Communications of the Association for Information Systems

Volume 28 Article 1

1-2011

Economic Analysis of Tradeoffs Between Security and Disaster Recovery

Mukul Gupta
Department of Information Systems and Technology Management, University of Texas at San Antonio,
Mukul.Gupta@utsa.edu

Alok Chaturvedi
Krannert Graduate School of Management, Purdue University

Shailendra Mehta
Indian Institute of Management, Ahmedabad, India

Communications of the Association for Information Systems

CAIS

Economic Analysis of Tradeoffs Between Security and Disaster Recovery

Mukul Gupta

Department of Information Systems and Technology Management, University of Texas at San Antonio

Mukul.Gupta@utsa.edu

Alok Chaturvedi

Krannert Graduate School of Management, Purdue University

Shailendra Mehta

Indian Institute of Management, Ahmedabad, India

Abstract:

The threat of computer crime is increasingly becoming a big concern for organizations. Organizations have to continuously manage their investment in information security technologies in an attempt to minimize the damage caused by information resource breaches. This article proposes an economic model in an attempt to evaluate the trade-offs between security and disaster-recovery technologies. The article intends to provide a directional strategy for managers in terms of increasing budgetary allocations for each of these technologies. The proposed model presents insights for managers.

Keywords: computer security, computer crime, disaster recovery, information security

Volume 28, Article 1, pp. 1-16, January 2011

The manuscript was received 1/8/2009 and was with the authors 6 months for 1 revision.

I. INTRODUCTION

In the twenty-first century, networked environments in the form of the public Internet and private Intranets are ubiquitous. E-mail has become a primary channel of communication, while the World Wide Web is changing how people collect, maintain, use, share, and disseminate information. The ubiquity, openness, immediacy, and global reach of the Internet have brought about new opportunities for businesses. This interconnectivity has provided a medium for organizations to manage their business activities with increased effectiveness, while continuously expanding their markets and service portfolio.

However, leveraging the benefits of global interconnectivity has introduced completely new sets of threats and risks into the business environment. Over the past few years, organizations have increasingly become a target of digital intrusions, denial of service, and corruption of digital data. Although illegal activities have persisted throughout human history and researchers have constantly persevered to understand criminal behavior and evaluate the psychological [Clarke, 1977; Hollin, 1989] as well as the economic aspects of criminal activity [Becker, 1968; Ehrlich, 1996], the Internet provides an anonymous and connected environment where criminals, such as hackers, crackers, terrorists, and foreign governments, can perpetrate their criminal activities by stealing information or denying service or by holding informational resources for ransom. The threat of computer crime has become a widely recognized predicament for organizations. In 2007, over 46 percent of organizations experienced intrusive activities targeted toward organizational information resources. Moreover, organizations have increasingly become victims of targeted or multiple attacks [Richardson, 2007]. These numbers are even higher for organizations in specific industry sectors. For instance, more than 50 percent of technology, media, and telecommunication companies indicated security breaches [Deloitte and Touché, 2007]. U.S. organizations are not alone in encountering these threats. In 2006, over 62 percent of organizations in the United Kingdom and over 87 percent of organizations in New Zealand experienced exploitation of information resources [Price Waterhouse Coopers, 2006; Quinn 2006]. Although manifestation of these threats is varied, viruses, phishing, denial of service, and theft of information have surfaced as the most predominantly occurring categories of incidents [Richardson, 2007]. In fact, globally, viruses have been the chief component of security breaches. Sixty-four percent of Asian organizations, 62 percent of European organizations, and 55 percent of American organizations have been infected by computer viruses [KPMG, 2002]. Moreover, viruses and other deliberate software attacks (like denial of service) have ranked at the top of the overall threat impact ratings [Whitman, 2003].

The threats have also become increasingly more sophisticated over the years. Dealing with new and sophisticated attacks is becoming the main challenge for organizations [Deloitte and Touché, 2005]. Moreover, the "professionalization" of computer crime has increased over the years [Richardson, 2007] and business competitors have joined independent hackers as the main external sources of computer crime [Deloitte and Touché, 2005]. However, this increased threat of computer crime has also resulted in increased awareness of information security among firms. Most organizations are now implementing information security technologies to counter these attacks and limit damages. Antivirus software and firewalls are still the most commonly used security technologies by organizations. However, the use of encryption and VPN technologies, antispyware software and intrusion detection systems has increased over the years [Richardson, 2007]. Moreover, in additional to these technologies, organizations have increased their expenditure on security awareness training, incident response, and recovery activities [Richardson, 2007].

Despite the increase in awareness of security technologies in organizations, Internet crime continues to have a huge financial impact on organizations. The financial impact is either a result of damages suffered by organizations attacked in some capacity or is a result of investments that organizations make in security technologies to guard against these attacks. Organizations suffered an average loss of $345,005 in 2006 up from $167,713 the previous year [Richardson, 2007]. Financial fraud ($21,124,750), viruses/worms/spyware ($8,391,800), system penetration from outsiders ($6,875,000), and theft of confidential information ($5,685,000) were the leading attack categories for total financial loss. The above numbers are even more revealing if one takes into account the fact that organizations are reluctant to fully disclose financial information on damages while reporting security breaches. The overall costs of security incidents have grown by 50 percent over the two year period from 2005 to 2006 [Price Waterhouse Coopers, 2006]. Despite the financial impact of these security incidents, investment in security and recovery technologies is still limited. About 35 percent of organizations spend less than 3 percent of their information technology budget on security technologies. On the other hand, only 9 percent of organizations report spending more than 10 percent of their technology budget on security [Richardson, 2007; Deloitte and Touché, 2007]. The

decrease in growth of IT budgets has also resulted in no radical change in the security funding scenario over the years. This reporting of security allocations in terms of IT budget also indicates that security is still not considered a strategic activity. Moreover, most organizations still base security allocations on ROI computations.

We argue that such static allocations of security budget are counterproductive and organizations should periodically re-evaluate their security allocations depending on the environment. Moreover, we argue that a distinction has to be made among security and recovery technologies, and trade-offs between security and recovery technologies should be evaluated more closely. Since the environment and perpetrator behavior constantly evolve, security and recovery allocations should also be adjusted. This article develops a simultaneous decision general equilibrium model and uses it to evaluate security and recovery tradeoffs and attempts to provide an answer regarding whether organizations should increase or decrease their security and recovery allocations based on changing environmental and legal conditions.

II. BACKGROUND LITERATURE

In our research, we attempt to allocate the organization's IT resources between information technology for organizational support activities, information security, and disaster recovery infrastructure. However, criminals also adapt their criminal activities in response to organizations' security investments. This results in a unique scenario in which organizations have to incorporate criminal behavior into their decisions regarding IT security investment levels. Incorporating criminal behavior into security decisions is not new. Economists have attempted to integrate criminal behavior profiles with decisions on dealing with criminal behavior. They have argued for years that both crime and demand for protection from crime are motivated by the simple principle of accumulation of wealth (incentives). Becker [1968], in his pioneering work, presented a market-based model for crime and punishment. He modeled the damage caused to society by crime as a function of the activity level of criminals. The criminal had monetary and psychological incentives to commit crime. However, if caught, the criminal was subject to punishment from the government. Ehrlich [1996] developed a "market model" that assumed that the offender, a potential victim, buyers of illegal goods and services, and law enforcement authorities all behaved in accord with the rules of optimizing behavior. He created a supply of offenses and demand for protection against crimes and explained the diversity of crime across time and space. Viren [2001] proposed a supply-of-labor model in which criminal activities could be considered both as work and leisure. The criminal divided his time among labor, leisure, and criminal activity, part of which the criminal considered to be leisure. Cox [1994] also developed a two-player game between the police and the public, where the public had a choice to engage in illegal activity (speeding) or not. Lacroix and Marceau [1995] developed a model through pair-wise interaction between the criminal and the owner. The owner made the protection decision, while the criminal observed whether the owner is protected and thus made a decision on stealing. Marjit et al. [2000] presented an incomplete information model where incomplete information available to the law enforcement agent might help to prevent crime and an agent was likely to engage in bribery. Cressman et al. [1998] developed a two-player game between property owners and potential criminals with exogenous levels of public policing and criminal sanctions. They used an evolutionary approach to show that the crime rate is cyclical over time and the average crime rate over the cycle is invariant on the magnitude of criminal sanctions. The authors derived scenarios in which a criminal would attack protected or unprotected owners.

The definition of crime covered in the above literature included murder, robbery, assault, theft, tax evasion, and bribery. However, the new category of crime, i.e., electronic crime conducted using a communication medium and primarily targeting computing and information resources, has not been studied using the above approach. Unique methods of perpetrating electronic crimes and their impact on today's highly interconnected e-commerce environment have warranted an independent analysis of such crimes. In the past few years, there have been efforts to determine the direction of economic analysis of computer crimes and the impact of security technologies. Gordon and Loeb performed economic analysis to compute optimal investments to protect specific information [2002]. Their model takes into account the vulnerabilities to information of specific breaches and associated losses. They argued that firms should not focus merely on information assets with the highest level of vulnerabilities. Gal-or and Ghose analyzed economic incentives to firms for joining security-related information sharing alliances [2005]. Davies attempted to evaluate the impact of the conjunction of firewall, intrusion detection, and vulnerability assessment technologies on the security effectiveness of the firm. Cavusoglu et al. based their security investment decisions on the modeling of specific technologies and evaluating the performance and interaction of these technologies [2004]. Yue and Çakanyildirim attempted to jointly optimize configuration decisions for the detection and response mechanism for an Intrusion Prevention System [2007]. Although all these articles provide valuable insights into managerial decision making and add significant value to the security literature, the current work, to the best of our knowledge, is the first attempt to evaluate the tradeoffs between security and recovery technologies. Moreover, we attempt to model a dynamic environment in which the perpetrators themselves alter their behaviors in response to environmental changes. We specifically attempt to evaluate the security and recovery decision tradeoffs for organizations and acceptable activity levels for perpetrators in response to changes in environmental conditions.

III. THE MODEL

This research creates a simultaneous decision making framework to identify strategies for firms and attackers. The framework is comprised of two players who make decisions to optimize their own objectives based on assumptions regarding the actions of the other player. The first player is the representative firm that characterizes organizations making resource allocation decisions to their technology, security, and disaster recovery infrastructure. Technology investment represents the information technology that is used to support business operations for productivity gains, to increase the effectiveness of activities, and to gain strategic advantage over competitors [Brynjolfsson, 2000; Lin, 2009; Melville, 2004]. Information security includes technology and administrative operations that aim at preventing the information assets of the organization from being exploited by perpetrating agencies [Swanson, 1996]. Disaster recovery or recovery resources represent the organization's attempts to create redundant capacities, establish contracts for emergency services, and create plans to reduce the impact of a successful breach of security of an organization's information assets[1] [Swanson, 2002]. The second player in the model is the perpetrator or attacker. This player represents the script kiddies, crackers, and elite hackers who spend their resources and skills in an effort to compromise organizations' information assets in order to fulfill their social, political, or financial agendas [Convery, 2004]. This section presents how the model has been constructed to capture each player's key behavioral and functional characteristics.

Player 1: The Firm

The first player in the setup represents the organizations that face the decision to allocate their technology budget to different categories of information technology. Henceforth, we refer to this representative organization as *the firm*. Most organizations attempt to operate within an IT budget.[2] They are often faced with the dilemma of whether to spend this budget to meet operational and competitive demands of the business or to spend it on the security technologies that would protect information assets of the business and prevent operations from suffering, due to intrusive activities by perpetrators, and maintain the reputation of the business.

The first component of allocation of the technology budget for the firm is the core and support information technologies that are needed to support the long term strategic goals of the organization as well as day-to-day operations of the organization. This allocation generates value for the firm through productivity gains and increased competitive advantage. We refer to this component of the technology as the *Infrastructure Technology* and represent it as T . The value generated by this allocation and the cost of the infrastructure technology incurred by the firm are represented in (1) and (2). t represents the marginal cost of infrastructure technology investment and v represents the marginal value to the firm from the infrastructure technology.

$$V = vT \quad (1)$$

$$C_T = tT \quad (2)$$

However, the use of technology infrastructure to help achieve business objectives does not come without a cost. The very technologies that help organizations increase their profitability are also vulnerable to exploitation from external agents like hackers, terrorists, and/or competitors. This results in direct or indirect damages to the firm [Mell, 200; Gupta, 2006]. Direct damages could be loss of resources, loss of proprietary information, and/or system outages. Indirect damages could be opportunity cost of time, loss of customer trust, and loss or damage to reputation. The firm has an option to allocate part of its technology budget toward technologies that would decrease the probability of such exploitations.

There are many security technologies that help reduce the probability of a perpetrator being able to successfully carry out an attack that could potentially result in damages to the firm. For instance, screening routers and firewalls typically investigate packets coming in or going out of a network segment and allow or block traffic based on a set of rules. These rules intend to classify benign connections vs. the connections that may be attacks. A recommended implementation of firewall technology is to use multiple firewalls and implement them in a layered topology [Scarfone, 2009]. However, though this technique decreases the probability of success of an attack, it also increases the total cost of implementation and maintenance of the technology. Similarly, Intrusion Detection Systems actively monitor traffic on the system in an attempt to identify intrusive activities on the system/network. If an intrusive activity is identified, action can be taken to stop the activity from exploiting system resources. However, though this technology reduces the probability of success, it is limited in its detection capability and increases the cost of technology stemming from the investigation of alarms. It also suffers from false positives, where the benign activity is

[1] Sometimes additional resources that are available for performance reasons can act as redundant resources in case of emergencies. However, the primary purpose of investment in these resources was performance and redundancy feature comes at the cost of performance. For the purpose of this research, we choose to classify these resources as strictly infrastructure technology.

[2] Security investments are typically reported as a percentage of IT budget.

classified as an attack [Scarfone, 2007]. Encryption technologies help provide confidentiality, integrity, and authentication services based on the algorithm used and implementation mechanism [Stallings, 2006]. These technologies can protect the critical information of the organization during both storage and transmission over the network. However, these technologies incur implementation costs as well as processing costs for encrypting and decrypting messages. Moreover, encryption technologies have a requirement of key management that may further add to administrative costs to maintain these technologies [Stallings, 2006].

We represent security technologies as S and the cost of these security technologies is presented by (3). s represents the marginal cost of acquiring the security technology.

$$C_S = sS \tag{3}$$

However, the firm's security is not just dependent on the investment in security technology. The bigger the firm's technology infrastructure, the higher would be the cost to secure it. The larger networks would require segmentation of the network and multiple devices at every choke point between the network segments. We define the term, *security level* ψ, to be dependent on both the security infrastructure and the technology infrastructure. The security level is computed as represented by (4).

$$\psi = \frac{S}{T} \tag{4}$$

The probability of the success of the attacker is dependent on the skill level θ that the attacker possesses and the volume of intrusive activity the attacker is willing to perform. (We address these two parameters in greater detail during our discussion of the perpetrators). The more skilled the attacker is, the higher the likelihood the attacker will successfully execute the attack. However, if the firm's security investments are high, the same probability would be reduced for the attacker. Technologies like IDS, firewalls, antivirus systems, and cryptography all have a negative impact on the probability of success for the attacker. We represent the probability of success of the attacker as ρ and compute it using (5).

$$\rho = \frac{\theta A}{S} \tag{5}$$

Despite the investment in security technology, the firm cannot guarantee protection of its information technology infrastructure. This is because as technology evolves and changes, so do vulnerabilities in the technology. Moreover, vulnerability assessment in itself is not a precise science. Attackers may also learn from their past mistakes and find innovative ways to exploit vulnerabilities which statically configured security devices may not detect. If the attacker is successful in circumventing the security of the firm and exploits the vulnerabilities, the firm may incur damages. The damages could include direct cost of replacement of hardware/software, loss of property/proprietary information, downtime for operations, and loss of reputation. None of these is a desirable scenarios, and, even if the firm cannot prevent exploitation from happening, the firm prefers to limit the impact of exploitation. For instance, the firm could invest in redundant resources so that, if the primary operational server goes offline, the firm can switch operations to the backup server and limit the impact of exploitation. The firm can also develop procedures and policies that would help guide decision makers in the event of an attack.

Investment in security technologies to an extent helps the firm limit the impact of successful exploitation of vulnerabilities. Intrusion Detection Systems, for instance, may help detect an attack while it is in progress and may help limit the damage resulting from that particular attack. Antivirus software can help repair and quarantine the affected files. Moreover, the firm can also choose to invest in resources that help maintain business continuity and quickly recover from disasters (security incidents). We classify these categories of technologies as recovery technologies and represent them by B. These recovery technologies could be redundant resources used to keep the operations running without downtime or contracts with other organizations to provide hardware/software/people in case of emergencies. The cost of these recovery technologies is represented by (6). b represents marginal cost of recovery resources.

$$C_B = bB \tag{6}$$

The extent of damage control that these recovery technologies provide is also dependent on the size of the infrastructure technology. The larger the firm's technology infrastructure, the more complicated and expensive the recovery process. We define the damage limiting factor, g, as the extent to which the recovery investment would limit the damage to the firm's resources, from a successful attack, given a level of technology infrastructure. The damage limiting factor is computed as in (7).

$$g = T(1-B) \quad (7)$$

The damage caused to the firm is also dependent on the skill level and effort exerted by the attacker. A less skillful attacker may get to the firm's network access resources remotely but, unlike a skillful attacker, may not be able to get into the core resources of the organization, thereby limiting the extent of damage the attacker can cause to the firm. Effort or activity level of the attacker would determine how long the attacker stays on the firm's system, increasing the likelihood of damage to the firm. We represent the damage caused to the firm as D. As described above, the damage can be limited by the security level and recovery limiting factor of the firm. The damage is computed as represent by equation (8).

$$D = \theta A \frac{g}{\psi} \quad (8)$$

Furthermore, the extent of the investment by the firm in infrastructure technology, security technology, and recovery technology will be limited by budgetary constraints. Most organizations have an information technology budget that is redistributed and allocated among these three technology categories.[3] We normalize the total available budget to 1. We assume the infrastructure technology T, security technology S, and recovery technology B are continuous variables. These variables are also constrained in the range $[0,1]$, i.e. $T,S,B \in [0,1]$ The budgetary constraint is represented in (9).

$$tT + sS + bB \leq 1 \quad (9)$$

Since the firm operates under this budget constraint, the problem for the firm becomes how to allocate these budgetary resources to infrastructure, security, and recovery technologies, such that the gains to the firm from the infrastructure technology are maximized, while minimizing the expected damage to the firm from intrusive activities perpetrated by the attacker. The resulting objective function of the firm subject to the constraint is represented by (10).

$$\begin{aligned} &\underset{B,S,T}{Max}\ \Pi = V - \rho D \\ &subject\ to \\ &tT + sS + bB \leq 1 \end{aligned} \quad (10)$$

Expanding the expressions and making the constraint binding, the objective function of the firm becomes:

$$\begin{aligned} &\underset{B,S,T}{Max}\ \Pi = V - \frac{\theta^2 A^2 (1-B) T^2}{S^2} \\ &subject\ to \\ &tT + sS + bB = 1 \end{aligned} \quad (11)$$

Solving the Firm's Decision Making Problem

We solved the firm's objective function subject to the constraints and obtained the following first-order conditions. (Note that one of the decision variables has been eliminated by making the budget constraint a binding constraint).

$$\Pi_T = v - \frac{\theta^2 A^2 \left[2(b-1)T + 2sST + 3tT^2\right]}{bS^2} = 0 \quad (12)$$

$$\Pi_S = \frac{\theta^2 A^2 T^2 \left[2(b-1) + sS + 2tT\right]}{bS^3} = 0 \quad (13)$$

These equations can be solved to obtain the budgetary allocation levels for infrastructure technology, security technology, and recovery technology. These results are reflected in equations(14), (15), and (16).

[3] In reality, some of these technologies would be hard to distinguish from each other, and an investment in hardware/software may bring a combination of these technologies. For instance, although an operating system is an infrastructure technology, it also provides support for security (e.g., authentication support, windows inbuilt firewall) and recovery technologies (e.g., automated backup and recovery in Windows).

$$T = \frac{(1-b)}{t}\left[1 - \frac{\theta A s}{\sqrt{\theta^2 A^2 s^2 + 4vbt}}\right] \quad (14)$$

$$S = 2\frac{(1-b)\theta A}{\sqrt{\theta^2 A^2 s^2 + 4vbt}} \quad (15)$$

$$B = 1 - \frac{(1-b)\theta A}{b\sqrt{\theta^2 A^2 s^2 + 4vbt}} \quad (16)$$

The above expressions show the relationships between the decision variables and the attacker skill level, marginal costs, and the attacker activity level. Although these expressions can help dictate decisions related to budgetary allocations, the outcomes may not be entirely desirable. The problem resides in the fact that these expressions are not all independent of attacker effort, that is, a decision that the attacker makes. Moreover, the attacker would alter its activity level, given the firm's technology and security infrastructure. Since the activity or effort level of the attacker is variable by itself and is dependent on the parameters, we will have to solve the attacker decision problem to make any credible judgments regarding the firm's allocation of technology resources.

Player 2: The Attacker

The second player in our model, the attacker, represents the perpetrators of the computer crime. These perpetrators could be script kiddies, crackers, hackers, terrorists, business competitors, foreign governments, or any other entity that is involved in computer crime, irrespective of their motives. Each of these entities indulges in criminal activities against the firm's information assets to fulfill its objectives, whether it is notoriety for script kiddies, financial gain for crackers and business competitors, or socio-political objectives of foreign governments and terrorists. No matter what the motivation of each of these criminals is, their indulgence in computer crime against the firm's information assets incurs costs to the firm, whether the costs are due to damage caused by successful breaches of security and exploitation of vulnerabilities or to the cost of efforts and technologies to try to keep criminals away. Each of these perpetrators has varying degrees of skills and available resources for criminal activities. Script kiddies may have lower skills and may be dependent on freely available automated tools to attack the firm's information assets; however, they may still be a significant nuisance to the firm. On the other hand, crackers or business competitors who have financial objectives may have enough resources to develop unique attacks that compromise the firm's assets. We attempt to capture this variability in skills and resources through the introduction of a variable—skill level $\theta \in [0,1]$. Each type of offender can be classified as a specific type of skill θ_T; the higher the skills, the higher the skill level. Researchers have implemented the type of criminal as a continuous variable within a specified range [Marjit, 2000]. We also assume θ to be continuous in the allowed range.

Each of the attackers also exerts a varying degree of effort into the criminal activity. We assume that the effort is directly reflected in the attacker's activity and thereby use the activity level, A as a measure of the attacker's effort. Both the attacker's skill level and the effort that the attacker exerts have a direct role to play in the success of the attacker's effort as well as the level of damage the attacker manages to cause to the firm. For instance, a less skilled script kiddy may not have exceptional skills but may be able to successfully perpetrate an attack by mere perseverance and a very high level of effort. On the other hand, a highly skilled cracker may develop a tool that increases the probability of success at minimal level of effort. The damage caused to the firm was represented by (8) and was discussed in the previous section. If the attacker is successfully able to cause damage to the firm's information assets, the attacker derives gains from the associated damage. Again, these gains could be psychological, financial, or political in nature. No matter what the type of gain, this gain is going to be a function of success of the attack as well as the level of damage that the attacker managed to cause to the firm. We represent the gain to the attacker as G and compute it using (18), where γ is the marginal gain that the attacker derives from a successful attack.

$$G = \gamma \rho D \quad (17)$$

$$G = \gamma \theta^2 A^2 \frac{(1-B)T^2}{S^2} \quad (18)$$

The attacker has to exert an effort to maintain a level of specific activity. The effort that the attacker spends is a cost to the criminal and could be a measure of time or financial resources that the attacker has to spend to indulge in criminal activity. This could also include the opportunity cost of time, i.e., the time that the attacker could have spent

performing benevolent activities and earning wages. The cost to the criminal, E, for the effort exerted by the criminal is a function of the activity level and is given by (19), where a is the marginal effort cost to the attacker to indulge in illegal activities.

$$E = aA^2 \tag{19}$$

However, the effort that the attacker exerts is not the only contributor to costs for the attacker. Additionally, the attacker faces a risk of getting caught and convicted for criminal activity. The chances of getting caught are inversely related to the skill level and directly related to the activity level of the criminal. The highly skilled attacker would use its skill to mask its activities and reduce the probability of getting caught. On the other hand, at the same level of activity, a less skilled attacker may get caught attempting to exploit the firm's vulnerabilities. This is also evident in security incident reports where the attackers who are caught most often are the script kiddies who possess a lower level of skills and were not successful in masking their activities. Also, an increased level of activity by the attacker may leave the attacker vulnerable to the attack being traced back to it, thereby increasing the chances of the attacker being caught. The probability of the attacker getting caught is also dependent on the law enforcement activity level, L. For the sake of simplicity, we model law enforcement activity just as a parameter and not as a decision variable. Moreover, law enforcement activity is a function of resources that the government allocates and cannot be controlled by either the firm or the attacker. The firms, though, can increase the probability of catching the attacker by investing in security technologies and reporting detected attacks to law enforcement. Intrusion Detection Systems, log analysis, and trace back technologies could help identify the intruder. Moreover, the evidence collected through these technologies could be used to convict the attacker of illegal activities. We represent the probability of catching the attacker by λ and compute is using (20).

$$\lambda = (1-\theta)A\psi L \tag{20}$$

If the attacker is caught and convicted, the attacker faces punishment, depending on the legal structure implemented by the government. Punishment for the attacker could be jail time or a fine. This punishment is going to be a function of crime and hence a function of the damage that the attacker managed to cause to the firm. We model the punishment to the criminal as a fine rate, f, that the criminal incurs if convicted. Although punishments can be prison time, probation, parole, fines, or restriction on choice of occupation, the cost of different punishments to the offender can be made comparable by converting them to a monetary equivalent, represented by fines [Becker, 1968; Ehrlich, 1996].[4] The fine is again dependent on the legal structure and is not in the control of the firm or the attacker. The total fine to the criminal if caught and convicted is represented by F and computed using (22).

$$F = f\rho D \tag{21}$$

Or,

$$F = f\theta^2 A^2 \frac{(1-B)T^2}{S^2} \tag{22}$$

The expected cost to the criminal for being caught and convicted would be a product of the probability of being caught and the fine that the criminal would incur as a result of being caught and convicted. This cost would be λF.

The dilemma of continuing to indulge in criminal activity and risk being caught and convicted makes it a complex decision for the attacker. We assume a rational attacker who would attempt to maximize the gains achieved through attacks while at the same time strive to keep the effort level to the minimum and reduce the chance of getting caught and convicted. The resulting objective function of the attacker is defined by (24).

$$\underset{A}{Max}\,\Gamma = G - E - \lambda F \tag{23}$$

Or,

$$\underset{A}{Max}\,\Gamma = \frac{\gamma\theta^2(1-B)T^2}{S^2}A^2 - aA^2 - \frac{(1-\theta)\theta^2 fL(1-B)T}{S}A^3 \tag{24}$$

Solving the Firm's Decision Making Problem

We solved the attacker's objective function and obtained the following first order condition.

[4] For example, the cost of imprisonment is the discounted sum of earnings forgone and the value placed on the restrictions in consumption and freedom [Becker, 1968].

$$\Gamma_A = 2\left[\gamma\theta^2\frac{(1-B)T^2}{S^2} - a\right]A - 3(1-\theta)\theta^2 fL\frac{(1-B)T}{S}A^2 = 0 \quad (25)$$

Equation (25) can be easily solved to compute the optimal activity level that the attacker needs to indulge to maximize its gain. The activity level is:

$$A = \frac{2}{3}\frac{1}{(1-\theta)fL}\left[\gamma\frac{T}{S} - a\frac{S}{\theta^2(1-B)T}\right] \quad (26)$$

However, the above value is dependent on the firm's decision variables, and the firm is entitled to change its technology resource allocation in response to the attacker's decisions. The attacker can use (26) to compute the optimal allocation for a given level of technology investments by the firm. This captures a static problem accurately, but not a dynamic two-player problem such as we are trying to address. Therefore, the attacker's problem and the firm's objective have to be solved simultaneously to make accurate judgments on their behavior.

IV. RESULTS AND DISCUSSION

We were not able to achieve a closed-form solution to a simultaneous two-player problem. However, the objective of the research does not require a closed-form solution. Our intent is to identify the directionality of the firm's or the attacker's decisions and not the absolute value of those decisions. Moreover, the absolute value of decision variables would be dependent on the specific values of the marginal costs and control parameters that we used. Our objective is to merely identify how the decisions of the firm and the attacker change as the environment around them changes. We have defined the environment as the cost of the technology resources (defined by the marginal cost), skill pool of the attackers (defined by skill level), and the legal structure (defined by fine rate). Our intent is to identify what the firm's reaction should be if any of the above conditions change. On the other hand, it is also important to study how the attacker is going to alter its behavior to changes in the above conditions. To answer the questions identified above, we performed the comparative statics on the simultaneous two-player problem. The propositions and insights derived from the analysis are presented below. (Detailed derivations of the comparative statics results can be found in the Appendix).

Proposition 1

If the penalty to the criminal is increased, the firm should (i) increase its infrastructure technology allocation (ii), decrease its security technology allocation, and (iii) increase its recovery technology allocation.

$$\frac{dT}{df} > 0 \quad (27)$$

$$\frac{dS}{df} < 0 \quad (28)$$

$$\frac{dB}{df} > 0 \quad (29)$$

This proposition reflects a change in legal structure. If the regulations are modified to incorporate electronic crime into the legal environment, it would relieve organizations of the burden of securing their resources through extremely high security investments. The current state of regulation for electronic crime is not well developed and still an evolving process. If a government has stern penalties for criminal activities against information assets, organizations can increase their business objectives and streamline business processes instead of consuming some of these resources for high levels of protection. This is not to say that organizations can completely forgo security; however, organizations can provide some minimal level of security allocation (can correspond to industry or government standards) and put more focus on infrastructure technology. Moreover, organizations should be better prepared to handle attacks if the security that the organization provides is successfully breached. In such scenarios, an organization should strive to minimize the impact of such breaches. This proposition suggests a strategic change in risk management strategies for addressing the risks associated with information assets. Organizations should strive more toward a risk mitigation strategy (reducing the impact of materialized risk) over a risk avoidance strategy (avoiding the risk from materializing). The legal structure alleviates some of the risks for the organization through the imposition of stricter penalties on the criminal. This proposition may also reflect the difference in legal strategies between Europe and the USA. Europe has stricter regulations against electronic crimes; however, organizations are also required to comply with well-developed security standards. This environment is supported through our model.

The USA, on the other hand, believes more in market dynamics and lets each individual organization decide its own course of action, with only a few well-developed standards and laws available.

Proposition 2

If the penalty to the criminal is increased, the criminal should decrease its activity level.

$$\frac{dA}{df} < 0 \tag{30}$$

This proposition is intuitive and, in fact, supports the findings of Becker in the context of physical crime and punishment. Becker concluded that crime doesn't pay and, under optimal fines, a rational criminal should scale down its illegal activities. If the legal structure for electronic crimes evolves and perpetrators start to face stricter regulations, perpetrators will have less incentive to indulge in illegal activities and can focus their energies on more constructive tasks. A better evolved legal environment may also raise awareness regarding computer crimes and help clearly classify what comprises a crime and what does not. In the current environment, awareness regarding electronic crimes is murky, and a large number of perpetrators (for instance script kiddies) indulge in illegal activities inadvertently as they don't even understand that they are doing something illegal. Stricter penalties would make such perpetrators reevaluate their decisions and would make them think twice if they are unsure about the impact and legality of their activities.

Proposition 3

If the skill set of the attacker increases, the firm should (i) increase its allocation to security technologies and decrease its allocation to recovery technologies below a threshold skill set $\theta < \theta'$ *(ii) decrease its allocation to security technologies and increase its allocation to recovery technologies above a threshold skill set* $\theta \geq \theta'$.

$$\left.\begin{aligned} \frac{dS}{d\theta} &> 0 \\ \frac{dB}{d\theta} &< 0 \end{aligned}\right\} \text{if } \theta < \theta' \tag{31}$$

$$\left.\begin{aligned} \frac{dS}{d\theta} &< 0 \\ \frac{dB}{d\theta} &> 0 \end{aligned}\right\} \text{if } \theta \geq \theta' \tag{32}$$

This proposition addresses the threats that an organization faces. If the primary threat to the organization is from less skillful perpetrators like script kiddies, there is a high likelihood that the organization can anticipate these threats and create strategies to avoid attacks. Less skillful perpetrators, like script kiddies, depend on available technologies to perpetrate an attack and often do not possess enough skill to develop customized attack strategies. Due to this lack of skill, these perpetrators often possess the capabilities to exploit a known set of vulnerabilities. The firm can often address the known set of vulnerabilities through security technologies and significantly reduce the probability of a successful attack against its information resources. Moreover, the extent of damage that low-skilled perpetrators can cause to the firm's information assets is also limited, thereby allowing the firm to reduce its allocation for recovery technologies.

On the other hand, if the firm is faced with a highly-skilled set of criminals, it needs to focus more on recovery technology. A highly-skilled perpetrator is likely to use creative and unique ways to perpetrate electronic crime. Even if the firm invests heavily in security technologies, it is highly likely that it still may not prevent these attacks from being successful. Moreover, security technologies by design are performance inhibiting (firewalls decrease effective throughput due to the time taken to evaluate packets; authentication technologies delay access to resources for authorized users) and can become a bottleneck for operations. The technology level that may be required to combat the level of threat from highly-skilled perpetrators may actually end up having a negative impact on the organization's business performance. In these scenarios, organizations can choose to implement a minimal level of security to comply with an industry standard and then aim to reduce additional risk through preparedness for the eventuality of a successful attack against its information assets. Thus, when faced with threats originating from a highly-skilled set of criminals, it is prudent to increase the allocation to recovery technologies.

Proposition 4

If the skill set of the attacker increases, the attacker should decrease its activity level beyond a threshold skill set $\theta \geq \theta'$.

$$\frac{dA}{d\theta} < 0 \text{ if } \theta \geq \theta' \quad (33)$$

This proposition addresses strategies for different attacker profiles. A highly-skilled perpetrator should be able to use its skills to compromise the security of the firm. Increasing the level of activity for a highly-skilled attacker will only increase the attacker's chances of being caught and convicted, with a marginal or no increase in the probability of success of the attack. Moreover, the attacker can utilize the additional skills that it acquired to increase its chance of success without increasing its chances or maybe even decreasing its chances to get caught.

V. CONCLUSIONS

Managers constantly face complex decision to commit the IT budget to various resources. If organizations exist in a risk-free environment, managers make the commitment purely to productivity enhancing and strategic technologies. However, in reality, IT resources are constantly at risk through exploitation of vulnerabilities from a diverse set of entities. The manager has to constantly evaluate risk and allocate resources judiciously between different categories of technologies. One such decision that the manager faces is the allocation of resources between disaster recovery technologies and security technologies. In this article, we performed an economic analysis to evaluate this tradeoff between security and recovery technologies. The article presents scenarios under which it would be prudent to increase investment in one type of technology at the cost of the other. Using the proposed model, we were able to obtain some valuable insights for managers. If the organization faces threats from a highly-skilled set of perpetrators or if the legal environment changes so that these perpetrators face stricter penalties, it was shown to be beneficial for organizations to increase allocation to recovery technologies at the cost of security technologies. However, if the skill set of attackers that are a threat to the organization is low, the better strategy is to increase investment in security technologies at the cost of recovery technologies. Moreover, if the legal environment remains static and laws do not evolve fast enough to keep up with electronic crimes, it would be beneficial to maintain or even increase the current level of investment in security technologies. Although this article presents some interesting insights, one should be careful when implementing these recommendations, as the model structure focuses only on external sources of threats. Evaluation of these strategies in response to insider threats would be a possible future extension to this research.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Becker, G.S. (1968) "Crime and Punishment: An Economic Approach", *The Journal of Political Economy* (76)2, March–April, pp. 169–217.

Brynjolfsson, E. and L.M. Hitt (2000) "Beyond Computation: Information Technology, Organizational Transformation and Business Performance", *Journal of Economic Perspectives* (14)4, pp. 23–48.

Cavusoglu, H., B. Mishra, C. Raghunathan (2004) "A Model for Evaluating IT Security Investments",*Communications of the ACM* (47)7, pp. 87–92.

Clarke, R.V. (1977) "Psychology and Crime", *Bulletin of British Psychological Society* (30), pp. 280–283.

Convery, S. (2004) "Network Security Architectures: Expert Guidance on Designing Secure Networks", Chapter 3: Attack Taxonomy, Indianapolis, IN: Cisco Press.

Cox, G.W. (1994) "A Note on Crime and Punishment", *Public Choice* (78)1, pp. 115–124.

Cressman, R., et al. (1998) "On the Evolutionary Dynamics of Crime", *Canadian Journal of Economics* (31)5, pp. 1101–1117.

Davies, R.M. (2002) “Firewalls, Intrusion Detection Systems and Vulnerability Assessment: A Superior Conjunction?” *Network Security* (9)1, pp. 8–11.

Deloitte and Touche (2005) “2005 Global Security Survey”, http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf (current Mar. 25, 2008).

Deloitte and Touche (2007) “Protecting the Digital Assets: The 2006 Technology, Media and Telecommunications Security Survey”, http://www.deloitte.com/dtt/cda/doc/content/CE_DigiAssets_130407.pdf (current Mar. 25, 2008).

Ehrlich, I. (1996) “Crime, Punishment, and the Market of Offenses”, *Journal of Economic Perspectives* (10)1, pp. 43–67.

Gal-Or, E. and A. Ghose (2005) “The Economic Incentives for Sharing Security Information”, *Information Systems Research* (16)2, pp. 186–208.

Gordon, L.A. and M.P. Loeb (2002) “The Economics of Information Security Investment”, *ACM Transactions on Information and System Security* (5)4, pp. 438–457.

Gupta M.J., et al. (2006) “Matching Information Security Vulnerabilities to Organizational Security Profiles: A Genetic Algorithm Approach”, *Decision Support Systems* 41(3).

Hollin, C.R. (1989) *Psychology and Crime: An Introduction to Criminal Psychology*, London, England: Routledge & Kegan Paul Ltd.

KPMG (2002) “Global Information Security Survey”, http://www.kpmg.com.mx/gobiernocorporativo//libreria_gc/fraude/Global%20Information%20Security%20Survey.pdf (current Mar. 25, 2008).

Lacroix, G and N. Marceau (1995) “Private Protection Against Crime”, *Journal of Urban Economics* (37)1, pp. 72–87.

Lin, W.T. (2009) “Business Value of Information Technology as Measured by Technical Efficiency: Evidence from Country-Level Data”, *Decision Support Systems* (46)4, pp. 865–874.

Marjit, S., et al. (2000) “Incomplete Information as a Deterrent to Crime”, *European Journal of Political Economy* (16)4, pp 763–773.

Mell, P., T. Bergeron, D. Henning (2005) “Creating a Patch and Vulnerability Management Program”, National Institute of Standards and Technology, SP 800–40.

Melville, N., K. Kraemer, V. Gurbaxani (2004) “Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value”, *Management Information Systems Quarterly* (28)2.

Price Waterhouse Coopers (2006) “Information Security Breaches Survey 2006”, http://www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf (current Mar. 25, 2008).

Quinn, K. and J. Spike (2006) “Second Annual New Zealand Computer Crime and Security Survey”, University of Otago, New Zealand—Business School.

Richardson, R. (2007) “2007 CSI Computer Crime and Security Survey”, Computer Security Institute, http://www.gocsi.com.

Scarfone, K. and P. Mell (2007) “Guide to Intrusion Detection and Prevention Systems”, National Institute of Standards and Technology, SP 800–94.

Scarfone, K. and P. Hoffman (2009) “Guidelines on Firewalls and Firewall Policy”, National Institute of Standards and Technology, SP 800–41.

Stallings, W. (2006) “Cryptography and Network Security: Principles and Practices”, Upper Saddle River, NJ: Prentice Hall.

Swanson, M. and B. Guttman (1996) “Generally Accepted Principles and Practices for Securing Information Technology Systems”, National Institute of Standards and Technology, SP 800–14.

Swanson, M., et al. (2002) “Contingency Planning Guide for Information Technology Systems”, National Institute of Standards and Technology, SP 800–34.

Viren, M. (2001) “Modeling Crime and Punishment”, *Applied Economics* (33)14, pp. 1869–1879.

Whitman, M.E. (2003) “Enemy at the Gates: Threats to Information Security”, *Communications of the ACM* (46)8, pp. 91–95.

Yue, W.T. and M. Çakanyildirim (2007) "Intrusion Prevention in Information Systems: Reactive and Proactive Responses", *Journal of Management Information Systems* (24)1, pp. 329–353.

APPENDIX

First Order Conditions from equations 12, 13, and 25

$$\Pi_T = v - \frac{\theta^2 A^2 \left[2(b-1)T + 2sST + 3tT^2\right]}{bS^2} = 0 \quad (34)$$

$$\Pi_S = \frac{\theta^2 A^2 T^2 \left[2(b-1) + sS + 2tT\right]}{bS^3} = 0 \quad (35)$$

$$\Gamma_A = 2\left[\gamma\theta^2 \frac{(1-B)T^2}{S^2} - a\right]A - 3(1-\theta)\theta^2 fL \frac{(1-B)T}{S} A^2 = 0 \quad (36)$$

Comparative Statics is performed by taking the total differentials of the first order conditions. Below are the equations used for comparative statics, where H is the parameter used for performing comparative statics.

$$-\left[\frac{v}{T} + 3\frac{\theta^2 A^2 tT}{bS^2}\right]dT + 2\frac{\theta^2 A^2 tT^2}{bS^3}dS - 2\frac{v}{A}dA = -\Pi_{HT}dH \quad (37)$$

$$2\frac{\theta^2 A^2 tT^2}{bS^3}dT + \frac{\theta^2 A^2 sT^2}{bS^3}dS = -\Pi_{HS}dH \quad (38)$$

$$\left[2\frac{aA}{T} + \frac{\gamma\theta^2 AsT}{bS^2}\right]dT - \left[2\frac{aA}{S} + \frac{\gamma\theta^2 AsT}{bS^3}\right]dS + \left[2a - \frac{\gamma\theta^2 sT^2}{bS^2}\right]dA = -\Gamma_{HA}dH \quad (39)$$

Proof for Proposition 1

Substituting f for H in equations 37, 38, and 39 and isolating $\frac{dS}{df}$, we obtain

$$\frac{dS}{df} = 6\frac{(1-\theta)\theta^2 ALstvS^2T^2}{\left[\left(2a - \frac{\gamma\theta^2 sT^2}{bS^2}\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] - 2v\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)\right]} \quad (40)$$

Reducing the first order conditions in equations 34, 35 and 36, we also obtain

$$2a - \frac{\gamma\theta^2 sT^2}{bS^2} < 0 \quad (41)$$

Hence,

$$\frac{dS}{df} = \frac{(+)}{\left[(-)(+) - (+)\right]} < 0 \quad (42)$$

Similarly, isolating $\frac{dT}{df}$ and $\frac{dB}{df}$ we obtain,

$$\frac{dT}{df} = -3\frac{(1-\theta)\theta^2 ALs^2\ vS^2T^2}{\left[\left(2a - \frac{\gamma\theta^2 sT^2}{bS^2}\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] - 2v\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)\right]} \quad (43)$$

Hence,

$$\frac{dT}{df} = -\frac{(+)}{[(-)(+)-(-)]} > 0 \tag{44}$$

$$\frac{dB}{df} = -3\frac{(1-\theta)\theta^2 ALs^2 tvS^2T^2}{b\left[\left(2a-\frac{\gamma\theta^2 sT^2}{bS^2}\right)\left[(3sS+4tT)\theta^2A^2T^2t+bsvS^3\right]-2v\left(2abS^2+\gamma\theta^2T^2s\right)(sS+2tT)\right]} \tag{45}$$

Hence,

$$\frac{dB}{df} = -\frac{(+)}{[(-)(+)-(+)]} > 0 \tag{46}$$

Proof for Proposition 2

$$\frac{dA}{df} = \frac{3(1-\theta)\theta^2A^2LsT\left[(3sS+4tT)\theta^2A^2T^2t+bsvS^3\right]}{2b\left[\left(2a-\frac{\gamma\theta^2sT^2}{bS^2}\right)\left[(3sS+4tT)\theta^2A^2T^2t+bsvS^3\right]-2v\left(2abS^2+\gamma\theta^2T^2s\right)(sS+2tT)\right]S} \tag{47}$$

Hence,

$$\frac{dA}{df} = \frac{(+)}{[(-)(+)-(+)]} < 0 \tag{48}$$

Proof for Proposition 3

$$\frac{dS}{d\theta} = -\frac{\frac{2ab(2-3\theta)S^2+\gamma\theta^3T^2s}{1-\theta}+\left(\gamma\theta^2T^2s-2abS^2\right)}{b\left[\left(2abS^2-\gamma\theta^2sT^2\right)\left[\frac{s}{4bS^2Tt}+\frac{3\theta^2A^2Ts}{4b^2S^4v}+\frac{\theta^2A^2T^2t}{b^2S^5v}\right]-\frac{\left(2abS^2+\gamma\theta^2T^2s\right)(sS+2tT)}{2bS^3Tt}\right]\theta S^2} \tag{49}$$

For $\theta > \theta'$

$$\frac{dS}{d\theta} = -\frac{(-)}{[(-)(+)-(+)]} < 0 \tag{50}$$

For $\theta \le \theta'$

$$\frac{dS}{d\theta} = -\frac{(+)}{[(-)(+)-(+)]} > 0 \tag{51}$$

$$\frac{dB}{d\theta} = \frac{s\left[\frac{2ab(2-3\theta)S^2+\gamma\theta^3T^2s}{1-\theta}+\left(\gamma\theta^2T^2s-2abS^2\right)\right]}{2b^2\left[\left(2abS^2-\gamma\theta^2sT^2\right)\left[\frac{s}{4bS^2Tt}+\frac{3\theta^2A^2Ts}{4b^2S^4v}+\frac{\theta^2A^2T^2t}{b^2S^5v}\right]-\frac{\left(2abS^2+\gamma\theta^2T^2s\right)(sS+2tT)}{2bS^3Tt}\right]\theta S^2} \tag{52}$$

For $\theta > \theta'$

$$\frac{dB}{d\theta} = \frac{(-)}{[(-)(+)-(+)]} > 0 \tag{53}$$

For $\theta \le \theta'$

$$\frac{dS}{d\theta} = \frac{(+)}{\left[(-)(+)-(+)\right]} < 0 \qquad (54)$$

Proof for Proposition 4

$$\frac{dA}{d\theta} = -\frac{A}{\theta}\left[1 + \frac{2STt\left(\frac{2ab(2-3\theta)S^2 + \gamma\theta^3T^2s}{1-\theta} + \left(\gamma\theta^2T^2s - 2abS^2\right)\right)}{\left[\left(2abS^2 - \gamma\theta^2sT^2\right) - \left(2abS^2 + \gamma\theta^2T^2s\right)(sS+2tT)\left(\frac{s}{4tT} + \frac{3\theta^2A^2Ts}{4bS^2v} + \frac{\theta^2A^2T^2t}{bS^3v}\right)\right]}\right] \qquad (55)$$

For $\theta > \theta'$

$$\frac{dA}{d\theta} = -\left[1 + \frac{(-)}{\left[(-)-(+)\right]}\right] < 0 \qquad (56)$$

ABOUT THE AUTHORS

Dr. Mukul Gupta is a Certified Information Systems Security Professional, Certified Information Systems Auditor, and Certified Authorization Professional working as an independent security consultant and as a faculty member at the College of Business at University of Texas at San Antonio (UTSA). He is instrumental in the development and delivery of NSA certified Information Assurance and Security program at UTSA. Prior to UTSA, he also served on the faculty of the University of Connecticut. His primary areas of research include information security management, intrusion detection systems, and data mining. He has published several articles in the area of information security in journals and conference proceedings. Dr. Gupta was a Principal Investigator in research grant administered by Air Force Research Laboratories. Dr. Gupta holds a PhD from Purdue University's Krannert Graduate School of Management in Management Information Systems, and Master's from Indian Institute of Technology, New Delhi.

Dr. Alok R. Chaturvedi is a Professor in Purdue University's Krannert Graduate School of Management and the Founder, Chairman, and the CEO of Simulex Inc., a Modeling and Simulation Company and Knowrtal, LLC, a collective intelligence company, both located in Purdue Technology Park. He is the technical lead for U.S. Department of Defense's Sentient World Simulation project. Dr. Chaturvedi is the founding Director of Purdue Homeland Security Institute and has also served as an Adjunct Research Staff Member at the Institute for Defense Analyses (IDA), Alexandria, Virginia. He received his PhD in Management Information Systems and Computer Science from the University of Wisconsin–Milwaukee. He is an accomplished scholar and thinker and has published extensively in major journals. He has been involved with several government task forces on important public policy and national security matters. Dr. Chaturvedi was named in Federal 100 by *Federal Computer Weekly* and was awarded the "Sagamore of the Wabash" by the Governor of Indiana, the highest civilian award for his service to the State.

Dr. Shailendra Raj Mehta is Visiting Professor of Business Policy at Indian Institute of Management, Ahmedabad, and Academic Director of Duke University's Corporate Education Arm–Duke CE. Prior to Duke and IIM–Ahmedabad, he was at Purdue University for sixteen years, where he taught Economics and then Strategy. His research interests span entrepreneurship, experimental economics, computational finance, and simulations. He has been on over two dozen PhD thesis committees. One of his papers was the subject of a full length review by the *Economist*. He has commercialized some of his research by helping create a start-up company in the Purdue Technology Park. He is also an award-winning teacher having won several prizes and citations for excellence in teaching. His BA and MA are from Delhi University, his M.Phil. is from Oxford and his PhD is from Harvard.

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems