Communications of the Association for Information Systems

ECONOMICS OF IT SECURITY MANAGEMENT: FOUR IMPROVEMENTS TO CURRENT SECURITY PRACTICES

Hasan Cavusoglu
Sauder School of Business
The University of British Columbia
cavusoglu@sauder.ubc.ca

Huseyin Cavusoglu
A.B. Freeman School of Business
Tulane University

Srinivasan Raghunathan
School of Management
The University Of Texas At Dallas

ABSTRACT

The importance of effective management of IT security from an economic perspective increased in recent years because of the increasing frequency and cost of security breaches. Each security breach incurs monetary damage, corporate liability, and loss of credibility. This article presents four important elements that every IT security manager should consider while managing the security function from an economic perspective. The four elements are: estimation of security breach cost, a risk management approach, cost effective technology configuration, and value from deployment of multiple technologies.

Keywords: security, economics of security, security practices, security management

I. INTRODUCTION

Increased interconnectivity among computers enabled by the Internet raised the scale and scope of information technology related crimes. As E-Commerce continues to grow, so does cybercrime. The Department of Justice caseload itself reflects the growth of cybercrime. The number of computer intrusion cases jumped from 547 in 1998 to 1154 in 1999. These figures represent only the reported cases. Many cybercrimes go unreported because firms fear potentially adverse publicity, embarrassment, and negative effects that such disclosures could

have on consumer and investor confidence. Some intrusions are not detected[1]. The cost of cybercrime increased over the last several years:

- In 2000, a global survey by InformationWeek and PriceWaterhouse Coopers LLP estimated that computer viruses and hacking took a $1.6 trillion toll on the worldwide economy and $266 billion in the United States alone [Denning 2000].

- In 2002, the losses from computer crime incidents reported to the Computer Security Institute (CSI) and FBI survey were $456 million in contrast to $266 million in 2000 and $124 million in 1999 [Power, 2002].

IT security is no longer purely the concern of the traditional high-risk category organizations such as those in the defense, military, or government sectors. Firms in all sectors of economy must address IT security concerns because the cost of a single security breach can be huge in terms of monetary damage, corporate liability, and credibility. Even though companies spend more money for the deployment of computer security technologies, the security problem is not getting better. Firms need to recognize that even the best technology is not fool- proof. Furthermore, even if such a fool-proof technology exists, it may not always be desirable for all firms.

The fundamental premise of this article is that firms should manage security investment as any other investment by analyzing the cost-benefit tradeoffs. The growing importance of analyzing these tradeoffs is evident from the emphasis and discussion on Return on Security Investment (ROSI) by both academics and practitioners [SBQ 2001, Cavusoglu et al. 2004b]. The focus of IT security management is shifting from what is technically possible to what is economically efficient.

> "*The first rule of IT security is that you [firms] should never spend more to protect something than a thing is actually worth*." Crume [2001]

In other words, each firm should strike an appropriate balance between its risk exposure and the opportunity to mitigate the risk through security controls. This balance must be defined within the operational context of the business: firm and hacker characteristics. The ultimate decision is what to protect and how much to protect it.

This article presents four important elements that every IT security manager should consider while managing the security function from an economic perspective. The four elements are: estimation of security breach cost (Section II), a risk management approach (Section III), cost effective technology configuration (Section IV), and value from deployment of multiple technologies (Section V). Our purpose is to draw attention to the reasons why current security practices are inadequate and propose solutions to address problems overlooked by current practices.

II. ESTIMATION OF COST OF A SECURITY BREACH

The foremost requirement for analyzing IT security from an economic perspective is estimating the cost of security, or lack thereof. This estimate directly impacts investment in security technologies since any economic decision for or against an investment is made based on such estimates. Unfortunately, current practices grossly underestimate the cost of security breaches, which often leads to underinvestment in security. Underestimates occur because firms consider only tangible short-term costs associated with security breaches. They do not consider long-term or intangible costs, often because they are unable to measure them.

---

[1] The FBI's National Computer Crime Squad estimates that between 85 and 97 percent of computer intrusions go undetected [Spencer 2000].

.

In the 2002 CSI-FBI survey of 503 respondents from organizations throughout the United States, 80% reported financial losses from security breaches but only 44% (223) of them were able to quantify them[2]. The total reported losses, as highlighted above, were $456 million and the average loss was $2.0 million per organization across all type of breaches. The highest reported losses were for theft of proprietary information, reported by 41 organizations with an average loss of $4.2 million per organization. The sabotage of data networks cost an average of $352 thousand while denial-of-service resulted in $245 thousand loss per organization [Power 2002].

The costs associated with restoring a system after a security breach and business loss during the disruption provide at best a partial picture. The true cost of a security breach is multifaceted. Information security is as a value creator that supports and enables e-business, rather than only as a cost of doing business. A secure environment for information and transaction flow can create value for the organization as well as its partners and customers [Cavusoglu et al. 2004a]. By the same token, security lapses can lead to breach of consumer confidence and trust in addition to lost business and third party liability. In a survey by Media Metrix, only 12.1% of the U.S. companies with a Web presence cite direct financial loss as a concern in a security breach, but more than 40% cite consumer trust and confidence [Pastore 2001].

The costs of security breaches can be broadly classified into transitory (or short-term) costs that are incurred only during the period in which the breach occurs and permanent (or long-term) costs that are incurred after the immediate effects of the breach are dealt with . The transitory costs of security breaches include (1) lost business and worker productivity because of breached information resources, labor, and material costs required to detect, contain, and repair and reconstitute the breached resources, (2) costs associated with finding, evidence collection, and prosecution of the attacker, and (3) media related costs to providing information to customers and the public.

In the long run a security breach affects the firm's future cash flows. These costs include those related to loss of customers that switch to competitors, inability to attract new customers because of perceived poor security, loss of trust of customers and business partners, potential future legal liabilities arising out of the breach, and cost of competitor's access to confidential or proprietary information. In addition, the firm may face increased insurance cost and higher capital cost in debt and equity markets because of perceived increase of business risk.

Costs can further be classified into tangible and intangible costs. It is possible to estimate some costs such as lost sales, material and labor, and insurance. However, costs such as those related to trust are difficult to estimate. Nonetheless these costs are important in measuring the true cost of a security breach for business. Table 1 shows the degree of uncertainty in estimation of each type of cost. The magnitude of costs will also vary based on the breach type and the business type.

Table 1. Degree of Uncertainty in Estimation of Costs

	Transitory	Long-term
Tangible	*Low*	*High*
Intangible	*High*	*Very High*

[2] Data were collected from security practitioners in U.S. corporations, government agencies, and universities. High-tech (19%), financial (19%), and manufacturing (11%) industries constituted almost half of the respondents. 45% of corporations represented in the sample reported gross income of more than $ 500 million.

One way to estimate the cost, especially the intangible cost, of security breaches is the loss in market value of the firm due security breach announcements. Security breaches signal to the market a lack of concern for customer privacy and/or poor security practices within the firm. These signals in turn lead investors to question the long-term performance of the firm. In efficient markets investors are believed to revise their expectations based on new information in announcements and reflect those expectations in the market value of the firm (Fama et al. 1969). Using investors' reactions in capital markets as a proxy to estimate security breach costs, Cavusoglu et al. [2004a] found that publicly traded breached firms, on average, lost approximately 2.1% of their market value within two days surrounding the security breaches[3]. This percentage translated into a $1.65 billion average loss in market capitalization per breach based on the mean market value of firms in their data set. The magnitude of the loss was the same across different breach types. Also, the average market value loss increased over time, which suggests that investors are becoming more aware of the security issues and are likely to penalize firms more for security breaches. This figure clearly is orders of magnitude different from the average loss estimate reported in the CSI-FBI surveys. The differences in estimates occur because capital market reactions capture both intangible costs and long-term costs of security breaches, which are difficult to estimate and therefore not captured in surveys.

The estimates based on market value may be noisy because of uncertainties. However, even if the estimates are discounted, there is an order of magnitude difference between the firms' reported estimates and the market value loss. The conclusion is that the intangible costs of security breaches can be much larger than the tangible costs. Hence, firms that ignore the intangible costs are perhaps grossly underestimating the loss from security breaches. Since the investments in IT security are directly dependent on the extent of potential loss of breaches, firms are likely to under-invest in IT security if they make security investment decisions based only on tangible costs[4].

III. RISK MANAGEMENT APPROACH

Firms use a variety of approaches to manage risks associated with IT security. Secure Business Quarterly, a trade publication, highlighted these approaches [SBQ 2001]:

1. The fear, uncertainty, and doubt (FUD). For years, it was used to sell investments in security.

2. The cost of deploying security. For example the approach based on cost effectiveness of investments asks, "What is the most I can get for $X, given that I am going to spend $X?" This analysis is tractable because it does not seek to quantify the benefits of security investment and assumes security investment simply as an overhead cost.

3. The traditional risk or decision analysis framework. The idea is to identify the potential risks, possible losses, and their likelihoods and compute the expected loss.

---

[3] This study was based on 66 security incidents occurred between 1996 and 2001. Although both small and large firms were represented in the sample, the data set was skewed towards larger firms. The market value of firms varied from $158 million to $461 billion with an average of $78.3 billion.

[4] The CSI-FBI surveys estimated only direct costs such as lost productivity or sales, and expenditure on restoring the breached systems, whereas the loss estimated through change in market capitalization may also include the investors' expectations about the impact on future cash flows, which requires considerations of intangible costs such as the loss of consumer confidence.

4. Several proposed variations of the decision analysis approach that manage IT security risks using non-technical controls, such as insurance.

While these approaches can provide a useful starting point for managing security risk, they are incomplete because of the security problem's strategic nature. The limitation of these approaches can be stated as one simple proposition: They do not allow a firm's investment level to influence the behavior of hackers.

The behavioral influences of security technology on hackers have long been recognized by researchers and practitioners in the security community. Many pointed out that security should be viewed as a "cat-and-mouse" game played by firms and hackers. Tighter security technology employed by firms requires higher investment but also makes hacking more difficult. Hackers do not select their targets randomly. They rationally make their choice based on how much effort will be required to succeed in hacking and the reward as a result. The strategic interaction between a firm's investment and hacking activity must be captured in the model used to determine investment levels. Because decision theory is designed to analyze decision making under uncertainty where "nature" is the only "opponent", it is fundamentally inadequate to deal with security investment decision making where these behavioral effects occur. Modeling the interaction between firm and hacker decisions requires game theory.

The game-theoretic aspect of IT security was first noted by Jajodia and Miller [1993, p. 85]:

> *"Computer security is a kind of game between two parties, the designer of a secure system, and a potential attacker."*

A video illustration of the strategic game played by the security experts in a firm and the hackers is provided by cable channel MSNBC at its website *http://www.msnbc.com/modules/hack_attack/hach.swf*. The interactive site shows, step-by-step, how an attack against a honeypot[5] computer is launched. The intruder is referred to as black-hat while the security expert is called the white-hat. Since an intrusion detection system (IDS)[6] is installed in the system, all the actions committed by the black-hat are captured. One can see that how the expert takes actions based on what (s)he learned from IDS logs.

We use a simple example to illustrate how the game theory and the decision analysis approaches can lead to different decisions. Suppose that the game between the hacker and the firm yields the payoff matrix given in Table 2. Each player can take two actions. The firm can invest to have *high* or *low* security, and the hacker can choose to hack *less* or *more*. If the firm invests low in security and the hacker chooses to intrude less, the payoff for the firm is -5, which includes the cost of investment and the cost of undetected intrusions while the hacker gets a payoff of 6, which is the utility from hacking minus cost if the hack is detected by security controls. We can interpret other payoffs in other cells in a similar fashion. That is, the first element in a cell is the firm's payoff and the second element in the same cell is the hacker's payoff corresponding to an actions pair. The dominant strategy equilibrium of the game is (high investment and high hack). Because the firm is always better off if it invests high in security as the payoff is higher when it invests high than when it invests low. At the same time the hacker is better off if he hacks high whatever the action the firm takes.

Suppose the firm does not act strategically, and assume that the firm thinks the hacker will hack low. Then it will choose to invest less because the cost of additional investment does not justify the savings associated with prevention or detection of possible security breaches (i.e. -5>-8).

---

[5] A computer system or portion of a network that has been set up to fool potential intruders into thinking that they are accessing real systems. Honeypots intentionally contain unsecured services to gather data about hacker attack methods.

[6] Intrusion Detection Systems are discussed in Section IV.

Because the hacker always prefers high hack to low hack, the game ends up in (low investment, high hack). Note that not incorporating the strategic nature of the game makes the firm actually worse off since it gets a payoff of -10, the worst case among all cases.

Table 2. Game Theory Matrix for Firm and Hackers

		Hacker: low	Hacker: high
Firm	low	-5, 6	-10, 8
	high	-8, 4	-7, 5

The example shows that how a firm can make a wrong choice about its security investment by ignoring the tactical battle with the hacker.

We conclude that strategic nature of the problem is a significant dimension that needs to be considered when dealing with security. To be able to compete, organizations should also act strategically when choosing controls and their capabilities. Several papers recognize the game theoretic aspect of IT security problem and report on how to use game theory to evaluate security investments [Cavusoglu et al. 2004b, Cavusoglu et al. 2002].

IV. CONFIGURATION OF SECURITY CONTROLS

Configuration management and performance evaluation of security controls is another dimension that is mostly overlooked in current security practices. Guidelines from commercial security firms[7] and research institutes such as Software Engineering Institute (SEI) emphasize the need for proper configuration of security implementations. For example, SEI's guidelines on installing intrusion detection systems [Allen et al. 2000] cautions firms against accepting the default settings automatically and advises appropriate configuration to balance security and operational requirements.

To understand the implications of security system configuration on the cost-benefit tradeoff, consider the following scenarios.

1. A firm sets up its authentication system to log-off a user if the user fails to enter his userid and password correctly three times consecutively.

2. Another firm sets the limit to only one incorrect login attempt.

The first configuration will result in fewer improper rejections compared to second. But on the other hand the first firm will fail to recognize a higher number of unauthorized accesses compared

[7] For example, Sriram [2002] discusses how to choose a threshold value to detect attacks by computer viruses in Novell's BorderManager.

to the second scenario because of higher chances of guessing true credentials in the first scenario The costs associated with a configuration are false positive (Type-I) and false negative (Type-II) costs. These two types of costs can vary widely. That is, depending on the firm, the cost of a false positive can be much higher than the cost of false negative, or vice versa. Different costs associated with Type-I and Type-II errors require that a firm calibrates its security controls appropriately to balance them.

We illustrate appropriate configuration of security controls using an Intrusion Detection System (IDS). In a good IDS, we would generally like the detection rate, P_D , to be as large as possible while keeping error rate, P_F , as small as possible. However, it is not always possible to increase P_D and decrease P_F simultaneously because of the variability associated with the data of legal and illegal transactions and imprecision of algorithms and models used by the IDS. Many IDSs classify a transaction as legal or fraudulent based on whether a numerical score computed from transaction data exceeds a threshold value and/or whether the transaction data satisfy a rule. The quality parameters P_D and P_F of an IDS can be fine-tuned, though not independently, by configuring its threshold value or rules.

The ideas of detecting intrusions in an IT system are grounded in classical decision theory. The basic components of a decision theory problem are shown in Figure 1. The first is a source that generates the inputs to the IDS is the user interacting with the system that IDS is designed to protect. The simplest case involves two types of sources: normal (H_0) and abnormal (H_1). The normal

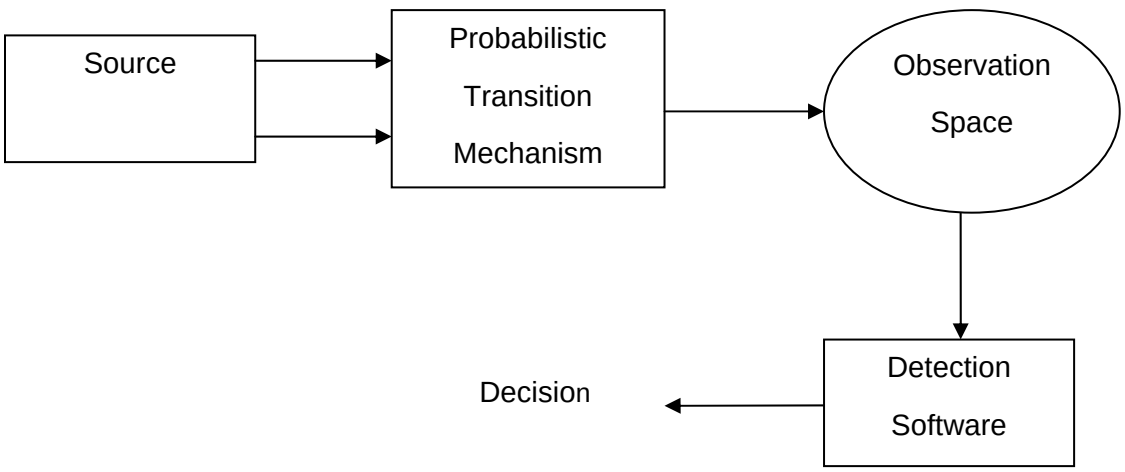

Figure 1. Components of a Decision Theory Problem

source generates legal or authorized transactions. The abnormal source generates illegal or fraudulent transactions. The probabilistic transition mechanism controls the relative frequencies of legal and illegal transactions. The IDS observes the transaction but does not know whether it came from a normal or an abnormal source. The goal of the IDS is to classify each transaction as legal or fraudulent, and to give a warning signal to security management in case of a fraudulent activity. Two types of errors can occur in this classification: (1) classification of an illegal transaction as a legal transaction (false negative) and (2) classification of a legal transaction as an illegal transaction (false positive).

For illustration purposes, assume that probability distributions for legal and fraudulent traffic are $f_L(x)$ and $f_F(x)$ respectively and normally distributed (Figure 2). Given x_L and x_F , P_D and P_F can be computed numerically for various values of *t*. We can easily verify that as *t* decreases,

both P_D and P_F increase. Consequently, the quality profile of an IDS is characterized by a curve that relates its P_D and P_F, known as the Receiver Operating Characteristics (ROC) curve. Figure 3 shows sample ROC curves for different *s* values.

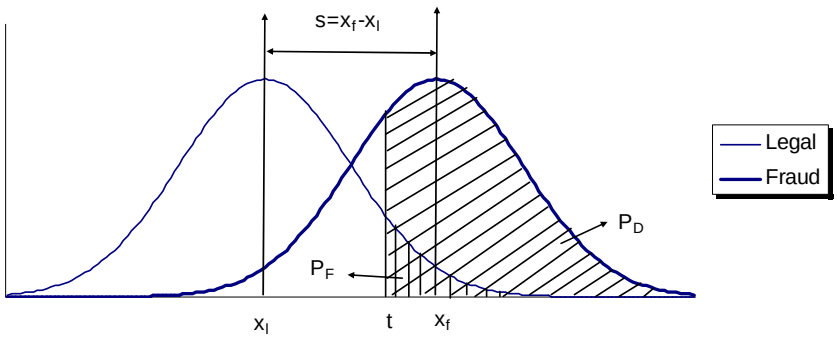

Figure 2. Computation of P_D and P_F

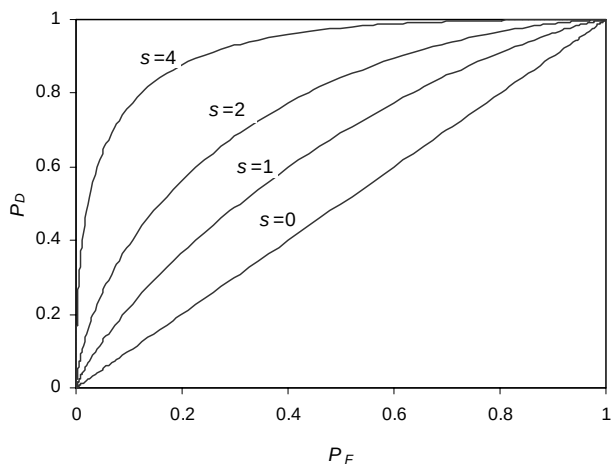

Figure 3. ROC curves

Firms need to configure their security controls carefully to achieve a balance between false positive and false negative rates. The firm's false positive and false negative costs will determine the optimal value of configuration parameter in a security control. If the cost associated with a false negative is extremely high, the firm may choose a higher level of false positive rate because the value of protected assets through the control is worth the added inconvenience of higher rate of false positives. For example, if the cost associated with an unauthorized access by an illegal user at the firewall is significantly higher than the cost of denying access to a legitimate user, the firm should implement a very tight firewall configuration. Conversely, if the cost associated with a false positive is extremely high, the firm then may choose a higher level of false negative rate because the cost of inconvenience associated with a false positive is higher than the value of protected assets through the control. In terms of configuration, if flagging an alarm for a normal user activity is more costly than missing a true intrusion at the IDS, then the wise decision should be to opt for a loose IDS configuration.

These tradeoffs are the focus of research on IDS design and configuration. For example, Lee et al. [2002] propose that design of IDSs be based on cost-sensitive machine learning algorithms. The purpose of their IDS is to generate signals only when it is economically beneficial to do. In the same spirit, Cavusoglu and Raghunathan [2004] develop a methodology based on costs to determine optimal configuration of IDSs.

V. DEPLOYMENT OF MULTIPLE SECURITY TECHNOLOGIES

No single control guarantees security by itself. Every security control is imperfect. Even if a security control is configured perfectly, which is generally impossible, and its software is free of bugs, which is also impossible, no single control can protect IT systems against all possible types of attacks. Some controls are designed for prevention, others for detection and response. Although no single control can be trusted to provide total protection, each control has its own unique place within a security architecture. This approach is called defense-in-depth or a layered system of defenses architecture. The basic principle behind this approach is that even if the hacker can crack the first line of defense, (s)he is likely to be stopped by the second or third layer. For example, if a hacker passes through the firewall to enter the system, other security layers, like an IDS or manual monitoring, will try to catch the hacker before the damage is incurred fully.

The problem with deployment of multiple controls was stated succinctly by Axelsson [2000],

> *"The best effort [security] is often achieved when several security measures are brought to bear together. How should intrusion detection collaborate with other security mechanisms to this synergy effect? How do we ensure that the combination of security measures provides at least the same level of security as each applied singly would provide, or that the combination does in fact lower the overall security of the protected system?"*

Axelsson went on to say that research is lacking on these questions.

Given that layered security architecture is a necessity for a secure environment, the crucial question to answer is how security controls interact when they are implemented together within the same security architecture. Do they complement each other or do they substitute each other? For example, is the value of a security architecture with both a firewall and an IDS greater or less than the sum of the values when each control is applied individually?

These questions are important because when a firm sets up its security architecture, it often considers how much value a security control will add to security in isolation with other controls already in place. This presumption is a selling point for security products. For example, the argument that the firewall will reduce hacker attacks by x percents and will result in $ y savings for the firm might be incorrect if the firm's security architecture already contains an IDS. Hence failing to recognize the interaction between security technologies may lead to security architecture design decisions that are not optimal.

Cavusoglu et al. [2002] showed that both complementary and substitution effects might exist between security technologies. By considering a security architecture that includes both a firewall and an IDS, they show that the firewall and the IDS may complement or substitute for one another depending on the firm's security cost structure and the detection rate of the IDS. For some firms, using both technologies may be worse than using only one of them. The conclusion of these results is that firms should carefully evaluate the value of an additional security mechanism based on already existing controls before estimating its return.

VI. CONCLUSION

Effective IT security management is the foundation of a secure operating environment. In this paper we pointed out four important elements of economics of security management that are mostly ignored or weakly addressed by current practices. These elements include

- estimation of breach costs,
- the strategic nature of security,
- configuration of security controls, and
- the complementary and substitute nature of security controls.

Academic researchers are starting to investigate each of these elements in detail. The purpose of this paper is to draw the attention to these economic aspects of IT security management in the hope that future research will yield valuable insights into poorly understood security economics.

Editor's note: This article was received on June 7, 2004 and was published on July __, 2004.

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these 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 authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner, E., (2000) State of the Practice of Intrusion Detection Technologies, Technical Report CMU/SEI-99-TR-028 ESC-99-028, Pittsburgh, PA: Carnegie Mellon University.

Axelsson, S.,(2000) "The Base-Rate Falllacy and the Difficulty of Intrusion Detection," *ACM Transactions on Information and Systems Security*, (3) 3, August.

Cavusoglu, H., B. K. Mishra and S. Raghunathan (2002), "Optimal Design of Information Technology (IT) Security Architecture," Proceedings of the *International Conference on Information Systems*, Barcelona, Spain: Association for Information Systems. December.

Cavusoglu, H., B. K. Mishra and S. Raghunathan (2004a) "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers, *International Journal of Electronic Commerce*, (8)4,

Cavusoglu, H., B. K. Mishra and S. Raghunathan, Forthcoming (2004b), "A Model for Evaluating IT Security Investments," *Communications of the ACM.*

Cavusoglu, H. and Raghunathan, S., Forthcoming, (2004) "Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches," *Decision Analysis*

Crume, J., (2001) *Inside Internet Security*, Reading, MA: Addison Wesley Denning, D.,(2000), "Reflections on Cyberweapons Controls," *Computer Security Journal*, (16) 4, pp. 3-53.

Fama, E., Fisher, L., Jensen, M. C., and Roll, R., (1969) "The Adjustment of Stock Prices to New Information," *International Economic Review*, (10) 1, pp. 1-21.

Jajodia, S. and Miller, J.(2003), "Editor's Preface," *Journal of Computer Security*. (2) 2/3, p. 85.

Lee, W., Fan, W., Miller, M., Stolfo, S., and Zadok, E.(2002), "Toward Cost-Sensitive Modeling for Intrusion Detection and Response," *Journal of Computer Security*, (10)1/2, pp. 5-22.

Pastore, M., (2001), Companies Lack Understanding of Information Security, Internet.com, October 10. **PLEASED GIVE URL**

Power, R. (2002), "2002 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends*, (8)1.

SBQ (2001), Special Issue on *Return on Security Investment*, Secure Business Quarterly, (1) 2.

Spencer, W. (2000), *Network Security Assessment*, White Paper, Denver, CO: Network System Architects Inc.,.

Sriram, T. (2002), *Blocking Virus Requests In Novell Bordermanager's Http Accelerator*. Novell Appnotes. Novell Inc.

ABOUT THE AUTHORS

Hasan Cavusoglu is Assistant Professor of Management Information Systems in Sauder School of Business at the University of British Columbia. He received his Ph.D. in Management Science with a specialization in Management Information Systems from the University of Texas at Dallas. His research areas include (1) economics of information technology investments; (2) impact of IT on customization and versioning; (3) impact of IT on customer life cycle; and (iv) IT security. He is a member of AIS and INFORMS.

Huseyin Cavusoglu is Assistant Professor of Information and Operations Management at the A. B. Freeman School of Business at Tulane University. He received his Ph.D. in Management Science with a specialization in MIS from the University of Texas at Dallas. He presented his work at various conferences, including ICIS, WISE, WITS and AMCIS. He has papers forthcoming in *Communications of the ACM, Decision Analysis,* and *International Journal of Electronic Commerce*. His major research interests are in the areas of information economics, assessment of the value of IT security, and IT security management. He is a member of AIS and INFORMS.

Srinivasan Raghunathan is Associate Professor of Management Information Systems in the School of Management at the University of Texas at Dallas. He received his Ph.D. in business from the University of Pittsburgh. His current research interests are in the economics of information systems. His publications appear in such journals as *Management Science*, *Information Systems Research*, *Journal of MIS*, and various *IEEE Transactions*.

Communications of the Association for Information Systems

ISSN: 1529-3181