Farahmand et al., "Security Tailored to the Needs of Business", In the Proceeding of the ACM CCS Workshop on Business Driven Security Engineering, ACM CCS BIZSEC 2003, Fairfax, VA, Oct. 2003.

Security Tailored to the Needs of Business

Fariborz Farahmand
College of Computing
Georgia Institute of Technology
ff@cc.gatech.edu

William J. Malik
Waveset Technologies Inc.
Bill.Malik@waveset.com

Shamkant B. Navathe
College of Computing
Georgia Institute of Technology
sham@cc.gatech.edu

Philip H. Enslow
College of Computing
Georgia Institute of Technology
enslow@cc.gatech.edu

ABSTRACT

Electronic commerce and Internet have enabled businesses to reduce costs, attain greater market reach, and develop closer partner and customer relationships. However, using the Internet has led to new risks and concerns. This paper enables managers to have a better understanding of the security needs of their businesses. We summarize the state of art of the security issues of information technology, the challenges for businesses, and the current process of deploying resources by companies to face these challenges by drawing from the substantial industrial experience of one of the authors. We describe the nature of the threats to information systems and reasons for variability of losses resulting from similar exploitation. This paper also presents a model for threat classification and control measures, and a statistical overview of information security incidents. The conclusion of our empirical analysis of the existing available literature is that the highest amount of damage in terms of the financial/market evaluation of companies is caused by the violation of confidentiality of data. Problems such as intrusion when confidentiality of data is not compromised typically only result in direct damage such as denial service which is directly quantifiable; but such damage is not comparable to the potential longer term damage of loss or disclosure of confidential information.

Keywords

Business, Cost, Risk, Security, Threat

1. INTRODUCTION

The proliferation of information technology has made the multi-national, multi-corporate, globally interconnected commercial enterprise a reality. The business community has near real-time information access with large numbers of users including customers/clients, strategic partners, teammates, vendors, and employees located worldwide. Physical and geographical boundaries are less limiting in performing electronic business transactions, as worldwide exchange of information is commonplace for today's business. However, misuse of enterprise information thorough intentional or accidental failure of enterprise information systems has the potential of causing significant damage to the economic well-being of an enterprise. One means of countering these risks is adopting suitable protection measures. This paper addresses some of the issues that industry is facing today in coping with the security of information systems and adoption of protection measures.

To have a better perspective of today's business and information security we need to know about deploying information security programs and taking its challenges by firms. We also need to follow on the performance of our professional managers from the time they learn to practice their knowledge. These issues and a quick overview of the process of learning about information security are addressed in Section 2, as the state of art of security practice in businesses.

In general, categorizing a phenomenon makes systematic studies possible. In particular, an organized classification of threats to information systems can help managers to build systems which are less vulnerable. In Section 3 we first provide an overview of coverage of security by today's business, then discuss our model for the classification of threats and control measures. Before investing on control measures, managers need to have a good understanding about the nature of the threats and their initiation and then need to decide how to deploy their resources to these threats. This is discussed in Section 4 and 5 of this paper.

Section 6 explains the belief of authors that the cost of a computer security incident to an organization has to be measured in terms of the impact on their business; hence identical incidents in two different organizations of the same industry or business type could have different costs. Evaluating

the dollar amount of damages caused by a security incident is a very complicated task. The impact of an incident may well be financial, in the form of immediate costs and intangible losses. Knowing about the possible cost of an incident can assist managers in making their assumptions explicit, capturing decision rationale, and seeing whether the investment is consistent with risk expectations. Section 7 addresses this issue.

2. THE STATE OF THE ART OF SECURITY PRACTICE IN BUSINESS

The vast majority of businesses deploy their information security programs in a piecemeal and poorly integrated fashion. In an ideal state, the security governance function is managed by a senior executive who reports to a committee of the senior leadership team on the overall state of the information security program. Once that program is established, the noteworthy elements of this report will be exceptions and upcoming changes. The information security policy will be brief but comprehensive, not mixing procedural details or instructions for specialists with the general guidelines, goals, and expectations outlined for users. The information security architecture will translate policy directives ("we will keep customer information private") into detailed platform-neutral directives ("users must authenticate themselves with a unique password that is changed every 90 days").

Most organizations are running some form of "awareness programs" to enable employees to become aware of the organizational security policies. The awareness program includes an introductory module for new hires covering the information security program as well as details on how to recognize and report a problem. Employees and contractors must take a second module covering updates to the information security program upon taking a new assignment or after there are substantial changes in the environment. Every employee attends an update seminar of a few hours annually.

Information security products and tools are acquired through a formal RFP process itself governed by an ongoing gap analysis assessing the variance between policy requirements and platform capabilities. Such tools are only deployed after a policy statement governing their use and goals is developed by the chief information security officer, who also owns responsibility for the architecture. When an information security event is suspected, a cyber emergency response team (typically a virtual team made up of a few specialists in key IT areas) acts quickly to review logs, configuration information, and assess damage. Normal requests for access (new, changed, or deleted) are processed through an automated provisioning system. Password change requests are handled by self-service capabilities. Finally, as part of an annual audit, the entire information security program is revalidated against changes in the technology, marketplace, risk profile, work force demographics, and business structure.

Businesses typically deploy a subset of the elements of an effective enterprise-wide information security program. Large, publicly traded firms recognize some obligation to their investors and recognize the potential for a) damage to their brand and reputation, b) legal and regulatory risk, or c) adverse financial consequences from an information security breech. The next tier of firms tends to be much less coordinated, relying on the talents of one or two information technology specialists who use their experience and contacts to deploy what in their individual opinion constitutes an appropriate set of countermeasures. The vast majority of smaller firms may do little or nothing to preserve or protect their IT environment. Spending on information security (not including disaster recovery) typically amounts to less than 3 percent of the IT budget, according to statistics developed by Gartner (William J. Malik was the Vice President and the Research Area Director at Gartner from 1990 through 2001, during which time he managed the Information Security Strategies service. This statistic and others sourced at Gartner are his primary research). Those elements of the information security program that are deployed find their funding justified only in response to a specific crisis: antivirus in response to a virus incident, firewalls in response to an Internet deployment issue. An awareness and training program may feature one anecdote concerning a recent problem, with no coordinated policy developed in its aftermath, and no lessons learned to enrich the corporate culture. For the majority of businesses, there may be no awareness of the scope of the vulnerabilities they face, and often there may be no awareness of security breaches as they occur.

From business school, professional managers learn what ought to be done to mitigate the risks of an information security breech, just as learning how to structure clear and effective management processes. However in the rough and tumble reality of day-to-day business, these lessons often get lost. It consumes resources to fully document procedures, review apparently completed work, deploy additional security measures, reset adequate default passwords, remove unused system ids, or apply patches to problems that have not been actually experienced. Too often businesses focus on near-term, tactical issues and ignore the strategic implications of such decisions. When a dominant firm in a particular geography or industry deploys an effective and integrated information security program, and reaps the reward through lower ongoing costs, reduced occurrences of unplanned outages, and enhanced brand and image, do some competitors begin to see how such benefits could be theirs as well. Similarly, businesses understand that clearly documented processes allow for improvement, audit, and training; but the reality is that few businesses actually document even their core procedures very well. Most managers understand that wasted time, effort, resources and product is costly; yet few are willing to invest the effort to perform a comprehensive survey of their processes to analyze and eliminate waste, redundancy, and delay. During the 1960s American industry embraced the notion of quality as a separate and distinct initiative. Major manufacturing firms designated senior managers as "Directors of Quality" and charged them with reducing product defects. These unfortunate individuals were totally ineffective, because they lacked the organizational clout to modify existing business processes. The standard process of design, development, manufacturing and field maintenance continued unchanged. The finding from this failed initiative was that quality is not an independent variable in the manufacturing process [5].

Eventually we learned that quality is an aspect of the product development life-cycle. In other words, the quality of a manufactured object is an intrinsic element of the method of the objects manufacture. The quality of a manufactured good is a

consequence of the way in which it was designed, manufactured, and serviced. Quality is not like paint – it cannot be added on after the object is finished. Similarly, we are beginning to learn that information security is not a separate discipline from information technology. Information security is an aspect of how information technology is specified, designed, acquired or developed, deployed, and maintained. A comprehensive information security program has to be deeply integrated with the system development lifecycle. The information security characteristics of an information technology environment are a consequence of its architecture, design, development, deployment, operations, and maintenance. Information security cannot be added on after an information technology environment is deployed. Information security is not a property of a product; it is a property of an environment.

3. COVERAGE OF SECURITY BY TODAY'S BUSINESS

A Literature review has identified several attempts in the classification of security threats [8, 9, 10, 11, 12]. These authors believe that these taxonomies, although they address the most important computer security threats, either do not cover all of them or do not allow them to be considered independently.

In broad terms, there are five problems that can affect data. ISO 7498-2 [6] provides the following classification of threats to data communication systems as: 1) Destruction of information and/or other resources, 2) Corruption or modification of information, 3) Theft, removal or loss of information and/or other resources, 4) Disclosure of information; and 5) Interruption of services.

The firm experiencing an event that causes such a problem might face legal difficulties, financial difficulties, or damage to its brand and reputation. By data we mean a type of intellectual property, embodied in the programs or information stored within a computer, a storage system or a computer network. The first problem facing a firm is to place a value on that intellectual property. This may be expressed in monetary terms (that pharmaceutical formula cost $x to create) or in non-monetary terms (that pharmaceutical formula would have given us a market-dominating lead for ten years). The firm needs to develop a realistic, comprehensive system of measurement to allow the relative valuation of its intellectual property, however that system is structured. Since such approaches are highly specific to each individual firm, most firms that attempt to classify intellectual property should design their IP valuation method to be extensible in the face of ongoing experience. That is, the valuation scheme itself should be able to adapt as circumstances change.

Once a firm recognizes the relative value of its intellectual property, it may choose to protect it in various ways. Specific measures might include the following. Separation of duties and need-to-know policies limit the opportunity for a single individual to affect data for whatever reason (personal gain, revenge, or self-aggrandizement). Effective audit procedures, awareness programs, and logging tools may deter aberrant behavior. Intrusion detection tools can detect and block certain classes of network security attacks. A comparison of intrusion detection systems has been done by Biermann [1]. Antivirus programs can intercept computer viruses. Provisioning tools can automate user account creation, update and deletion. Individually each of these measures may mitigate a specific class of risk. Collectively these measures are elements of an information security program. Assessing the relative impact of one measure compared with another is at present a difficult task. Each of these measures brings in a set of costs (license fees, maintenance fees, performance impact, resource consumption, technical support, operations training, user education, deployment time and expense, possibly organizational change, and so forth). Most firms have some standard manner for assessing the total cost of ownership of technology. Few firms have a standard manner for evaluating the benefit in terms of enhanced risk mitigation that procedures and tools might provide. As a result, the optimum ways to guard intellectual property rights has become a major legal and financial concern in most corporations.

It is the goal of this paper to advance the state of the art in understanding the risks involved and the measures that must be adopted toward developing an efficient security and IP protection approach. We consider the following as the security services (countermeasures) to confront these threats:

1) Authentication: The corroboration that the source of data received is as claimed.
2) Access Control: The prevention of unauthorized use of a resource, including prevention of use of a resource in an unauthorized manner.
3) Data confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
4) Data integrity: The property that data has not been altered or destroyed in an unauthorized manner.
5) Non-repudiation: Keeping audit records and logs and archiving them so that denial of communication can be disproved.

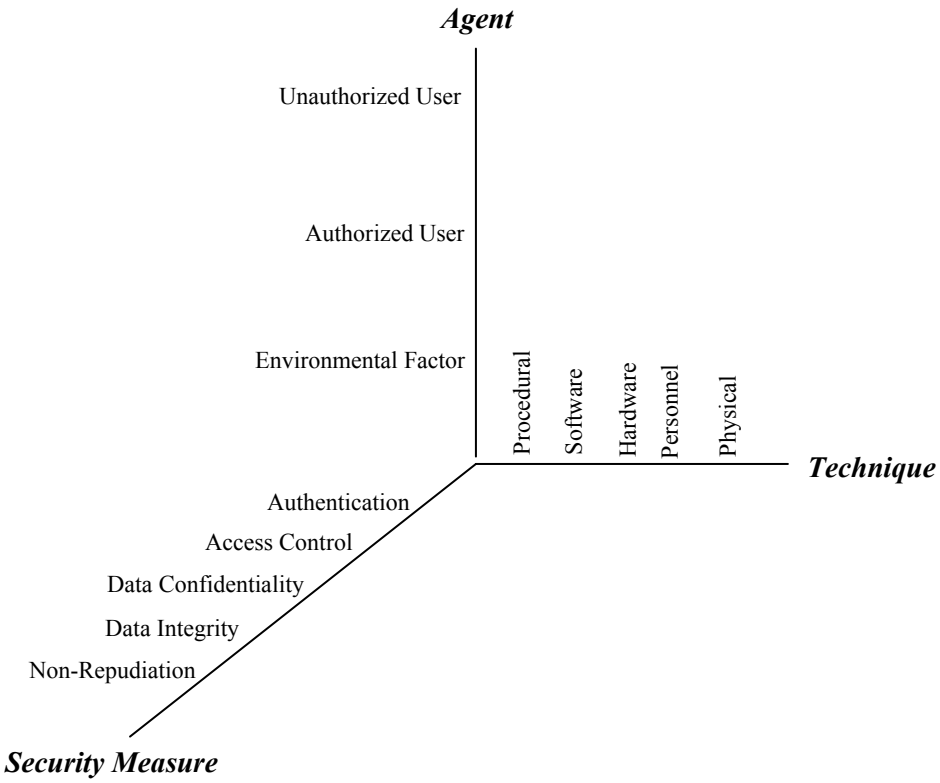

Figure 1. Combination of agents, techniques, and security measures

This classification is widely accepted among computer security experts, and the authors also recommend it as a good framework for coming with and developing control measures (ISO 7498-2, supra). These security measures along with agents and techniques are shown in Figure 1. One can use this figure to classify threats (agents and techniques) to information security and security measures to confront these threats. For example, access control is one of the security measures to confront the threats, which may be caused by an unauthorized user through software. In total, according to the proposed classification there are $5 \times 3 \times 5 = 75$ combinations of threat technique, agent, and security measure; however not all of these combinations are applicable and valid.

Information security consists of the set of procedural and technical measures a firm might consider to mitigate the risk that information might be lost, altered, or disclosed. By properly deploying an information security program a firm decreases the likelihood that it will face legal difficulties, financial difficulties, or damage to its brand and reputation. Proper deployment includes following a rational, repeatable technology selection process; developing effective business processes that leverage existing skills and organizational capabilities, designing processes that can be dynamically improved in response to experience and new insight, while not introducing waste or delay.

4. THE NATURE OF THE SECURITY THREATS

One useful model of the information security problem is to define three classes of objects. First, firms have intellectual property that represents value and therefore brings risk of some form to the firm. Second, intellectual property is embodied in a technology environment that is imperfect, that exhibits design flaws, trade-offs, defects and obscure documentation. Third, there is an individual inside or outside the firm who for some reason or another wishes to exploit those technological or procedural weaknesses with the goal of exploiting the risk, or damaging or transferring the value of that intellectual property. What kinds of individuals might do this? At a high level, there are two traits of some relevance. First, the level of technical skill of the attacker, and second, the level of insider knowledge the attacker might have. An unskilled outsider may represent a low-grade threat: someone who might steal a laptop opportunistically and sell it. An unskilled insider actually represents a fairly significant threat. By knowing the procedures, such a person can exploit weaknesses in the design of a system without having to modify sophisticated algorithms.

Skilled outsiders (quadrant 1 in Figure 2) are the notorious hackers – of which there are only a few hundred in the world. However these individuals develop toolkits so hundreds of thousands of less skilled users can leverage the skill of the hacker to attack a broader range of sites. These individuals are dangerous but till now most of their activities have been unguided. However there is reason to believe that malevolent

organizations are making contact with hacker groups to cultivate relationships. It is easy to believe that hackers are more likely to attack someone else; in fact attacks are generally random and the technically skilled insiders (quadrant 2 in Figure 2) represent the most dangerous threat. However they are rarely caught, and generally they are a very small population. Procedural remedies – surveillance, audit, job rotation and so forth – allow the firm to minimize its exposure to this particular problem.

This could be shown graphically as a two x two matrix with skill level as the vertical axis, and insider knowledge as the horizontal axis shown in Figure 2. Quadrant 3 refers to low-skilled outsiders who are typically not involved in information security related incidents, other than theft of equipment. Quadrant 4 refers to insiders with nominal technical skill but substantial inside knowledge. These individuals may exploit procedural weaknesses to commit crimes. Over 90 percent of all financially significant information security incidents reported by Gartner clients between 1990 and 2001 involved insiders (approx. 500 incidents during the 11-year period). The apparent increase in 2002 and 2003 in financially significant, targeted crimes originating from outside the victim organization and apparently not involving a current or former insider speaks to the continuing erosion of the perimeter and the increasing transparency of business processes as embodied in common, off-the-shelf software (COTS).

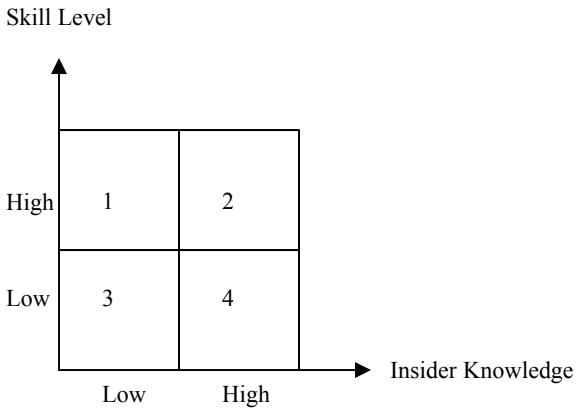

Figure 2. Skill Level- Insider Knowledge Matrix

In general, insiders (in quadrants 2 and 4) are responsible for most financially significant information security problems. The CSI/FBI 2002 report [4] indicates that 78% of respondents to the survey report insider abuse of net access. Therefore, firms must acknowledge that people with inside knowledge are a significant source of attacks, and structure their business processes and technology deployment to account for that fact.

5. DEPLOYING RESOURCES IN INFORMATION SECURITY

Unfortunately most firms do not have a transparent, repeatable process for determining when or how to deploy resources (money, staff, and time). At the senior management level, information security is often perceived as simply another of the systems management disciplines, requiring either a code patch or a software tool to fix the underlying problem.

Such piecemeal approaches fail because they usually are driven by a haphazard occurrence, the most recent incident, or the most recently publicized threat. A series of uncoordinated activities, focused on fixing discrete problems alone, will leave gaps that will be exploited easily. Some larger organizations that have more experience with information security have chosen to deploy a comprehensive information security program. While there is no generally accepted model for such an initiative, the common elements are:

Governance – translating business value and mission statements into principles relevant to information security

Policy – a clear, direct, concise high level statement of desired behavior and expected controls for users of an IT environment

Architecture – Translates the policy directives into platform neutral, low level actions (such as the ISO 7498-2 security functions)

Awareness and Training – insuring that staff are aware of management's expectations and procedures to follow

Technology – selection, deployment, operation and continuing evaluation of tools to amplify the directives in the policy

Auditing, reporting and monitoring – detection, ongoing examination of the output from tools and processes for forensic and analytical purposes

Validation – as the environment changes, the prior steps are adjusted to maintain their relevance and effectiveness

Deciding how much to spend on an information security program should be driven by the magnitude of the risk the firm acknowledges. If the firm has developed some sense of the value of its intellectual property, then spending can be governed by attempting to mitigate the largest realistic risks first. While piecemeal approaches will always fail, approaches governed by both a comprehensive model like this (or the CobiT model, or the principles included in ISO 17799/BS 7799) as well as a sense of the magnitude of the risk the firm faces will make strategic sense over time.

Firms rarely overspend on information security. One approach, used by a few large financial institutions, is to marry the SEI (Carnegie Mellon University's Software Engineering Institute) CMM (Capability Maturity Model) with the processes outlined in the ISACA CobiT model, and assess the relative maturity of the organizational processes. This is described in the ISACA (Information Systems Audit and Control Association) web site http://www.isaca.org. The purpose is to develop a gap analysis that can help guide resource commitment not by attempting to identify the most likely expensive risk (and address that), but by strengthening the weakest element of the information security program.

6. VARIABLITY OF LOSSES RESULTING FROM SIMILAR EXPLOITATION

When a firm experiences an information security problem, the consequences to the firm can vary dramatically from instance to instance. When two firms both experience the same incident, one may be able to contain the damage, while the other may not.

One may have effective backup procedures allowing the evidence to be used for a prosecution, while the other may face a difficult choice between resuming operations (by refreshing the environment) and supporting an investigation (by allowing systems to be sequestered, check-pointed, and analyzed). One firm may have an effective liaison with its information security vendors and outsourcers, while the other may not. One may have properly tuned intrusion detection tools and able staff, while the other may not. One may have rigorous screening and background checks of candidates for key positions, while the other may not. One may have an effective awareness program, while the other may not. One may truly support the culture of security, while the other may only provide occasional support but no enduring commitment.

Even with similar overall structure, firms never have similar configurations at the detailed, operational level. As a result, an incident may barely impact one firm while another similar one may be overwhelmed with consequential damage. This happens often when firms experience a virus attack. Seemingly minor configuration differences may allow a particular virus to spread rapidly in one firm, while a similar firm notes the event but does not suffer greatly from it.

Following a privacy violation, one firm might face vigorous prosecution from authorities in one jurisdiction, while a similar firm in another jurisdiction might not face any investigation at all.

Should a security breach threaten a firms' brand (for instance, a financial services firm which builds itself around trust), the quality of the response will have much to do with the manner in which the brand is perceived. Consider the impact of the Tylenol scare on Johnson & Johnson's brand, compared with the ultimately fatal damage done to Bon Vivant following its tainted food incident.

The simple fact is that the consequences from an information security breach are contingent on a vast number of factors, many of which are not under the control of the firm experiencing the breach. So rather than adopt an approach requiring precision where it is not obtainable, we advocate an approach that allows for a statistically useful range of impacts.

7. COST ANALYSIS OF SECURITY BREACH ANNOUNCEMENTS ON FIRMS

The relationship between information system security and market valuations can be traced to the trust placed by customers and partners who do business with the firm through the Internet. Customer and partner trust assume more significance in electronic commerce transactions because of concerns related to data privacy. A security incident can irrevocably damage the trust and confidence required to build a long-term relationship with customer and partner. Dissatisfied customers can switch to competitors that are just a click away. Thus, a perception of low security can have a profound financial impact on the firm. Security problems may also signal to the market a lack of concern for customer privacy and poor security practices within the firm. These signals in turn lead investors to question the long-term performance of the firm. In efficient capital markets investors are believed to revise their expectations based on new information in announcements. Investor expectations are reflected in stock prices. If security breaches are expected to reduce future cash flows, capital markets would respond unfavorably to announcements of security breaches by driving stock prices down.

We have conducted personal interviews with law enforcement agencies dealing with computer crime and executives from financial institutions dealing with security issues. In addition, we did a literature review of cases prosecuted by the Department of Justice including the evaluation of damages and financial awards. This review provides a significant negative market reaction to information security breaches involving unauthorized access to confidential data, but no significant market reaction when the breach does not involve access to confidential data (e.g. [2]). This finding is actually consistent with the findings from the 2002 CSI/FBI survey, which suggests that among information security breaches, the most serious financial losses were related to theft or proprietary information. This is also consistent with the recently prosecuted computer cases by the Computer Crime and Intellectual Property Section, CCIPS, of the Criminal Division of the US Department of Justice. According to CCIPS, 91% of cases which have been under the computer crime statute, 18 U.S.C. 1030, are the cases which related to the violation of confidentiality of information. As an example of these cases, in November 2001, two former Cisco Systems, Inc., accountants were sentenced to 34 months in prison for "exceeding their authorized access to the computer systems" of Cisco Systems in order to illegally issue almost $8 million in Cisco stock to themselves. We have sorted the information provided by the 2002 CSI/FBI according to percentage of detected attacks by respondents and mapped these attacks into our three dimensional model (As shown in Figure 1) and expressed it in Table 1.

These findings reveal that breaches involving unauthorized access to confidential information are quite different than attacks that do not involve access to confidential information. Once confidential information has been accessed in an unauthorized manner, the value of such a strategic asset may be permanently compromised. For example, a firm's customer list may be an important proprietary asset. Once this list has been accessed without authorization, others may be able to use the list for marketing and other purposes. This may permanently impair the list's value to the firm that created and owned it. In the cases of breaches that do not involve unauthorized access to confidential information, the underlying assets generally relate to operations. While the firm may lose the ability to use these assets for some period of time, the loss is usually temporary. Consider the case of a denial of service attack. During the attack, the firm may not be able to conduct operations, take customer orders, reservations etc. Once the attack ends and any necessary system changes are made, however, the firm can commence operations and the value of its operating system is not permanently impaired. Findings provide some limited support for a negative stock market reaction to the widely reported information security breaches. This means that, customers, stockholders, and other stakeholders would likely be willing to accept some types of information security breaches, for example denial of service attacks, as a routine risk and a normal cost of doing business.

The literature review also indicates that compromised firms, on average, lose approximately 2.1% of their market

Table 1. Combination of agents, techniques, security measures, and % detected in 2002 (Using the data from 2002 CSI/FBI survey)

Attack	Agent	Threat	% Detected	Security Measure
Virus	Unauthorized	SW	85	Data Integrity
Insider Abuse of Net Access	Authorized	SW & Personnel	78	Authentication & Access Control
Laptop	Unauthorized & Authorized	Physical & Personnel	55	ALL five Measures
Denial of Service	Unauthorized	SW	40	Authentication & Access Control
System Penetration	Unauthorized	SW & HW	40	Authentication & Access Control
Unauthorized Access by Insiders	Unauthorized	Personnel	38	Authentication & Access Control
Theft of Proprietary	Unauthorized & Authorized	SW & Procedural	20	Authentication & Access Control
Financial Fraud	Unauthorized & Authorized	Procedural	12	Authentication & Access Control
Telecom Fraud	Unauthorized	SW & HW	9	Authentication & Access Control
Sabotage	Unauthorized & Authorized & Environmental	HW & Physical	8	Access Control
Telecom Eavesdropping	Unauthorized	HW	6	Data Confidentiality
Active Wiretap	Unauthorized	HW	1	Data Confidentiality & Data Integrity

values within two days surrounding the events while security vendors gain an average of 1.36% from each such announcement [3]. It also shows that negative average impact associated with announcements decreases with the size of the firm and this suggests that smaller firms are panelized more than larger firms. This result for the managers of small firms serves as a reminder of the importance of security for survivability of these firms. However, the authors do not present detailed data, and thus it is not possible for readers to draw conclusions about the absolute loss of market values. Although the market penalizes all firms for security breaches, Internet firms are penalized more compared to conventional firms. A possible explanation for this effect is the greater dependency by the firms on Internet to generate revenues. Firms that solely depend on the Internet as a revenue generating mechanism pay higher prices in case of a security breach than firms that have multiple sale channels.

8-SUMMARY

As businesses adopt newer forms of information systems, the complexity of protecting those systems has been increasing. The lack of standards for quantifying the potential cost of computer security incidents is another major problem for the management of information systems. Considering these facts, this paper provides assistance for managers to have a better understanding of the security needs of their businesses. We review the state of the art of the security practice and its coverage by today's businesses.

We explain how firms determine where to deploy resources in information security and how cost of similar incidents can vary from one company to another; therefore, it is very difficult to "standardize" a procedure or to come up with a single universal model to apply in estimating the costs of measures and the damages due to breach of security. We list governance, policy, architecture, awareness and training, technology, auditing, reporting and monitoring, and validation as elements of information security programs.

We provide a classification of the threats to information systems as a combination of agents: unauthorized user, authorized user, and environmental factor, and techniques: procedural, software, hardware, personnel, and physical, and discuss the potential damages of attacks on information assets, and their countermeasures. We consider authentication, access control, data confidentiality, data integrity, and non-repudiation as security measures to these threats. We bring real world information about past information security incidents into our discussion and conclude that the threats to confidentiality of data can cause the most of damage to a firm. Overall, this paper has provided an overview of the challenges which information security has brought into today's business and also have attempted to assist managers in developing, disseminating, and implementing appropriate protection policies and control measures for critical enterprise assets.

9. ACKNOWLEDGMENT

The authors would like to express their sincere thanks to Dean Richard DeMillo and Prof. Gunter P. Sharp from Georgia Institute of Technology, Prof. Gene Spafford from Purdue University, and Mr. Chris Klaus and Mr. Tom Noonan from ISS Corporation for providing advice and support.

10. BIBLIOGRAPHY

[1] Biermann, et. al, A comparison of Intrusion Detection systems, *Computers & Security,* Volume 20, Issue 8, 1 December 2001, pp. 676-683.

[2] Campbell, K., Gordon, L. A., Loeb, M. P., Zhou, L., The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Science*, Dec. 2002.

[3] Cavusoglu, H., Mishra B., Raghunthan S., *The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers*, The University of Texas at Dallas, Feb. 2002.

[4] CSI/FBI, *Computer Crime and Security Survey*, Computer Security Institute, 2002.

[5] Gabor, A., *The Man Who discovered Quality*, Penguin USA, 1992

[6] ISO, *Information Processing Systems- Open Systems Interconnection-Basic Reference Model, Part 2: Security Architecture*, ISO 7498-2, 1989.

[7] IT Governance Institute, http://www.isaca.org/cobit.

[8] Landwehr, C. E., et. al, *A Taxonomy of Computer Program Security Flaws, with Examples*, Naval Research Laboratory, Nov. 1993.

[9] Lipmann, R., et. al, The 1999 DARPA off-line Intrusion Detection Evaluation, *Computer Networks*, Vol. 34, 2000, pp. 579-595.

[10] Neumann, P. G., and Parker, D. B., A Summary of Computer Misuse Techniques*, Proceedings of the 12th National Computer Security Conference*, pp. 396-407, Oct. 1989, National Institute of Standards and Technology/National Computer Security Center.

[11] Pfleeger, C. P., *Security in Computing*, Prentice Hall, 1997.

[12] Schummacher, H., J., and Ghosh, S., A Fundamental Framework for Network Security, *Journal of Network and Computer Applications*, 1997, pp. 305- 322.