available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Enterprise information security strategies

*Evan E. Anderson*[a,b,*], *Joobin Choobineh*[a,b]

[a]*Center for Information Assurance and Security, College Station, TX, USA*
[b]*Mays Business School, Texas A&M University, 322 Wehner Building, College Station, TX 77843-4217, USA*

ARTICLE INFO

*Article history:*
Received 6 September 2006
Received in revised form
19 January 2007
Accepted 12 March 2008

*Keywords:*
Security costs and benefits
Enterprise security requirements
Information security
Best practices
Models of risk management

ABSTRACT

Security decisions are made at every level of an organization and from diverse perspectives. At the tactical and operational levels of an organization, decision making focuses on the optimization of security resources, that is, an integrated combination of plans, personnel, procedures, guidelines and technology that minimize damages and losses. While these actions and tactics reduce the frequency and/or consequences of security breaches, they are bounded by the organization's global security budget. At the strategic, enterprise level management must answer the question, "What is the security budget (cost expenditures), where each dollar spent on security must be weighed against alternative non-security expenditures, that is justified by the foregone (prevented) losses and damages?" The answer to that question depends on the tolerances of decision makers for risk and the information employed to reach it.



## 1. Introduction

Every organization's ability to fulfill its missions is based on the meaningful and productive utilization of its assets. The form and sources of threats to assets have changed and grown substantially with the development of computer systems, electronic networks, stored data and information exchange (Gerber and von Solms, 2001). Information technologies support, control, and manage business processes, and have become some of the private sector's most valued and **vulnerable** assets. The emergence of the cyber-economy accelerated these developments by redefining markets, organizational scope, the sources of knowledge and creativity, business logic, and resource criticality (Shih and Wen, 2003). Information assets that could be broadly shared became more and more valuable and, concomitantly, more vulnerable to new classes of threats that are not constrained by the time and place boundaries of the physical world.

Beyond creating new threats, vulnerabilities and organizational risks, the growth of information assets has introduced several new management problems requiring new policies, technologies and organizational capabilities (Gordon and Loeb, 2002; Karyda et al., 2005). First, the protection of information assets, like their physical counterparts, creates new and **unwanted** costs, where costs are defined as expenditures for resources that detect and prevent security breaches. These costs depend on the extent and robustness of threats seeking to impose damages and losses through the exploitation of vulnerabilities (Sklovos and Souros, 2006). The protection of information assets, regardless of its necessity, creates a diversion of resources from alternative applications that could be used to build new capabilities and enhance productivity. Second, at the point of implementation, many of the tools and procedures used to protect information assets reduce throughputs, access, transparency, and create new complexities and inflexibilities in resource utilization. Finally, solutions are frequently temporary and

* *Corresponding author*. Mays Business School, Texas A&M University, 322 Wehner Building, College Station, TX 77843-4217, USA.
E-mail address: eanderson@mays.tamu.edu (E.E. Anderson).
0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.03.002

imperfect against the growth, intelligence and virulence of emerging threats.

## 2. Information systems, risks and protection: a brief history

In the late 1960s the U.S. Department of Defense recognized the risks associated with using information systems for critical tasks. In response, the Advanced Research Projects Agency (ARPA) formed a taskforce to study the risks introduced by the widespread use of resource-sharing information systems and to make recommendations to improve their security (Ware, 1970). The National Bureau of Standards, which subsequently became the National Institute of Standards and Technology (NIST), codified many of the strategies identified in the ARPA studies and published the first U.S. government guidelines for computer security risk management (Farquhar, 1991; NBS, 1974). Since that time, NIST's Computer Security Resource Center (CSRC) has become a valuable repository for U.S. government guidelines on information system security and risk management (Hoffman, 1989; NIST, 2006). Numerous other private and public sector organizations, domestic and international, have contributed guidelines, frameworks, and methodologies to assist management to understand risks and find acceptable levels thereof (Hoffman, 1989; Soo Hoo, 2000). These efforts have contributed enormously to awareness, the identification of threats and potential attack trees, specification of security requirements and to a very extensive knowledge base of technical and operational solutions that have formed what the authors will collectively refer to as "best practices."

While these recommendations, tools and methods are invaluable to the deployment and operationalization of security resources, they have several important limitations. First, they tend to focus on the incident(s), its characterization, and the threat-vulnerability combinations that can lead to potential losses. That is, they operationalize security tools and methods at the asset level to detect and/or prevent potential damages (Cavusoglu et al., 2005). The tradeoffs considered are between solutions and not between expenditures and resources devoted to information security versus other alternative applications. Second, they do not provide an "enterprise-wide" perspective that aggregates horizontally and vertically across threats, vulnerabilities, protected assets and organizational impacts (Anderson, 2001; Woodlock and Ross, 2001). At the **strategic level** of an organization, the benefits of information security, that is, reduced damages and losses must be balanced against security costs (Sklovos and Souros, 2006). Expenditures for security that exceed this balance may further reduce expected losses, but may be excessive given their opportunity costs (Gordon and Loeb, 2006). Third, existing security guidelines, prescriptions and best practices take an operational view of risks (Blakley et al., 2001). They quantify the likelihood of attacks and argue that plans, programs and actions that reduce the frequency and/or seriousness of incidents thereby reduce risks (Gehani, 2004; Peltier, 2004). They tend to imply that risk is a universal, absolute construct, rather than a value judgment unique to contexts and decision makers. Indeed, at a strategic level risk taking involves tradeoffs and depends on the costs and rewards for accepting risk (Walwyn et al., 2002).

## 3. Framing the management problem at the enterprise level

The management of information security occurs at many levels within an organization (Tsiakis and Stephanides, 2005). The authors assume, at technical and operational levels, that security budgets have been optimized (Cavusoglu et al., 2004; Gordon and Loeb, 2006; Hamill et al., 2005). That is, expenditures for enterprise security have been distributed over tools, policies, technology, procedures and personnel so as to achieve the highest level of asset protection (Eloff and von Solms, 2000). However, at the strategic level, management has a different perspective and must answer the following question: "What is the optimal enterprise-wide security budget that minimizes aggregate losses/damages due to attacks **plus** the dollar costs (security budget) for the acquisition and deployment of detection, prevention and recovery resources?" The answer to this question establishes the budgetary boundaries for building a security capability and for acceptable dollar losses, given the risk tolerances of decision makers. It involves modeling the costs of achieving various levels of best practice implementation in the presence of uncertain losses and establishes the optimal enterprise security budget using various decision criteria. The strategic management of security focuses on the competing demands for enterprise resources and their opportunity costs, and seeks to identify security benefits that justify related costs. If there were **no** threats, security resources would not exist, costs would be lower, profits higher, and entities would have higher equity values.

Every enterprise, based on its requirements, has a wide range of security solutions (Gerber and von Solms, 2001). That is, there exist integrated combinations of policies, procedures, guidelines, personnel and technologies, appropriately tiered, configured and customized. In this paper, they will be collectively referred to as best practices. The components of best practices and the resources required for implementation are identifiable and can be operationalized. Organizations define/choose a best practice (subset) appropriate to their needs from the set of all possible best practices, but implement it with varying degrees of completeness, functionality and robustness (Cavusoglu et al., 2004). If, for example, an organization chooses from the set of best practices a best practice that includes an awareness program, the degree of implementation may vary enormously across the employees included, delivery media, content, repetition, and examination or certification requirement. In this paper, the degree of implementation is defined as a percent, $0 \leq \lambda_i \leq 100,\ i = 0, 1, \ldots, n$, of the maximum achievable against known standards, protocols and benchmarks. It is assumed that higher levels of implementation are increasingly difficult to achieve, resource intensive and time consuming. The **costs** of implementation per period $c(\lambda_i)$ include all detectors and preventors contained within a best practice and its implementations. Since higher levels of $\lambda_i$ are increasingly difficult to achieve, it is assumed that their costs increase monotonically at an increasing rate.

It is assumed that these costs are equivalent to the enterprise security budget, that is, all approved expenditures are incurred.

Attacks can take many different forms, derive from numerous sources, and have widely varying outcomes. Potential losses $0 \leq \ell(\lambda_i)_j,\ j = 0, 1, \ldots, m$ may derive from damage(s) to computers, operating systems, network technologies, stored data and/or applications and require diagnosis, repair, replacement and re-deployment. Additionally, losses may result from interruptions to the real-time availability of data exchange and transaction processing services that affect commercial activity. Finally, losses may derive from the loss of trust and confidence in an organization's ability to meet the expectations of users and/or to protect their identity and privacy (Cavusoglu et al., 2004). The latter can cause shrinking sales, loss of suppliers and legal penalties. It is assumed that potential losses are unimodal, symmetrically distributed around their expected values $E[\ell(\lambda_i)]$ and that expected losses decrease at a decreasing rate with higher levels of best practice implemented. The probability of potential losses is defined as $0 \leq p_r(\ell(\lambda_i)_j) \leq 1$ and sum to one for all $j$.

Fig. 1 presents the graphs of per period expected losses and security cost. Underlying factors affecting each would, of course, change their slopes and cause them to shift up or down. For any level (percent) of best practice implemented, potential losses $\ell(\lambda_i)_j \geq 0$ may vary substantially. For purposes of this paper, it is unnecessary to give form to the density function of losses. In practice a gamma or exponential distribution might be appropriate, recognizing that losses cannot be negative and that very large losses have a positive, though perhaps very small probability. It is assumed that organizations deploy the most productive security solutions first, and as $\lambda_i$ increases, they will add capabilities that continue to reduce losses but are less and less effective per dollar expended. Expected losses at $\lambda_0 = 0$, where there is **no** funding for security, $E[\ell(\lambda_0)]$ are maximum and decrease at a decreasing rate as $\lambda_i$ increases. It should be noted that a very robust, comprehensive implementation of each best practice contained within the set of all best practices, e.g. $\lambda_n$, is imperfect, that is $E[\ell(\lambda_n)] > 0$ (Tsiakis and Stephanides, 2005). Organizations with fewer (more) threats and/or vulnerabilities, fewer (more) commercial dependencies on the public web, and a more (less) stable, trained workforce would be expected to have lower (higher) expected losses at $\lambda_n$. Furthermore, there is a family of expected loss graphs, one for each possible best practice.

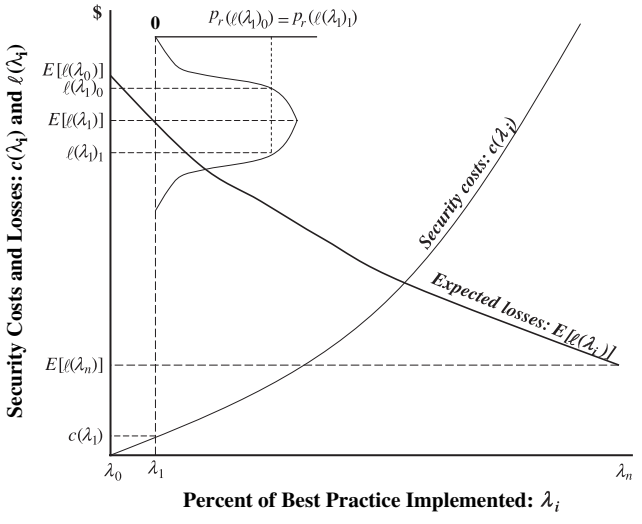


**Fig. 1 – Enterprise security: best practice, costs and losses.**

The uncertainty of losses can be seen at $\lambda_1$, where $\ell(\lambda_1)_0$ and $\ell(\lambda_1)_1$ are **potential** losses occurring with probabilities $p_r(\ell(\lambda_1)_0)$ and $p_r(\ell(\lambda_1)_1)$ and have an expected value $E[\ell(\lambda_1)]$. Larger and smaller losses than $\ell(\lambda_1)_0$ and $\ell(\lambda_1)_1$, respectively, are less likely to occur. **Probable** losses for any $\lambda_i$ are defined as $L(\lambda_i)_j$ and are the potential losses weighted by their probabilities of occurrence, that is, $p_r(\ell(\lambda_i)_j)\ell(\lambda_i)_j$.

Embedded in potential and expected losses are aggregated damages to information assets, the costs of repair and restoration, as well as the negative impacts on commercial activity and equity valuation. Expected losses decrease, but at a decreasing rate, as the percent of best practice implemented increases because the most productive solutions are deployed first and greater $\lambda_i$ are less and less productive. It is possible that expected losses will reach their minimum before $\lambda_n$ implying that further spending for security is without benefit(s). That is, there may exist a segment of the expected losses graph that is flat (horizontal) at its minimum.

In general, the costs of best practice implementations will not increase proportionately with $\lambda_i$, but rather will increase at an increasing rate. Hence, the **incremental** costs of improving best practices from 90 to 100% will be substantially higher than from 10 to 20%. The graph of security costs would shift to the left (steeper) or to the right (flatter) depending on the prices paid for resources employed in the implementations, the complexities of their integrations, and the length of their life cycles.

## 4. Enterprise strategy: costs and benefits

The attitudes and tolerances for risks vary substantially from context to context for an individual decision maker and from person to person in the same context and under the same degree of uncertainty (Finne, 2000; Gollier and Pratt, 1996; Tversky and Kahneman, 1986). They also can vary with the absolute magnitude of probable and expected (average) losses. The authors have assumed that decision makers are risk neutral, but may have an upper bound on their tolerance for expected or probable losses. That is, there may be expected or probable losses sufficiently large so as to jeopardize the continuity and/or sustainability of the organization and, therefore, condition their decisions. These responses to risks will be considered in the following section (Gerber and von Solms, 2005).

If decision makers have no upper bound on expected or probable losses, and if potential losses such as $\ell(\lambda_1)_0$ and $\ell(\lambda_1)_1$ are symmetric and equally likely $\{p_r(\ell(\lambda_1)_0) = p_r(\ell(\lambda_1)_1)\}$, they are risk neutral. Risk neutral decision makers will ignore potential losses and employ only the information captured in their expected value. In some periods, actual losses will exceed the expected and in others will fall below it. Over multiple periods, these deviations will offset one another

and average to zero. Furthermore, risk neutral decision makers will regard expected losses and security costs as purely **compensatory.** That is, dollar for dollar reductions in either is **equally** desirable. Preventing a dollar of losses is not preferred, per se, to a dollar reduction in security costs.

Commencing at the origin $\lambda_0$, an improvement in best practice to $\lambda_1$ will increase the costs of security to $c(\lambda_1)$, but will yield benefits equal to the decrease in expected losses, $E[\ell(\lambda_0)]-E[\ell(\lambda_1)]$. Since expected losses are reduced by more than the increase in security costs, the aggregate value of losses plus security costs is reduced and the firm has financial incentives to continue to increase $\lambda_i$. Continued improvements in best practices to $\lambda_*$ increase security costs by an amount $(c(\lambda_*) - c(\lambda_1))$ which is equal to the decrease in expected losses $(E[\ell(\lambda_1)]-E[\ell(\lambda_*)])$. If there is no maximum unacceptable expected or probable losses, $\lambda_*$ is preferred to $\lambda_1$ since each incremental dollar spent on improving best practices yields a return of more than one dollar in foregone, prevented losses. The firm is willing to spend more and more on security as long as each dollar spent produces a benefit, that is, reduced expected losses, that is at least as large. In Fig. 2a, this occurs where the slope of the graph of security costs is equal to absolute value of the slope of the expected losses graph.

From the functions of $c(\lambda_i)$ and $E[\ell(\lambda_i)]$ and their derivatives, one may define the marginal costs and marginal expected losses of security, $Mc(\lambda_1)$ and $ME[\ell(\lambda_i)]$, respectively. They represent the incremental changes in each variable associated with increases or decreases in $\lambda_i$. Without explicitly defining the functions $c$ and $E$, by assumption and observation, one would expect marginal costs (marginal expected losses) to increase (decrease) with increases in $\lambda_i$. However, neither would necessarily increase (decrease) linearly.

In Fig. 2b, the optimum strategy is shown using marginal analyses. Since the marginal expected losses are negative, the authors have taken its absolute value. The optimum $\lambda_i$ occurs at $\lambda_*$ where there is an intersection of $Mc(\lambda_i)$ and $|ME[\ell(\lambda_i)]|$. Best practice implementations to the left of $\lambda_*$ yield marginal benefits for security that exceed its marginal costs and, therefore, encourage organizations to increase their security capabilities. The converse is true for $\lambda_* < \lambda_i$.

Enterprise Strategic Security: Risk Neutral Decision Rule

If there is no maximum unacceptable expected or probable losses and decision makers are risk neutral, the optimal security budget and best practice implementation occurs where the marginal (incremental) costs of best practice $Mc(\lambda_i)$ is equal to the absolute value of marginal (incremental) expected losses $|ME[\ell(\lambda_i)]|$.

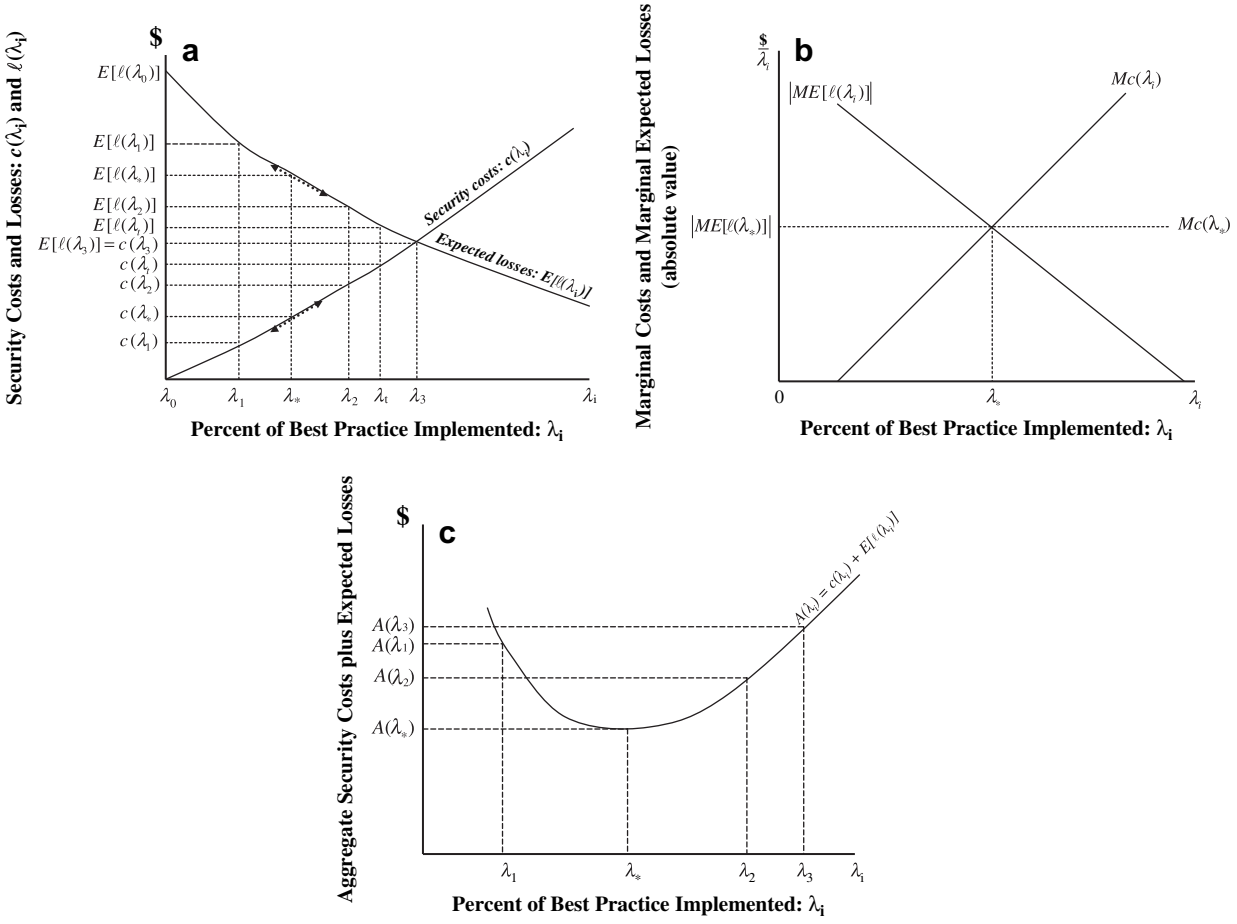


**Fig. 2 – (a) Optimal strategy under risk neutrality: $\lambda_i = \lambda_*$, (b) optimal strategy: marginal costs and marginal expected losses, and (c) optimal strategy: aggregate charges against revenue.**

Fig. 2a and b is based on an analysis and comparison of tradeoffs between the marginal costs and marginal benefits of security. A useful insight into this decision can be seen from the recognition that security costs and losses are a drain of enterprise resources from alternative value creating activities related to product development, differentiation and sales, customer services, relationship building and/or infrastructure investment. Hence, the optimal security strategy occurs where aggregate expected losses plus security costs, $A(\lambda_i) = E[\ell(\lambda_i)] + c(\lambda_i)$, are minimized at $\lambda_i = \lambda_*$ (Fig. 2c). All security cost expenditures (budgets) and best practice implementations to the left of $\lambda_*$ have marginal expected losses that exceed marginal security costs. Hence, aggregate losses plus security costs can be reduced by increasing $\lambda_i$. That is, improvements in $\lambda_i$ add less to security costs than the reduction in expected losses. Further increases in $\lambda_i$, for example $\lambda_2$, will increase costs more than it reduces expected losses and, therefore, increase $A(\lambda_i)$. That is, $A(\lambda_2) > A(\lambda_*)$. Therefore, enterprise profits, as they relate to information security should be largest when the charges against period revenues are the smallest and the allocation of revenues to revenue enhancing or cost saving activities are maximized.

One might have expected that the enterprise optimum is $\lambda_3$, where security costs equal expected losses, since it is widely believed that organizations should commit resources to protect assets up to the value of expected losses against those assets (Fig. 2a). This rarely will be the optimal security strategy, and will occur only when the costs of improved best practices increase very slowly and the decrease in expected losses is rapid and sustained.

## 5. Risk tolerance and critical losses: an extension

In some cases, the optimal security budget $c(\lambda_*)$, and the security capabilities it affords, may result in expected or probable losses that imperil the organization. That is, it creates risks that are intolerable and unacceptable (Miller and Bromiley, 1990). Managing risk tolerances may take one of two forms. First, and least restrictive, management may implement best practices such that expected losses do not exceed some **critical threshold**, for example, $E[l(\lambda_t)]$ (Fig. 2a). This decision continues to accept potential losses above $E[l(\lambda_t)]$ if there are equivalent and equally likely losses below that value. If $E[\ell(\lambda_t)] \geq E[\ell(\lambda_*)]$, $\lambda_*$ remains the optimal implementation of best practice. However, if $E[\ell(\lambda_t)] < E[\ell(\lambda_*)]$, as illustrated in Fig. 2a, a best practice implementation of $\lambda_t$ becomes optimal.

This level of risk tolerance for critical losses may still be too high, since there remains substantial likelihood of probable losses that exceed $E[\ell(\lambda_t)]$. In this case, management may establish an upper bound on the magnitude of **probable losses** (Fig. 3). Suppose management has a critical threshold for **absolute** dollar losses per period, defined as $L_t$. The magnitude of $L_t$ will be larger or smaller depending on the size of organizational assets, its business continuity and recovery capabilities, profitability, and the risk tolerances of its management.

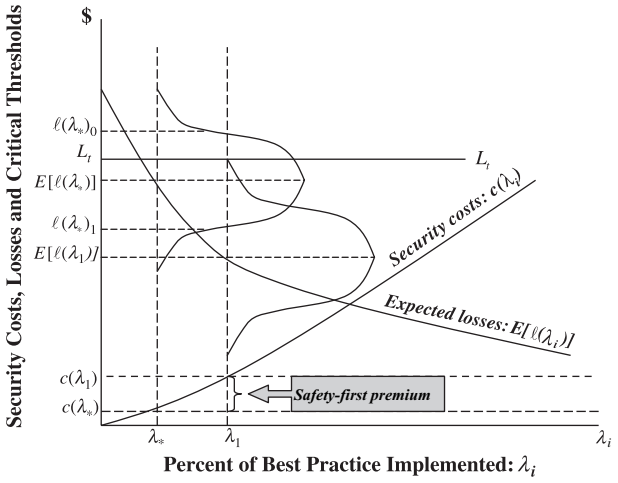


**Fig. 3 – Loss thresholds and security premiums.**

If $(c(\lambda_*), \lambda_*)$ are the optimal security costs (budget) and best practice implementation, the presence of $L_t$ conditions previous decisions only if there exists a probable loss which is greater than $L_t$. Hence, if $\ell(\lambda_*)_j p_r(\ell(\lambda_*)_j) \leq L_t$ for all $j$, $\lambda_*$ would remain the optimal strategy. Suppose, however, for purposes of illustration that there exists a potential loss $\ell(\lambda_*)_0$ and that $p_r(\ell(\lambda_*)_0)\ell(\lambda_*)_0 > L_t$, the optimal strategy to protect the integrity of an organization's assets and insure its continuity would require increased spending for security and a higher level of best practice implementation. In order to limit its risks, management would be willing to spend $c(\lambda_1)$ and implement best practice $\lambda_1$ where the $p_r(\ell(\lambda_1)_j)\ell(\lambda_1)_j \leq L_t$ for all potential losses $j$. By increasing security spending, management is able to reduce the magnitude of probable losses. From Fig. 3 it can be seen that the tail of the density function of losses that exceeds $L_t$ becomes smaller and smaller as $\lambda_i$ increases, though there may continue to exist some very large potential losses with very small probabilities. The impact of critical loss management is asymmetric by nature. That is, it strongly favors loss prevention rather than cost saving. For example, if $\ell(\lambda_*)_0$ and $\ell(\lambda_*)_1$ are equally likely, that is, $p_r(\ell(\lambda_*)_0) = p_r(\ell(\lambda_*)_1)$, but $p_r(\ell(\lambda_*)_0)\ell(\lambda_*)_0 > L_t$, the firm will increase security spending and best practice implementation until a $\lambda_i$ is reached such that all of its probable losses are equal to or less than $L_t$.

Suppose that all probable losses for $\lambda_1$ are equal to or less than $L_t$ and that at least one probable loss for all other $\lambda_i < \lambda_1$ exceeds $L_t$, then $c(\lambda_1)$ becomes the optimal security budget. Decision makers, in the presence of $L_t$ will choose the minimum $c(\lambda_i)$ such that all of the probable losses associated with $\lambda_i$ are equal to or less than $L_t$. If for example, the new optimal security budget and best practice implementation are $(c(\lambda_1), \lambda_1)$, the firm is willing to pay a "safety-first premium" of $[c(\lambda_1) - c(\lambda_*)]$ to avoid losses greater than the critical threshold $L_t$ (Arzac and Bawa, 1977). A safety-first premium is most likely when the unrestricted optimum strategy $[c(\lambda_*), \lambda_*]$ is small, decision makers are highly risk averse, the presence of threats is high and/or the survivability of the organization is fragile.

Enterprise Strategic Security: Risk Averse Decision Rule

If decision makers place an upper bound (critical threshold) on unacceptable expected losses, $E[\ell(\lambda_t)]$, the optimal security budget is $c(\lambda_*)$ if $E[\ell(\lambda_*)] \leq E[\ell(\lambda_t)]$ or $c(\lambda_t)$ otherwise. Alternatively, if an upper bound is established for the absolute magnitude of losses, $L_t$, the optimal security budget is $c(\lambda_*)$ or the smallest budget $c(\lambda_i) > c(\lambda_*)$ such that $p_r(\ell(\lambda_i)_j)\ell(\lambda_i)_j \leq L_t$ for all $j$.

## 6. Conclusion

With the emergence of data exchange, shared networks, public infrastructure and substantial cost saving and performance gains from the electronic distribution of information, a new type of enterprise asset has developed. However, like their physical counterparts, they endure threats to their integrity, availability and value creating capabilities. The organizational response depends on many factors including the quantity and quality of information available to decision makers about threats, vulnerabilities, potential damages and likelihoods, the modularity, interdependence and integration of systems, and the scope of responsibilities and risk tolerances of decision makers (Tversky and Kahneman, 1986).

Considerable frustration has emerged with the adequacy of information assurance and security. Many knowledgeable security specialists believe that organizations routinely fail to comprehend the seriousness of threats to enterprise information assets and, thereby, under resource their protection. For example, a survey of global companies recently reported that, ''Companies are spending so much of their IT budgets on complying with regulation they are neglecting other security threats….''[1] This paper has presented, by taking an enterprise perspective and allowing for multiple risk taking behaviors, a strategic analysis for establishing security budgets.

The authors have argued that security decisions, with diverse perspectives, are made at every level of an organization. At the tactical and operational level of an organization, decision making focuses on the optimization of security resources. That is, given a security budget, ''What combination of plans, personnel, procedures, guidelines and technology will maximize the protection of information assets?'' The analysis and security choice set are between competing solutions and are constrained by the security budget. Decision makers at this level are judged on the effectiveness of the optimization and deployment of detector and protector resources. They tend to argue for larger security budgets and seek to drive down expected losses until they reach the horizontal segment of the $E[\ell(\lambda_i)]$ graph.

While these actions and tactics may reduce the frequency and/or consequences of security breaches, they are bounded by the global, strategic enterprise question, ''What is the optimal security budget, where each dollar spent on security must be weighed against alternative non-security expenditures and justified by the benefits of reduced damages and losses?'' The answer to this question is not, for various reasons, a ''universal truth'' nor does it necessarily maximize information security. Furthermore, it is heavily influenced by organizational risk taking and tolerances thereof.

If decision makers are risk neutral, they accept the symmetry of probable losses around their expected values and equally favor reductions in security costs and expected losses. They will increase spending for information security, but only up to a capability where each additional dollar spent on security prevents an equivalent amount of dollar losses. This will rarely minimize expected losses. Indeed, it knowingly accepts losses against information assets to avoid additional costs. Hence, some of the disagreements over funding for information security derive from differences in the scope of responsibilities and risk tolerances of decision makers at different levels of the organization.

Nevertheless, the authors recognize, apart from the rationality of risk neutral decisions, that the enterprise may be best served by risk aversion. In particular, there may be expected or probable losses sufficiently large, such that if they were to occur, the organization could be seriously impaired or jeopardized. Hence, decision makers will act to limit the magnitude of losses, even where these outcomes would be probably offset by equivalent smaller than expected losses in the future. In some cases, where the thresholds for expected or probable losses are high, the optimal security budget may be equivalent to the risk neutral budget. In others, it will result in larger security budgets that are justified by preventing the ''unthinkable'' and involve paying a premium to insure a **safety-first** strategy.

Within risk adjusted security budgets, the implementation of best practices presents many challenges. Some of the most daunting include the pace and sources of change in computing and network environments created by new business strategy, merger and acquisition, infrastructure investment, personnel turnover, and changes in sourcing practices and supply chains. Stakeholders expect computing and network solutions that are modern, leveraged across the enterprise and its relationships, accessible and reasonably transparent to users, and aligned with the objectives and needs of business units. Organizational change alters the combinations of vulnerabilities and threats, some of which are known and others are not, and necessitates a continuous evaluation and reordering of security initiatives and priorities so that security expenditures achieve their maximum effectiveness.

Successful implementation of best practices requires information, executive sponsorship and management leadership, and involves choices between alternative solutions. These decisions and actions, to be effective and timely, are based on data and information concerning assets and processes to be protected, impacts and likelihood of breaches, and costs and effectiveness of best practices. In particular, management must be able to evaluate the current state of detection and prevention capabilities for purposes of compliance and fulfillment of security plans, and to discover gaps between current capabilities and future period needs. Implementation cannot be viewed as a static execution of plans, and like other managed activities require performance metrics, periodic revision of plans, and incentives for achieving security goals.

[1] ''IT security goes by the board in bid to obey rules,'' Financial Times, November 2, 2005.

## REFERENCES


Anderson R. Why information security is hard – an economic perspective. In: IEEE Proceedings of the 17th Annual Computer Security Applications Conference; 2001. p. 358–65.

Arzac E, Bawa V. Portfolio choice and equilibrium in capital markets with safety-first investors. Journal of Financial Economics 1977;14(3):277–88.

Blakley B, McDermott E, Greer D. Information security is information risk management. In: ACM proceedings of the workshop on new security paradigms; 2001. p. 97–104.

Cavusoglu H, Mishra B, Raghunathan S. A model for evaluating it security investments. Communications of the ACM 2004;47(7): 87–92.

Cavusoglu H, Mishra B, Raghunathan S. The value of intrusion detection systems in information technology security architecture. Information Systems Research 2005;16(l):28–46.

Eloff MM, von Solms SH. Information security management: a hierarchical framework for various approaches. Computers and Security 2000;19(3):243–56.

Farquhar B. one approach to risk assessment. Computers and Security 1991;10(l):21–3.

Finne T. Information systems risk management: key concepts and business processes. Computers and Security 2000;19(3): 234–42.

Gehani A. Performance-sensitive real-time risk management is NP-Hard. In: Proceedings of the workshop on foundations of computer security affiliated with 19th IEEE symposium on logic in computer science (LICS); 2004. p. 1–12.

Gerber M, von Solms R. From risk analysis to security requirements. Computers and Security 2001;20(7):577–84.

Gerber M, von Solms R. Management of risk in the information age. Computers and Security 2005;24(l):16–30.

Gollier C, Pratt JW. Risk vulnerability and the tempering effect of background risk. Econometrica 1996;64(5):1109–23.

Gordon LA, Loeb MP. The economics of information security investment. ACM Transactions on Information and System Security 2002;5(4):438–57.

Gordon LA, Loeb MP. Budgeting process for information security expenditures. Communications of the ACM 2006; 49(1):121–5.

Hamill JT, Dekro RF, Kloeber JM. Evaluating information assurance strategies. Decision Support Systems 2005;39(3): 463–84.

Hoffman LJ. Risk analysis and computer security: towards a theory at last. Computers and Security 1989;8(l):23–4.

Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: a contextual perspective. Computers and Security 2005;24(3):246–60.

Miller KD, Bromiley P. Strategic risk and corporate performance: an analysis of alternative risk. Academy of Management Journal 1990;33(4):756–79.

National Bureau of Standards. FIPS PUB 31: guidelines for automatic data processing physical security and risk management. Washington, DC: U.S. General Printing Office; 1974.

NIST (National Institute of Standards and Technology). Series 800 guidelines on security national institute of standards and technology. Available from: <http://csrc.nist.gov/publications/nistpubs/index.html>; 2006.

Peltier TR. Risk analysis and risk management. Information Systems Security 2004;13(4):44–56.

Shih SC, Wen HJ. Building E-enterprise security: a business view. Information Systems Security 2003;12(4):41–9.

Sklovos N, Souros P. Economic models and approaches in information security for computer networks. International Journal of Network Security 2006;2(1):243–56.

Soo Hoo KJ. How much is enough? A risk-management approach to computer security. Consortium for Research on Information Security and Policy (CRISP) Stanford University; 2000.

Tsiakis T, Stephanides G. The economic approach of information security. Computers and Security 2005;24(2):105–8.

Tversky A, Kahneman D. Rational choice and the framing of decisions. The Journal of Business 1986;59(4 part 2): S251–78.

Walwyn DR, Taylor D, Brickhill G. How to manage risk better. Research Technology Management 2002;45(5):37–42.

Ware W. Security controls for computer systems (U). Report of defense science board task force on computer security. Santa Monica, CA: The RAND Corporation; Feb 1970.

Woodlock P, Ross R. managing risks at the enterprise level. National Public Accountant 2001;46(9):19–21.



**Evan E. Anderson** is E.D. Brockett Professor of Information and Operations Management at Texas A&M University, and co-founder of the Texas A&M Center for Information Assurance and Security, which has been designated as an NSA Center of Educational Excellence. Prior to joining Texas A&M, he was GMU Foundation Professor and Director of Technology Management in the Graduate Business Institute at George Mason University. At GMU, he was a member of the core faculty of the Institute for Computational Sciences and Informatics and Director of an IT Industry Consortium. He received a B.B.A. (1965) from the University of Iowa, an M.B.A. (1966) from the University of Wisconsin, Madison and Ph.D. (1970) from Cornell University. He has served as Associate Dean for Graduate Studies and Faculty Affairs, Professor, and Area Coordinator of Managerial Economics and MIS in the School of Management at the University of Texas-Dallas; Associate Professor of Managerial Economics in the A.B. Freeman Graduate School of Business at Tulane University; Visiting Associate Professor of Management in the Owen Graduate School of Management, Vanderbilt University; Visiting Scholar at the Graduate School of Business, University of Chicago; and Distinguished Visiting Professor of Technology Management at the Graziadio School of Business and Management, Pepperdine University. Since 1973, he has held periodically an appointment as a Senior Member of St. Anthony's College, Oxford University, England. His research has appeared in journals such as: *Accounting Review, Decision Sciences, Operations Research, Naval Research Logistics, Management Science, University of Chicago's Journal of Business, IIE Transaction, Journal of Management Information Systems, MIS Quarterly, and IEEE Transactions: Engineering Management.* His research and educational initiatives have been funded by grants from organizations such as: Bell Atlantic-Nynex, CISCO Systems, EDS, Hughes Electronics, IBM, Perot Systems, the National Security Agency and Teradata (NCR). His current research focuses on Information Security, Privacy and Risk Management, and eServices.

**Dr. Joobin Choobineh**, B.S., MBA, Ph.D. received his Ph.D. degree in Management Information Systems from the University of Arizona in 1985. Currently he is an Associate Professor in the Department of Information and Operations Management at Texas A&M University. Dr. Choobineh's current research interest is on cyber security with a focus on the management of information security. He and his collaborators have worked with firms such as CISCO Systems, EDS, HP, and Texas

Instruments in charting research directions in this area. Dr. Choobineh's research areas include information systems security, data modeling, electronic commerce, integration of data and mathematical models, and creation of intelligent systems to solve organizational problems. He has written more than fifty (50) articles that have appeared in conference proceedings and journals such as (in alphabetical order) *Annals of Operations Research, Communications of the ACM, Database Engineering, Decision Support Systems, IEEE Transactions on Software Engineering, Information and Management, Information Strategy, Information Systems, Information Systems Management, INFORMS Journal on Computing, Intl. J. Of Operations & Production Management, J. of Database Management, J. of Management Information Systems, Omega, and The Database for Advances in Information Systems*. Since 1986, Dr. Choobineh has successfully delivered results on research and educational grants that were funded by firms such as CISCO Systems, EDS, HP, and Texas Instruments. He has served as the chair of 8 and committee member of 11 Ph.D. students. He has served as the chair and committee member of hundreds of Master of Science students. Dr. Choobineh is currently an Associate Editor of INFORMS Journal on Computing and serves on the editorial board of the International Journal of Business Information Systems.