

Fall 12-1-2005

Economics of Information Security - Developing a Model for Information Security Cost Minimization

Solomon Ogara
Dakota State University

Follow this and additional works at: <https://scholar.dsu.edu/theses>

Recommended Citation

Ogara, Solomon, "Economics of Information Security - Developing a Model for Information Security Cost Minimization" (2005). *Masters Theses*. 247.
<https://scholar.dsu.edu/theses/247>

This Thesis is brought to you for free and open access by Beadle Scholar. It has been accepted for inclusion in Masters Theses by an authorized administrator of Beadle Scholar. For more information, please contact repository@dsu.edu.

Economics of Information Security – Developing A Model for Information Security Cost Minimization

A graduate project submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Master of Science

in

Information Systems

December, 2005

By

Solomon Ogara

Project Committee:

Prof: Rick Christoph

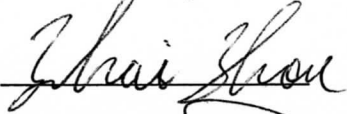
Prof: Zehai Zhou

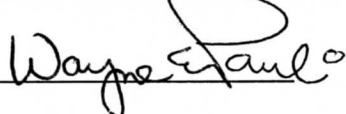
Prof: Wayne Pauli

We certify that we have read this project and that, in our opinion, it is satisfactory in scope and quality as a project for the degree of Master of Science in Information Systems.

Project Committee

Faculty supervisor:  Date: 12/09/05

Committee member:  Date: 12/09/05

Committee member:  Date: 12/09/05

ACKNOWLEDGMENT

I want to take this opportunity to thank the following professors for kindly accepting to be part of my thesis committee – Richard Christoph, Paul Wayne and Zehai Zhou. Special thanks go to Professor Richard Christoph, who guided me on the technical aspects of this thesis. Thank you so much my wife Phoebe and children; Sharon, Shalom and Steve for your patience during the many hours I spent alone on my thesis.

ABSTRACT

In an increasingly global environment, any organization and or individual who seek to make a positive difference cannot ignore the need for an information strategy that would position them to be winners rather than losers in the market place. Given the growing scarcity of resources, such a strategy has to be carefully planned in such a way that it is cost effective and financially sustainable. The internal security measures should be such that they don't consume the resources of the organization and leave it unable to build a sustainable information security base. On the other hand there is always the risk of an under investment in information security and this may have disastrous effects.

A fundamental question to be explored in this study is how to come up with an optimal level of investment in information security. The costs and benefits of security should be carefully examined in monetary terms to ensure that the cost of controls does not exceed expected benefits. Information technology departments are finding themselves working under strict budget allocation. Security expenditure is considered an expense and every manager is under obligation to justify such expenditure using business metrics such as Returns on Investment (ROI). Managers are faced with making difficult decisions on what security measures to employ or how to balance the human factors and technology. It's this balancing that is critical to a successful security program.

This thesis discusses three dimensions of information security i.e. technical, human and economic dimensions. While attempting to discuss these dimensions, this thesis will try to address the following questions from an economic point of view:

- Why is cost effectiveness an issue and for who is it an issue? In order to address this question, secondary data from financial analyses of trends in expenditure from a selected number of companies will be presented and questions raised as to the issues those trends present to the sustainability of such organizations.
- What is a bad practice in information security management? An attempt will be made to highlight some of the bad practices and a justification to the effect that the underlying issue in such practices is more financial than anything else, hence the need for this cost effectiveness study.
- What is an efficient secure system and what lenses are we using to assess efficiency? What constitutes an economical security system? Here an economic model will be developed that can be used to answer the questions above.

This thesis presents an economic model that management can use to make appropriate decisions on how best to utilize dollars allocated for security. Whilst this model does not underestimate the significance of human and technical dimensions of the information security, it is important that any economically sound security program create a balance between the technical and human dimensions of an information security system. The model emphasizes the tradeoff between the technology and human dimensions of security thus increasing the opportunity cost of the human dimensions.

DECLARATION

I hereby certify that this project constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another. I declare that the project describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,



Solomon O. Ogara

TABLE OF CONTENTS

| | |
|---|------|
| ACKNOWLEDGEMENT..... | III |
| ABSTRACT..... | IV |
| DECLARATION..... | VI |
| TABLE OF CONTENT..... | VII |
| LIST OF TABLES..... | VIII |
| LIST OF FIGURES..... | IX |
| INTRODUCTION..... | 1 |
| BACKGROUND TO THE PROBLEM..... | 1 |
| STATEMENT OF THE PROBLEM..... | 4 |
| OBJECTIVE OF THE PROJECT..... | 4 |
| LITERATURE REVIEW..... | 6 |
| RESEARCH METHODOLOGY..... | 14 |
| RESULTS AND DISCUSSIONS..... | 20 |
| CONCLUSION..... | 24 |
| REFERENCES..... | 25 |
| APPENDIX A – PROJECT PLAN DOCUMENTATION..... | 27 |
| APPENDIX B – WORK BREAKDOWN STRUCTURE AND GANTT CHART..... | 30 |
| APPENDIX C – INTRODUCTION TO PRODUCTION POSSIBILIZTIES MODEL..... | 32 |
| APPENDIX D–COMPARISON OF EMPLOYEE EDUCATION, TRAINING AND AWARENESS..... | 34 |
| APPENDIX E – MORE FIGURES AND TABLES..... | 37 |

LIST OF TABLES

| | |
|--|----|
| Table 1: Comparing awareness, training and education (NIST handbook 2002)..... | 34 |
| Table 2: Annual budget for information security | 37 |
| Table 3: Comparing performance and cost of different IDS. | 37 |
| Table 4: Disposition of policies and procedures..... | 38 |
| Table 5: Types of e-crimes | 39 |
| Table 6: Most effective technologies used..... | 40 |

LIST OF FIGURES

| | |
|---|----|
| Figure 1. Optimal Security Investment Curve | 7 |
| Figure 2. Proposed Path Diagram for Information System Security Effectiveness | 11 |
| Figure 3. Secure Possibilities Model | 17 |
| Figure 4. Effect of a unit increase in investment in employee training and awareness.... | 18 |
| Figure 5: Gantt Chart. | 31 |
| Figure 6. Production Possibilities Frontier | 32 |
| Figure 7: Comparison increase in total number of e-crimes and intrusions 2003 and 2004 | 40 |
| Figure 8: Expected change in monetary losses for 2005 | 41 |
| Figure 9: Prevalence of e-Crime | 41 |
| Figure 10: Average computer security expenditure per employee. | 42 |
| Figure 11: Unauthorized use of computer systems within last 12 months. | 43 |
| Figure 12: Dollar amount losses by type | 43 |
| Figure 13: Security Technologies Used..... | 44 |

CHAPTER 1

INTRODUCTION

BACKGROUND TO THE PROBLEM

Do we spend enough on keeping `hackers' out of our computer systems? Do we not spend enough? Or do we spend too much? And do we spend our security budgets on the right things? These are some questions that have puzzled information security experts according to Ross Anderson (2002). Several authors in the field of information security have attempted to research on the same areas but with little success. Responses to these questions can be so blurred given the sacred manner in which security matters are treated today. The costs and benefits of a sound security program should be carefully examined to ensure that the cost of controls do not exceed expected benefits. Information technology departments are finding themselves working under strict budget allocation. Security expenditure is being considered an expense and every manager is under obligation to justify such expenditure and also be able to justify the Returns on Investment (ROI). Managers are faced with making difficult decisions on what security measures to employ and more so how to balance the human factors and technology.

According to Jupiter Media Metrix, cyber-security issues could potentially cost e-businesses almost \$25 billion by 2006 - up from \$5.5 billion in 2001. This trend is worrying and is leading many organizations to invest in security measures without an elaborate plan. Many corporations in many industries have recognized a strong need to beef up their cyber-security against potentially debilitating attacks and to treat computer

security like a strategic marketing initiative, rather than a compliance burden - (Gal-Or and Ghose, 2005).

Schnieier and Anderson, in an editorial page of *Economics of Information security Journal* (Schnieier, 2002), says that many of the most basic security questions are at least as much economic as technical. Do we spend enough keeping hackers out of our computer systems? Or do we spend too much? And are we spending our security budgets on the right things. They suggest that Economics can actually explain many of the puzzling realities of Internet security. Firewalls are common; email encryption is rare: not because of the relative effectiveness of the technologies, but because of the economic pressures that drive companies to install them. Gordon and Loeb authored a paper in which they demonstrated that for a given potential loss and a given threat level, the optimal amount to spend on such security is an increasing function of the information's vulnerability but only up to a certain optimum level (Gordon and Loeb, 2002). According to this paper, the authors suggest that little or no information security is economically justified for extremely high, as well as extremely low levels of vulnerability and that even within the range of justifiable investments in information security, the maximum amount a risk-neutral firm should spend is only a fraction which should never exceed 37% of the expected loss due to security breaches. Another very interesting finding is that companies are spending much of their IT budgets on complying with regulations such as Sarbanes-Oxley and the European Union's 8th Directive that they are neglecting other security threats, according to a new survey published on November 1 2005 by Ernst & Young's annual security survey (Palmer, 2005). The survey found that compliance with regulations had become the key driver for information security spending at nearly two-

thirds of companies around the world, eclipsing concerns such as protection against computer viruses and worms. According to Palmer, regulations stipulating that company executives take personal responsibility for the accuracy of corporate data, such as accounts, have caused many companies to tighten internal IT controls, ensuring for example, that only authorized employees have access to accounts databases. Failure to follow these regulations could result in imprisonment of company officers, fines as well as have devastating effects on the business itself – potentially causing existing and potential customers to lose faith in the company’s ability to protect the integrity, privacy and confidentiality of their personal information.

According to the 2005 CSI/FBI survey report, there is an increase in the number of companies that are now using business formulas such as ROI, NPV, and IRR to determine the returns on security investments. The report further adds that many companies are increasingly allocating a portion of their budget to security but these investments must be justified. Michael Whiteman has authored a paper on “threat to information security” in which he says that technologists often overlook the human solutions and instead opt for technology solutions, when in fact the human factors must be addressed first, with technology assisting in the enforcement of desired human behaviors (Whiteman, 2003). Information security and assurance has been of particular concern to government, businesses, and academia for several decades. Beginning with the use of time sharing systems, and more recently, with the wide spread acceptance of broadband access to the Internet, managing the security of information systems has become vital. Although organizations that have typically employed high bandwidth connections to the Internet have developed both the technical infrastructure and intellectual capital to manage security risks, those organizations and individuals who have not historically had

such access must now develop similar capabilities. Failure to appropriately manage information system security can potentially expose the organization, and others to which it is connected, to loss of time, money, and public trust.

STATEMENT OF THE PROBLEM

The underlying question behind this thesis is how to make wise, efficient and cost effective market security decisions in a global world where the dollar gets scarce by the day and yet the need to produce an efficient and economical information security system is more urgent than ever? This leads to the following questions:

- ✓ *Is the business better off by choosing to use cheaper or freeware security tools such as Snort and divert the dollars saved to improve employee security education, training and awareness program?*
- ✓ *Is the business better off by buying security tools bundled together and offering different functionalities as opposed to purchasing different security tools from different vendors?*

The answers to both questions are contained in the model proposed in this thesis.

From the research questions is the following core issue that is central to this research

“That the determination of an optimal level of expenditure on security is critical to ensuring a cost effective and sustainable information security system”

OBJECTIVE OF THIS THESIS

The model developed in this thesis discusses the three dimensions of an information security system - technical, human and economic. By exploring the

economic dimensions of information security, this thesis will try to answer the following questions: What is an efficient security system? What is an economically sound security system? Many papers have been written on the role of both technology and human factors in protecting information security breaches. However, there is no paper out there that has tackled this puzzling question – “how do we balance the technical and human factors in order to create an efficient and economical security level?” In general, what then is the added value of this thesis? They as follows: That in an economy with scarce resources, making security decisions should be driven by cost conditions and that there are other dimensions – technical and human factors. This is the question that this thesis will try to answer using the secure possibilities model developed. Managers are increasingly under pressure to justify security expenditure. Some organizations are increasingly using ROI, IRR and the NPV according to CSI/FBI survey report 2005 - Gordon and et al. (2005). Previous research shows that computer/network abuse is more prevalent from within the organizations (insider abuse) than from outside (outsider abuse) – CSI (2005), Ryan and Jefferson (2002). Related research includes protecting information through encryption, access control, and firewalls - Denning and Branstad (1996), Schnieier (1996), Pfleeger (1997), Larsen (1999), and Osborn et al. (2000). Research on behavioral aspects of reducing information security breaches - Straub (1990), Loch et al. (1992), and Straub and Welke (1998). The arguments in this thesis will be supported by information and data obtained with permission from different surveys on economics of information security.

CHAPTER 2

LITERATURE REVIEW

How much should be invested in information security? There are many articles out there that discuss this topic. Gordon and Loeb have written a paper in which they developed an economic model that determines the optimal amount to invest in order to protect a given set of information (Gordon and Loeb, 2002). According to the authors, this model is applicable to investments related to various information security goals, such as protecting the confidentiality, availability, authenticity, non-repudiation, and integrity of information. The authors demonstrate that under certain sets of assumptions concerning the relationship between *vulnerability* and the *marginal productivity of the security investment*, the optimal investment in information security may either be strictly increasing or first increase and then decrease as vulnerability increases. Thus, under plausible assumptions, investment in information security may well be justified only for a midrange of information vulnerabilities. That is, little or no information security is economically justified for extremely high, as well as extremely low, levels of vulnerability. They suggest further that even within the range of justifiable investments in information security, the maximum amount a risk-neutral firm should spend is only a fraction, which should never exceed 37% of the expected loss due to security breaches. Graphically their argument will look like this:

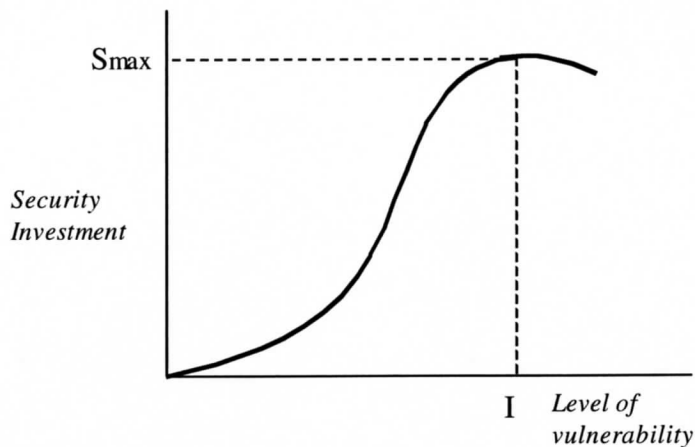


Figure 1: Optimal Security Investment Curve

The graph suggests that investments in security increases with increase in the level of vulnerability until an optimal point “*I*” corresponding to investments in security “ S_{max} ” point where a further increase in vulnerability will not yield any further investments in security. Beyond this point, the level of investments in security does not increase as shown above. Kevin Soo Hoo in his article “How much is enough, A Risk Management Approach to Computer,” developed a model that showed quite convincingly that the current level of reported computer-security-related risks warranted only the most inexpensive of additional safeguards. Unless the costs and consequences of computer security breaches used were radically erroneous, the optimal solution for managing computer security risks called for very minimal security measures. Thus, the reluctance of both private and government organizations to pursue computer security aggressively may have been well justified at the time. Of course, this conclusion is very weak because the model relied upon anecdotal data that many security experts agree underestimate the true extent and consequences of computer crime.

Bruce Schneier authored an article entitled “No, we don't spend enough!” argues that organizations optimize themselves to minimize their risk, and understanding those motivations is key to understanding computer security today – Schneier (2002). According to Schneier, most organizations don't spend a lot of money on network security. Why? Because the costs are significant: time, expense, reduced functionality, frustrated end users. On the other hand, the costs of ignoring security and getting hacked are small: the possibility of bad press and angry customers, maybe some network downtime, none of which is permanent. And there's some regulatory pressure, from audits or lawsuits that add additional costs. The result: a smart organization does what everyone else does, and no more. Schneier adds that the same economic reasoning explains why software vendors don't spend a lot of effort securing their products. The costs of adding good security are significant—large expenses, reduced functionality, delayed product releases, annoyed users—while the costs of ignoring security are minor: occasional bad press, and maybe some users switching to competitors' products. Any smart software vendor will talk big about security, but do as little as possible.

One of the challenges that organizations face today is how to allocate resources for information security. Research has shown that there is no correlation between security spending and performance. On the other hand, companies are increasingly using business metrics such as ROI, IRR in an effort to justify spending according to the 2005 Computer security Institute survey report – CSI/FBI (2005). Carini argues that security investments are judged successful to the extent that they reduce the probability of loss from attacks. Each would obtain a different value from the same information security investment. Therefore the optimal amount and type of security investment is different for each

individual, firm, and network participant – Carini (2002). Carini points out that the economics of information security is not a “one size fits all” problem but instead involves extending principles and paradigms from the field of economics to that of information security, examining investment in information security and how it relates to the risks and expected losses associated with diverse cyber-attacks, using a conceptual framework borrowed from the economics of risk analysis. As a result he proposes that using these economic concepts introduces transparency in the opaque world of information security, and also provides a basis for some normative analysis.

The second important review is the security policy and employee education and awareness program. Security policy is a very important aspect of the employee awareness although the former is often discussed separately. In this thesis, employee education and awareness program is considered to include security policy. The security policy is the first and potentially most important layer of security available to an organization. Security policies define the security philosophy and posture the organization takes, and is the basis for all subsequent security decisions and implementations. The three concepts of confidentiality, integrity and availability (CIA) are the true fundamentals of information security. These three concepts are critical when designing a security policy. Privacy is about preserving the confidentiality of customer data. Survey by the 2003 FTC report (Federal Trade Commission, 2004, p.3-4) found that 42% of all complaints were related to identity theft, up from 40% in 2002. In 1999, Congress passed the Gramm-Leach-Bliley Act (GLB Act) that in part, serves to protect the privacy of customer information held by financial institutions. GLB requires all financial institutions to establish safeguards that ensure the security and confidentiality of customer information, protect

against known and anticipated threats to the security of data, and protect against unauthorized access to or use of such information that could result in harm or inconvenience to customers - Berns and Neclerio (2003). Congress also passed the Health Insurance Portability and Accountability Act of 1996 (HIPPA) to improve and enforce patient confidentiality. In July 2002, President George W. Bush signed the Sarbanes – Oxley Act into law. The purpose of the law is to restore public trust in corporate governance by making chief executives of publicly traded companies personally validate financial statement and other information- Hurley (2003). The passage of these law and acts attest to the fact that the government recognizes the importance of the three facets of information security mentioned above i.e.

Confidentiality, Integrity and Availability. A survey by Ryan and Jefferson in a paper entitled “*The use, misuse, and abuse of statistics in information security research*”(Ryan and Jefferson, 2003) found out that some organizations do not have a security policy.

Whiteman in his paper “Enemy at the gate: Threats to information security” (Whiteman, 2003), reports that only about 63% indicated a consistent security policy. According to Whiteman, what are indistinguishable are the effectiveness, comprehensiveness, and quality of the security policies of those indicating the presence of a policy. Equally concerning is the low response in the area of ethics training. Whiteman points out that a fundamental part of an organization’s security function is the implementation of a security education, training, and awareness (SETA) program. Whiteman emphasizes that as technologists we often overlook the human solutions- relatively low-cost protection mechanisms with the potential for high returns-on investment - and instead opt for technology solutions, when in fact the human factors must be addressed first, with

technology assisting in the enforcement of desired human behaviors. This argument is fundamental to the model developed in this paper.

Phelps’s dissertation on “ Information system security: self-efficacy and security effectiveness in Florida libraries” proposed a model (Figure 2), for measuring information system security self-efficacy and examines the relationship between the educational preparation of systems librarians and the effectiveness of their information system security implementation (Phelps, 2005). It differentiates education based on whether or not the participant has received other, formal information technology training. It examines the relationship between information technology training and information system security effectiveness through the intervening variables of information system security experience, information system security self-efficacy - belief in one's capacity to succeed at tasks, information system security task initiation, and information system security task persistence.

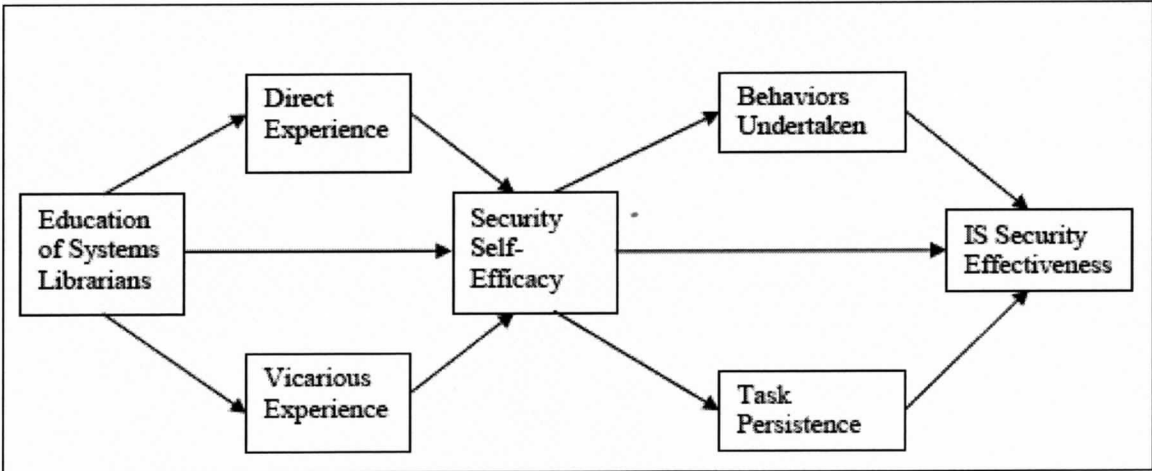


Figure 2. Proposed Path Diagram for Information System Security Effectiveness (Phelps, p.10)

The findings of the study suggest that prior IT training is positively related to information security implementation effectiveness.

According to the 2004 annual report to Congress on agency compliance with information technology (IT) security requirements, in law and policy, as required by the Federal Information Security Act (FISMA), 88% of employees were trained in IT security at a total cost of \$55,001,002. The estimated cost per employee trained amounted to \$13.33 - FISMA (2004).

In conclusion, this review points out the following: The question "How much to invest in information security" is still puzzling many information security economist. Some of the arguments have not been convincing enough for example; Hoo S.K. suggestion that the optimal solution for managing computer security risks called for very minimal security measures, has been found deficient because it creates the impression that very little input is required to safeguard information security. Schnieier's paper, which suggests that motivation plays a crucial role in the development of security, does not hold considering the increasing and sophisticated level of attacks and other security breaches.

Security advocates emphasize that any security profile begins with valid security policy. This policy is then translated into action through an effective security plan focusing on the prevention, detection, and correction of threats. An additional activity that should be developed early is the design and implementation of an employee security education, training, and awareness program. These programs seek to educate employees on the importance of security, security policy and its implementation within the organization. The awareness program seeks to keep security on the minds of employees as they deal with vital information on a daily basis. A solid policy planning and a good employee security education and awareness program, should allow an organization to better focus its security efforts, thus

increasing its probability of protecting the information and reducing its vulnerability to attack.

CHAPTER 3

RESEARCH METHODOLOGY

How was data collected and analyzed? The original intent of this research was to conduct a statistical analysis for both technology and human factors, but the amount of data required to conduct such study was hard to obtain because of the difficulty of obtaining such information. For example, a company will not release information on amount of dollars used for security and the type of technology employed in their network, for privacy and competitive reasons. Most of the data used in this thesis were obtained from the Computer Security Institute/Federal Bureau of Investigations survey reports, 2005 e-Crime Watch survey, SecurityStats.com website, Cyber Crime statistics website-www.cybertelecom.com, NIST Handbook, papers presented at the Workshop on Economics and Information Security – WEIS 2002, WEIS 2003, WEIS 2004, WEIS 2005, Economics of Information Security handbook, computer security journals, etc.

Developing A Secure Possibilities Model (SPM)

The development of this model is just an example of how economic principles can be applied in information security. An efficient information security system is not limited to technology and security policy and procedures alone, but must include the economic aspects as well. The economic aspects answers questions such as: Is the organization better off by investing in information security? How can organization maximize benefits from security investments given scarce resources in terms of dollars?

The Secure Possibilities Model (SPM) is adopted from the concept of the Production Possibility Frontier (PPF) (Appendix C), and represents the maximum level of security that can be attained given the resource constraints. For example, the 2005 CSI/FBI computer crime and security survey show the percentage of IT budgets that were allocated to security. This figure varies from one organization to the other, and represents the dollars that Managers use to provide adequate security (CSI/FBI, 2005). The challenge is how to maximize security with the limited resources. This model will serve as an important tool to help managers make appropriate and efficient decisions on how to spend organizational dollars within the budget limits (resource constraints). The underlying principle is that organizations can trade off technology with human behaviors that prevent information security breaches. In this model, technology range from encryption, antivirus programs, firewalls, Intrusion detection system, biometrics, etc. The desired human behavior is facilitated through improved security policy and a good security education and awareness program.

Why trade off technology with human factors?

Technology is human driven. It's easy to buy security tool and employ it into the network after a short time and it will function as designed. But it's another thing to change behavior of employees and incorporate them into the system. It takes time, effort and training. Companies investing much in technology but less employee security training and awareness program discover that this is true. Technology alone can only provide a limited amount of security. Chapter one reviewed Gordon and Loeb's findings, which suggest that investment in information security may well be justified only for a midrange of information vulnerabilities. That is, little or no information security is

economically justified for extremely high, as well as extremely low, levels of vulnerability.

Calculating the monetary value of technology and human factors

The cost of technology is defined by factors such as the cost of buying, leasing technology or outsourcing security function. The major cost considerations in awareness, training, and education programs are:

- preparing, preparing and updating materials
- those providing the instruction
- employee time attending courses and lectures or watching videos
- outside courses and consultants (both of which may including travel expenses), including course maintenance

Assumptions of this model

- Resource endowment is fixed and finite.
- Level of technology is fixed
- Operate with fixed budget

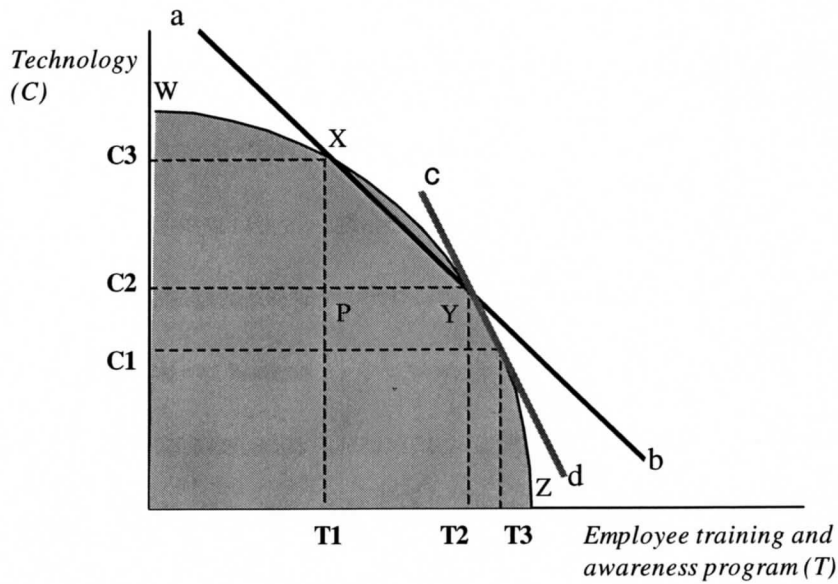


Figure 3. Secure Possibilities Model

Given the resource constraints as discussed above, a manager will not be able to achieve a security level beyond the curve “WXYZ”. On the contrary operating at any point inside the shaded region is inefficient because it will yield a low security. The manager must strive to operate at any point along the curve “WXYZ” in order to maximize security level using available resources. The movement along the curve “WXYZ” is based on the principle of tradeoffs, where the organization can increase the inputs from one resource by giving up some units of another input resource.

The slope of the SPM is equal to $\Delta C / \Delta T$ and is defined as the opportunity cost of *employee training and awareness program* (OC_T). Suppose that an organization begins by operating at point X on the SPM (refer to figure 3). Also suppose that at point X, T_1 is 5 units and C_3 is 40 units then the slope of the SPM is equal to 8.0 (C/T). This value represents the *opportunity cost of employee training and awareness program* meaning

that in order to invest one more unit of employee training and awareness program, 8 units of amount invested on technology must be given up.

The slope of segment XPY is represented by the tangent ab , and is calculated as the change in units invested on technology (C) divided by the change in units invested in employee training and awareness program (T) along the length of the segment XPY .

Suppose that at point Y, C_2 is 20 and T_2 is 7, then

$$\Delta C = C_3 - C_2 = 40 - 20 = 20 \text{ (C)}$$

$$\Delta T = T_2 - T_1 = 7 - 5 = 2 \text{ (T)}$$

$$\text{Slope of the tangent is } \Delta C / \Delta T = 20 / 2 = 10$$

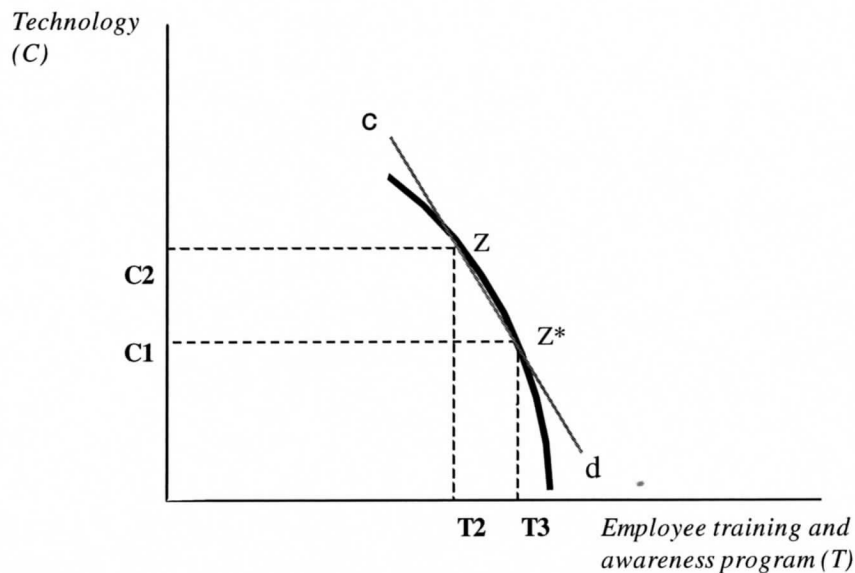


Figure 4. Effect of a unit increase in investment in employee training and awareness

The diagram above shows what would happen if there is a one unit increase in the amount invested in *employee training and awareness program*, starting at point Z to point Z*. The amount of dollars invested on *Technology* will reduce from C_2 to C_1 . The

amount of dollars ($C_2 - C_1$) freed from investments in *Technology* becomes the input to increase investment in *Employee training and awareness program* by one unit.

Table 4 (Appendix C) gives a comparison of performance and cost of different types of Intrusion Detection System – a security tool that is widely used by many organizations and individuals – Network World (2002). The scores are based on a scale of 1 to 5. Cost of Dragon IDS is \$15,000.00. Cost of Snort is \$0. Both IDS are average in performance hence one can be used as a substitute for the other. Suppose a company deploys Snort instead of Dragon?

$$\begin{aligned}\text{Then Savings} &= \text{Cost of Dragon} - \text{Cost of Snort} \\ &= \$15,000 - \$0 \\ &= \$15,000.\end{aligned}$$

From Figure 10 (Appendix C), assume a company with revenue of \$100 million to \$1 billion employs on average 1000 employees. Average security expenditure per employee is \$300.00. Savings from purchasing Snort would train $15,000/300 = 50$ additional employees.

CHAPTER 4

RESULTS AND DISCUSSIONS

Is training 50 additional employees on information security awareness an added value to an organization? The answer to this question can be found indirectly by looking at Table 5 (Appendix C), which show that *employee training and awareness* was the third most effective criteria for deterrence of security breaches behind regular security communication from management and new employee security training. The answer is yes; the organization is better off training the additional 50 employees by trading off Dragon IDS system for Snort.

Table 6 (Appendix C) show that the leading and most effective security tools currently used in the market are firewalls, antivirus scanners and encryption. The use of firewalls dropped slightly from 71 percent to 68 percent between 2003 and 2004. On the other hand, table 7 (Appendix C) show that viruses, spyware and phishing access are still the leading forms of attack, with viruses attacks increasing from 77 percent in 2003 to 82 percent in 2004. Probable explanation is that current security tools – firewalls, IDS, antivirus software alone, are not adequate to combat these attacks. Once again we see the effect that employee security education, training and awareness would have on maintaining an effective and economically sound security system. What is the implication of these findings? From an economic point of view and using the model developed here, an organization is better off by reducing spending on technology and diverting those extra dollars into employee security education, training and awareness program.

From the literature review, this thesis shows that the question “How much to invest in information security” is still puzzling many information security economist. Gordon has suggested that within the range of justifiable investments in information security, the maximum amount a risk-neutral firm should spend is only a fraction, which should never exceed 37% of the expected loss due to security breaches. Hoo S.K. suggested that the optimal solution for managing computer security risks called for very minimal security measures. This argument has been found deficient because it creates the impression that very little input is required to safeguard information security. Schnieier’s paper suggests that motivation plays a crucial role in the development of security. He adds that most organizations don’t spend a lot of money on network security because the cost of installing security is higher than not having one. This argument does not hold considering the increasing and sophisticated level of attacks and other security breaches.

Organizations and commercial institutions have detected and continue to experience security breaches inspite of the several technologies currently in the market. In 2004 reported financial losses as a result of the attacks was quantified as over US\$455 million, according to a nationwide computer security survey by Computer security Institute (CSI) and the FBI. Organizations have continued to experience attacks from viruses, hackers and insider abuse despite the deployment of technologies such as firewalls, intrusion detection systems as well as developing employee training and awareness program.

Barriers to good security appear to be diminishing slightly according to a study conducted by Ware L.C. of CIO magazine. The study found out that the top barriers to security this year are limited budget (57% this year vs. 64% in 2003), limited staff

dedicated to security (44% vs. 39% in 2003), limited or no time to focus on security (34% vs. 47% in 2003), limited or no security training/awareness (24% vs. 32% in 2003) and complex technology infrastructure (24% vs. 27% in 2003.) Also dropping in importance in terms of barriers, limited support from executives dropped from 27 percent to 20 percent in this year's study, and limited intra-department cooperation dropped from 24 percent in 2003 to 11 percent this year. This study also suggests that government regulations and potential liability continue to be the biggest factor driving security investments, indicating that in addition to IT investments in security, security spending may be occurring in departments other than IT such as finance in order to comply with Sarbanes Oxley act, for example.

From the review, it's become clear that technical computer security measures such as use of passwords, biometrics, antivirus software, firewalls and intrusion detection systems alone cannot totally reduce an organization's risk of computer breaches. As technology improves, the hackers become wiser in their designs and viruses become more lethal. This is why Whiteman emphasizes the need for an organization to develop an elaborate, effective and efficient employee education, training and awareness program. Whiteman argues that the human factor is the driving force behind the technologies employed to reduce the risk of computer security breaches. In short, Whiteman is saying that you don't emphasize importance of technology software without emphasizing importance of the human factor that drives it. Statistics have clearly shown that various respondents cited employee training and awareness program as contributing to deterrence of security breaches in many organizations. The high percentage of insider abuse cited by many respondents in the organizations surveyed probably suggest that inadequate

employee training and awareness may play a role. What does this conclusion lead us to? I suggest and develop an economic model that will hopefully help security decision makers develop an efficient security system that uses both technology and human factors at minimal cost.

The Secure Possibilities Model developed in this paper shows how economics principles can be used to develop an efficient and economically sound information security system. One major draw back about this model is the inability to quantify in dollar amounts what organizations invest in technology and employee education, training and awareness program. Analysis done however, strongly point to the fact that an efficient information security system will require both the deployment of technology as well as a good employee education, training and awareness program.

CHAPTER 5

CONCLUSION

Using technology tools alone such as use of passwords, encryption, biometrics, anti-virus software and intrusion detection systems, cannot completely eliminate an organization's risk of computer security breaches and the associated financial losses. Organizations should therefore turn to other alternative methods such as putting in place an effective and efficient policy and procedures- in this case an employee education, training and awareness program, to reduce security breaches that are likely to occur even after technical security measures have been instituted. For this reason, this thesis has developed a model- Secure Possibilities Model (SPM), which will help organizations to implement an effective and efficient security system that creates a balance between the technology tools employed and the policy and procedures through employee training and awareness program. The Secure Possibilities Model developed in this paper shows how economics principles can be used to develop an efficient and economically sound information security system.

REFERENCES

- Computer Security Institute, (2005). 2005 CSI/FBI computer crime and security survey. Retrieved May 15, 2005, from <http://www.gocsi.com/;jsessionid=YNSLJPL5OVJOGQSNDBGCKHSCJUMEKJVN>
- E-Watch Crime, (n.d.). 2005 e-watch crime survey. Retrieved July 20, 2005, from <http://www.itu.int/osg/spu/newslog/2005+ECrimeWatch+Survey+Summary+Of+Findings+.aspx..>
- Anonymous. (2002). *Gigabit IDS test results* (November 4, 2002). Network World. Retrieved on October 20, 2005, from <http://www.networkworld.com/review/2002/1104revnetr.html>
- Anonymous. (n.d.). An Introduction to Computer Security: The NIST Handbook Special publication 800-12. Retrieved May 20, 2005, from <http://csrc.nist.gov/publications/nistpubs/800-12/NIST-SP800-12.pdf>
- Anderson, R and Schneier, B. Economics of Information Security. Retrieved May 15, 2005, from <http://www.infosecon.net/workshop/index.html>.
- Berns, J. and Neclerio, T. (2003). Information Security and GLB Compliance for Community Banks. Western Banking Magazine. Retrieved August 10, 2005, from http://www.wib.org/wb_articles/fraud_aug03/info_sec_aug03.htm
- Black, Ted. (2002). The Economics Net-Textbook 2002. Retrieved June 20, 2005, from <http://nova.umuc.edu/~black/pageg.html>
- Federal Information Security Management Act (FISMA): 2004 Report to Congress (2005, Mar. 1). Retrieved on July 20, 2005, from <http://www.gao.gov/new.items/d05552.pdf>
- Gal-Or, E., A. Ghose. (2005). The Economic Incentives for Sharing Security Information. Information Systems Research 16(2), 186-208. Retrieved June 12, 2005, from http://www.cpppe.umd.edu/rhsmith3/papers/Final_session7_galor.ghose.pdf
- Gordon, LA & Loeb, MP 2002, 'The Economics of Information Security Investment', ACM Transactions on Information and System Security, vol. 5, no. 4, pp. ... Retrieved on July 20, 2005, from <http://www.geocities.com/amz/>

- Palmer, M. (2005, Nov 1). It security goes by the board. *Financial Times*, Retrieved Nov 3, 2005, from <http://news.ft.com/cms/s/b2568c1e-4b25-11da-aadc-0000779e2340.html>..
- Phelps, D. C. (2005). Information system security: self-efficacy and security effectiveness in Florida libraries. Ph.D. Dissertation. . Retrieved Aug. 21, 2005, from <http://etd.lib.fsu.edu/theses/available/etd-02082005-035903/unrestricted/dissertation.pdf>..
- Schnieier, B, "No, we don't spend enough!" In proceedings of the Workshop on Economics and Information Security University of California, Berkeley May 2002
- Soo Hoo Kevin, J, "How Much Is Enough? A Risk Management Approach to Computer," from <http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/>
- Stuart E. Schechter, "Computer Security Strength & Risk: A Quantitative Approach", Ph.D. Thesis, Harvard University, May 2004.
- Stuart E. Schechter, "Toward Econometric Models of the Security Risk" from Remote Attacks", *IEEE Security & Privacy Magazine*, vol 3(1), 2005. pp. 40- 44
- Keizzer Greg, "Cyber Crime Rates, Losses Fall, Says Survey" *InternetWeek*. Retrieved November 1, 2005, from <http://www.internetweek.com/165702566?cid=RSSfeed>
- Whitman, M. E. (2003). Enemy at the gate: threats to information security *Communications of the ACM*, 46(8), 91 - 95. Retrieved Dec 16, 2005, from <http://portal.acm.org/citation.cfm?id=859670.859675>

APPENDIX A – PROJECT PLAN DOCUMENTATION



MSIS Project Plan Approval Form (Form #2)

Important: Your project plan must be reviewed and approved by your project supervisor before you can register for the implementation course. (See Project Guidelines on grad office website - current students link for detailed description of requirements)

Student Name: Solomon Omondi Ogara

Expected Graduation Date: December 2005

Committee:

Faculty Project Supervisor: _____ Prof: Christoph Rick

Committee member: _____ Prof: Zhou Zehai

Committee member: _____ Prof: Wayne Pauli

Master's Project Title: Economics of Information Security – Developing a model for information security cost minimization

Description of Project: 100-word summary of your formal plan. You may attach additional pages to this form. The signed approval form with additional pages should be attached as first page of your formal plan. Be sure to include:

1. Introduction (very brief overview of what you proposing to do and why you are doing it.)
2. Statement of problem or question you have identified and brief summary of current situation (literature search)
3. Goals, objectives, purpose (what you plan to achieve - desired outcome of this project)
4. Scope of Work, Plan of Action, Activities (how you plan to achieve the objectives, the specific activities you will undertake)
5. Work Breakdown Structure (WBS) and Gantt chart.
6. Deliverables (what you will actually have once you have completed your project, e.g., a database, a website, a program, etc.)

DO NOT WRITE THE DESCRIPTION HERE. ATTACH WORD-PROCESSED DOCUMENT

Students must bring the original form to the Graduate Programs Office. Graduate Office personnel will make copies and return them to your project supervisor and the MSIS Program Coordinator. You should retain a copy for your files.

Approvals/Signatures:

Student: _____

Date: _____

Faculty supervisor: _____

Date: _____

Committee member: _____

Date: _____

Committee member: _____

Date: _____

Copies to: Original to Graduate Office; copies to: Advisor, Program Coordinator, and Student

Introduction

The purpose of this thesis is to derive an economic model that determines the optimal amount to invest in information security by trading off between spending/Cost of security and behavioral aspects that reduce information security. This model relates to protecting the confidentiality, authenticity and integrity of information (CAI). First we show that for a given potential loss and a given threat level, the optimal amount to spend on such security is an increasing function of the information's vulnerability but only up to a certain optimum level. Next we use the production possibility curve to derive our model, which will be called **secure possibilities model**. This model relates to the concept of the production possibilities frontier -- a standard macroeconomic model in which a country can produce two goods -- food and cloths - and faces a trade-off between the amount of one good that can be produced and the amount of the other good that can be produced (Black, 2002). It's on this basis that this model will be developed.

Statement Of Problem.

In this model an organization is assumed to have a finite level of security and must choose to trade off between behavioral aspects of reducing information security breaches and spending. Related research include protecting information through encryption, access control, and firewalls - Muralidhar et al. (1995), Denning and Branstad (1996), Sandhu et al. (1996), Schnieier (1996), Pfleeger (1997), Larsen (1999), Peyravian et al. (1999), and Osborn et al. (2000) . Research on behavioral aspects of reducing information security breaches - Straub (1990), Loch et al. (1992), and Straub and Welke (1998). Research on intrusion detection systems include - Daniels and Spafford (1999), Vigna and Kemmerer (1999), Axelsson (2000), and Frincke (2000). The arguments in this thesis will be

supported by a number of these literatures but the approach used to develop this model is what makes the difference.

Objectives of this thesis

Organizations aim to maximize profit but at the same time most of them are spending much on security. Organizations also possess limited resources. This thesis will develop a model that provides managers with a framework for making decisions regarding the allocation of scarce information security dollars. This model uncovers an area that is often given less weight i.e. behavioral aspects of reducing information breaches. An improvement in the way that customers and employees handle the confidentiality, integrity and authenticity of information will lead to lesser spending on technology.

Scope of work/ Work Plan

Details of the work plan are covered in the Gantt chart

1. Project planning and design
 - 1.1 Choose a topic? Thesis title
 - 1.2 Identify problem
 - 1.3 Complete project idea form
 - 1.4 Form a committee
 - 1.5 Literature review
 - 1.6 Develop written plan
 - 1.7 Get approval of proposal plan
 - 1.8 Analysis
 - 1.9 Design a model
2. Project Implementation
 - 2.1 Register for course
 - 2.2 Write draft / Review draft
 - 2.3 Write final report
 - 2.4 Other activities
3. Project Presentation

Work Breakdown Structure/Gantt Chart

See appendix B

Deliverables

An economic model called Secure Possibilities Model (SPM), which will help organizations to minimize spending on security by trading off between behavioral aspects that reduce information security and high spending on technology.
Project report.

APPENDIX B – WORK BREAKDOWN STRUCTURE AND GANTT CHART

Work Breakdown Structure

Project Start Date: 5/6/05

Project Finish Date: 12/06/05

| No | Task Name | Duration | Start | Finish | % Work Complete |
|----|--|----------|----------|----------|-----------------|
| 1 | Project Planning and Design | 120 days | 5/6/05 | 08/30/05 | 100 |
| | Choose ideal Topic | 4 days | 5/9/05 | 5/13/05 | 100 |
| | Complete Project Idea Form | 2 days | 5/13/05 | 5/15/05 | 100 |
| | Form a committee | 6 days | 5/16/05 | 5/22/05 | 100 |
| | Literature Review/Research | 93 days | 5/6/05 | 8/15/05 | 100 |
| | Develop WBS (Work Breakdown Structure) | 2 days | 8/10/05 | 8/12/05 | 100 |
| | Develop a Gantt Chart | 1 day | 8/15/05 | 8/16/05 | 100 |
| | Develop a written plan summary | 3 days | 8/17/05 | 8/20/05 | 100 |
| | Complete planning – Get Proposal Plan approved | 3 days | 8/23/05 | 8/26/05 | 100 |
| | Analysis | 7 days | 9/3/05 | 9/11/05 | 100 |
| | Design a model | 2 days | | | 100 |
| 2 | Project Implementation | 80 days | 9/3/05 | 12/2/05 | 100 |
| | Review the model | 6 days | 9/13/05 | 9/20/05 | 100 |
| | Write a draft report | 25 days | 9/19/05 | 10/21/05 | 100 |
| | Compile feedback | 2 days | 10/27/05 | 10/28/05 | 100 |
| | Write final report | 15 days | 11/3/05 | 11/21/05 | 100 |
| | Miscellaneous activities | 7 days | 11/25/05 | 12/06/05 | 100 |
| 3 | Project presentation | 1 day | TBA | TBA | |

Table 1: Work Breakdown Structure.

Gantt Chart

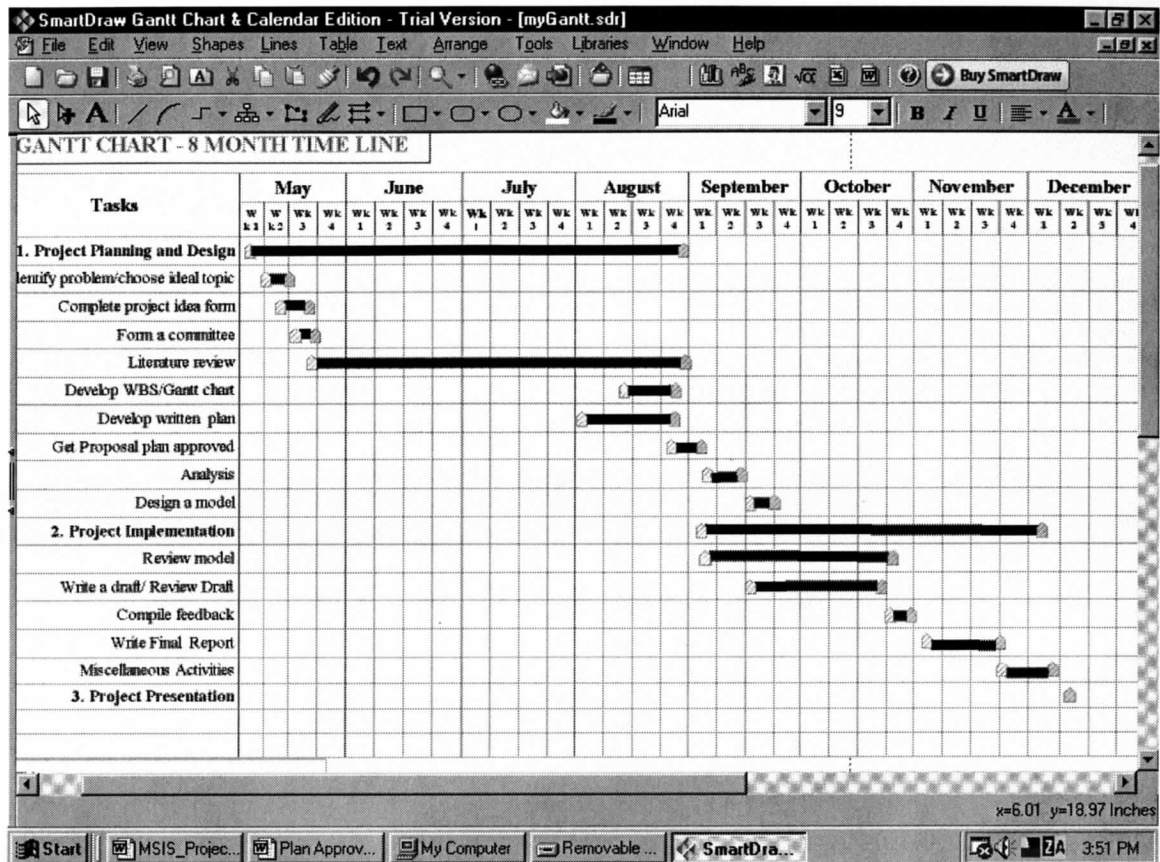


Figure 5: Gantt chart.

APPENDIX C – INTRODUCTION TO PRODUCTION POSSIBILITY FRONTIER MODEL

The Production Possibility Frontier (PPF) is a tool used to illustrate the principle of “opportunity cost”. According to Black, PPF is a stylized model of a macro economy that is presented to examine the production decisions in the economy and the problem of scarcity. The purpose is to show how scarce resources may be allocated to produce alternative products, and the associated trade offs that arise when there is a change in the mix of production (Black, 2002).

Assumptions of PPF

- Resource endowment is fixed and finite (including all inputs to production).
- Level of technology is fixed
- Economy operates at full employment
- No other products or money are available.

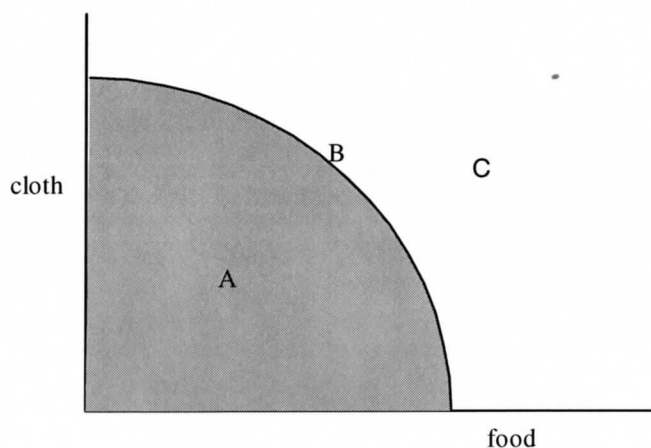


Figure 6: Production Possibilities Frontier (Black, 2002)

The PPF shows all the combinations of the two goods (food and cloth) that could be produced by the economy if resources are efficiently utilized.

Point A below the PPF is feasible but inefficient.

Point B along the PPF shows the maximum output of the economy.

Point C beyond the PPF is not attainable given the resource constraints

APPENDIX D – COMPARISON OF EMPLOYEE EDUCATION, TRAINING AND AWARENESS.

Employee security training and awareness program Purpose

- improving awareness of the need to protect system resources;
- developing skills and knowledge so computer users can perform their jobs more securely; and
- building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Benefits of awareness, training, and education,

- improving employee behavior and
- increasing the ability to hold employees accountable for their actions.

Comparison of awareness, training and education

| | AWARENESS | TRAINING | EDUCATION |
|--------------------------|--|---|--|
| Attribute: | "What" | "How" | "Why" |
| Level: | Information | Knowledge | Insight |
| Objective: | Recognition | Skill | Understanding |
| Teaching Method: | <u>Media</u> - Videos -Newsletters -Posters, etc. | <u>Practical Instruction</u> - Lecture - Case study workshop - Hands-on practice | <u>Theoretical Instruction</u> - Discussion Seminar - Background reading |
| Test Measure: | True/False Multiple Choice (identify learning) | Problem Solving (apply learning) | Eassay (interpret learning) |
| Impact Timeframe: | Short-term | Intermediate | Long-term |

Table 2: Comparing awareness, training and education (NIST handbook 2002)

Awareness

Awareness stimulates and motivates those being trained to care about security and to remind them of important security practices. Explaining what happens to an organization, its mission, customers, and employees if security fails motivates people to take security seriously. Security *awareness* programs:

- set the stage for *training* by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; and
- remind users of the procedures to be followed.

Awareness is used to reinforce the fact that security supports the mission of the organization by protecting valuable resources. If employees view security as just bothersome rules and procedures, they are more likely to ignore them. In addition, they may not make needed suggestions about improving security nor recognize and report security threats and vulnerabilities. Awareness also is used to remind people of basic security practices, such as logging off a computer system or locking doors.

Training

The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. This includes teaching people *what* they should do and *how* they should (or can) do it. Training can address many levels, from basic security practices to more advanced or specialized skills. It can be specific to one computer system or generic enough to address all systems. Training is most effective when targeted to a specific audience. This enables the training to focus on security-related job skills and knowledge that people need performing their duties. Two types of audiences are general users and those who require specialized or advanced skills.

General Users. Most users need to understand good computer security practices, such as: protecting the physical area and equipment (e.g., locking doors, caring for floppy diskettes); protecting passwords (if used) or other authentication data or tokens (e.g., never divulge PINs); and reporting security violations or incidents (e.g., whom to call if a virus is suspected). In addition, general users should be taught the organization's policies for protecting information and computer systems and the roles and responsibilities of various organizational units with which they may have to interact.

Education

Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require *expertise* in security.

Techniques. Security education is normally outside the scope of most organization awareness and training programs. It is more appropriately a part of *employee career development*. Security education is obtained through college or graduate classes or through specialized training. Because of this, most computer security programs focus primarily on awareness and training.

APPENDIX E – MORE FIGURES AND TABLES

| What was your organization's approximate annual budget for information and corporate/physical security products, systems, services and/or staff in 2004? | IT Security Spending* (base: 819) |
|--|-----------------------------------|
| Over \$100 Million | 4% |
| \$10 Million - \$99.9 Million | 5% |
| \$1 Million - \$9.9 Million | 15% |
| \$500,000 - \$999,999 | 4% |
| \$250,000 - \$499,999 | 5% |
| \$100,000 - \$249,999 | 10% |
| \$50,000 - \$99,999 | 9% |
| Less than \$50,000 | 18% |
| Don't know | 30% |

Table 3: Annual budget for information security. Source: 2005 e-Crime Watch survey report

| | Dragon IDS Suite | SecureNet 7145C | IntruShield 4000 | RealSecure | Snort | ManHunt |
|-----------------------------------|------------------|-----------------|------------------|------------|--------------------|------------|
| Performance 45% | 2 | 2 | 4 | 4 | 2 | 3 |
| Management and administration 25% | 3 | 4 | 4 | 4 | 2 | 3 |
| Features 20% | 3 | 3 | 5 | 3 | 2 | 4 |
| Configuration 10% | 3 | 3 | 5 | 3 | 3 | 3 |
| TOTAL SCORE | 2.6 | 2.8 | 4.3 | 3.7 | 2.1 | 3.2 |
| Approximate Cost | \$15,000 | \$17,000 | \$100,000 | \$25,000 | Free (Open source) | \$50,000 |

Table 4: Comparing performance and cost of different IDS. Source: Network World (2002).

| <i>Disposition of policies/procedures (base: total responding with policy/procedure in place)</i> | In Use | Deterrence | Detection | Termination | Prosecution | Don't know |
|---|--------|------------|-----------|-------------|-------------|------------|
| Account/password management policies | 74% | 72% | 27% | 6% | 4% | 18% |
| Conduct regular security audits | 57% | 51% | 51% | 17% | 7% | 18% |
| Corporate security policy | 62% | 69% | 20% | 27% | 10% | 17% |
| Employee education & awareness programs | 67% | 78% | 17% | 7% | 3% | 16% |
| Employee monitoring | 42% | 57% | 50% | 37% | 11% | 12% |
| Employee/contractor background examinations | 48% | 60% | 30% | 16% | 3% | 24% |
| Formal inappropriate use policy | 71% | 70% | 19% | 32% | 6% | 13% |
| Government security clearances | 22% | 58% | 20% | 8% | 4% | 29% |
| Hired a CSO or CISO | 24% | 67% | 38% | 16% | 13% | 24% |
| Include security in contract negotiations with vendors/suppliers | 34% | 72% | 17% | 11% | 5% | 20% |
| Mandatory internal reporting to management of misuse or abuse by employees & contractors | 35% | 66% | 39% | 32% | 10% | 14% |
| Monitor Internet connections | 65% | 52% | 56% | 31% | 6% | 15% |
| New employee security training | 46% | 80% | 9% | 9% | 3% | 16% |
| Periodic risk assessments | 55% | 51% | 43% | 5% | 2% | 22% |
| Periodic systems penetration testing | 44% | 48% | 50% | 5% | 2% | 20% |
| Random security audits | 40% | 61% | 52% | 14% | 5% | 14% |
| Regular security communication from management | 33% | 80% | 11% | 2% | 2% | 16% |
| Require employees/contractors to sign acceptable use policies | 59% | 74% | 14% | 24% | 7% | 19% |
| Segregation of duties | 43% | 73% | 28% | 7% | 3% | 17% |
| Storage & review of e-mail or computer files | 30% | 56% | 48% | 34% | 12% | 18% |
| Use of "white hat" hackers | 14% | 46% | 59% | 3% | 7% | 15% |
| Use of incident response team | 34% | 42% | 49% | 22% | 15% | 19% |

Table 5: Disposition of policies and procedures Source: 2005 e-Crime Watch survey

| Which of the following electronic crimes were committed against your organization in 2004? (base: among those experiencing electronic crimes) | 2005 (base: 554) | 2004* (base: 342) |
|---|---------------------|----------------------|
| Virus or other malicious code | 82% | 77% |
| Spyware | 61% | N/A |
| Phishing | 57% | 31% |
| Illegal generation of spam email | 48% | 38% |
| Unauthorized access to information, systems or networks | 43% | 47% |
| Denial of service attacks | 32% | 44% |
| Rogue wireless access point | 21% | N/A |
| Exposure of private or sensitive information | 19% | N/A |
| Fraud | 19% | 22% |
| (2004: Employee) Identity theft | 17% | 12% |
| Password sniffing | 16% | N/A |
| Theft of intellectual property | 14% | 20% |
| Zombie machines on organization's network | 13% | N/A |
| Theft of other (proprietary) info | 12% | 16% |
| Sabotage | 11% | 18% |
| Web site defacement | 9% | N/A |
| Extortion | 2% | 5% |
| Other | 4% | 11% |
| Don't know/not sure | 3% | 8% |

Table 6: Types of e-crimes Source: 2005 e-Crime Watch survey

| Most Effective (Extremely or Very Effective) Technologies in Use (2005 base: among those with technology in use at organization) | 2005 | 2004 |
|---|------|------|
| Firewalls (base: 810) | 68% | 71% |
| Automated virus scanning (base: 810) | 66% | N/A |
| Encryption (base: 715) | 58% | N/A |
| Two-factor authentication (base: 517) | 56% | 56% |
| Intrusion detection systems (base: 743) | 50% | N/A |
| Physical security systems (base: 771) | 49% | 48% |
| Network traffic monitoring/network based forensic tools (base: 722) | 46% | N/A |
| Spyware/adware detection software (base: 758) | 43% | N/A |
| Role-based access control (base: 677) | 42% | 44% |
| Automated patch management (base: 704) | 40% | 39% |
| Configuration management/periodic checks for non-baseline files to detect Trojan horses, logic bombs, etc. (base: 704) | 39% | N/A |
| Technologies tracking access & use of corporate data/information assurance technologies (base: 682)—2004: that track the access & use of corporate data | 35% | 35% |
| Anti-fraud technologies working with ERP/accounts payable & billing systems (base: 560) | 28% | 33% |
| Wireless monitoring (base: 544) | 26% | 26% |
| Keystroke monitoring of individual users (base: 434) | 22% | 24% |
| Manual patch management (base: 741) | 21% | 26% |

Table 7: Most effective technologies used Source: 2005 e-Crime Watch Report

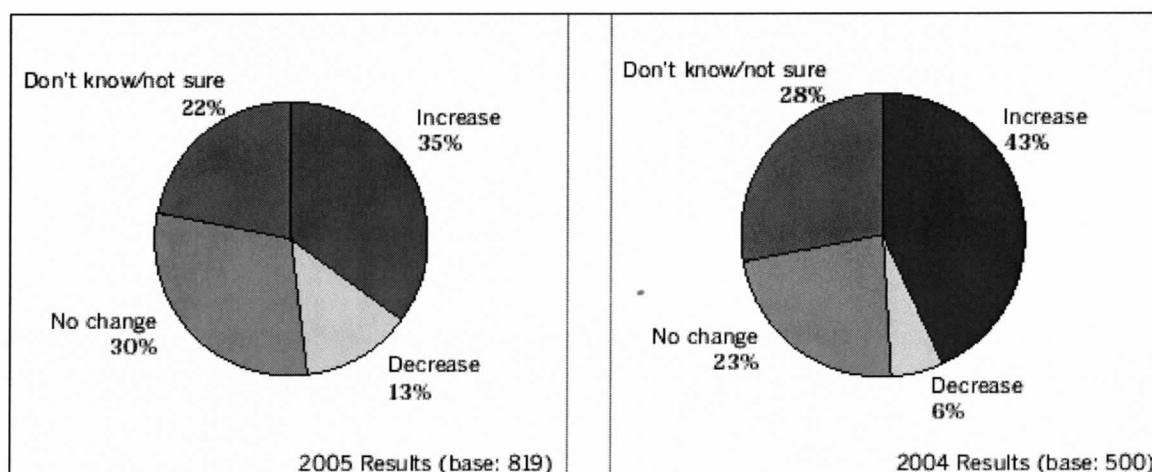


Figure 7: Comparison increase in total number of e-crimes and intrusions 2003 and 2004. Source: 2005 e-Crime Watch Survey.

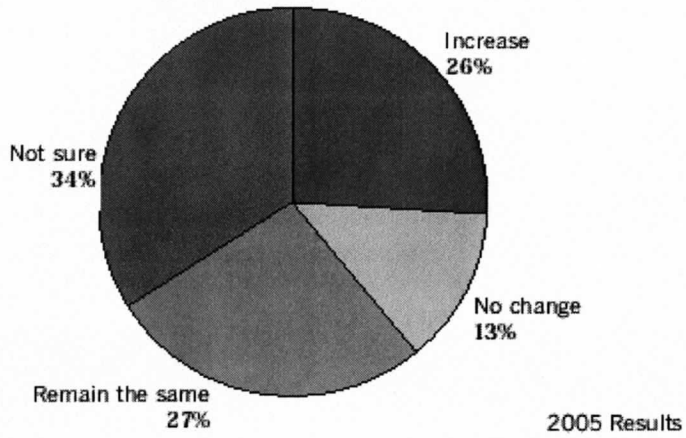


Figure 8: Expected change in monetary losses for 2005 Source: 2005 e-Crime Watch Survey

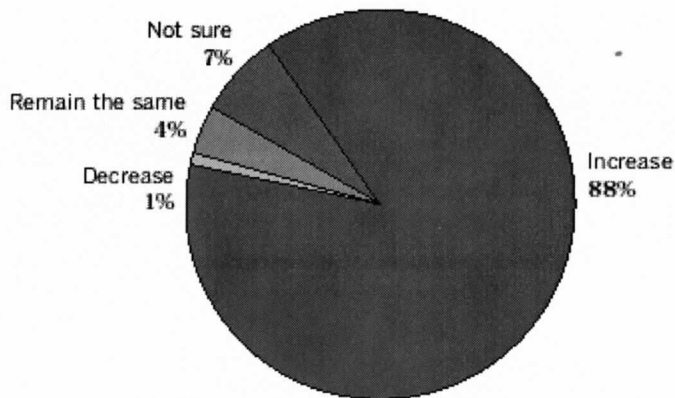


Figure 9: Prevalence of e-Crime Source: 2005 e-Crime Watch Report

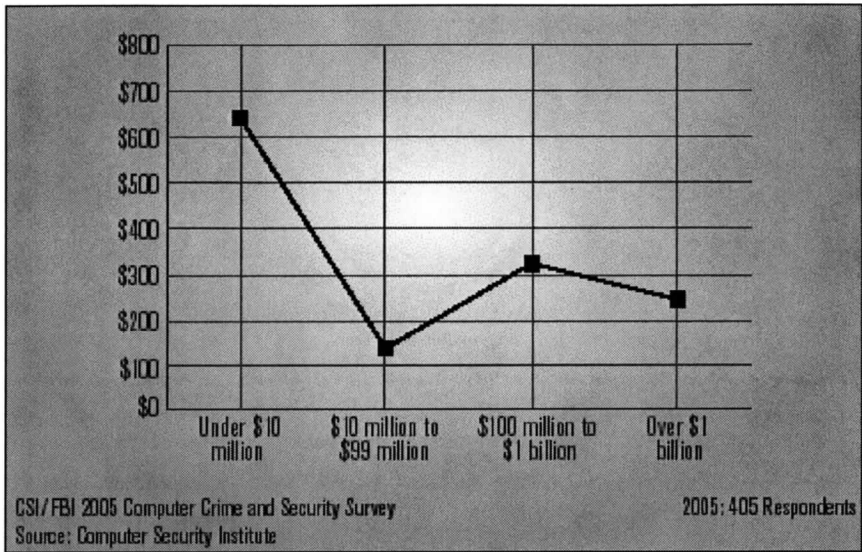


Figure 10: Average computer security expenditure per employee. Source: Computer Security Institute (2005).

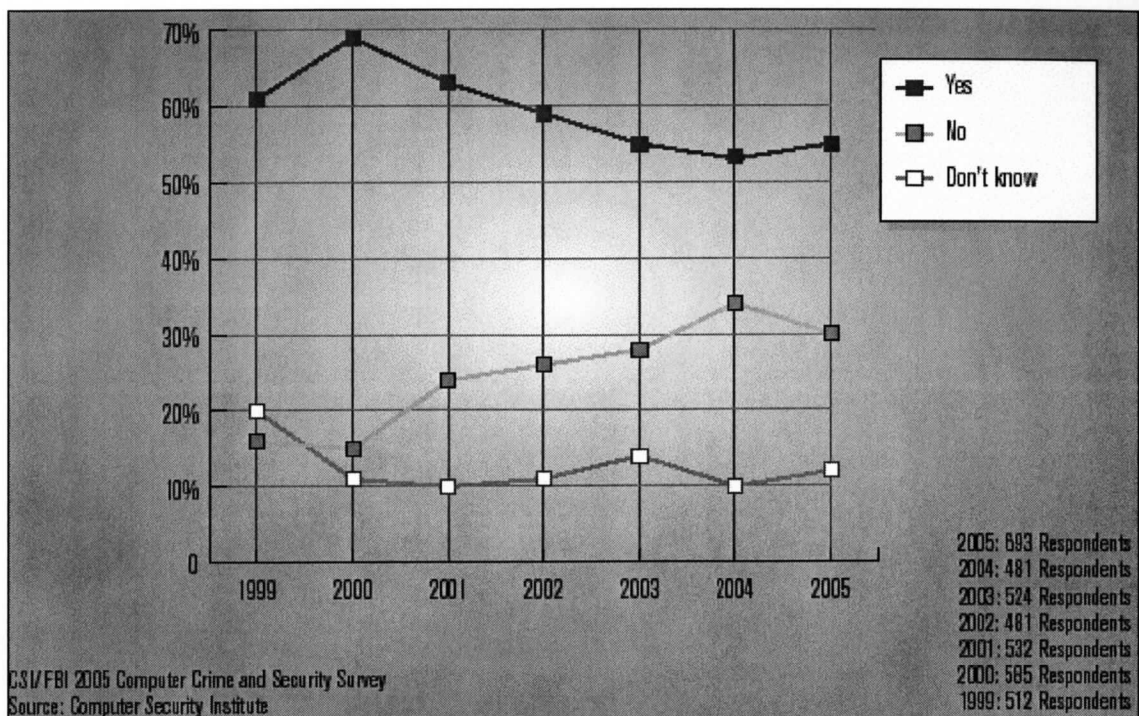


Figure 11: Unauthorized use of computer systems within last 12 months Source: Computer Security Institute (2005).

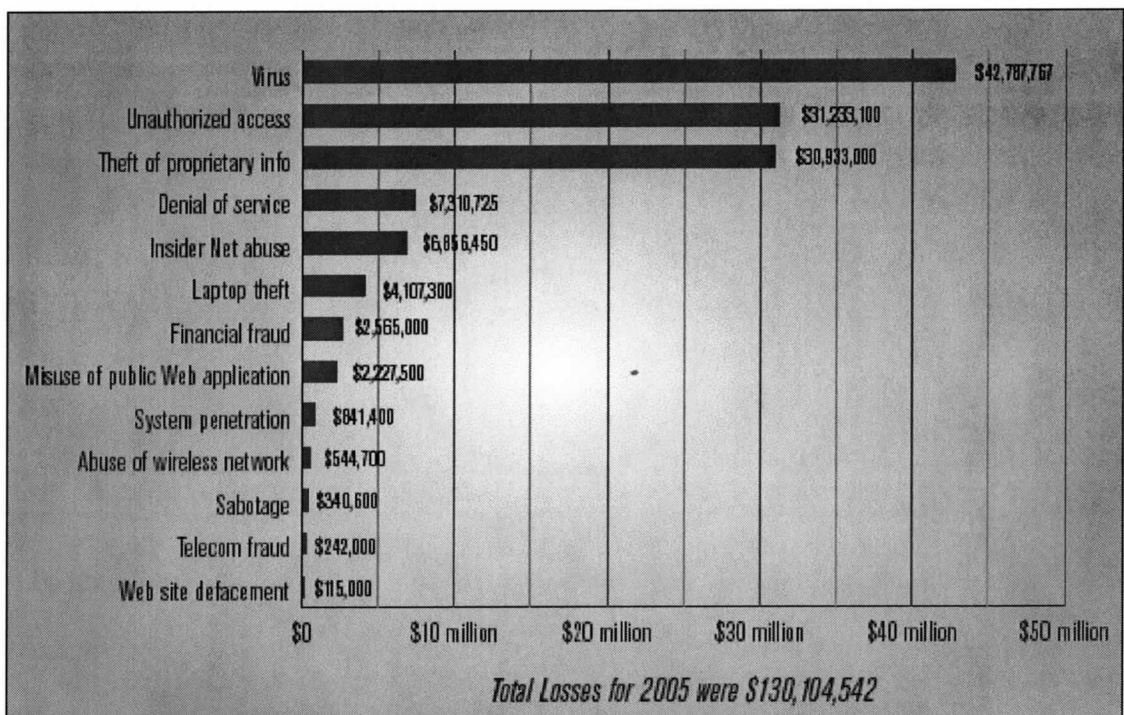


Figure 12: Dollar amount losses by type Source: Computer Security Institute (2005)

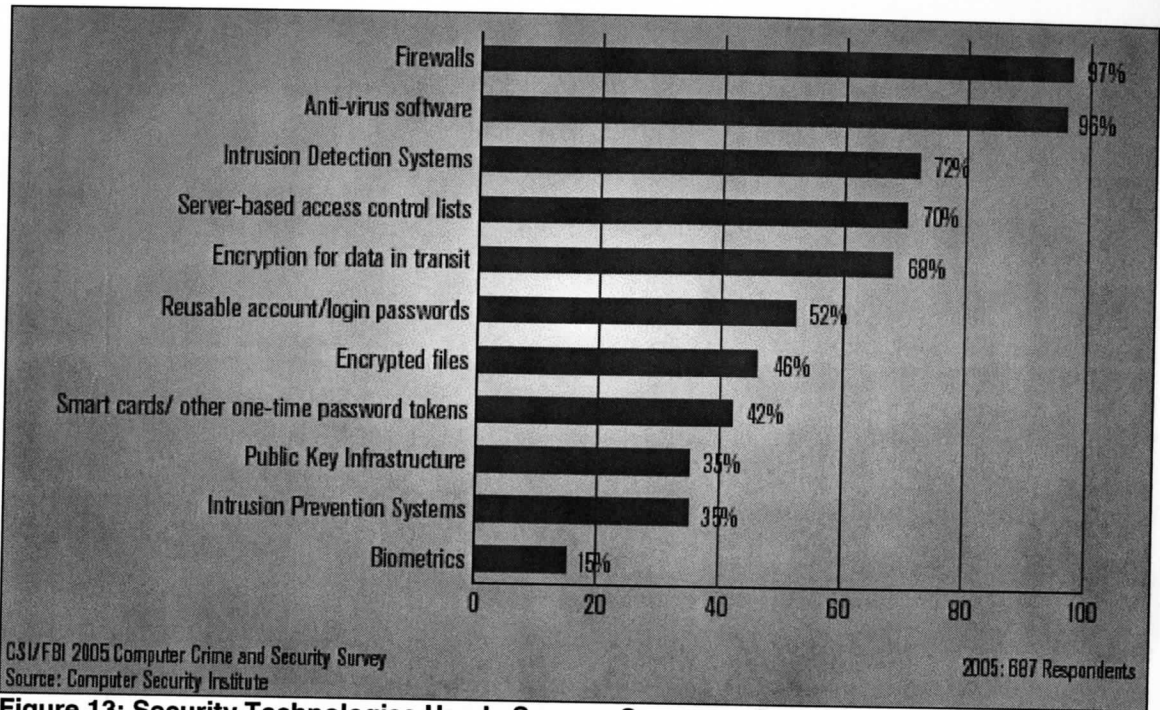


Figure 13: Security Technologies Used Source: Computer Security Institute (2005)