed. Exploratory and empirical tests can be performed to identify and explore the relationships in further detail. Besides the two new factors that we identified, there could be other factors that play a significant role in implementing security in start-ups. Behavioral theories can also be introduced to explore other factors that may influence the security concerns of managers. This study can also be extended to other small businesses of a different nature or in a different country.

8. Conclusion
In this study, we have discovered that security concern of technology start-ups is relatively low and we have identified some factors that influence security concerns of technology start-ups. Rich data and valuable insights have also been collected and organized to give us a deeper understanding of managers’ perception of security. This gives us a more comprehensive and in-depth understanding of factors that influence manager’s security concerns and perception of risk, leading to useful insights to the planning and implementation of security in start-ups.

References


