STRATEGY RESEARCH PROJECT

THE ECONOMICS OF INFORMATION SECURITY

BY

LIEUTENANT COLONEL WILLIAM S. MOSER
United States Army National Guard

USAWC CLASS OF 2002
Senior Service College Fellow

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20020806 332

USAWC STRATEGY RESEARCH PROJECT

THE ECONOMICS OF INFORMATION SECURITY

by

Lieutenant Colonel William S. Moser
U.S. Army National Guard

Colonel Ralph Ghent, USAWC
Dr. Donald McGillen, Carnegie Mellon University
Project Advisors

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel William S. Moser, SC, ARNG

TITLE: The Economics of Information Security

FORMAT: Strategy Research Project

DATE: 09 April 2002   PAGES: 33   CLASSIFICATION: Unclassified

Information Security breaches have a major economic impact on organizations. The costs of Information Security breaches world wide in the year 2000 exceeded one trillion U.S. dollars. To increase Information security and lower attributed costs, organizations are spending billions in software, hardware and outsourcing. The Federal Government has also passed legislation and implemented policy designed to increase Information Security. These measures have not had the desired effect.   With the latest wave of malicious code such as Code Red and SirCam, as well as the multitude of other Information Security breaches, it is estimated the economic impact will continue to be significant. This paper focuses on the challenge presented by the need to assess the economic impact of breaches in Information Security. The economic risks of Information Security breaches are compared to the methods currently being undertaken to mitigate those risks to determine if the resources are being applied in the most efficient manner. The desired outcome of this research is to develop a framework that will assist organizations in identifying the economic risk due to Information Security breaches, and facilitate the application of resources to decrease these risks in the most effective and efficient manner.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

THE ECONOMICS OF INFORMATION SECURITY

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards, Even then I wouldn't stake my life on it."

— Dr. Gene Spafford, Purdue University

It seems that everyday there is the announcement of a new Information Security breach. They range from the discovery a new e-mail virus to the compromise of sensitive credit card data. The broadcast of new security breaches has become routine, hardly registering concern on the part of organizations. Unfortunately, organizations cannot afford to ignore Information Security. Losses attributed to Information Security breaches world wide in the year 2000 exceed one trillion U.S. dollars.[1] The current approach of most organizations is to place the challenge of decreasing these losses on their Information Technology departments. To accomplish this they are spending billions of dollars on security technology. They are also looking outside for help, and outsourcing is evolving to a multi million-dollar business as internal Information Technology departments fail to reverse the trend. Organizations are also looking for cyber insurance to lower risk, and to the Federal Government to pass legislation and implement policy to increase Information Security. So far, these measures have not had the desired effect, and losses due to Information Security breaches continue.

The goal of this paper is to provide a comprehensive framework to aid organizations in understanding the economics of Information Security, as well as a basis for reversing the trend of increasing information security-related expenditures. The paper is divided into four sections: The first section reviews the economics of Information Security, demonstrating financial challenges faced by organizations. This section also includes information on the funds being expended for information technology investments, security technology investments, insurance, outsourcing, and legislation. The second section provides basic methodology to understand Information Security breaches. The methodology is based upon assessments of four key elements – Organizational Profile, Methods of Protection, Threats, and Methods of Attack. The third section builds on the second by applying the elements to well-publicized Information Security breaches. Section four culminates in the presentation of a comprehensive framework and application requirement that incorporates the first three sections of the paper to determine the best way to apply limited resources to protect organizations economically from the effects of Information Security breaches.

THE ECONOMICS OF INFORMATION SECURITY BREACHES

The costs of Information Security Breaches are more than an eye-catching headline used to sell magazines or services. They have a real impact on the economy. The 2001 Global Information Security Survey states, "in the U.S. alone, damages due to viruses and computer hacking totaled $266 billion or more than 2.5% of the Nation's Gross Domestic Product (GDP). And the price tag worldwide soared to $1.6 trillion."[2] These numbers are shocking and provide a starting point to determine the economic impact, but they merit closer scrutiny. The main method of obtaining the data is through surveys, which are an excellent, but imperfect, source of information. Of primary concern is the way in which the estimates of losses are calculated. Often, surveys require only that organizations provide a number, but little or no information about the methodology by which that number was derived.

To accurately determine overall losses, both direct and indirect costs must be estimated, and to do so requires that, several essentials be examined. The simplest direct costs are those costs applied directly to correct the damage caused by an Information Security breach. They may include the resources required for repairing damaged software and hardware. Organizations can also track the touch labor required to make these repairs. Other direct costs, such as loss of productivity, are more challenging to assess. Associating cost with the inability to use e-mail or access data, for example, is difficult, as some work can certainly be accomplished despite the e-mail being down and data not being accessible. The problems are aptly illustrated by considering and attempting to quantify losses associated with stolen or compromised data, particularly of data that may be specified as proprietary or sensitive. The costs of simply replacing the lost data may be minimal. However, proprietary data may include technical specifications for an organization's latest product, for example, and if a competitor obtains such data, the damage may be substantially higher, and the associated cost to the organization harder to determine.

Indirect costs includes such things as opportunity costs of lost business, public embarrassment and damaged reputation. These costs may well be considerably higher than direct costs, and even harder to measure. "As CD Universe – which was hacked in January 2000 amid much publicity – can attest, fraud's most devastating effects are not the material costs associated with chargebacks or bank fees. What's often worse is the resulting damage to a merchant's reputation, erosion of consumer trust, and, ultimately, lost sales."[3] The problems involved are illustrated by considering the case of a bank that is the victim of an Information Security breach resulting in the loss of one million dollars. The direct costs are relatively easy to compute, as they include the one million dollars, as well as subsequent expenditures to prevent

a repeat occurrence, labor costs of personnel involved in detecting, analyzing, and fixing the problem, etc. However, indirect costs may be incurred in the form of lost business. It is straightforward to account for existing customers who decide to take their business elsewhere as a result of a publicized security breach. Much less clear is how to measure the effects of the loss of customers who might otherwise have done business at this bank, but decided not to, because they doubted the bank could protect their assets.

Disclosure of such incidents can be embarrassing and detrimental to the business, and so they tend to discourage organizations from reporting Information Security breaches. "Negative press and public embarrassment make many companies unwilling to report when attacks have successfully infiltrated their operation. Only when companies set aside their own individual concerns will the full extent of security breaches be grasped."[4] This brief discussion shows that the quantification of costs attributed to Information Security breaches is not straightforward and requires additional study. This will not happen until organizations become less reluctant to report these losses, and a more rigorous and academic study of the problem is undertaken. Regardless of the shortcomings in the available data, it is obvious that hundreds of millions of dollars are being drained from the economy.

The economic ramifications of information security breaches will continue to increase as the worldwide Information Technology market continues to grow at a rapid rate. "The Global Information Economy, Executive Summary, November 2000, found that momentum within the global ICT (Information and Communication Technology) industry is on a sustained increase. Having surpassed the $2 trillion mark in 1999, the industry will smash through the $3 trillion threshold in just four short years."[5] As more and more organizations increasingly depend on Information Technology, Information Security vulnerabilities will increase and require greater expenditures to protect these organizations. As a result, the economic impact of Information Security breaches will continue to rise.

Organizations are not standing by waiting to become victims to Information Security breaches – they are spending money to decrease the threats. The latest from the TrueSecure Corporation, 2001 Industry Survey showed that the average mean spent by all industries responding to the survey was $1,963,375 and the median budget for middle organizations was $260,000.[6] The amount spent on security software alone is significant. Internet Security Software: 1999 Worldwide Markets and Trends – indicates that "the projected 1999 totals of $4.4 billion represent a 39% increase over 1998's $3.2 billion mark. The market isn't slowing down either. International Data Corp (IDC) says that the escalating number of netizens will push the market for security software up an average of 21% per year, hitting $8.3 billion."[7] This

3

represents security technology investments being made across the board. However, despite these impressive amounts, investments in security technology are not having the desired impact, and organizations are looking to other means of protection.

A common practice is to use insurance to protect valuable assets. Insurance is an operational cost and makes good business sense. It is highly unlikely that a business would field a fleet of vehicles without first insuring them. "Similarly businesses achieve security through insurance. They take the risks they are not willing to accept themselves, bundle them up, and pay someone else to worry about them. If a warehouse is insured properly, the owner really doesn't care if it burns down or not. If he does care, he's underinsured. Similarly, if a network is insured properly, the owner won't care whether it's hacked or not."[8] While the analogy is appealing, it is still too early to determine if insurance provides the desired level of protection against Information Security breaches. Current insurance packages are expensive, as "policies can carry premiums starting at $7,000 all the way to $3 million dollars."[9] The premiums are based on potential loss estimates and contain numerous requirements that must be accomplished before a policy can be written. These include having sound information security practices already in place, and may require the services of an outside consultant for verification. This is one factor that contributes to another, increasingly popular, means of achieving protection – outsourcing it.

Many organizations are doing more than just upgrading their infrastructure. They are giving up on handling Information Security in-house for a variety of reasons, such as a lack of qualified personnel and a reluctance to deal with the increasing complexity of information security. "The Yankee Group, a leading IT Security consulting firm, forecasts that companies will buy $1.7 billion in security services by 2005, up from just $140 million in 1999."[10] By outsourcing a portion or all of their information security requirements, many organizations think that they can concentrate on their core business competencies. As with all means of protection, outsourcing is not a silver bullet and has not succeeded in fully meeting the challenge. Outsourcing firms face the same difficulties in meeting Information Security threats as the organizations they are paid to protect.

With the continuing increase in Information Security breaches, organizations are also looking to legal sources for protection. Legislation is used as a means to prosecute those entering one's system illegally. Although this has been helpful, organizations are looking for Congress to regulate the Information Technology industry to increase the quality of application software. "Legislation is pending that could use liability as a way of gaining compliance with a set of national cybersecurity standards. The proposals are supported by a new National

4

Academy of Science study calling for policymakers to consider laws that would increase the exposure of software and system vendors and system operators to liability for system breaches."[11] Unfortunately, current legislation is not addressing the issue of buggy software. "In the United States, Congress is still bogged down on basic privacy issues and anti-spam legislation – a far cry from the growing problems presented by hackers and the economic and security damage they are causing, which ranges from theft of sensitive information to loss of credibility."[12] The negative aspect of increased legislative oversight is that the laws enacted may require organizations to apply resources in a manner that may not offer the best return in decreasing the threat.

INFORMATION SECURITY ELEMENTS

To allow for better understanding of the impact of Information Security breaches, the framework being developed includes the following elements: Organization Profile, Methods of Protection, Threats, and Methods of Attack. These elements provide the basis of Information Security. The current framework focuses primarily on Threats, Methods of Attack and the Methods of Protection, and the Organization Profile is frequently under considered – or not considered at all. To effectively evaluate what takes place during an Information Security breach, as well as to increase the effectiveness of Information Security, all elements must be considered equally important. The elements examples are not meant to be all-inclusive; they demonstrate the complexity of the challenges faced.
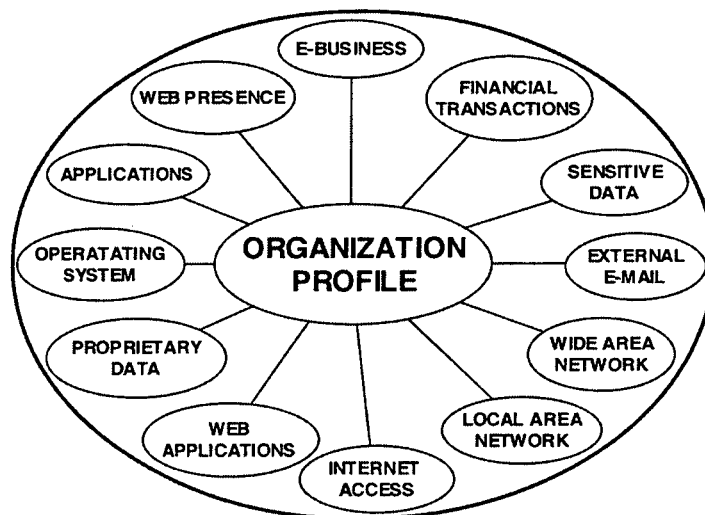

FIGURE 1: ORGANIZATION PROFILE

5

ORGANIZATION PROFILE

All organizations are vulnerable to Information Security breaches – unless they use no Information Technology. As an organization increases its reliance on Information Technology, there is a proportional increase in its vulnerability. To illustrate, we consider the simplified progression in the use of Information Technology by a fictitious organization. Suppose the organization introduces the use of computers for administrative purposes to increase efficiency. The primary concern is the physical protection of the assets. With the successful infusion of the new technology, the organization begins to install business applications. These applications may contain proprietary or sensitive data, and therefore increase the consequences of compromise. To increase the sharing of information, the organization implements a local area network and e-mail capability. This increases the chance that unauthorized individuals can access the information. For added convenience, the organization provides Internet access and dial-up service to the network computers. The organization is now vulnerable to outside threats, such as malicious e-mail and unauthorized outsider access. An organization may then implement a wide area network so they can share data with remote offices and vendors. To take advantage of this technology their web servers allow access to web applications by those outside their location. They are now susceptible to unauthorized access or system penetration. To benefit from the web presence through their operating system, the organization begins to conduct e-business. Since the organization is selling a product, they are conducting financial transactions through web applications and web servers. They now have incurred a considerable amount of risk and increased their organizational profile significantly. This is a simple example, of course, and most organizations do not progress in such a methodical manner. Most organizations simply evolve into their current profile, and can quite unexpectedly find themselves the victim of an Information Security breach – or at least come to the realization they have become highly susceptible to such attacks.
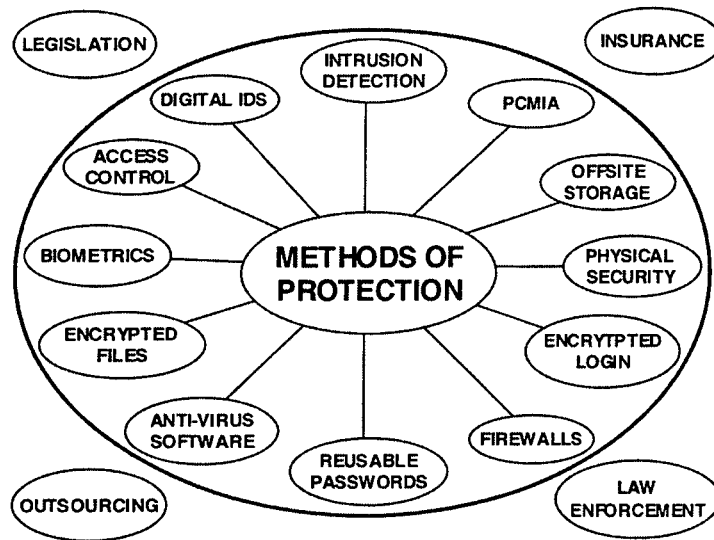
FIGURE 2: METHODS OF PROTECTION

METHODS OF PROTECTION

Methods of protection for Information Security breaches are evolving in an effort to keep up with the methods of attack and threats. When organizations began fielding computers, they were not networked and the primary method of protection was physical security. As the value of the information has increased, access control has grown in importance. Access Control is accomplished through the assignment of passwords and user accounts. Passwords are still one of the most effective means of protection and are growing in importance and complexity with the increase in the number of computer users and networks. Anti-Virus software is another common means of protection. It was first used to prevent the spread of viruses from floppy disks. With the increase in web presence and e-mail, viruses are able to spread rapidly and more sophisticated means of fighting them are required. "A better solution may be to create a full, biology-inspired immune system for computer protection, so systems can deal with invaders as automatically as your body deals with microorganisms. A joint research effort by IBM and Symantec is striving for that goal."[13] In addition, protection is required against the increase in unauthorized users breaking into systems. Firewalls are meant to keep undesirable traffic out while at the same time letting authorized traffic exit. Unfortunately, firewalls are fallible and additional methods of protection are needed. Intrusion Detection Systems are a tool to determine if someone has breached the firewall and gained access to an organization's system. Additional methods of protection may include biometrics, encrypted files, Personal Computer

7

Memory Card International Association (PCMIA) cards, offsite storage and encrypted login. Organizations also look outward for protection through legislation, insurance, outsourcing and law enforcement.

FIGURE 3: THREATS

THREATS

This paper is not intended as a tutorial on all Information Security threats, as that is beyond the paper's scope. Rather, several of the more common threats are presented to demonstrate the need for a framework to help in decreasing risk. Information Security threats are growing in number, sophistication, and promulgation. They have kept or exceeded the pace with which organizations increase their reliance on Information Technology. "Keeping up to date on the latest threats becomes more difficult as the number of new vulnerabilities rises. The federally funded Computer Emergency Response Team (CERT®) Coordination Center, operated by Carnegie Mellon University to track Internet security statistics, recorded 171 new vulnerabilities in 1995, a figure that reached 417 in 1999. Last year, that number hit 1,090, and in just the first three months of this year, 633 new vulnerabilities were reported."[14] The proliferation of viruses grows as organizations use web presence to share information and send e-mail. The increasing reliance on the Internet also creates the possibility that an employee may misuse it. The misuse may be modest, such as when employees access the Internet for non-work purposes, or destructive, as when they illegally download software or gain unauthorized access to information systems. The threat of denial of service attacks also

increases as organizations use the World Wide Web to share information and conduct e-business. Denial of service attacks are increasing in complexity and can prevent traffic from entering or exiting an organization's web site. Prepackaged commercial applications ranging from office suites to enterprise-wide applications are responsible for a growing number of threats. "Microsoft's newest version of Windows, billed as the most secure ever, contains several serious flaws that allow hackers to steal or destroy a victim's data files across the Internet or implant rogue computer software."[15] The significance of this threat is that it opens an organization to unauthorized outsider access that may result in the theft of proprietary data. Additional threats include telecom eavesdropping, laptop theft, active wiretap, telecom fraud and financial fraud.
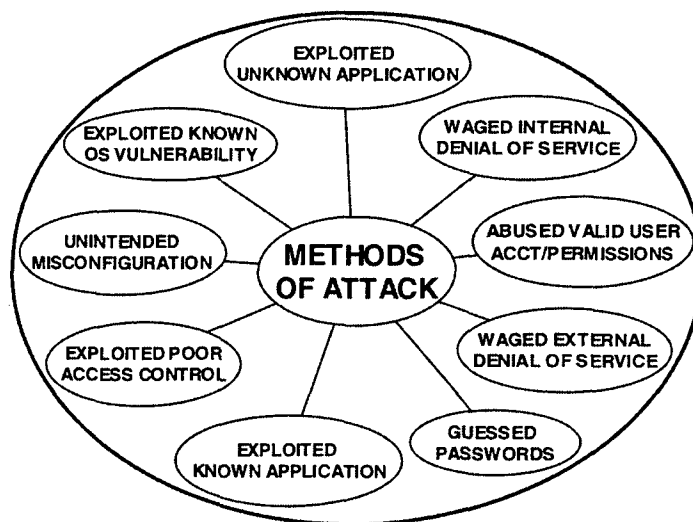
FIGURE 4: METHODS OF ATTACK

METHODS OF ATTACK

A commonly held image of the typical perpetrator of cyber attacks is that of a precocious teenager sitting behind a computer with a modem breaking into systems. This was popularized in the movie War Games, for example. In reality, those gaining access to computers without authorization are as varied as the means they use to attack. In order to develop a better understanding of the methods of attack, organizations must first look within. Abused valid user accounts/permissions are frequently called insider threats, and occur when valid system users access computer data they are not authorized to access. The damage resulting from such an

attack ranges from the theft of proprietary/sensitive data to malicious damage of the information system. When looking at threats that originate outside the organization, it is important to understand that attackers take the path of least resistance. A frequently exploited weak point is poor access control. One of the easiest ways to gain access, for example, is through compromised passwords. This process is sequential in nature, and begins with looking for areas that are not password-protected, and progresses to the use of password cracking tools. A more sophisticated method of attack is the exploitation of known and unknown application vulnerabilities. Very few applications are shipped without holes and there is an ongoing effort to develop patches to fix them. Would-be attackers monitor this effort with the intention of illegally entering the organization's system while the system is exposed. Organizations also find their systems being penetrated through openings created by unintended misconfiguration. The unintended misconfiguration may occur while installing applications and hardware. For example, Information Technology products are often shipped with certain security features disabled to ease in installation, and it is not uncommon for such features to be left in the disabled mode after installation. Of course, misconfiguration may also result from lack of knowledge on the part of Information Technology professional.
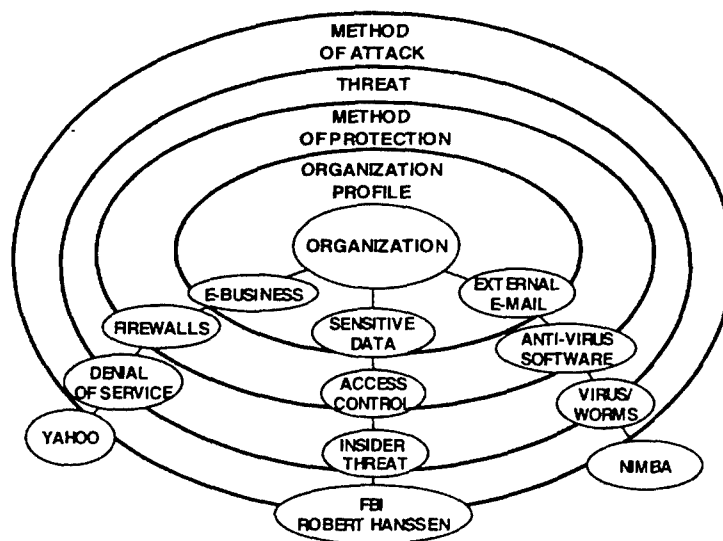

FIGURE 5: WELL KNOWN INFORMATION SECURITY BREACHES

PRESENTATION OF WELL KNOWN INFORMATION SECURITY BREACHES

Having reviewed the four elements – Methods of Attack, Threats, Methods of Protection, and Organizational Profile - we now apply them to well-publicized Information Security

10

breaches. By covering each element in detail, as it affects organizations, and the economic impact a better understanding of what takes place is provided. A graphical depiction of the Information Security breaches is provided in Figure 5. The examples given are not meant to be all-inclusive. "The CERT® Coordination Center at Carnegie Mellon University in Pittsburgh estimates that the number of security incidents reported this year will surpass 40,000, more than twice the number of incidents reported last year."[16] The examples provide a valuable way to demonstrate both what organizations face, as well as the need for more inclusive ways to conduct Information Security.
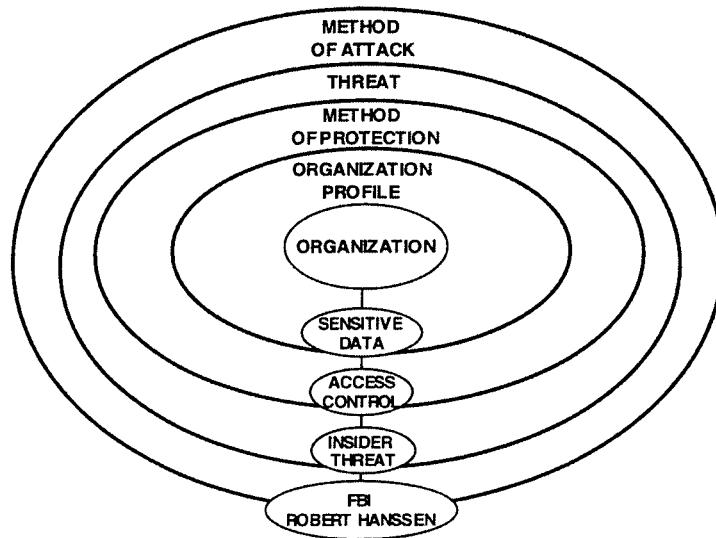
FIGURE 6: SECURITY BREACH EXAMPLE 1 – FBI/ROBERT HANSSEN

SECURITY BREACH EXAMPLE 1 – FBI/ROBERT HANSSEN

Method of Attack – Abused User Account/Permissions

The focus of Information Security is often on the external threat. There is the perception that if a screening process is in place for employees, those making it through the screening process can be trusted. This was the case with former FBI agent Robert Hanssen. The process which candidates must go through to become FBI agents is extensive and more rigorous than the processes used by most organizations. In the case of Robert Hanssen, the process did not work. "In the affidavit, federal prosecutors contend that Hanssen routinely used his access and computer skills to glean classified information from government databases, encrypt electronic communiqués he passed to the Russians, and conceal his spying activities.

11

Officials say he would regularly surf the internal computer networks for indications that he was under investigation for espionage."[17] Robert Hanssen was not part of the Information Technology staff however, his technology skills were above average. He collected information using the tools the organization provided to perform his job. That he could gather so much critical information with the access provided him by the organization demonstrates that good access oversight procedures were not in place. Organizations are in a difficult position in having to provide access to information for employees to do their jobs, while at the same time not allowing that access to be misused.

Threat – Insider Unauthorized Access

The insider-unauthorized threat can come from any location in an organization. It may be a trusted employee or a temporary worker. With the increasing reliance on technology in today's environment, the threat has expanded. "Although all employees in your organization potentially are a threat for computer security breaches, organizations should focus on the information technology specialist. These personnel design, maintain or manage critical information systems."[18] With the increasingly temporary nature of these positions, loyalty to the organization is not a priority, and this problem has the potential to get much worse as the shortage of qualified Information Technology experts becomes more acute. Information Technology experts are continuing to look for better opportunities as they become overwhelmed with the increase in requirements. The depth of organization loyalty decreases as the possibilities of layoffs increase. Disgruntled employees can cause severe damage by corrupting or deleting sensitive databases or stealing valuable data.

Method of Protection – Access Control

Access control is the most effective means to prevent unauthorized insider access. Control is accomplished through the use of passwords. Craig Donovan of the SANs Institute provides the following perspective on passwords: "Sadly, this first line, and all too often, only line of defense is the weakest link in the security chain. This is due in part to the "routineness" of it all. After all lament employees "who really wants to read my e-mail?" It is the security professional's task to help employees understand the larger scope and implications for choosing strong passwords."[19] In addition to being confronted with more passwords, system users are faced with the need to make these passwords more sophisticated as the threat becomes more adept at password cracking. As passwords become more complex, memorizing them becomes harder and users often resort to unsafe practices, such as leaving passwords written down in

places easy to find, or using the same password for all accounts. This is an example of an organizational vulnerability that can be decreased by good training and policy. Good policy insures that passwords are alphanumeric, have a minimal character length, are periodically changed, do not include common words, are not written down or passed to others and are periodically audited for compliance. For policy to be effective it must implemented with proper training so that employees understand the importance of complying with the policy to protect the organization from Information Security breaches.

Organization Profile – Sensitive Data

Not all sensitive data are tied to national security. The compromise of employee personnel data, such as payroll records, can have a negative impact on an organization. "The economic impact of the Unauthorized Insider Access ranges from $1K to $5 million. The average loss of such incidents was $275,636 with total annual losses of $6,064,000 for the year according to the 2001 CSI/FBI Computer Crime and Security Survey."[20] In the Robert Hanssen example, lives were lost, and applying a dollar amount is clearly inadequate to describe the loss. However, there is solid data that support the contention that, in business, millions of dollars are lost each year as a result of the compromise of sensitive data.
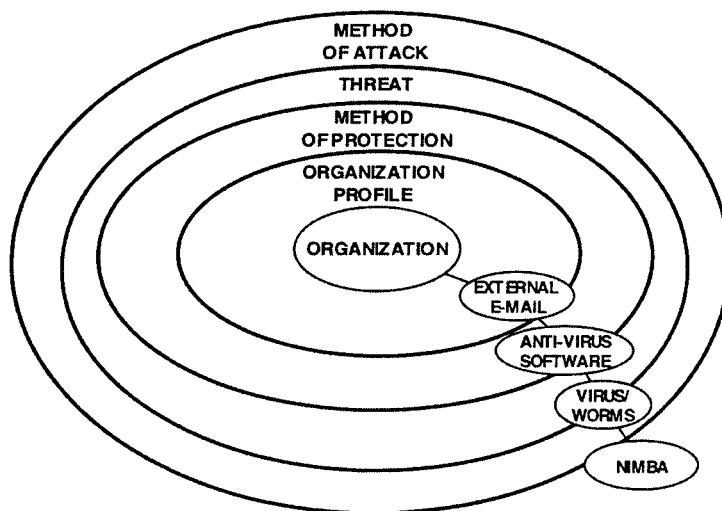

FIGURE 7: SECURITY BREACH EXAMPLE 2 – W32/NIMDA VIRUS/WORM

SECURITY BREACH EXAMPLE 2 – W32/NIMDA VIRUS/WORM

Method of Attack – Exploited Known Application

Applications are routinely fielded with vulnerabilities and would-be attackers are continually looking for new ways to exploit these vulnerabilities. Exploitation is increasingly accomplished with computer viruses and worms. "A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate."[21] The term virus is often used generically to describe a worm however they are uniquely different. "A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user."[22] Worms and viruses are not new, but the way in which they are applied is changing. The newest strains are hybrids, with attributes of both a virus and a worm, as demonstrated in the example of the W32/Nimda Virus/Worm. "This worm, W32/Nimda.A-mm, is dangerously different than virtually all other e-mail and network-borne viruses: It can infect a computer when a user simply clicks on the subject line of an e-mail in an attempt to open it, or visits a Web page housed on an infected server."[23] This characteristic represents a significant evolution beyond past viruses, for which the attachment had to be opened to activate the virus. The W32/Nimda worms most damaging attributes were virtually invisible to the organization. "The worm spreads by sending e-mail messages with infected attachments and then scanning for and infecting vulnerable Web servers running Microsoft's Internet Information Server software. It then copies itself to shared disk drives on business networks and appends JavaScript code to Web pages that will download the worm to surfers' PCs when they view the page."[24] Many organizations were unaware of the attack until their systems' service decreased. At this stage, recovery becomes difficult because the worm has had significant time to spread throughout the system. Completely eradicating the worm may require the organization to systematically take each of their servers off line to rebuild them. As a result, according to Sophos Anti-Virus, W32/Nimda was the most reported virus/worm in 2001.[25]

Threat – Virus/Worms

The virus threat cannot be underestimated. "MessageLabs says the latest figures show one in every 300 emails is infected - up from one in 700 in October 2000. It predicts as many as one in two could be infected by 2013."[26] Not all these viruses are as lethal as W32/Nimda. However, as the number of infected messages grows, the level of lethality is also increasing. The threat affects the way in which organizations conduct business. "The escalation in email

14

born viruses, and the spread of hybrids that attack on many different fronts means that, while the Internet will not collapse, it will certainly cease to be usable as a safe and credible means of communication for business and home users."[27] Organizations have historically used Information Technology as a tool to increase productivity. Virus/worms are an example of a threat that can reverse this trend and have significant economic impact on an organization. "Computer Economics estimates the expenses incurred from W32/Nimda Worldwide in 2001 to be $635 million."[28]

Method of Protection – Antivirus software

Antivirus software is the primary method of protection employed by organizations. The Information Security 2001 Industry Survey states that 79% of the organizations responding acquired or deployed Antivirus products in 2000 or earlier.[29] However, organizations cannot simply install such software and forget it. As the threat increases in complexity and lethality, anti-virus software providers are in a race to keep pace with the result that the number of updates an organization receives has increased. Organizations are continuously required to apply these updates through touch labor. If they fail to keep up, they can become the victims of the latest attack. To complicate matters, the method of looking for viruses on a system is no longer enough. Anti-virus software must scan incoming traffic to detect viruses before they are delivered to the desktop. With the increasing threat, organizations are increasing their investments in anti-virus software. "According to IDC, the worldwide anti-virus software market is forecast to increase from US$1.2 billion in 1999 to US$2.7 billion by year 2004."[30]

Organization Profile – External E-mail

E-mail is no longer just a communications method, rather, it has become an integral part of the way an organization does business. Organizations use e-mail to exchange critical data and are becoming increasingly reliant on attachments. These attachments contain valuable documents such as invoices and purchase orders. The importance increases as organizations use this technology to replace manual processes, and many organizations no longer have the means in place to perform those functions without e-mail. As the reliance on e-mail increases, organizations vulnerability increases. According to the 2001 CSI/FBI Computer Crime and Security Survey the economic impact of viruses ranges from $100 to $20 million per organization. The average loss of such incidents was $243,845 with total annual losses of $45,288,150 for 2001."[31]
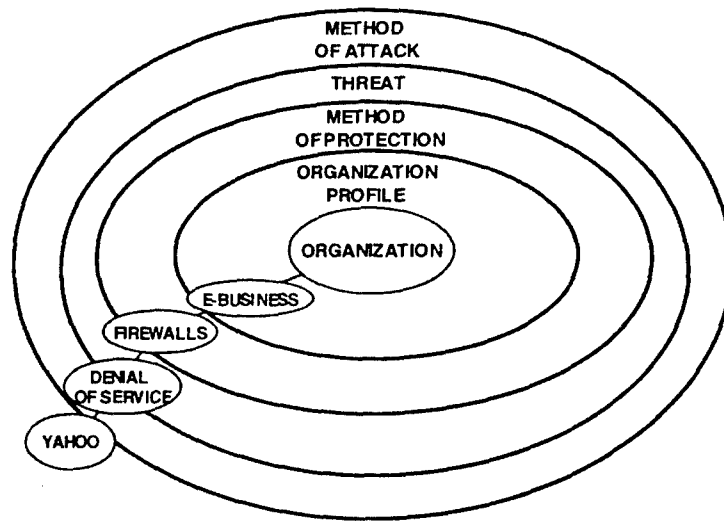
15

FIGURE 8: SECURITY BREACH EXAMPLE 3 – YAHOO

SECURITY BREACH EXAMPLE 3 – YAHOO

Method of Attack – Waged Denial of Service

A brick and mortar business is dependent on the access of customers to its outlet. Customers must be able to gain access to the business or they will go elsewhere. An e-business is reliant on customers accessing the web to reach its site. If the web site is not available, the e-business will lose customers. On February 7, 2000 Yahoo, a popular portal and e-business, was the victim of a cyber attack. "Yahoo's Web site, www.yahoo.com, was rendered completely inaccessible from approximately 10:15 a.m. to 1:15 p.m. PST on Monday. The site lay frozen because of a successful denial of service launch that overwhelmed a router on the path to the company's Web site with a bogus traffic jam."[32] Such an attack differs from what is normally viewed as an Information Security breach, where would-be attackers attempt to breach an organizations defenses and penetrate its systems. From a financial perspective a denial of service attack can be just as damaging, and can be compared to thugs physically preventing customers and employees from entering an organization.

Threat – Distributed Denial of Service

It is not only e-businesses that are vulnerable to the denial of service threat. Any organization that relies on the web to provide information to the public is at risk, and the complexity of the threat is increasing. "In a distributed denial-of service attack, a hacker breaks

16

into other people's servers and programs them to flood a Web site with massive amounts of bogus traffic until the Web site crashes."[33] Home computer users with broadband Internet access are unwittingly becoming a threat to organizations. Attackers take advantage of users leaving their systems on by taking control of the system and combining it with others to conduct distributed denial of service attacks. "Last year's sabotage to Yahoo's site resulted in over 3 hours of downtime. An estimated 100 million pages would have been viewed at this time. This amounted to a potential loss of more than $500,000."[34] Indirect costs include damage to reputation, lost opportunity and the risk of lost customers.

Method of Protection – Firewalls

Firewalls are a key method of protection in the defense of denial of service attacks. According to the Information Security 2001 Industry Survey, 74% of the organizations responding acquired or deployed Firewalls in 2000 or earlier.[35] In a distributed denial of service attack, the firewall mission is to keep broadcast traffic out. However, firewalls can create a false sense of security. If configured incorrectly, a firewall can let unwanted traffic in and not let legitimate traffic out. In addition, as with anti-virus software, firewall software is evolving with the threat and so must be frequently updated. If firewalls are not properly maintained, they quickly become ineffective. These concerns have not slowed their implementation as a method of protection. "Buoyed by triple-digit growth for the past two years, the worldwide firewall/virtual private network (VPN) security appliance market is poised to break past the $1 billion barrier this year. According to IDC, revenues increased 153% in 2000 to reach $943 million. By 2005, the market will generate $4 billion."[36]

Organization Profile – E-Business

As organizations go on-line, their web profile increases. If a brick and mortar organization builds a business in a physically dangerous area, the owners and managers respond appropriately to protect their investment. The threat should not be considered less important when repositioning to the web, and this places an increasing level of importance on the implementation of Information Security. Even with the apparent risk, organizations continue to transition to e-business. "E-business spending averaged $58 million per company last year. That figure is expected to decline to $52.9 million this year, but rebound to $68.4 million next year."[37] As the spending increases organizational vulnerability also grows. The 2001 CSI/FBI Computer Crime and Security Survey reports that the economic impact of the Denial of Service attacks range from $100 to $2 million. The average loss of such incidents was $357,160 with

total annual losses of $35,001,650 for 2001.[38] Along with the direct financial losses, there are also growing indirect losses, such as damage to an organization's reputation. It is difficult to determine the economic impact of an organization being on the cover of a major periodical for poor Information Security practices, but it could be substantial. "The 2001 Global e.fraud.survey found eighty-eight percent of respondents feel that the public perceives traditional, more established "bricks and mortar" business as being more secure than e-commerce based, or dot.com companies."[39]
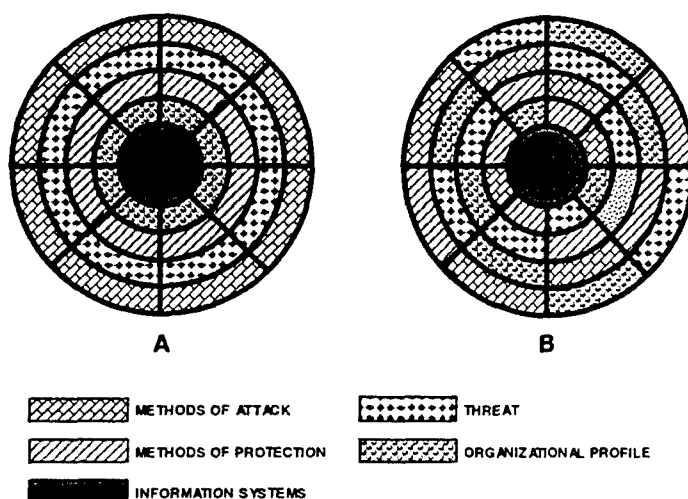

	METHODS OF ATTACK		THREAT
	METHODS OF PROTECTION		ORGANIZATIONAL PROFILE
	INFORMATION SYSTEMS		

FIGURE 9: SYMMETRICAL VERSUS ASYMMETRICAL ALIGNMENT OF ELEMENTS

INFORMATION SECURITY FRAMEWORK

SYMMETRICAL VERSUS ASYMMETRICAL ELEMENT ALIGNMENT

Finding a solution to the Information Security threat is difficult. If it were as symmetrical as the examples presented and depicted in Figure 9 A, it would be an easier process to control and the economic impact would be smaller. The security breach examples provided where developed after the incident occurred. By applying the breach to each of the elements, a clear picture of what occurred is produced. This type of analysis is valuable in developing methods of protection. The challenge of this approach is keeping up with the threat and attack methods while deploying an active method of protection. Organizations attempt to be proactive by continuously monitoring the announcement of new threats and attack methods. Organizations respond by applying patches and adjusting the methods of protection. Basing the method of protection on past events can be compared to the military analogy of fighting the last war. This

puts organizations in the difficult position of always trying to catch up; making it hard to be proactive.

The challenge is further complicated by the asymmetry of the challenges organization face. In practice, the elements do not always line up and may in fact be quite random as depicted Figure 9 B. Those looking to breach organization's information systems are opportunistic and are continually looking for ways into their systems. There is no need to attack an organizations method of protection if the breach can apply directly against the organizational profile. At the same time those responsible for implementing the methods of protection are strengthening the defense other parts of the organization may be unintentionally sabotaging these efforts with the infusion of new Information Technology. In addition, a method of attack may occur with no corresponding threat. This in turn will nullify the method of protection that is based on the known threats; thereby making the organization profile susceptible to attack. Taking these challenges into consideration it is important to understand how organizations are currently addressing Information Security.

INTERNAL

ORGANIZATION
PROFILE

INTERNAL

METHODS OF
PROTECTION

EXTERNAL

THREATS

EXTERNAL

METHODS
OF ATTACK
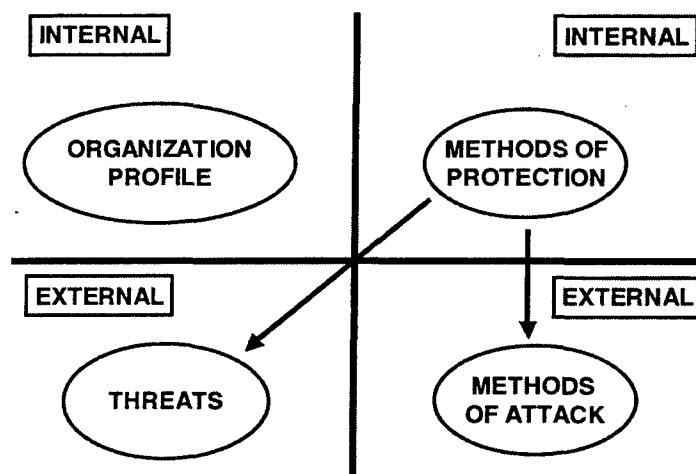
FIGURE 10: CURRENT INFORMATION SECURITY FRAMEWORK

CURRENT INFORMATION SECURITY FRAMEWORK

The current approach to Information Security places the burden within the Information Technology department, and this has led to a technology-centric approach focusing on the methods of protection. Deployment of technological "fixes" often takes place independently of the development of an organization profile that characterizes the value of data. Organizations

19

continue to employ better methods of protection focused on the external elements threats and methods of attack. At the same time, those looking to attack systems are improving ways to breach these means of protection. Threat and method of attack-based protection is accomplished with a standard toolbox consisting of, at a minimum, tools needed to protect the network and the organization, including firewalls, access control, intrusion detection systems and anti-virus software. As previously demonstrated, these methods of protection have not had the desired effect of protecting the organization from Information Security breaches. Information Technology professionals must, however, compete for scarce organizational resources and funding, and they often oversell the capability of these methods of protection. In the 2001 CSI/FBI Computer Crime and Security Survey, Bruce Schneir of Counterpane Systems provides the following analysis: "What's interesting is that all of these attacks occurred despite the wide deployment of security technologies: 95% have firewalls, 61% an IDS, 90% access control of some sort, 42% digital IDS, etc. Clearly the technologies are not working."[40] With the current approach, Information Technology staffs are forced to request funds from management that, given economic conditions, is reluctant to purchase additional security technologies. Senior Management is concerned with the return on investment, but it can be quite difficult to quantify return on security technology investments when the threat to the organization has not been adequately tied to the organizational profile. Unlike the purchase of a customer ordering system that has the potential to increase sales, Information Security is carried out to avoid losses. Adding to the problem is the fact that security breaches continue to occur even after additional expenditures in security technology. To reverse this trend another approach is needed.
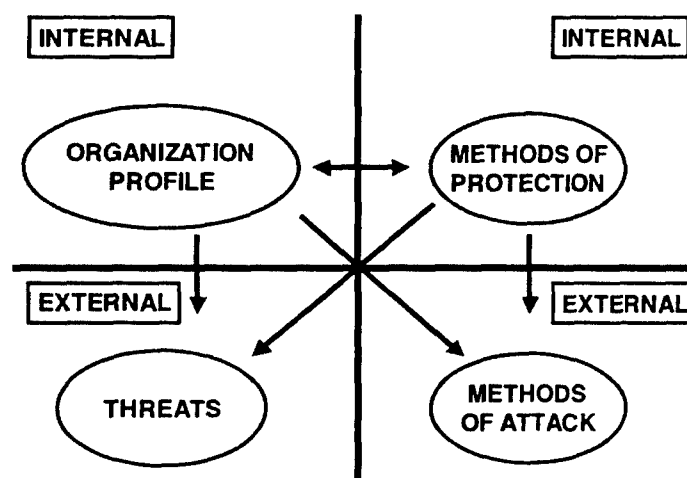

FIGURE 11: PROPOSED INFORMATION SECURITY FRAMEWORK

20

PROPOSED INFORMATION SECURITY FRAMEWORK

Reversing the dual trends of increasing expenditures for protection and increasing economic impact of security breaches must become an organization-wide priority. It is clearly not an easy task, but there are measures organizations can take immediately to improve their Information Security. Given the documented deficiencies of current methods, a new framework must be implemented that addresses the relationship between the organizational profile and methods of protection, as well as the impact of threats and methods of attack on both. To implement a comprehensive framework Information Security must become a priority throughout the organization. As a first step, the organization must look internally to determine the potential for economic loss related to the organization profile. They must quantify the value at risk, and this requires, among other things, that they place a value on their Information Technology. IBM has developed a tool to account for downtime of critical applications with their Information Technology Cost of Downtime Calculator.[41] While this tool provides the basis for determining the economic impact of an application being offline, the focus is on direct costs. Organizations must, however, also identify indirect costs, which is one of the more daunting challenges associated with a comprehensive Information Security assessment. This requires a team approach, as line of business personnel are in a better position to determine these costs than the security professionals are. Organizations must also place a value on proprietary and sensitive data. These steps are critical for they provide a basis for prioritizing an organization's Information Technology.

Organizations must also determine their current Information Security spending posture as it relates to the methods of protection. Reviewing the enterprise architecture and conducting an inventory of all Information Security technology assets can accomplish this. There are tools available to help in this process. One example is Gartner's Total Cost of Ownership (TCO) model for Information Security that will show organizations where they are currently spending their security technology dollars.[42] The goal of this process is to develop an Information Security architecture to be applied to the organization's methods of protection. The Information Security architecture must also be evaluated to determine if the technology is properly deployed. Here again, more and better tools are becoming available to assist in this process. "The Center for Internet Security (CIS) members are developing and propagating the widespread application of Security Benchmarks through a global consensus process that brings together industry, government, academia and consultants. CIS Benchmarks enumerate the 'When, Why, and How' aspects of technical security configurations across a wide range of

21

operating system platforms and Internet software applications."[43] This can be applied to the existing framework. However, its effectiveness will be diluted if it is not coupled to the organization profile.

Key to this framework is the relationship between the organization profile and methods of protection. This relationship is vital to determine and characterize if Information Security resources are to be spent effectively and efficiently. Are the methods of protection focused on the organization's center of gravity, such as the core proprietary data, or are they being disproportionably applied to lesser threats, such as protecting the network from mischievous vandals? The CERT® Coordination Center has developed the Operationally Critical Threat Asset Vulnerability Evaluation (OCTAVE) tool to assist organizations making these comparisons. "Thus, an evaluation needs to incorporate the context in which people use the infrastructure to meet the business objectives of the organization, as well as technological security issues related to infrastructure. "[44] By comparing the organizational profile and methods of protection, management can better direct information security spending.

There are other immediately available Information Security measures that do not involve the acquisition of additional technology. Organizations should review their Information Security policy with particular attention paid to passwords and access control. This may require development, or at least amendment, of organizational policy, and must be accompanied by an implementing plan to make sure Information Security policy is distributed throughout the organization. An additional step organizations can take is to implement an Information Security training program, with emphasis on the importance of security. Again, what drives the success of such efforts is the connection between the organization profile and methods of protection that in turn drives the implementation of policy and training.

External factors are also important to this framework. The threat and methods of attack must be considered from both a method of protection perspective as well as that of the organizational profile. This is critical when considering the impact of new technology on the organization and determining risk.

A problem organizations face is how to determine that the investment in Information Security is in fact reducing risk. To determine if the methods of protection are effective, demonstrating and quantifying risk is crucial. Risk analysis models such as the basic Annual Loss Exposure (ALE) are commonly used by organizations. To demonstrate the tool, we consider the example of a manufacturing plant. The value (V) of the manufacturing plant is multiplied by the probability of loss (L), from such things as natural disaster, and the product

22

then equals the ALE (V x L = ALE).[45] This formula provides a basis for determining how much should be spent each year to protect the manufacturing plant against that particular loss. While it is relatively easy to determine value of the manufacturing plant, and considerable data on the threat of losses due to natural disasters exist, it is more difficult when dealing with Information Security. The threat and method of attack are continuously evolving, and there is as yet insufficient data to allow reliable estimation of the probability of loss due to accident or malicious activity. It is, of course, difficult to determine the value of the information, but the framework presented here offers a starting point, and the methodology will help produce a better, more comprehensive risk reduction program. When better information becomes available on the Information Security threat, organizations will be in the position to take advantage of such a risk model.
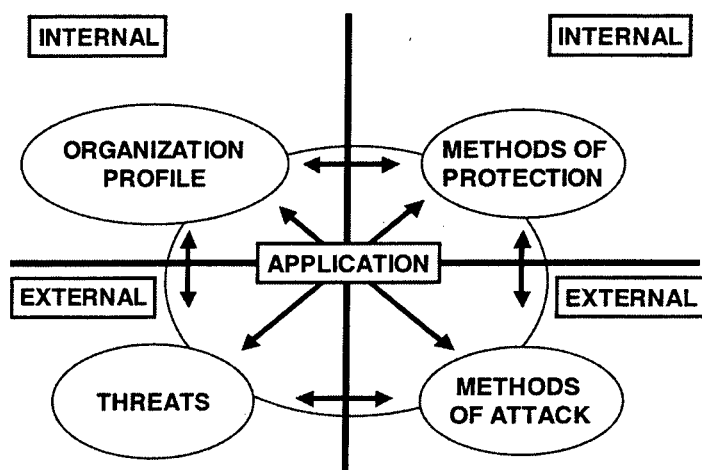
FIGURE 12: APPLICATION REQUIREMENT

APPLICATION REQUIREMENT

If organizations are to get the most out of the proposed framework, there is an obvious requirement for the development of an interactive application to evaluate the effect of changes to the organization profile, methods of protection, threat and method of attack elements.
The first two elements – organizational profile and existing methods of protection – are provided by the organization. They should include the organizational profile, as well as a prioritized list of the organization's existing Information Technology and methods of protection. Outside sources

of protection such as insurance, law enforcement, and legislation – as they relate to the organization and its mission and function – should also be included.

The threats and methods of attack are external to the organization, and the information must necessarily come from external sources. This information should include threats and methods of attacks (such data can be collected from various sources, including security organizations like CERT® Coordination Center, SANS Institute, and Computer Security Institute (CSI)). Data will also be required from Information Security vendors. By combining and analyzing both parts, i.e. the internally available and externally available information, an organization can determine its overall risk profile.

The benefit of such an application will be the ability it will provide organizations to perform sensitivity analysis, and adjust their organization profile and methods of protection to determine how they affect risk. For example, an organization considering providing Internet access to its employees could determine and quantify the result of this change in the organization's profile. In this way, the impact on risk would be apparent. The organization may find this increase in risk acceptable based on the benefits derived, and decide it is willing to pay the price for the increased risk. The importance of the application is that the decision can be made quickly with the consequences known up front. Another example would be the fielding of a web server. Through the application, it may be determined that the increase in risk is unacceptable. However, the organization may determine that the web server is necessary to stay competitive. Various methods of protection could then analyzed using the application to determine how to bring the risk back to an acceptable level. This would also show the organization the direct correlation between the fielding of Information Technology and the increased requirement for security technology. The tool may also be used to determine the best security technology investments by allowing for direct comparison of the impact different measures will have on the organizational profile. Such a comparison provides the added benefit of a sound basis on which to justify investments.

To make this application a reality and increase its effectiveness, considerable data on the threat and method of attack are required, which in turn requires organizations to overcome their apprehension and aversion to reporting Information Security breaches. That this is a problem is apparent in The Global Information Security Survey, 2001 findings, which indicate, "At most firms, security breaches remain a private matter. Forty-three percent of sites don't report such intrusions, although this is down from 56% in 2000. Forty percent of U.S. sites also refuse to fess-up."[46] Once this data becomes more readily available, rigorous analysis will be

required. Much of the data currently available is the result of market surveys, with the inherent weaknesses alluded to earlier in this paper. Academic interest must be generated and the rigor of quantitative analysis brought to bear.

CONCLUSION

Consideration of the economics of Information Security strongly suggests that the current approach to Information Security is not working, and that direct and non-direct costs are growing at an alarming rate. In addition, considerable funds are being applied to security technology investments, insurance, outsourcing, and legislation, with as-yet unclear results. By applying a basic methodology, that systematically addresses Methods of Attack, Threats, Methods of Protection, and Organizational Profile to well publicized Information Security breaches, the need for a comprehensive framework is clearly demonstrated. The goal of presenting the Proposed Organizational Information Security Framework and application requirement is to encourage discussion. In the end, it may not be the perfect solution. However, if it encourages organizations to reevaluate the way they look at Information Security then it will be successful.

WORD COUNT = 8015

ENDNOTES

[1] Informationweek Research "Global Information Security Survey, 2001," Informationweekresearch.com, (September 2001): 8.

[2] Ibid.

[3] Maria Atanasov, "The truth about Internet fraud, Merchants pay the price," ZDNet Tech Update, March 12, 2001; Available from <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2688776-4,00.html>; Internet; accessed 27 November 2001.

[4] Informationweek Research, 8.

[5] "Digital Planet 2000: "The Global Information Economy, Executive Summary," World Information Technology and Services Alliance, (November 2000): 1.

[6] Andy Briney, "2001 Industry Survey," Information Security, TrueSecure Corporation, (October 2001): 36.

[7] Mathew Beal, "IDC: Internet Security Market is Booming," E-Commerce Times, August 12, 1999; Available from <http://www.ecommercetimes.com/perl/story/980.html>; Internet; accessed 18 February 2002.

[8] Bruce Schneier, "Schneier On Security: The Insurance Takeover," Information Security, Security Wire Digest February 2001; Available from <http://www.infosecuritymag.com/articles/february01/columns_sos.shtml>; Internet; accessed 25 September 2001.

[9] Heather Eikenberry, "Hacker's Insurance: When All Else Fails," SANS Institute 2 January 2001; Available from < http://rr.sans.org/casestudies/insurance.php>; Internet; accessed 18 October 2001.

[10] George V. Hulme, "Security's Best Friend? -- Companies are outsourcing IT security to cut costs of around-the-clock surveillance. But some doubt the risk is worth the savings," Information Week.com 16 July 2001; Available from <http://www.informationweek.com/story/IWK20010713S0009>; Internet; accessed 18 February 2002.

[11] Sean Corcoran, "Shifting Liabilities," Information Security, March 2002, 16.

[12] Daniel F. Long, "Hackers Said To Cost U.S. Billions," NewsFactor 8 February 2001; Available from <http://www.newsfactor.com/perl/story/7349.html>; Internet; accessed 6 September 2001.

[13] Michal Dluginski, "Worms That Won't Let Go," PC Magazine 16 October 2001; Available from <http://www.pcmag.com/article/0,2997,s=1490&a=14541,00.asp>; Internet; accessed 18 February 2002.

[14] George V. Hulme

[15] "Windows XP vulnerable to 'serious' attacks, Microsoft releases fix for security flaw," CNN.COM/SCI-TECH 20 December 2001; Available from <http://www.cnn.com/2001/TECH/ptech/12/20/microsoft.hackers.ap/index.html Internet; accessed 20 December 2001.

[16] Dan Verton, "Record-breaking year for security incidents expected: Experts criticize 'reactive' nature of responses, tell Congress to lead charge," Computerworld 26 November 2001; Available from <http://www.computerworld.com/itresources/rcstory/0,4167,STO66054_KEY73,00.html>; Internet; accessed 27 November 2001.

[17] "Feds Try To Estimate Computer Damage Caused By Accused Spy," Security Wire Digest 8 March 2001; Available from <http://www.infosecuritymag.com/digest/2001/03-08-01.shtml>; Internet; accessed 19 November 2001.

[18] Harry Krimkowitz, "Mitigating Risks to the Insider Threat within your Organization," SANS Institute 24 October 2000; Available from < http://rr.sans.org/policy/password.php>; Internet; accessed 17 November 2002.

[19] Craig Donovan, "Strong Passwords," SANS Institute 2 June 2000; Available from <http://www.sans.org/infosecFAQ/policy/password.htm>; Internet; accessed 18 February 2002

[20] Richard Power, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues & trends," CSI Computer Security Institute (Spring 2001): 10-11.

[21] "Virus Pimer," TREND Micro, Available from <http://www.antivirus.com/vinfo/vprimer.htm>; Internet; accessed 18 February 2002.

[22] "worm," searchSecurity.com, Available from <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213386,00.html>; Internet; accessed 18 February 2002.

[23] Michelle Delio, "Scary Hybrid Internet Worm Loose," Wired News 18 September 2001; Available from <http://www.wired.com/news/technology/0,1282,46944,00.html>; Internet; accessed 8 October 2001.

[24] Robert Lemos, "Nimda winds down; companies recover," CNET News.com 20 September 2001; Available from <http://news.com.com/2100-1001-273286.html?legacy=cnet>; Internet; accessed 22 January 2002.

[25] Sophos Press Release, <u>SOPHOS Anti-Virus</u>, Available from <http://www.sophos.com/pressoffice/pressrel/uk/20011127yeartopten.html>; Internet; accessed 21 January 2002.

[26] "Viruses could make email system unusable," <u>ANANOVA</u> 24 September 2001; Available from <http://www.ananova.com/news/story/sm_406529.html?menu+news.technology>; Internet; accessed 25 September 2001.

[27] Ibid.

[28] "2001 Economic Impact of Malicious Code Attacks," <u>Computer Economics</u> 2 January 2002; Available from <http://www.computereconomics.com/cei/press/pr92101.html>; Internet; accessed 22 January 2002.

[29] Andy Briney, 39.

[30] Sophos Press Release, "SOPHOS Anti-Virus Opens Office in Singapore as Part of Global Expansion," <u>SOPHOS Anti-Virus</u> 13 November 2001; Available from <http://www.sophos.com/pressoffice/pressrel/sg/20011113office.html>; Internet; accessed 18 February 2002.

[31] Richard Power, 10-11.

[32] Brian Fonseca, "Yahoo outage raises Web concerns," <u>NetworkWorldFusion News</u> 9 February 2000; Available from <http://www.nwfusion.com/news/2000/0209yahoo2.html>; Internet; accessed 22 January 2002.

[33] Carolyn Duffy Marsan, "Denial-of-service threat gets IETF's attention," <u>NetworkWorldFusion News</u> 24 July 2000; Available from <http://www.nwfusion.com/news/2000/0724itrace.html>; Internet; accessed 18 February 2002.

[34] <u>Gilian Technologies</u>, Available from <http://www.gilian.com/webassets.pdf>; Internet; accessed 18 February 2002. 3.

[35] Andy Briney, 39.

[36] IDC Press Release, "Analyze the Future, The Worldwide Firewall/VPN Security Appliance Market Is Headed to $4 Billion by 2005, IDC Says," <u>IDC</u> 27 June 2001; Available from <http://www.idc.com/getdoc.jhtml?containerId=pr2001_09_02_180913>; Internet; accessed 18 February 2002.

[37] Suzanne Gaspar, "Security concerns dominate NW500 survey," <u>Network World</u> 5 July 2001; Available from <http://www.itworld.com/Sec/2052/NWW010507feat2/>; Internet; accessed 18 February 2002.

[38] Richard Power, 10-11.

[39] "The 2001 Global e.fraud.survey," KPMG Forensic & Litigation Services, (2001):16.

[40] Richard Power, 2.

[41] "IBM IT Cost of Downtime Calculator," 2001 International Business Machines Corporation.

[42] William Malik, Robert Witty, "Gartner, Security TCO Model Helps With More Than Cost Savings," Gartner 12 June 2001, Available from <http://www4.gartner.com>; Internet; accessed 11 October 2001.

[43] The Center for Internet Security (CIS), Available from <http://www.cisecurity.org/>; Internet; accessed 27 February 2001.

[44] Christopher J. Alberts, Audrey J. Dorofee, OCTAVE Criteria Version 2.0 (Pittsburgh: PA. Carnegie Mellon, Software Engineering Institute, 2001), 5.

[45] Thomas R. Peltier, Information Security Risk Analysis, (Boca Raton, FL, Auerbach Publications, 2001) 15.

[46] Informationweek Research, 7.

BIBLIOGRAPHY

"2001 Economic Impact of Malicious Code Attacks," Computer Economics 2 January 2002. Available from <http://www.computereconomics.com/cei/press/pr92101.html>. Internet. Accessed 22 January 2002.

Alberts, Christopher J., and Audrey J. Dorofee. OCTAVE Criteria Version 2.0. (Pittsburgh: PA. Carnegie Mellon, Software Engineering Institute, 2001

Atanasov, Maria. "The truth about Internet fraud, Merchants pay the price," ZDNet Tech Update 12 March 2001. Available from <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,26887764,00.html>. Internet. Accessed 27 January 2002.

Beal, Mathew. "IDC: Internet Security Market is Booming" E-Commerce Times, August 12, 1999. Available from <http://www.ecommercetimes.com/perl/story/980.html>. Internet. Accessed 18 February 2002.

Briney, Andy. "2001 Industry Survey," Information Security, TrueSecure Corporation, (October 2001)

Corcoran, Sean "Shifting Liabilities," Information Security, March 2002, 16.

Delio, Michelle. "Scary Hybrid Internet Worm Loose," Wired News 18 September 2001. Available from <http://www.wired.com/news/technology/0,1282,46944,00.html>. Internet. Accessed 8 October 2001

"Digital Planet 2000: The Global Information Economy," World Information Technology and Services Alliance, (November 2000)

Dluginski, Michal. "Worms That Won't Let Go," PC Magazine 16 October 2001. Executive Summary", Available from <http://www.pcmag.com/article/0,2997,s=1490&a=14541,00.asp>. Internet. Accessed 18 February 2002.

Donovan, Craig. "Strong Passwords," SANS Institute 2 June 2000. Available from <http://www.sans.org/infosecFAQ/policy/password.htm>. Internet. Accessed 18 February 2002.

Eikenberry, Heather. "Hacker's Insurance: When All Else Fails," SANS Institute 2 January 2001. Available from < http://rr.sans.org/casestudies/insurance.php>. Internet. Accessed 18 October 2001.

"Feds Try To Estimate Computer Damage Caused By Accused Spy," Security Wire Digest 8 March 2001. Available from <http://www.infosecuritymag.com/digest/2001/03-08-01.shtml>. Internet. Accessed 19 November 2001.

Fonseca, Brian. "Yahoo outage raises Web concerns," NetworkWorldFusion News 9 February 2000. Available from <http://www.nwfusion.com/news/2000/0209yahoo2.html>. Internet. Accessed 22 January 2002.

Gaspar, Suzanne. "Security concerns dominate NW500 survey," <u>Network World</u> 5 July 2001. Available from <http://www.itworld.com/Sec/2052/NWW010507feat2/>. Internet. Accessed 28 February 2002.

Gilian Technologies, Available from http://www.gilian.com/webassets.pdf.Internet>. Accessed 18 February 2002.

Harrison, Ann "Punish software makers for bad security' – NAS," <u>The Guardian</u> 9 January 2002. Available from http://www.theregister.co.uk/content/4/23595.html. Internet. Accessed 28 February 2002.

Hulme, George V. Security's Best Friend? -- Companies are outsourcing IT security to cut costs of around-the-clock surveillance. But some doubt the risk is worth the savings," <u>Information Week.com</u> 16 July 2001. Available from <http://www.informationweek.com/story/IWK20010713S0009>. Internet. Accessed 18 February 2002.

<u>IDC Press Release</u>, "Analyze the Future, The Worldwide Firewall/VPN Security Appliance Market Is Headed to $4 Billion by 2005, IDC Says," IDC 27 June 2001. Available from <http://www.idc.com/getdoc.jhtml?containerId=pr2001_09_02_180913>. Internet. Accessed 18 February 2002.

"IBM IT Cost of Downtime Calculator," 2001 International Business Machines Corporation.

Informationweek Research "Global Information Security Survey, 2001," <u>Informationweekresearch.com</u>, (September 2001)

Krimkowitz, Harry. "Mitigating Risks to the Insider Threat within your Organization," <u>SANS Institute</u> 24 October 2000. Available from < http://rr.sans.org/policy/password.php>. Internet. Accessed 17 November 2002.

Lemos, Robert. "Nimda winds down; companies recover," <u>CNET News.com</u> 20 September, 2001. Available from <http://news.com.com/2100-1001-273286.html?legacy=cnet>. Internet. Accessed 28 February 2002.

Long, Daniel F. "Hackers Said To Cost U.S. Billions," <u>NewsFactor</u> 8 February 2001. Available from <http://www.newsfactor.com/perl/story/7349.html>. Internet. Accessed 28 February 2002.

Malik, William. and Robert Witty. "Gartner, Security TCO Model Helps With More Than Cost Savings," <u>Gartner</u> 12 June 2001. Available from <http://www4.gartner.com>. Internet. Accessed 22 January 2002.

Marsan, Carolyn Duffy. "Denial-of-service threat gets IETF's attention," <u>NetworkWorldFusion News</u> 24 July 2000. Available from <http://www.nwfusion.com/news/2000/0724itrace.html>. Internet. Accessed 18 January 2002.

Peltier, Thomas R. <u>Information Security Risk Analysis</u>, Boca Raton, FL, Auerbach Publications, 2001

Pfleeger, Charles P. Security in Computing, Upper Saddle NJ, Prentice-Hall Inc.1997, reprinted 2000

Power, Richard. 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues & trends," CSI Computer Security Institute (Spring 2001)

Schneier, Bruce. "Schneier On Security: The Insurance Takeover," Information Security, Security Wire Digest February 2001. Available from <http://www.infosecuritymag.com/articles/february01/columns_sos.shtml>. Internet. 25 September 2001.

Sophos Press Release, SOPHOS Anti-Virus Available from <http://www.sophos.com/virusinfo/topten/200112summary.html>. Internet. Accessed 21 January 2002.

Sophos Press Release, "SOPHOS Anti-Virus Opens Office in Singapore as Part of Global Expansion," SOPHOS Anti-Virus 13 November 2001. Available from <http://www.sophos.com/pressoffice/pressrel/sg/20011113office.html>. Internet. Accessed 18 February 2002.

"The 2001 Global e.fraud.survey," KPMG Forensic & Litigation Services, (2001)

The Center for Internet Security (CIS), Available from <http://www.cisecurity.org/. Internet. Accessed 27 February 2001.

Verton, Dan "Record-breaking year for security incidents expected: Experts criticize 'reactive' nature of responses, tell Congress to lead charge," Computerworld 26 November 2001. Available from <http://www.computerworld.com/itresources/rcstory/0,4167,STO66054_KEY73,00.html>. Internet. Accessed 27 November 2001.

"Viruses could make email system unusable," ANANOVA 24 September 2001. Available from <http://www.ananova.com/news/story/sm_406529.html?menu+news.technology>. Internet. Accessed 25 September 2001.

"Virus Pimer," TREND Micro, Available from <http://www.antivirus.com/vinfo/vprimer.htm>. Internet. Accessed 18 February 2002.

"Windows XP vulnerable to 'serious' attacks, Microsoft releases fix for security flaw," CNN.COM/SCI-TECH 20 December 2001. Available from <http://www.cnn.com/2001/TECH/ptech/12/20/microsoft.hackers.ap/index.html>. Internet. Accessed 20 December 2001.

"worm" searchSecurity.com Available from <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213386,00.html>; Internet; Accessed 18 February 2002