Strategic Decision Support For Information Protection: A Facilitation Framework For Small And Medium Enterprises

Myron Z. Sheu, (Email: {Email: msheu@csudh.edu), California State University, Dominguez Hills
Wang C. Wong, (Email: wcwong@csudh.edu), California State University, Dominguez Hills

ABSTRACT

Information security seriously concerns Corporate America but the soaring cost on protecting information assets raises equal concerns. These concerns appear to be more threatening to the small and medium enterprises (SMEs) as the percentage of their IT budgets spent on information security protection sharply surpasses those percentages budgeted by large enterprises. In light of these concerns, we propose an integrated and attainable framework that could heuristically promote strategic decision thinking on protecting information assets for the SMEs. In comparison to other approaches that aim at reaching an optimal decision through complex mathematical models, our framework requires no such computations. The goal of our approach is to help a SME reach such decisions with a framework that takes business, technological and managerial issues into account. The proposed framework fosters strategic thinking of security issues with simple and practical steps to achieve a balanced, consistent, and efficient protection with total involvement from all stakeholders of the information assets that need to be protected.

CHALLENGES TO PROTECTING INFORMATION ASSETS

Security is going main stream; it is fundamental to e-business and it is not an afterthought strategy anymore. It is tightly integrated into e-business infrastructure and becomes increasingly less of separate function within IT. Security is also going to Main Street. Every small and medium business will have some sort of e-business functions. With rapid increased outsourcing of solutions and services, security is even more critical and requires simplification and integration to the entire business operation. On the other hand, the soaring cost on protecting enterprise information assets equally concerns Corporate America. As a survey conducted by Information Security Magazine (ISM) as shown in Figure 1, these challenges appear to be more threatening to the competitiveness of small firms: the percentage of their IT budget devoted to security protection sharply surpasses the corresponding percentage budgeted by large enterprises. Due to a much smaller IT unit, a small or medium enterprise (SME) often does not possess strong expertise and resource to support its information security. As a result, it is likely for the SME to handle security protection in an ad-hoc manner. The protection is often at the price of sacrificing the total utility of its information assets. Such a practice is definitely detrimental to its competitiveness due to the following reasons:

- Ad hoc security measures don't maximize the protection on information assets.
- Ad hoc security protection oftentimes hinders the strategic uses of information assets.
- Investments on ad hoc security protection perish more quickly, attributable to inconsistent policy and technology being endorsed.

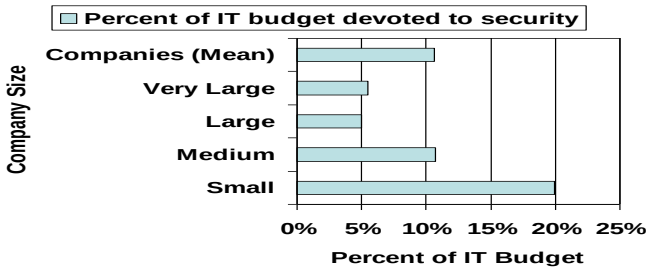

Figure 1. Spending by company size (Source: 2002 ISM Annual Survey of 215 information security practitioners).

Security is always a *delicate* combination of practice, policy, technology and know-how. The ultimate goal of security control is to protect the information assets of a company. To understand why a SME is easily overwhelmed by the complexity of securing and protecting its information assets, we summarize the most common security concerns and their corresponding technological solutions in Table 1.

Table 1: Security Concerns And Protection Tools/Solutions

Security Concerns	**Tools/Solutions**
Secure Connectivity	Virtual Private Networks (Herscovitz, 1999), Public Key Infrastructure (Bosworth & Tedeschi, 2001)
Perimeter Security	IP Firewall, Site Management Tools
Security Monitoring	Intrusion Detection, Virus Scanning
Identity	AAA Principle (Authentication, Authorization, Accountability)
Security Management	Policy, Trust
Content Security	Role-based or Task-based Access Control (Oh and Park, 2003), Semantic Firewall (Callahan, 2002)

Without a dedicated IT security team, it will be almost impossible for a SME to grasp the whole picture of security, let alone making strategic planning on protecting its information assets. The return on investments in security protection is so volatile but at the same time such investments become inevitable, knowing how to protect its information asset effectively and efficiently has emerged as a new battlefield for maintaining the strategic advantages of an enterprise. Obviously, if SMEs do not have a good understanding on these issues, they will stand to lose against the corporate giants. A significantly smaller return on investments in security protection certainly is not acceptable; it threatens the long-term prosperity of the SMEs. To offer effective facilitation, we first identify the causes to their weaknesses. We have investigated the practices on information security in two small IT consulting firms. We then develop a model that is suitable to help SMEs to make strategic decisions on security protection. While applying the model to real situations, we discover that a model itself is not sufficient; we need to define the process on executing the model.

The organization of the paper is as follows. We analyze and identify the common practice in security protection at two SMEs in section 2. In section 3, for clarifying our research motivation and focus, we summarize our survey of existing facilitation methods for security protection. We then discuss the quality attributes of security protection in section 4 and the value attributes of information assets in section 5. With all the factors identified, we present our version of a decision-support model in section 6 and an execution process for the model in section 7. Afterwards, in two sections that follow, we examine an application and conduct an effectiveness analysis of our facilitation framework. Finally, we highlight the significance of this research in section 10.

ANALYSIS OF COMMON PRACTICE IN SECURITY PROTECTION OF A TYPICAL SME

We have investigated the practices on information security in two small IT consulting firms (we hereafter refer them as Firm A and Firm B). While both firms have similar size in terms of the number of employees, approximately, around 30, Firm A is relatively young in terms of business maturity whereas Firm B has been in the consulting business for more than two decades. Consequently, Firm A struggles for cash flows while Firm B can operate on accrued revenues due to its established credit and account receivables. Since both are in IT consulting business, they have made extraordinary efforts on protecting information assets. Surprisingly the efforts at both firms on information assets protection remain quite primitive and often without direction. We summarize both positive and negative findings of their practices on information security protection as follows.

- Management has been highly decisive but manages the issues largely by hearsay. The management is highly supportive for protecting information assets and often makes a commitment right on the spot. We were told by their system engineers that **t**he best chance to get management's support was when some successful hacks or security concerns were reported on the news media. There is no separate budget on information security but, as needed, the total budget allocated for general system infrastructure could be used to block the security holes.
- Security protection is considered as a strict technical issue. It is interesting to notice that the senior managers at both firms do not know much about protecting the data that they access daily. Functional and administrative personnel nearly never get involved in discussions of information security. While the firewalls and anti-virus programs have been heavily deployed and frequently upgraded, internal access control nearly does not exist.
- Inconsistent decisions on investments in information security heavily rely on a few silver bullets. There is no formal security policy established for the firms to communicate with their staff about the security issues. Nearly all the security projects are launched in a reactive manner. A change in key security personnel usually brings about severe interference to security protection and often triggers a dramatic shift of security software and hardware being deployed.

Although these deficiencies are troublesome, they are by no means *atypical* in SMEs. On the upside, we also observed some good qualities that may be naturally inherited to SMEs. If leveraged properly, they could become significant advantages over large firms. They are highlighted below.

- The decision cycle is brief. Unlike a large organization, a commitment or an approval to security initiatives can be obtained in a timely manner at both firms. Usually such a decision is made by the senior management upon their intuitions without significant involvement from the functional managers. However, the decision is always responsive and directly addresses the current situation and provides solutions at least for the short run.
- The information system infrastructure is quite uniform. Both firms are specialized in certain business sectors and certain types of applications. For example, Firm A has been focusing on customer-relationship applications and Firm B serves the clients in the legal service sector by integrating the data from various legacy systems. The specialization allows them to maintain somewhat homogeneous system infrastructure. Consequently, the required protection schema is much simpler and can be uniformly applied, which lessens the integration issue and improves the efficiency.
- A strong sense of accountability is shared between the management and security personnel. Both firms hold a system architecture team that consists of two to four system engineers who respond to all the computing needs for the entire firm. The small team thus possesses a vertically integrated knowledge of the system infrastructure and its needs for information security. If a security problem occurs, the designated engineers would work dedicatedly around the clock to resolve the problem without going through a bureaucratic process of approval and multiple remedy tickets that are usually required in large firms.

Concerned with the fact that a higher percentage of IT budget spent on security protection by small firms and the findings from these two firms, we believe SMEs need a simplified and attainable facilitation that can help them overcome their weaknesses and at the same time brace their strengths. With such a motivation, we have studied the

existing research on facilitating information security protection and have developed an alternative approach to facilitation, particularly suitable for SMEs.

EXISTING FACILITATION METHODS FOR SECURITY PROTECTION

Researchers and industrialists have been intensely exploring facilitative approaches to protecting information assets. One representative direction is to advance the technologies for access control. Extended from database management, role-based access control models characterized by (Sandhu, 1996) have improved the versatility of security control. Bertino et al. (1998) presented a temporal access control model and made such a model more expressive. While early research results represented a logical programming approach to role-based access control, successive research results advanced the status quo with graph transformations as exemplified by Koch et al. (2000). Although these two facilitation schemes share the same theoretical foundation and in principle can be converted to each other, the graph approach involves the stakeholders in security management much easier.

To further enhance the declarative strength of security deployment in response to the increased complexity of enterprise information systems, some researchers investigated the feasibility of incorporating more intelligence into access control scheme. Botha et al. (2002) proposed a dynamic model, based on trend analysis, fuzzy logic and neural networks. In efforts on maximizing the benefits from security control, some approaches suggested that information assets be protected in terms of specific concerns from major stakeholders. Typically, Walton (2002) proposed a multi-tiered model that consists of network infrastructure, middleware, Web infrastructure, and a set of applications and services available to the user community. The resultant architecture would cover policies, business practice changes, and user awareness concerns. In the same direction, Bakry (2003) recommended a general procedure for specifying security protection in which the effectiveness of security protection relevant to cost and legal rights was considered. To assist in centralized control on security deployment, Rees et al. (2003) suggested that policy development be an iterative process that should have feedback at every step.

As the cost on security protection continued to soar, other researchers have been in search of valid models to figure out optimal investments in security protection. Gordon and Loeb (2002) in their research emphasized that firms should pursue an optimal level of information security investments in lieu of the return on such investments because the traditional formulas for ROI simply did not apply. Another representative model by Cavusoglu et al. (2004) is to evaluate security investments in terms of three purposes, namely prevention, detection, and response, for each of which they proposed specific mathematical models based on game theories to estimate the return on IT security investments.

DESIRED QUALITY ATTRIBUTES OF SECURITY DECISIONS

These recent advancements suffer from some critical deficiencies, among which, two are addressed in our research. First, these models still too narrowly interpret security protection and largely overlook the effect of security measures on the total utility of protected assets of which the stakeholders usually possess different valuations (Seddon et al., 1999). Second, their proposed models are increasingly complex and demand in-depth expertise in a variety of fields. Such approaches to facilitating information security planning not only exceed the affordability but also highly likely clash with the management style of SMEs. Even if SMEs would applaud a holistic approach to security protection (Eloff and Eloff, 2003) for the fear of devastating consequences of information security breaches (Campbell et al., 2003), the complexity resulting from all the issues involved in security protection (Knapp et al., 2004) would make such a goal unattainable to them. Any effective facilitation must be simple and practical. Security protection profoundly impacts the total utility of its information assets and closely affects the strategic competitiveness of an enterprise. As firms stretch their affordability to costly security protection, those invest for a sustainable return would be able to gain a competitive edge. In accordance, we believe the return on IT security investments should be tied to the corporate competence in protecting its information assets. Such competence should be assessed in terms of three key quality attributes:

- Is it durable?
- Is it invincible?
- Is it intrinsic?

The durable attribute implies that such competence should give a firm a handsome return over a longer period of time than what its competitors could reach. The invincible quality attribute requires that such competence continue to foster even if key security personnel have changed and key technologies underpinning the protection have evolved. The third desired attribute denotes that such competence must be inherent to the firm and hard to be copied by others, and thus become the firm's sustainable competitiveness.

TOTAL UTILITY OF INFORMATION ASSETS

Similar to the concept of utility in economics and finance (Sharpe et al., 1999, pages 142 – 144), we use the term *total utility* as a measure of the aggregated, rather than partial, reward or satisfaction gained from owning and protecting the information assets of a company. Three quality attributes, namely, *availability*, *integration*, and *reliability*, have been proposed in the past, suggesting that they represent the core value of information assets of a business (Strong et al., 1997; Tayi and Ballou, 1998; Parssian et al., 1999). Consequently, we focus on these three quality attributes for evaluating the total utility. If necessary, the set of quality attributes can be further extended. Equilibrium of these three attribute exists, which means that the value of each quality attribute may vary but the total utility of information assets could remain optimal. This is because the valuation of optimality changes over time and among different user groups. An analysis of the impact of security protection on the primary quality attributes allows a balanced assessment of the short- and long-term returns on investments in security measures. The concept can be better illustrated graphically. Figure 2 shows two curves, namely, the attacking curve and the efficiency curve in relation to the security protection of information assets of a company.

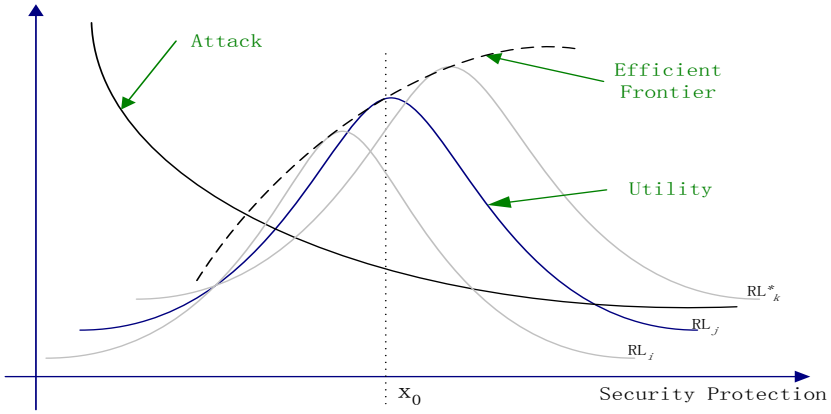

Figure 2. The relationship between security protection and utility of protected assets. *RL: Risk Level.

As shown in the figure, the X-axis indicates the degree of security protection on information assets while the Y-axis indicates the efficiency of both sides of efforts, namely, the intrusion side and the protection side. Each utility curve represents the efficiency that measures the total utility of the three quality attributes (i.e. *availability*, *integration*, and *reliability*) at a preferred risk tolerance level that a company is willing to invest to safeguard its information assets. The efficiency frontier is formed by connecting the optimal returns of each of the utility curves. The *Attack* curve describes the relationship between successful intrusions and the extent of security protection. Traditionally, the decisions on information security are made solely based on such a relationship. The effect of security protection on other business attributes is often overlooked. For example, while keeping other factors unchanged, the relationship between the access control and the resultant utility of protected information should be

measured to find out what the optimal extent of security protection is. As the intrusions increase, security protection has to be further tightened. The possible benefit may be the better reliability of information. However, as security control becomes excessive, the utility of information asset will likely shift in a reverse direction for a couple of reasons. First, the availability suffers as more strict access control is deployed. Second, the integrity of information deteriorates as information exchanges from various data sources become complicated and impassive. To a certain point, the disadvantages will overwhelm the perceived advantages. Therefore, the goal of our facilitation framework for sound strategic decisions should enhance all these three quality attributes in accordance with the feasible efficiency zone defined for a firm in support of its ultimate business goals.

Akin to many investments, we believe ultimately we should only pursue a sound and practical, rather than an optimal, decision on information security protection. This should be especially instrumental to SMEs where cost effectiveness is essential for survival and growth. Because of numerous interrelated factors affecting the return on investments in information security, it is extremely difficult to ascertain whether an individual decision on security protection is optimal. While pursuing an optimal result sounds attractive, there is no way to justify the ultimate return on such efforts and even worse, oftentimes, there is no way to verify upfront that such an optimal result does exist. Furthermore, when the business environment and conditions change, a previously made optimal decision could become obsolete. Therefore, any facilitation should heuristically guide the decision maker to stick to the principles as fundamental as possible.

NEEDS FOR STRATEGIC THINKING OF SECURITY PROTECTION

On the one hand, we have suggested a firm should cultivate the competence in information security protection and, on the other hand, we have proposed that a firm should exercise its competency in accordance with the desired total utility of its information assets. Clearly, what we need is a framework for facilitating strategic decisions that accomplish both. In reality, due to the intimate correlation between information security protection and other business performance attributes, any facilitation should promote inclusion of security protection into the corporate business strategic plan. We also believe that the return on security investments should be assessed over both the short- and the long- term results. To achieve that, our facilitation should help a decision maker gain an integrated assessment of the security issue in conjunction with other business issues. Nevertheless, as we pursue integrated thinking of security issues, the complexity unavoidably increases. Hence, decisions must be drawn upon an intuitive and analytical model in which concerns are represented in multi-layer resolutions so that decision makers can address them in a declarative and yet consistent manner. Constrained by such a decision-support model, for example, a security measure that least contradicts the concerns at a higher layer could be identified as the most desirable unless exceptional reasons uphold against such a decision.

Security decisions affect business prosperity. Reversely, business decisions also influence information security. Enterprise information assets are exposed to a variety of risks that in general can be classified into two main categories, namely, *natural disasters,* due to natural causes, and *artificial disasters,* due to negligent or malicious behaviors, which vary partially in accordance with business models. It is true that the ultimate threats of either type of hazard could result in the irrecoverable damage to the competitiveness of a firm, but the patterns of these two types of threat could significantly differ. Although the traditional statistical analysis may work acceptably well in predicting the risk of natural disasters, the occurrence of artificial disasters is quite unpredictable and varies from time to time and from hacker to hacker. As the frequency of such attacks is difficult to fit any patterns, the intensity of them could be gravely severe. The corporate competence in protecting its information assets could sharply reduce the likelihood of artificial disasters whereas it has little effect on natural disasters. Additionally, security leaks due to internal employees' unintentional mishandling can be classified as either kind of disaster since, on the one hand, human errors are inevitable but, on the other hand, the frequency of occurrence can be much reduced through effective prevention such as trainings. Ultimately, nearly every business decision would impact the security risk of information assets. At the highest level, the evolution of a business model may significantly change the risk factor of security protection. As shown in Table 2, a centralized information infrastructure may be able to better control and respond to artificial disasters while it exposes more to natural disasters.

Table 2: Security Risks Are Associated With Business Models

Risk versus Model		
Natural Disasters	High	Low
Artificial Disasters	Low	High

As another example to show the consequential effect of a business decision on security risk, a decision to mobilize the workforce is to deploy more wireless and portable computing devices. As a result, the enterprise information assets could be exposes to much more risks than ever. From these examples, we can see most measures applied to improve some quality attributes of a business, which likely incur an expense of information security. Therefore, the goal of any facilitation should encourage an intimate involvement from all levels of stakeholders.

OVERVIEW OF A DECISION MAKING MODEL FOR SMES

Preceding discussions identify the specific challenges and complexity of security issues that SMEs face. Our research has concluded that any effective facilitation for SMEs to think strategically about information security should take into account other business issues. At the same time it needs to be intuitive and attainable. It must also have provision to include total and systematic involvement of all stakeholders. With these principles in mind, our facilitation is to focus on the pragmatics, rather than optimality, of a security decision. As depicted in Figure 3, the model consists of three key components that must function cooperatively to deal with interrelated factors involved in security protection.

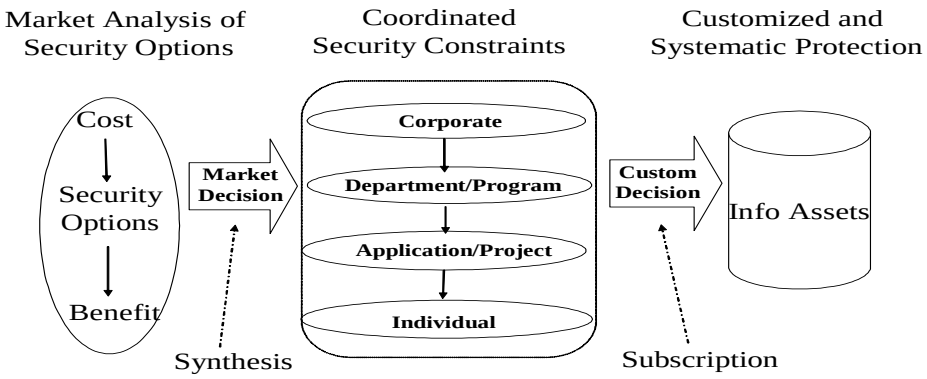

Figure 3. The architecture of a strategic decision model for protecting information assets.

The first component of the decision-support model, shown in the middle of the figure, is a layered constraint-based representation model that readily supports knowledge generalization and aggregation. Even though information assets are physically distributed, however, they are logically integrated. A supportive and well-defined representing schema could mitigate the weakness that security measures are usually applied to information entities without considering other more general levels of security protection. With a coherent but decomposable knowledge representation framework, multi-dimension concerns can be visualized since each security measure no longer functions in an isolated manner. Business requirements organized in terms of layers could affect low-level technical decisions in a justifiable fashion. Consequently, an inclusive comprehension of a complex security issue can be better supported at a chosen level of resolution. Due to specialization and distribution of responsibilities, decision makers need to understand an issue at an abstract layer of their level to avoid drilling down for excessive details.

Internal to the layered representation hierarchy, as the second component of the decision-support model, on the left in Figure 2, is a set of relevant default constraints that are grouped in terms of industrial security options. The ability to systematically identify security needs with minimal conflicts to the protection on other information entities profoundly correlates to the total utility of protected information assets. Therefore, our model supports that individual security protections must be measured in relevance to industrial practice in security protection so that the unique risk undertaken can be controlled and the total cost on security protection can be contained. In addition, custom constraints are organized in such a way that individualized security needs can be accommodated to the extent consistent to their parent constraints of the representation model. With our model, a security initiative that has minimal negative impact to the concerns of a parent layer would be first accepted unless exceptional reasons are against it.

Dynamic syntheses and subscription to granulated information entities is the third component of our model, on the right in Figure 2. They ensure a strong integration of security control but allow a higher degree of flexibility. As the business environment keeps changing, so does the protection on information assets. Such changes must be adapted in a reckonable manner, especially when measures are impacted. We propose that, on the one hand, all security measures be applied as a set of complementary measures and that, on the other hand, a clear subscription policy be specified such that exceptional needs can be accommodated. The third component of our decision-support model should help balance across multiple attributes of the valuation of information assets. For example, the response time to behavioral changes of a managed system could be a noteworthy indication of the effectiveness of security control. At the same time, the increased traffic monitoring should only be adjusted in accordance with the possibility of attack and severity of attack. Dynamic synthesis and subscription would offer an adaptable mechanism for users to deal with security risks. For example, while neither delayed response time nor slow detection on attacks is desirable, they should all be assessed in conjunction with other concerns that may be more overwhelming in scope and duration.

The model highlighted above would not happen without a full participation from all stakeholders. When we initially introduced our model to Firm A and Firm B, the general response was that it sounded reasonable but the stakeholders were uncertain how the goals could be achieved. We then ascertained the missing link in most of the previous research was the ***process*** of facilitation. Subsequently, we defined a process with both firms and customized the process to gain support from all decision makers at various levels. In the following sections, we describe the process in general and then illustrate how it works.

THE PROCESS FOR CONSTRUCTING THE DECISION SUPPORT MODEL

As identified above, the decision framework that promotes strategic thinking has to be accompanied with a process. The process will take into considerations not only technical but also functional and managerial requirements. The followings summarize the main steps of the process:

- Identify business applications, and classify them in terms of ownership, e.g. owned by corporate, by department, by group, or by individual.
- Compose an individual utility table (or utility tree, as shown in Kazman et al., 2001, if subsets of utility attributes need to be identified) for calculating the total utility of each application by conducting mainly the following two steps:
    - Identify all the user representatives at the corresponding level and collect the quality attributes from them.
    - Consolidate the required quality attributes by consulting with the user representatives and quantify the benefit of each quality attribute in relation to others.
    - Identify all the information assets accessed by the application and associate the set of quality attributes to these assets.
- Consolidate individual utility tables for the applications that share the same information assets either partially or fully through the following steps:
    - Collect the quality attributes and corresponding weights for all the group applications.

  - Select a common set of quality attributes and search for the efficient zone where the total utility reaches the maximal value as perceived by all concerned stakeholders.
  - Classify all the applications in respect to their needs for security protection and then repeat the same step until the discrepancies of their security needs within each resultant set of applications are insignificant.

- Identify and characterize the protection options available at the corresponding layer such that the chosen set of security measures yields the minimal redundancies over the measures at the previous layers and the maximal consistency with the measures on the sibling information assets.
- Identify and characterize the security options that would best support the delivery of the required utility as a group.
- Establish the security protection standard for each level of ownership in descending order by conducting the following two steps:

  - Identify the common security measures shared by the applications owned by the organizational units at the same level.
  - Remove the measures that have already been covered by the upper-layer security protection standard.

The outcome of this process would be a multiple-layer model that defines the security protection needs and security measures with minimal inconsistency. Each business unit is asked to define a subscription policy in a similar top-down manner to ensure the consistency and flexibility. For those without an explicit subscription policy, a default set of security protection will prevail.

By following these steps, a model for facilitating strategic decision making is generated to capture the unique security needs of an enterprise. The model for strategic thinking of security protection should remain valid for as long as the business model does not change. Because the mission and goals of an enterprise do not change radically, business models are relatively stable in most cases, including both Firm A and Firm B in our study. Therefore, the utility tables constructed for each level of the organizational units are also stable. All of these support the practicability of our decision-support model.

FEASIBILITY ANALYSIS OF THE PROPOSED DECISION-SUPPORT MODEL AND PROCESS

We have presented the strategic decision model and accompanying process to the two firms for their endorsement. The feedback was quite encouraging. The leadership of both companies was interested in complying with the model to change their traditional decision making approaches. In this section, we describe the customized process that has been adopted by these two firms. Note that the process closely follows the steps specified in our framework as discussed in the previous section.

At the corporate level, we asked the top management to identify the importance of each business function in support of the corporate mission. Such identifications provided us with the ultimate utility of corporate information assets. Interestingly, as shown in Table 3, the top management of these two companies perceived the ideal utility quite differently, in part because they are in different stages of business maturity. In accordance, we recommended a set of corporate-level security measures to each company, such as control on email services and virtual private networks.

Table 3: The Total Utility Of Corporate Information Asset Perceived By Senior Leaders At Two Companies In Different Stages Of Business Maturity

Stakeholder/Composite Weight	Integrity	Availability	Reliability
Company A	20	40	40
Company B	30	30	40

The differences between two sets of measures are subtle but distinctive. Particularly, access control and traffic monitoring vary significantly between these two companies because each firm has different response time requirements. We later requested the same kind of input for the same set of utility attributes from the accounting and marketing departments. The marketing department in Firm A does not have specific opinions on that while the accounting department weighed data integrity higher than two other attributes. We then asked the top management to assign an ***influence coefficient*** to each of these two departments in terms of corporate goals. An influence coefficient is as an indicator of importance of quality attribute relative to each other. After identifying the corporate-level security needs, the process moves down to the department level to define the department-level needs. Table 4 shows the resultant utility at the department level of Firm A. The utility expectation indicates somewhat inconsistent valuations of the total utility of information asset between the two departments. For example, the accounting department requires more on integrity while the marketing department prefers higher availability. As a result, security measures are proposed differently to ensure the delivery of each specific utility of information assets. For instance, more encryption software were acquired to support data exchange among various accounting applications while a parallel server was installed for the marketing department to guarantee a nearly 100% availability of its website. Similar analysis was conducted at Firm B and the results are quite different from Firm A's. Overall, the utility perceived at the department level is reasonably consistent with its corporate-level total utility. After minor adjustments to the standard set of security measures both departments at Firm B were satisfied. At the next level, we focused on the total utility of information assets perceived by each application group. In that phase, application stakeholders could voice their concerns and requirements. Although most applications did not demand anything conflicting to the valuations perceived at higher levels in each firm, one application in Firm B was developed to target a new market segment which required significantly more bandwidth if it had to comply with the same security measures. The top management supported the upgrade of the network infrastructure instead of relaxing the security measures.

Table 4: The Total Utility Of Information Asset Perceived By Main Business Units At Firm A

Stakeholder / Composite Weight	Influence Coefficient	Integrity	Availability	Reliability
Accounting	0.4	30	35	35
Marketing	0.6	20	40	40
Composite Weight	1	24 (= 30*0.4 + 20*0.6)	38 (same formula)	38 (= 35*0.4 + 40*0.6)

The same processes were carried out to establish similar security protection for all group applications. Everyone was surprised to notice that these group applications largely fed data to department applications and thus could easily comply with the level of security protection specified for the department applications.

Finally, to find out an acceptable level of security protection, we adjusted the weight of the total utility that comprised of the significant quality attributes in an opposite direction to the level of security protection. This exercise shows that each firm, as a whole, has to balance between the total utility of its information assets and the level of security risk it bears. Similar adjustments can be conducted for individual business units so that security protection can be synthesized at various levels of granularity. Note that we were aware that the relationship between the total utility and security protection could be derived from statistical data collected within the same industry. If a firm has a unique valuation of its information assets or exceptional security needs, then explicit computational analysis should be applied to gauge the corresponding ROI in security protection. Referring to the graph in Figure 2, we denote the degree of security protection as *x.* In accordance, the loss or gain of the total utility due to security protection can be a function of security protection in terms of each quality attribute. Specifically, the lost availability, which includes throughput and response time, is defined as $\Delta_a(x)$; the lost reliability, which can be attributed to error rates and data quality, as $\Delta_r(x)$, and the lost integrity, which usually refers the value of integrated information, as $\Delta_i(x)$. These functions could be derived primarily from performance benchmarks furnished by vendors. We then have the weighted total utility loss, due to the security measures, defined as $\Delta_{utility}(x) = w_a*\Delta_a(x) + w_r*\Delta_r(x) + w_i*\Delta_i(x)$, where w_a, w_r, and w_i are the weights for availability, reliability, and integration that are determined by the stakeholders as discussed

above. By adjusting the degree of security control, we could improve the utility, of course, at the expense of increased security risk. Our objective is to find out $x_{optimal}$ such that when $x = x_{optimal}$, we would have the optimal amount of total utility equal to $1 - \Delta_{utility}(x)$. Consider, for instance, the impact of adding firewall protection on the total utility of information assets. From statistical data of vendors or from the industry, on the average a firewall reduced the throughput and the authentication schema built in the firewall may further measurably slow down the response time. By letting $\Delta_a(firewall)$ be +0.4, $\Delta_r(firewall)$ be -0.2, and $\Delta_i(firewall)$ be +0.2, we mean that adding firewall protection as a security measure, the company will lose 40% of utility on the availability and 20% on integrity, but it will gain 20% of its reliability. These numbers reflect the relative gains or losses that are unique and specific to the company in concern. Besides, some of them are objective while others are subjective. In this example, the loss of availability due to firewall protection is measurable and thus objective, but the degradation of information integration due to the firewall protection could not be readily assessable and therefore somewhat subjective. Although the estimates of this kind are only approximate, they should converge over time, especially when multiple kinds of firewall, such as semantic firewalls, are in operation and can serve as a comparison. Once the impact of security protection on the total utility of information assets is assessed, the resultant numbers, along with the composite weights such as those listed in Table 4, are applied to the equation to yield the total loss due to the firewall protection; that is, $\Delta_{utility}(firewall) = .24 * .4 - .38 * .2 + .38 * .2 = 0.096$. It means that the firewall protection results in a loss of total utility of their information assets, amounted to 9.6% of the prior total utility. The normalized residual utility then is 1 – 0.096 = 0.904. Obviously, deploying firewall protection without compensating its side effect does not make a business sense. Based on such an analysis, additional computing power and bandwidth should be considered as a part of the security protection. The additional cost can be evaluated and justified whether the protection plan is viable or not. We admit that these figures are not based on a rigorous mathematical model. However, the ***process*** that generates these figures renders the needed discipline to enforce an affordable, meaningful, and qualitative way for SMEs to think systematically about security protection. Finally, as a part of our facilitation framework, each firm should set up a security subscription policy that mirrors the layered model of security protection. Through the layered model, each business application must follow a procedure to determine if it needs exceptional subscription, either to intensify or to relax the security protection in question.

EVALUATION OF THE OVERALL APPROACH

Through the process above, we established a decision-support model on deploying security measures. None of senior managers had realized their achievement until we presented the documented security plan resulting from the process they had gone through. As characterized previously in Figure 3, the resultant decision-support model was an integration of three components, namely, a constraint-based security protection model, customized constraint objects, and synthesis and subscription. To convince our industrial clients, we analyzed the quality attributes of the decision-support model and identified the following characteristics of the model:

- *Simplicity:* The model offers layered resolutions of security issues to isolate the complexity of interrelated business requirements. Considering security measures in terms of various resolutions could help a decision maker focus on the issues with a clearly defined scope and depth. Therefore, the resultant abstract representation of the protected information assets establishes a foundation to provide a systematic defense. The protection could remain at the highest resolution layer without losing full coverage of protection since each identifiable information asset, with exceptional security concerns or without, could be tied to default protection. For example, even though many groups are not aware of certain security risks, their information assets are protected to the extent defined at their parent level. As another example, some employees are never concerned or aware about security risks of their desktops, but they are protected because the security measures of both their PCs and the applications installed on their desktops are enforced at the level set by their departments.
- *Consistency:* The model also establishes a hierarchical inheritance for consistent security enforcement that supports heuristic enforcement. In addition to clarifying the organizational accountability to protecting information assets, the model can help visualize any inconsistency of security protection needs at different levels. For example, to encourage the system administrator to consider the corporate security policy, we should recommend that, by default, such a policy render the minimal protection. Unless certain business functions need special protection, its policy should inherit the security policy defined for the functional group

at a higher layer. By organizing the security protection in terms of organizational units, our model supports aggregation. By classifying the needs for security protection within an aggregation, our model leverages generalization. Generalized protection is not equivalent to aggregated protection. The former maintains internal consistency whereas the latter represents external consistency.

- *Measured Risk:* The model is capable of incorporating exceptional security requirements with standard security policy. As a prudent measure, our decision- support facilitation framework allows flexibility for exceptional protection via the synthesis and subscription component. Such exceptional security measures can be integrated into the model and additional efforts on protection can be measured in comparison to the standard protection. Consequently, the unique risk taken by a firm is calculated.
- *Total Accountability:* Our framework enforces the involvement from appropriate functional groups at appropriate times. Each role plays in a restrictive manner (because of designated layers) and allows incorporation of specific security protection from others and even from subordinates. Following such a structured approach, senior managers and security architects especially endued less stress. Line managers sense more ownership of the information assets and subsequently balance the needs and measures more carefully. Consequently, security risk management becomes every group's responsibility.

The whole process of constructing such a decision model usually does not require much computational analysis for preserving its validity because the resultant model develops from one layer to another in an intuitive, iterative and incremental manner. However, if a firm dramatically differs from a typical business model in its industry or is at an unusual stage of its corporate life cycle, it may have a unique valuation of total utility of its information assets. In such a situation, we recommend mixing a more rigorous formal model with our framework. For example, an explicit risk assessment should be conducted using, say, Markowitz factor models [Kritzman 93] for assessing unique risks. However, instead of applying such a model to determining the total utility of information assets for the entire corporation, the model should be applied only to the layer of the organizational units of concern and the resultant analysis should also be relatively easy due to much reduced complexity and can be conducted in comparison to the typical cases from the same industry.

CONCLUDING REMARKS

As the cost on protecting corporate information assets soars, SMEs are facing more challenges than large firms do. To help them cope with their disadvantageous situations, we have investigated a facilitation framework that inherently promotes strategic thinking of security protection issues and results in a decision-support model that systematically enhance the total utility of corporate information assets with minimal conflicts among organizational units. The process of developing such a strategic decision model in general does not require explicit computational analysis while it can still ensure its logical soundness and practicality. Our approach has been built upon the real case analyses and then has been applied to the same cases to gauge its validity. Therefore, our approach has both theoretical and practical significance and will provide a meaningful solution, particularly feasible for SMEs.

REFERENCES

1. Bakry, S. (2003). Development of Security Policies for Private Networks. *International Journal of Network Management,* 13, 3, 203-210.
2. Bertino, E., Bettini, C., Ferrari, D., and Samarati, P. (1998). An Access Control Model Supporting Periodicity Constraints and Temporal Reasoning. *ACM TODS,* Vol. 23, No. 3, pp. 231–285.
3. Bosworth, K.P. and Tedeschi, N. (2001). Public Key Infrastructure – The Next Generation, *BT Technology Journal*, Vol. 19, No. 3, pp. 44 – 59.
4. Botha, M., et al. (2002). The Utilization of Artificial Intelligence in a Hybrid Intrusion Detection System. *Proceedings of the 2002 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, Port Elizabeth, South Africa, 149 – 155.
5. Callahan, J. (2002). Intelligent XML Content Firewalls: Preprocess Requests and Postprocess Responses at a Semantic Level, *XML Journal*, February 2002.

6. Campbell, K., Gordon, L., Loeb, M., and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Security*, Vol. 11, No. 3, pp. 431 – 448.
7. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM*, Vol. 47, No. 7, pp. 87-92.
8. Eloff, J. and Eloff, M. (2003). Information Security Management – A New Paradigm, *Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologies on Enablement through Technology*, South Africa, pp. 130 – 136.
9. Gordon, L. and Loeb, M. (2002). Return on Information Security Investments: Myths vs. Realities, *Strategic Finance*, November.
10. Herscovitz, Eli (1999). Secure Vitual Private Networks: The Future of Data Communications, *International Journal of Network Management*, Vol. 9, No. 4, pp. 213 – 220.
11. Kazman, R., Asundi, J., and Klein, M. (2001). Quantifying the Costs and Benefits of Architectural Decisions, *Proceedings of the 23rd International Conference on Software Engineering*, Toronto, pp. 297 – 306.
12. Knapp, K., Marshall, T., Rainer, R. K., and Morrow, D. (2004). Top ranked information security issues: the 2004 international information systems security certification survey results, *unpublished Working Paper*, Auburn University.
13. Koch, M., Mancini, L., and Parisi-Presicce, F. (2000). A Formal Model for Role-Based Access Control Using Graph Transformation. In *Proceedings of the 6th European Symposium on Research in Computer Security*, pp. 122–139.
14. Kritzman, M. (1993). …About Factor Models, *Financial Analysts Journal*, Vol. 49, No. 1, pp. 12 – 15.
15. Oh, S. and Park, S. (2003). Task-Role-Based Access Control Model, *Information Systems*, Vol. 28, No. 6, pp. 533 – 562.
16. Parssian, A., Sarkar, S., and Jacob, V.S. (1999). Assessing Data Quality for Information Products, *Proceeding of the 20th International Conference on Information Systems*, Charlotte, NC, pp. 428 – 433.
17. Rees, J., Bandyopadhyay, S., and Spafford, E. (2003). PFIRES: A Policy Framework for Information Security, *Communications of ACM*, Vol. 46, No. 7, pp. 101-106.
18. Sandhu, R., Coyne, E., Feinstein, H., and Youman, C. (1996). Role-based access control models. *IEEE Computer*, Vol. 29, No. 2, pp. 38–47.
19. Seddon, P., Staples, S., Patnayahuni, R., and Bowtell, M. (1999). Dimensions of Information Systems Success, *Communications of the AIS*, Vol. 2, No. 3, Article No. 4.
20. Sharpe, W.F., Alexander, G.J., and Bailey, J.V. (1999). *Investments*, Prentice Hall, Upper Saddle River, NJ.
21. Tayi, G.K. and Ballou, D.P. (1998). Examining data quality, *Communications of the ACM*, Vol. 41, Issue 2, pp. 54 – 57.
22. Strong, D.M., Lee, Y.W., and Wang, R.Y. (1997). Data Quality in Context, *Communications of the ACM*, Vol. 40, No. 5, pp. 103 – 110.
23. Walton. J. (2002). Developing an Enterprise Information Security Policy. *Proceeding of the 30th annual ACM SIGUCCS fall conference on User services conference, 2002,* Rhode Island, pp. 153 – 156.

NOTES