



# **Calhoun: The NPS Institutional Archive**

# **DSpace Repository**

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2007-03

# Risk of cyberterrorism to naval ships inport Naval Station Everett a model based project utilizing SIAM

Tester, Rodrick A.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/3574

Downloaded from NPS Archive: Calhoun



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

> Dudley Knox Library / Naval Postgraduate School 411 Dyer Road / 1 University Circle Monterey, California USA 93943

http://www.nps.edu/library



# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA** 

# THESIS

# RISK OF CYBERTERRORISM TO NAVAL SHIPS INPORT NAVAL STATION EVERETT: A MODEL BASED PROJECT UTILIZING SIAM

by

Rodrick "Rick" A. Tester

March 2007

Thesis Advisor: Second Reader: Dorothy Denning Steve Iatrou

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE		Form Approved	l OMB No. 0704-0188		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.					
1. AGENCY USE ONLY (Leave l	blank)	<b>2. REPORT DATE</b> March 2007	3. RE	PORT TYPE AN Master	ND DATES COVERED r's Thesis
4. TITLE AND SUBTITLE Risk Station Everett: A Model Based Pr	of Cyber Attack	to Naval Ships Inport N	aval	5. FUNDING N	NUMBERS
6. AUTHOR(S) LT Rodrick A. Te	ester, USN				
<ul> <li>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000</li> </ul>			8. PERFORMI REPORT NUM	NG ORGANIZATION /IBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSOR AGENCY R	ING/MONITORING EPORT NUMBER	
<b>11. SUPPLEMENTARY NOTES</b> or position of the Department of De	The views expr efense or the U.S.	essed in this thesis are a Government.	hose of the	e author and do no	ot reflect the official policy
<b>12a. DISTRIBUTION / AVAILA</b> Approved for public release; distrib	BILITY STATE oution is unlimited	C <b>MENT</b> d		12b. DISTRIB	UTION CODE A
13. ABSTRACT (maximum 200 words) Based on numerous high level concerns that the cyber threat is expected to increase, as well as the already documented uses of cyber warfare, it is necessary to ensure our naval ships are hardened against such attacks. In doing so, an influence net model was designed to discover the likelihood of a successful cyber attack. However, first it was necessary to establish what the best mitigation tools are in defense of cyber attack methods. In order to do so, an expert opinion survey was designed and completed by individuals currently working in the field of network security. In combination with the expert opinion surveys and in looking at research and established security techniques it should become apparent whether or not ships are taking all the required steps to best secure themselves against an attack. Though the initial model was designed around a theoretical Naval Station Everett ship, with modification the model can be utilized for any naval asset throughout the United States and the risk for each particular U.S. asset can be evaluated. Additionally, this tool can also facilitate security funding as well as establishing a means of prioritizing the tools for protection if the network needs to be hastily re-established after an attack. Ultimately, the protection of a ship's computer networks against cyber terrorist threats is fundamental in ensuring continued effective command and control and ultimately the security of this nation.					
<b>14. SUBJECT TERMS</b> Cyberterrorism, information assurat Assessment Module (SIAM)	nce, computer see	curity, influence net mo	del, Situatio	onal Influence	15. NUMBER OF PAGES 95
					16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICAT PAGE Unc	TION OF THIS	19. SECUI CLASSIFI ABSTRAC Unc	RITY ICATION OF CT classified	20. LIMITATION OF ABSTRACT UL

Prescribed by ANSI Std. 239-18

#### Approved for public release; distribution is unlimited.

#### RISK OF CYBER ATTACK TO NAVAL SHIPS INPORT NAVAL STATION EVERETT: A MODEL BASED PROJECT UTILIZING SIAM

Rodrick A. Tester Lieutenant, United States Navy B.A., University of Minnesota, 2000

Submitted in partial fulfillment of the requirements for the degree of

#### MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

### NAVAL POSTGRADUATE SCHOOL March 2007

Author: LT Rodrick A. Tester, U.S. Navy

Approved by:

Dr. Dorothy Denning Thesis Advisor

Mr. Steven Iatrou Second Reader

Dr. Dan Boger Chairman, Department of Information Sciences

### ABSTRACT

Based on numerous high level concerns that the cyber threat is expected to increase, as well as the already documented uses of cyber warfare, it is necessary to ensure our naval ships are hardened against such attacks. In doing so, an influence net model was designed to discover the likelihood of a successful cyber attack. However, first it was necessary to establish what the best mitigation tools are in defense of cyber attack methods. In order to do so, an expert opinion survey was designed and completed by individuals currently working in the field of network security. In combination with the expert opinion surveys and in looking at research and established security techniques it should become apparent whether or not ships are taking all the required steps to best secure themselves against an attack.

Though the initial model was designed around a theoretical Naval Station Everett ship, with modification the model can be utilized for any naval asset throughout the United States and the risk for each particular U.S. asset can be evaluated. Additionally, this tool can also facilitate security funding as well as establishing a means of prioritizing the tools for protection if the network needs to be hastily re-established after an attack. Ultimately, the protection of a ship's computer networks against cyber terrorist threats is fundamental in ensuring continued effective command and control and ultimately the security of this nation.

# TABLE OF CONTENTS

I.	INT	ODUCTION	1
	А.	BACKGROUND AND MOTIVATION BEHIND THE RESEARCH	1
	В.	GENERAL SCOPE OF THE THESIS	3
	C.	BRIEF EXPLANATION OF METHODOLOGY	3
	D.	BENEFITS OF STUDY	4
	Е.	THESIS STRUCTURE:	4
п	BAC	KGROUND INFORMATION	7
11.	Δ	INTRODUCTION TO INFORMATION OPERATIONS	7
	B	INFORMATION ASSURANCE	,
	Б.	1 Availability	8
		2. Integrity	8
		3. Authentication	
		4. Confidentiality	
		5. Non-repudiation	
	C.	CYBER THREATS AND THEIR MOTIVES	
	с.	1. Insiders	
		2. Hackers	9
		3. Criminals	.10
		4. Corporations	.10
		5. Government Agencies	.10
		6. Terrorists	10
	D.	VULNERABILITIES	.11
	<b>E</b> .	TOOLS OF THE CYBER CRIMINALS	.12
		1. Backdoor	.12
		2. Denial of Service (DOS) Attack	.12
		3. Distributed Denial of Service (DDOS) Attack	.12
		4. E-mail Spoofing	.12
		5. IP Address Spoofing	.12
		6. Kev Logger	.12
		7. Logic Bomb	.13
		8. Packet Sniffing	.13
		9. Spoofing	.13
		10. Spyware	.13
		11. Trojan Horse	.13
		12. Viruses	.14
		13. Worms	.14
		14. Zombie	.14
III.	SITI	ATIONAL INFLUENCE ASSESSMENT MODULE (SIAM)	.15
-	<b>A.</b>	SIAM DESCRIBED	.15
	В.	SIAM INFLUENCE NET SAMPLE	.16
IV	MOI	EL SET-UP	21
- · ·			_

V.	MOI	DEL DEMONSTRATION AND RESULTS	27
	А.	EXCURSION ONE	28
		1. All Security Measures Utilized	28
		2. <b>Results</b>	28
	В.	EXCURSION TWO	29
		1. No Anti-Virus	29
		2. Results:	30
	C.	EXCURSION THREE	30
		1. No Firewall	30
		2. <b>Results</b>	31
VI.	REC	OMMENDATIONS AND CONCLUSIONS	33
	А.	RECOMMENDATIONS	33
		1. Model Improvements	33
		a. Survey Improvements	
		b. Add in all Security Tools and Attack Methods	34
		c. Conduct More Testing of the Model	34
		2. Recommended Applications	34
		3. Future Research	34
		a. Conduct a Classified Continuation of This Thesis	34
		b. Keep the Model Current	35
		c. Conduct Cost Benefit Analysis	35
	В.	CONCLUSIONS	35
APP	ENDIX	A EXPERT OPINION SURVEY	
	1.	FIREWALL SECTION OF SURVEY	
	2.	IDS/IPS SECTION OF SURVEY	42
	3.	HARDENING SECTION OF SURVEY	46
	4.	TRAINING SECTION OF SURVEY	50
	5.	ANTI-VIRUS SECTION OF SURVEY	54
	6.	ANTI-SPAM SECTION OF SURVEY	58
	7.	ANTI-SPYWARE SECTION OF SURVEY	62
	FNDIX	R EXPERT OPINION SUMMARY RESULTS	67
		RESULTS IF FIREWALL WERE LISED	
	1. 2	RESULTS IF FIREWALL WERE NOT USED	
	3	RESULTS IF IDS/IPS WERE USED	69
	3. 4	RESULTS IF IDS/IPS WERE NOT USED	69
	 5	RESULTS IF HARDENING WAS USED	70
	5. 6	RESULTS IF HARDENING WAS NOT USED	70
	<b>7</b> .	RESULTS IF ADEOUATE TRAINING WAS USED	
	8.	RESULTS IF ADEQUATE TRAINING WERE NOT USED	
	9.	RESULTS IF ANTI-VIRUS SOFTWARE WAS USED	
	10.	RESULTS IF ANTI-VIRUS SOFTWARE WAS NOT USED	
	11.	RESULTS IF SPAM FILTER WERE USED	
	12.	RESULTS IF SPAM FILTER WERE NOT USED	
	13.	RESULTS IF ANTI-SPYWARE WERE USED	
	14.	RESULTS IF ANTI-SPYWARE WERE NOT USED	

LIST OF REFERENCES	75
INITIAL DISTRIBUTION LIST	79

# LIST OF FIGURES

Figure 1.	Basic Influence Net Diagram (of buying a car)	17
Figure 2.	Node Properties	19
Figure 3.	Link Properties	20
Figure 4.	Root Node and Parents	
Figure 5.	Security Tools and links	23
Figure 6.	Excursion 1 (All security measures used)	
Figure 7.	Excursion 2 (No anti-virus software used)	
Figure 8.	Excursion 3 (No firewall used)	

#### ACKNOWLEDGMENTS

First, I would like to thank my thesis advisor, Dr. Dorothy Denning for her impeccable advice and guidance throughout this project. Her superb knowledge in the field and her patience with my inadequacies made this tedious process actually enjoyable. I would also like to thank Mr. Steve Iatrou, my second reader, whom on numerous occasions helped relieve me of my thesis anxieties and always lead me down the right path. His golfing counsel isn't bad either. I would also like to thank all the individuals whom filled out and returned the expert opinion surveys; Professors, Karen Burke, Paul Clark, Daniel Warren and ITCS(SW/AW) Billy Freeman from the Bureau of Naval Personnel. Special thanks must go out to my good friend Ian Brown, for all of his assistance throughout my stay in the Monterey Area and especially for the vital assistance he graciously provided during the last few weeks of my thesis.

I would also like to thank my wonderful bride Heather, who while working on her own degree at California State University Monterey Bay managed to support me and share tasks to ensure our goals were met. Additionally, I would like to thank my three daughters; Sabrina, Victoria, and Selena for their understanding during crunch times both during finals and throughout this thesis process. Their love and tremendous support were an encouragement and greatly lead to my successful completion of Master's of Science in Information Systems and Operations.

# I. INTRODUCTION

#### A. BACKGROUND AND MOTIVATION BEHIND THE RESEARCH

As stated by the founder of the term "Cyber War," Dr. John Arquilla, in a PBS FRONTLINE interview referring to Operation Iraqi Freedom, "It occurred to me, in the wake of that tremendous and lopsided victory of ours, that much of what we did could have been held hostage to the disruption of any of those information systems. That was the beginning of cyber war – the idea that the vulnerability of communications could cripple an advanced army. What makes it strong also made it weak." The military acknowledges this frightful fact and understands the increasingly indispensable nature of information technology, as well as how this indispensable technology has transformed these systems into high value targets of cyber terrorists, which presents a significant threat to both the military and national security.

In a study by Charles Billo and Welton Chang, Senior Research Associate and Research Intern, respectively, for the Institute for Security Technology Studies at Dartmouth College, <u>Cyber Warfare; An Analysis of the Means and Motivations of</u> <u>Selected Nation States</u> (2004), noted "cyber warfare" as warfare that involves,

...units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. Hackers and other individuals trained in software programming and exploiting the intricacies of computer networks are the primary executors of these attacks. These individuals often operate under auspices and possible support of nation-state actors. In the future, if not already common practice, individual cyber warfare units will execute attacks against targets in a cooperative and simultaneous manner.

Information Operations Issue Manager for the CIA, John Serbian, in a Statement for the Record before the Joint Economics Committee, U.S. Congress on 23 February 2000, paints a vivid picture. Serbian states that for adversaries who cannot match US strength, the use of asymmetric strategies to exploit vulnerabilities will continue to have incentives. The incentives cyber attacks provide as stated by Serbian include economic, industrial, and military rationales. By way of example: "Trillions of dollars in financial transactions and commerce move over a medium with minimal protection and only sporadic law enforcement - a structure the most complex the world has ever known. Increasing quantities of intellectual property reside on networked systems; and opportunities abound to disrupt military effectiveness and public safety while maintaining the elements of surprise and anonymity" (Serbian, 2000).

John Serbian continues in his explanation of the "threat" to Congress, that the information infrastructure that was built is interoperable, easy to access, and easy to use. Also, with attributes like openness and ease of connectivity are the same ones that now make the systems vulnerable to attacks against automated information systems. He further explains that the cyber threat can "originate from any location, affect systems anywhere in the world, disguise origins and travel routes, and do it instantaneously." Further, Serbian explains how being a part of the "cyber attack game" does not take a great deal of skill or investment and explains that cyber tools are readily available on the internet for anyone to download and use maliciously. Some tools, he states, even use a point-and-click feature to start an attack (Serbian, 2000).

Serbian also refers to a testimony before the Senate Select Committee on Intelligence by Director of Central Intelligence George Tenet in February of 2000. In DCI Tenet's testimony he stated that the, "foreign cyber threat is one of the key transnational issues that we face as a nation." Also in that testimony, Director Tenet noted that the US is increasingly dependent on "...the unimpeded and secure flow of technology" and that "any adversary that could develop the ability to interrupt that flow...will have the potential to weaken us dramatically or even render us helpless" (Serbian, 2000).

Cyber warfare has already been used as a tool of military warfare against this country, as addressed by Dr. Dorothy Denning, Professor of Defense Analysis at the Naval Postgraduate School in Monterey California and former Professor of Computer Science at Georgetown University. In her book, <u>Information Warfare and Security</u> she explains how the US military encountered Netherland hackers during the first Gulf War. The hackers were able to penetrate 34 American military internet sites, gathering information on military supply systems, troop locations and their weapons, as well as US

Navy ship movements and the capabilities of the Army's Patriot Missile (Denning, 1999). Had the Iraqi government suspicions of a trap not prevented them from purchasing this data, the length of the war perhaps may have been longer, though it is unlikely the information stolen would have actually changed the outcome of the war. However, this does give a general idea of the possibilities and potential use of cyber warfare in the future.

It was the aforementioned CIA statements concerning cyber threats and their expected increased use, coupled with the already documented uses of cyber warfare addressed by Dr. Denning, that has spawned this research.

#### **B.** GENERAL SCOPE OF THE THESIS

The main thrust of this study will be the design of a model which will help to discover whether ships are hard targets, targets of opportunity, targets of choice, or simply soft targets. Looking at research and established security techniques it will become apparent whether or not ships are taking all the required steps to best secure themselves against an attack.

Though the "insider" may be the biggest threat to an organization (Denning, 1999) for the purposes of this study the focus will be on the "outsider" hacker/terrorist. To prevent this research from becoming classified, only theoretical data are presented concerning what may be considered a typical ship in the Everett, WA region. Some of the past terrorist information and threats addressed in making the model are also theoretical unless noted otherwise. In such cases the information was taken only from open source materials such as the internet or unclassified research.

#### C. BRIEF EXPLANATION OF METHODOLOGY

This thesis will focus on identifying the likelihood of a successful cyber attack on an Everett based ship. In order to do so, an expert opinion survey was designed and completed by individuals currently working in the field of network security, to determine expected levels of protection each mitigation tool provides against known cyberterrorist attack methods. Once the expert opinion analysis was completed it was built into an influence net model, along with cyber terrorist motivations and means to determine whether or not a cyberterrorist attack is likely to succeed against a U.S. ship. Additionally, the model was tested using various boundary case scenarios to evaluate usability, completeness, and accuracy. The model allows many scenarios (or case studies) to be considered in order to produce the optimal outcome for Navy ships. A worst case scenario can also be analyzed to show how much more likely the ship will be at risk not having a particular security mechanism in place.

#### **D. BENEFITS OF STUDY**

The benefits of the study are numerous. First, the expert opinion survey data alone will prove vital in determining the best security practices available to counter individual attack methods. Additionally, the work will strive to determine the amount of risk navy ships are in, as well as determining what they can do to mitigate the risk of becoming targets of opportunity. Such information will assist in protecting ships from attack by giving decision makers the ability to see the main vulnerabilities of a typical ship's computer networks, as well as how important certain mitigation tools are toward the defense of a network. The use of the completed model can also facilitate security funding as well as establishing a means of prioritizing the security mechanisms for protection if a network needs to be hastily re-established after an attack.

Though the initial model was designed around a theoretical Naval Station Everett ship, with modification the model can be utilized for any naval asset throughout the United States, and the risk for each particular U.S. asset can be evaluated. Ultimately, the protection of a ship's computer networks against cyber terrorist threats is fundamental in ensuring continued effective command and control and ultimately the security of this nation.

#### E. THESIS STRUCTURE:

Chapter I – Introduction – This chapter provides the thesis statement and describes the general scope of the thesis. It gives an overview of the chapters, figures and annexes of the paper.

Chapter II - Background Information – This chapter describes many of the general Information Operations' terms and key concepts. Additionally, it explores the motivations of hackers and cyberterrorists as well as the expected tools used by these criminals. The chapter concludes by addressing the protection mechanisms used to protect against terrorists (i.e., the DITSCAP process as well as individual mitigation tools).

Chapter III - Situational Influence Assessment Module - This chapter introduces influence net modeling and the SIAM program.

Chapter IV – Model Set-up – This chapter describes how the model for this thesis was designed, including node breakdown and link strength assignments.

Chapter V - Model Demonstration and Results – This chapter describes the results of the model.

Chapter VI - Future Work & Conclusion – This chapter looks at areas of potential further research, and gives a brief summary of the work accomplished by this thesis.

# **II. BACKGROUND INFORMATION**

The United States of America is fighting a war against terrorists of global reach. The enemy is not a single political regime or person or religion or ideology. The enemy is terrorism—premeditated, politically motivated violence perpetrated against innocents.

-The National Security Strategy of the United States of America, September 2002

#### A. INTRODUCTION TO INFORMATION OPERATIONS

Joint Publication 3-13, titled, <u>Information Operations</u> of 13 February 2006 is the joint doctrine for U.S. military conducting Information Operations (IO). It provides the guidance to help prepare, plan, execute, and assess IO in support of joint military operations. Information Operations is described by Pub 3-13 as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

In support of this thesis we will look only at Computer Network Operations. CNO is the newest of the core capabilities and consists of Computer Network Attack (CNA), Computer Network Defense (CND), which will be the focus of this paper, and the related computer network exploitation (CNE). In this day and age of technology, CNO capabilities are ever increasing, in parallel with the increasing numbers of networked computers and supporting IT infrastructure systems. CNO is primarily used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure and thus is the IO capability best designed to exploit the new opportunities and vulnerabilities of our adversaries as well as protecting our own. (JP 3-13, 2006)

Specifically, CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense (DoD) information systems and computer networks. CND actions not only protect DoD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations.

CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

As the capability of computers and the range of their employment broaden, new vulnerabilities and opportunities will continue to develop. This offers both opportunities to attack and exploit an adversary's computer system weaknesses and a requirement to identify and protect our own from similar attack or exploitation. Therefore, with the broad definitions of IO described above it is practical to explain the means in which we measure and protect these systems.

#### **B.** INFORMATION ASSURANCE

Per DoD Directive 8500.1 (2002): Information Assurance is defined as: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. The Committee on National Security Systems (CNSS) defines these key terms in their National Information Assurance (IA) Glossary:

#### 1. Availability

Timely, reliable access to data and information services for authorized users

#### 2. Integrity

Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

#### **3.** Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or means of verifying an individual's authorization to receive specific categories of information.

#### 4. Confidentiality

Assurance that information is not disclosed to unauthorized persons, processes, or devices.

#### 5. Non-repudiation

Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of sender's identity, so neither can later deny having processed the data.

With key information assurance terms defined we will now look at those that threaten information systems as well as their motives.

#### C. CYBER THREATS AND THEIR MOTIVES

Dr. Denning in her book <u>Information Warfare and Security</u> (1999) addresses many of the offensive actors of information warfare. These groups consist of insiders, hackers, criminals, corporations, and terrorists, any of which may use information systems to conduct intelligence gathering, conduct financial gain endeavors or disruption operations (i.e., block legitimate access to information) or, simply as a means of thrill seeking. Though, this thesis is primarily concerned with hackers, criminals and cyber terrorists, all of the aforementioned groups from Dr. Denning's book will be briefly explained along with their principle motivations.

#### 1. Insiders

This category consists of trusted individuals with inside access (i.e., employees and contractors) to a particular organization's information resources. Insiders may act as salesmen of corporate information, selling the information to organized crime syndicates, foreign governments, and/or competitors. Aside from exploiting information, certain disgruntled insiders may use their inside access to destroy their employers information and information resources.

#### 2. Hackers

This group of offensive players typically consists of those that "gain access to or break into electronic systems, particularly computers and telecommunications equipment." Motivations behind hacking can be numerous including thrills, challenge, power and financial gain. Regardless of a hacker's motive; their actions damage the integrity of systems and can be a major nuisance (Denning, 1999).

#### 3. Criminals

This category of threat targets financial information resources, and as expected are motivated by money. Criminals look for information such as credit card numbers, bank account information and basically anything that can be converted to, or sold for cash. Criminals also utilize internet and other information resources to engage in any number of internet scams and frauds.

#### 4. Corporations

Corporations are also motivated by money, as well as competitive position. They actively seek intelligence from their competitors, such as trade secrets and frequently rely on the aforementioned "insider" for such information.

#### 5. Government Agencies

This category consists of law enforcement and intelligence agencies motivated to protect public safety and national security. Dr. Denning describes an example use by law enforcement as they target a criminal's communications and other structures for gathering evidence in support of criminal cases, whereas, intelligence agencies seek "military, diplomatic, and economic secrets of foreign governments, foreign corporations, and foreign adversaries" in support of our nation's goals of national security (Denning, 1999).

#### 6. Terrorists

Though cyber terrorists have yet to make any major appearances, they are considered to be of particular interest because of their potential to do damage. In promoting their cause, terrorists may conduct intelligence gathering to collect information about their targets, spread propaganda and conduct attacks "against critical infrastructures such as emergency services and financial systems." Terrorists may also utilize the Internet in the same manner as the aforementioned criminals in order to earn funds to support there next mission.

The various groups above have various motivations for their actions, however, for this thesis we will focus on four main categories, which are, "financial gain," "intelligence gathering," "disruption of operations," and lastly, "thrill seeking." Insiders, criminals, and corporations are mainly motivated by financial gain, however, a personal vendetta could also cause an employee to divulge insider information or commit sabotage against his organization. Hackers, on the other hand, though sometimes motivated by money, are more motivated by thrills, challenge, and power as addressed by Dr. Denning.

With the various actors described, this thesis will now attempt to describe how the aforementioned actors accomplish their objectives.

#### D. VULNERABILITIES

Cyber criminals attack an information system via its vulnerabilities, which the CNSS Glossary defines as, "a weakness in an information system (IS), or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited" (CNSS, 2007). A key point about IS vulnerabilities is that they are similar for everyone and can be exploited by anyone via an Internet connection. Additionally, information about IS vulnerabilities and tools that exploit them are publicly available for anyone interested enough to look using any Internet search engine. Navy IS's are just as vulnerable as other systems and just as susceptible to exploitation if they are not properly protected.

SANS Institute<sup>1</sup> publishes what they consider to be the 20 most critical vulnerabilities of information systems. These critical vulnerabilities include versions of Microsoft Windows, MAC OS X and UNIX operating system vulnerabilities, as well as vulnerabilities with cross-platform applications such as databases, and web applications (e.g., Content Management Systems (CMS), wikis, portals, bulletin boards, and discussion forums). Another critical vulnerability SANS addresses is with the Microsoft Internet Explorer browser, which is installed by default with Microsoft operating systems. This browser has numerous vulnerabilities that if not patched can allow an attacker to corrupt memory, conduct spoofing and even execute arbitrary scripts (SANS, 2007).

Another category of vulnerabilities listed by SANs is "network devices" which incorporates vulnerabilities with "various products such as Cisco Unified Call Manager, Asterisk and a number of VoIP phones from various vendors." These particular network devices were discovered to contain vulnerabilities that can either lead to a crash or cause

<sup>&</sup>lt;sup>1</sup> SANS Institute (SysAdmin, Audit, Networking, and Security) is a trade name owned by the for-profit Escal Institute of Advanced Technologies. SANS provides computer security training, professional certification, and a research archive. It was founded in 1989.

a complete control over the vulnerable server/device. By gaining control over the VoIP server and phones, an attacker could carry out VoIP phishing scams, eavesdropping, toll fraud or denial-of-service attacks. (SANS, 2007)

#### E. TOOLS OF THE CYBER CRIMINALS

Cyber criminals have a myriad of tools to choose from in an attempt to accomplish their objectives. The following list of tools was derived from the US Army's Training Handbook, "A Military Guide to Terrorism in the Twenty-First Century" (2004). This list is not all inclusive but is a very good starting point.

#### 1. Backdoor

Hidden software or hardware mechanism used to circumvent security controls. A backdoor is synonymous with trapdoor.

#### 2. Denial of Service (DOS) Attack

An attack designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash.

#### **3.** Distributed Denial of Service (DDOS) Attack

A denial of service attack that involves the use of numerous computers to simultaneously flood the target.

#### 4. E-mail Spoofing

A method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source. This method is often an attempt to trick the user into releasing sensitive information (such as passwords).

#### 5. IP Address Spoofing

A method that creates Internet Protocol (IP) packets using somebody else's IP address. Routers use the destination IP address to forward packets through the Internet, but ignore the source IP address. This method is often used in DDOS attacks in order to hide the true identity of the attacker.

#### 6. Key Logger

A software program or hardware device that is used to monitor and log each of the keys a user types on a computer keyboard. The adversary who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the actual keys being typed, the adversary can easily obtain passwords and other information the computer operator may not wish others to know. Key loggers are a type of spyware, which are detailed below.

#### 7. Logic Bomb

A software program with malicious code that lies dormant until some event occurs, at which point it executes to destroy data on a computer. If execution is triggered by a date or time, as is often the case, the program is also called a "time bomb" (Denning, 1999).

#### 8. Packet Sniffing

A program and/or device that monitors data traveling over a network. Although sniffers are used for legitimate network management functions, they also are used during cyber attacks for stealing information, including passwords, off a network. Once emplaced, they are very difficult to detect and can be inserted almost anywhere.

# 9. Spoofing

Attempt to gain access to an information system by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

#### 10. Spyware

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is software that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

#### 11. Trojan Horse

A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed, it performs a function in the background such as allowing other users to have access to your computer. The users can then send information from your computer to other computers, or allow unauthorized collection, falsification, or destruction of information.

#### 12. Viruses

A malicious software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. Viruses replicate and attach themselves to a host, (e.g., files) with no obvious signs of its presence. There are many different types of viruses, a few examples include: boot sector virus, companion virus, executable virus, overwrite virus, polymorphic virus, resident and stealth viruses.

#### 13. Worms

A destructive software program containing code capable of gaining access to networked computers and, once within a computer, causing that computer harm, for example, by deleting, modifying, distributing, or otherwise manipulating the data. Worms can replicate from machine to machine across network connections, often clogging networks and computer systems as it spreads.

### 14. Zombie

A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a Distributed Denial of Service attack (DDOS) or send out spam.

With the tools of cyber criminals and other background information explained above, this thesis will now describe SIAM modeling as well as give a basic model to give the reader a foundation for SIAM's use in later chapters.

# **III. SITUATIONAL INFLUENCE ASSESSMENT MODULE (SIAM)**

#### A. SIAM DESCRIBED

The SIAM software application is a collaborative decision support tool, designed to assist people in analyzing complex problems and issues by breaking them down into smaller more workable parts. The smaller parts allow the modeler to more easily recognize and evaluate critical relationships among the varying parts, as well as determine the importance each particular part plays in the larger scheme (Rosen and Smith, 2006).

SIAM designers, Dr. Julie Rosen and Mr. Wayne Smith of the Science Applications International Corporation (SAIC), state that their product eases the building and analysis of an Influence Net Model, which they define as "a user-created model that depicts events and their causal interrelationships. It is a graphical model that facilitates brain-storming and complex decision making." (Influence Nets will be described in greater detail later.) Dr. Rosen and Mr. Smith further state that SIAM is a time saving tool which helps users in examining complex problems by use of the various capabilities it provides, for example:

1. "A graphical model that depicts complex, possibly conflicting, cause-and –effect relationships in an easy-to-manipulate fashion; and

2. Comparative quantitative assessment techniques that evaluate the relative influencing impacts of these accumulated relationships."

Rosen and Smith also note that with these tools and others, SIAM helps "users organize and evaluate large amounts of information, and collaborate with others in analyzing complex factors and causal dependencies of any given issue" (Rosen and Smith, 2006).

In their description of SIAM, Professors Hayes and Sands of the Naval War College, Center for Naval Warfare Studies, Decision Support Department state "the networks created in SIAM can be used to identify important issues, actions, or factors that can and do influence a specific outcome in a given situation" (Hayes and Sands, 2001).

Rosen and Smith further state that complex problems are typically solved in a group environment (i.e., seminar or workshop) with multiple subject matter experts working toward a similar goal. SIAM can be used in this environment, allowing the seminar group to brainstorm, conduct "what-if" scenarios, and break down issues into their simplest form to be depicted graphically. All the while the group can continually critique and challenge one another's logic and quickly make changes to the model, or simply revise the model as "data changes or experts' opinions change," which can then be reassessed for their impact. Additionally, with the use of SIAM's documentation capabilities, notes can be taken within SIAM to retain the reasoning behind certain decisions and changes, as well as documenting reference material and other pertinent information (Brodhun III 2001, Rosen and Smith 2006).

#### **B. SIAM INFLUENCE NET SAMPLE**

An Influence Net is defined as, "A graphical representation of a model, which incorporates perceptions and events the user identifies as important in examining an issue or question. Additionally, an Influence Net is a chain of casual influences that, taken independently, may appear meaningless, but when linked together, establish patterns of behavior and motivating factors in a situation" (Rosen and Smith, 2006).

A simple Influence Net is provided below to show the basic topology of an Influence Net and to help in describing the key elements of the Influence Net model.



Figure 1. Basic Influence Net Diagram (of buying a car)

Within the SIAM application, the graphical objects which display the chains of causal influences are called "nodes" and "links." A node "is one of a series of related ideas or events that influence an overreaching issue," and a "link" is the "one-way connection between two nodes" and is graphically depicted as a line.

Nodes within the SIAM model serve various roles: root, parent, child, and initial, and are depicted in the model as colored rectangles. The "root node" is essentially the ultimate conclusion, "or desired end state of the analysis." In Figure 1 the root node is, "Should I buy a new car?" A "parent node," which is also sometimes referred to as the "cause node," is an idea or event that influences other events. A "child node," also sometimes referred to as the "effect node" is an idea or event that results from the parent

node. Sometimes a node can be both a parent and a child, when such a case occurs, then the node would be considered a parent when at the source of the link, and a child when at the destination. To reemphasize, child nodes are those that are affected by other nodes and parent nodes are those that affect the outcome. For purposes of the root node above the parent nodes are: opportunity (i.e., Is there a car available?), capability (i.e., Can I afford it?), practicality (i.e., Is there a need?), and desire. The last type of node is the "initial node." They are the originating causal influences, and thus lack parental influences. Basically, initial nodes represent the primary assumptions used to construct the Influence Net.

Each node in the influence chain is assigned a belief value to its occurrence, either by the user for initial nodes, or by SIAMs' Bayesian algorithms for all others. The assignment of "the belief value is based on the conditions specified by its influencing events and relationships in the Influence Net." In looking at Figure 2, we can see for the node, "My wife is strongly..." has been assigned a belief value corresponding to, "I am very certain that this is a true statement by the user." Additionally, you can see how the author added other information deemed pertinent into the "description block" for further reference.

Node Properties	$\mathbf{\mathbf{x}}$			
Node Title My wife is strongly against me getting a new car until after we buy our new house.	-∿-			
Wife is against buying a car now because it will dramatically change debt/ratio. Thus, the amount of house loan to be approved with be much less. Plus, if I do this she will be very angry and hard to live with. Based on these two things I probably shouldn't buy a new car.				
I ⑦ Sources Arewords Arewords Arew Classification Are Excursions ■ Current Belief The Baseline Belief Arew Library Arewords I Comments	_			
False     Unknown     True       I     I     I     I       Certain     Uncertain     Certain       Synopsis     I am very certain that this is a TRUE statement.     Clear Constraints				
Node Properties Classification Unspecified Change.				
Node Information         This is a causal strengths initial node.         Its belief may be set with the belief slider.         Its baseline belief equals its current belief.         OK       Apply	*			
Figure 2. Node Properties				

The belief value, whether assigned by the user or by SIAM, is easily distinguished by a node's color. The color key can be seen on the far left side of Figure 1. The color of a particular node allows the user to quickly identify the relative belief value of that node. "Four shades of blue represent the degrees of uncertainty in the influencing event's truth. Similarly four shades of red depict the degrees of uncertainty that the influencing event is false." If a node color is grey, then this is an indication of complete uncertainty in the likelihood of the influencing event's occurrence. Additionally, for each connecting link there are two link values which must be assigned by the user, one for when the cause (parent) is true and one for when it is not. These link value strengths representing the impact of the cause on the effect, and can be seen in Figure 3 (Rosen and Smith 2006).

By looking back at Figure 1 you will notice the link between the nodes "My wife is strongly..." and "Should I buy a new car" has a filled terminator circle (or ball) at one end of the link. The ball illustrates "that the parent has a reversing influence on the
occurrence of the child node," whereas, an arrowhead terminator would indicate "that the parent node has a reinforcing influence on the occurrence of the child node."

Link Properties	
Cause (Premise) Node My wife is strongly against me getting a new car until	Effect (Conclusion) Node Should I buy a new car
after we buy our new house. Cause (Premise) Node Description Wife is against buying a car now because it will dramatically	Effect (Conclusion) Node Description
<ul> <li>E Link Strengths Strengths Strengths</li> <li>What if the premise were TRUE?</li> <li>How would this impact the conclusion?</li> </ul>	Impact       Impact
Image: Constraint of the premise's occurrence strongly inhibits the conclusion.	Image: Constraint of the premise's non-occurrence strongly promotes the conclusion.
Link Properties Classification	Change
Link Information	
This link represents a strong reversing influence. The link strengths in the default excursion have been manually rea	assigned.
<u>o</u> k Apr	ly <u>C</u> ancel

Figure 3. Link Properties

With a basic SIAM model explained, this thesis will now show how the SIAM software was used to demonstrate a potential cyber attack scenario.

### IV. MODEL SET-UP

As previously mentioned the work encompassed in this thesis was designed to model a cyber attack on a US ship, which can also be used to help determine the amount of risk to a particular naval ship. To do so, an Influence Net model was designed around the premise of whether or not a ship can successfully defend against a myriad of cyber attack methods. As Chapter II of this thesis briefly discussed, potential attackers can be motivated by numerous factors, including intelligence gathering, thrill seeking, disrupting operations, and financial gain. Even more importantly, potential attackers have the opportunity, as well as the capability to conduct an attack. The potential of these three key components (i.e., motive, opportunity, and means) coming together could prove disastrous for a Navy ship, or at minimum a nuisance if not properly defended against.

Thousands of attacks occur daily on internet-connected systems. In the first half of 2005 alone, IBM reported that virus-laden emails and criminal driven security attacks increased by 50 percent, with over 237 million overall security attacks. IBM further reported that the US government was the most targeted industry during that period, "with more than 54 million attacks." (IBM, 2005) At that rate it was likely there were over half a billion attacks in 2005, with over 100 million of those attacks being directed toward government systems, including Navy and other DoD systems. In addition to directed attacks, indiscriminate mass attacks such Nimda, Code Red, Slammer, and Blaster, all of which spread rapidly throughout the Internet without sparing vulnerable government computers, are also a considerable threat (Common Sense Guide, 2004). Thus, the threat of attack is real and the need to protect against said attacks requires considerable attention.

The prevalence of attacks and attempted attacks provide evidence of motivation, capability and opportunity, so we will build the model with the assumption that an attack has taken place, as will be demonstrated later in this thesis. Overall, the end goal of network security is to defend against attack – which means defending against each possible type of attack. That being said, the root node, "Ship defends against cyber attack

methods" was established, along with the eleven parent nodes, which correspond to the different types of attacks we need to defend against, as illustrated by Figure 4. A summary list is provided:

- a. Worm attack aborted
- b. Virus attack aborted
- c. Trojan Horse penetration aborted
- d. Attempt to take over system and turn into Zombie is aborted
- e. Denial of Service attack is aborted
- f. Keylogger utilization attempt is aborted
- g. Sniffer utilization attempt is aborted
- h. IP address Spoofing attack is aborted
- i. Email spoofing attack is aborted
- j. Backdoor installation attempt is aborted
- k. Logic Bomb attack is aborted





After determining the end goal (root node) and the many attack methods (parents) to defend against, it was necessary to consider the likely security measures utilized by U.S. assets and the effect each of these security tools has against the previously mentioned attack methods. Figure 5 illustrates the likely security tools in place to help prevent attacks, which are also listed below.

- a. Firewall
- b. Hardening
- c. Anti-virus software
- d. Anti-spyware software
- e. Spam filter
- f. Training
- g. IDS/IPS



Figure 5. Security Tools and links

In establishing link values for the amount of expected protection a particular security tool provides against common attack methods an expert opinion survey to gather collective experience and compiled opinions was created. The surveys were then

distributed to a small group of graduate level instructors at Naval Postgraduate School in fields of computer science and information assurance, as well as to current network IT security personnel working in the field. Each survey was accompanied by a cover letter describing the survey along with some clarification statements, as well as a terms and definitions list to assist in standardizing responses.

The survey was comprised of seven sets of questions. Each set of questions focused on one mitigation tool (i.e., system hardening, use of firewall, IDS/IPS, training, anti-virus software, anti-spam and anti-spyware software) and the probability that tool could prevent a likely attack method. The attacks considered were those listed in the U.S. Army Intelligence Department and described in Chapter II, section E: virus, worm, trojan horse, denial of service, backdoor, keylogger, sniffer, IP address spoofing, E-mail spoofing, logic bomb, and lastly, being taken over and turned into a zombie. A blank copy of the survey questions is contained in Appendix A.

The survey questions were in pairs according to specific security measures. The first question was designed to capture the survey takers judgment of the security measures impact on attack prevention if the measure is employed; the second question was designed to reflect the survey taker's judgment of the impact on not using the security measure. Each question had an eleven category range, spanning from "severely inhibits" to "severely promotes," which, purposefully matches up with SIAM's measurement techniques for assigning linkage values between nodes. Each of the eleven possible selections has a corresponding numerical value for use in the influence net model, with +1 being severely promoting and a -1 corresponding to severely inhibiting. A total of four surveys were returned and the discrete analysis of the results is provided in Appendix B.

The results as shown in Appendix B were then used to assign link values between each of the seven security tools and each of the 13 attack method (outcome) nodes.

In summary, if a virus attack were to take place as illustrated in Figure 5, then that node would be assigned a 100% truth value to indicate an attack taking place. The attack information would then be linked to the seven different security tools, which on their output side were assigned the values corresponding to the likelihood of preventing an

attack. Then after the simulation was ran, the node titled, "virus attack aborted" would reflect the likelihood of whether the attack was successfully thwarted given deployment of the security mechanisms. The Bayesian algorithm would then continue through the model to the root node titled, "Ship defends against cyber attack methods" to determine its probability as well.

With all the major parts of the model described and illustrated, the model will be populated with a theoretical situation in the next chapter to demonstrate its possible application. THIS PAGE INTENTIONALLY LEFT BLANK

# V. MODEL DEMONSTRATION AND RESULTS

To demonstrate the model a notional situation was constructed for use in populating the model. The situation is as follows:

Let's say a software company in Seattle, WA fires one of their most knowledgably programmers, named Jim, for being habitually late and disrespectful to other employees. Aside from being a very skillful programmer, Jim also takes pride in being a pretty savvy hacker and is thrilled to put his skills to work. Earlier that morning Jim, now a disgruntled ex-employee, was stuck behind a slow Navy van which he blames for his not making it to work on-time and subsequently getting fired. Jim, instead of taking his frustrations out in a healthy and legal manner, decides to try and pay back the local Navy by hacking into an Everett based ship's network to conduct a virus and worm attack to cause havoc and attempt to bring down the ship's network.

The above scenario describes a hacker with both a strong motive as well as the means to conduct an attack. The opportunity is also available since Jim has access to a computer which is connected to the Internet. The potential success of the attack thus depends almost entirely on the ship's vulnerabilities and the effectiveness of the mitigation tools used. As was shown in an earlier chapter of this thesis, numerous vulnerabilities exist that if not properly mitigated can be exploited, thus leading to a successful attack.

With the previous chapter providing a detailed description of the initial model construction and the above scenario, the remainder of this chapter will focus on populating the model with the scenario results and running three separate excursions, or examples to show the models versatility as well as to show the likelihood of successful attacks based on different criteria. The first excursion was designed to show how effective the attack would be with all primary mitigation tools in place. The second excursion was designed to show how effective the attack would be if the ship did not utilize anti-virus software. The last excursion was set-up to show the likelihood of a successful attack if no firewall is utilized.

#### A. EXCURSION ONE

#### 1. All Security Measures Utilized

For this demonstration the aforementioned scenario of a virus and worm attack takes place. Therefore, the initial nodes, "Virus Attack Takes Place" and "Worm Attack Takes Place" were both set to true in order to indicate that the attack took place. Next, the linkages between the attack nodes utilized, and each of the mitigation tools were set to "Severely Promotes the Conclusion," to allow 100% of the attack to take place. The next step was to assign the linkages between each particular mitigation tool and its likelihood of stopping the attack method which were inferred from the expert opinion survey results (Appendix A). The model was then run and provided the following figure and results:



Figure 6. Excursion 1 (All security measures used)

2. **Results**: "Virus Attack Aborted" and "Worm Attack Aborted" were both determined to have a belief value of .99, and the root node, "Ship Defends Against Cyber Attack Methods" was determined to have a belief value of .87. By looking at the color table to the left of Figure 6, we can confirm similar results at a glance. The dark blue colors would translate to the belief "I am extremely certain that this is a true statement."

By interpreting these results the reader should be convinced that the tools in place should protect the ship from attack, however, they also show that the prevention of attack is not 100 percent, therefore, even with all protections in place the possibility of attack does exist. As we will see next, the following results will not be as comforting.

#### **B. EXCURSION TWO**

#### 1. No Anti-Virus

For this demonstration the same virus and worm attack occurred, however, this time the protection of the anti-virus software was removed from the equation. To do so the link between the causal node, "Virus Attack Takes Place" and the effect node "Anti-Virus Software Stops Virus" is assigned a value of -1. This then propagates through the model setting the "Anti-virus Software Stops Virus" node to -1, which indicates "I am extremely certain this is a false statement," thereby allowing the virus attack to propagate through the model with no impact from that node. The model was then run again and provided the following figure and results:



#### 2. Results

"Virus Attack Aborted" was determined to have a belief value of .69, or a synopsis of "I am reasonably certain that this is a true statement." The node "Worm Attack Aborted" was determined to have a belief value of .38, or a synopsis of "I am slightly certain that this is a false statement." The overall root node had a belief value of .53, or unknown value. Again by looking at the color table on the left side of Figure 7, we should be able to make a similar determination. The worm attack node is a light shade of red instead of dark blue, and the virus attack node is about two to three shades lighter of blue. These results indicate that with no Anti-virus protection there is a 31% likelihood that the virus would have gotten through and a 62% likelihood that the worm attack would be successful. In conclusion, the results of the model show that the antivirus software is more effective at stopping a worm attack than a virus attack, as well as showing that with no anti-virus protection the probability of aborting a virus or worm attack is substantially reduced. The overall likelihood that the ship could defend against this dual attack with no anti-virus was approximately 50%, thus, leading to the final conclusion - that employing updated anti-virus software is a vital mitigation tool against worms and a very good tool for protecting against virus attack. Though Anti-virus protection does prove to provide a large percentage of protection for the above scenario, the aggregate of the other mitigation tools can not be discounted since they do add up to greater than 65% protection in defense of a virus and 35% for a worm. The next excursion was then set-up to show the effect of having no firewall.

## C. EXCURSION THREE

#### 1. No Firewall

For this demonstration the same virus and worm attack occurred once again, however, this time instead of not utilizing anti-virus software, the effect of the firewall was disabled by following similar steps as Excursion Two. The model resulted in the following figure.



Figure 8. Excursion 3 (No firewall used)

#### 2. **Results**

The belief values for "Virus Attack Aborted" and "Worm Attack Aborted" were both determined to be .97, similar to the .99 results in Excursion 1. The root node was also very similar with a belief value of .85. The color table to the left of Figure 8 shows that the nodes are dark blue once again, and would translate to the belief "I am extremely certain that this is a true statement." These results show that the firewall had very little effect toward protecting against a virus or worm attack, which is consistent with the Appendix B data. Also, in referring to Appendix B we can see that the firewall is an effective tool in protecting against DOS attacks, IP address spoofing and being taken over and turned into a Zombie. Whereas, protecting against viruses and worms the best tools were Anti-virus software and adequate training to personnel. Therefore, if the firewall goes down, and all other security tools are in place the ship is still fairly well protected from a successful worm or virus attack, though the potential for a DOS attack, IP address spoofing, and being taken over and turned into a Zombie significantly increase. THIS PAGE INTENTIONALLY LEFT BLANK

# VI. RECOMMENDATIONS AND CONCLUSIONS

A few key recommendations are listed below which could improve this research project, starting with model improvements, and then followed by future research recommendations, and lastly the thesis conclusions.

#### A. **RECOMMENDATIONS**

#### **1.** Model Improvements

The model presented in this thesis overall met nearly all initial expectations, however, to improve its structure and validity for future use, certain points should be taken into consideration.

#### a. Survey Improvements

The survey utilized was an appropriate approach for a thesis of this scope, it provided expert opinions on the key security practices and their expected effectiveness, and then by taking an average of these results a baseline for assigning link values was established. However, to get a more accurate representation of overall expert opinions, either a much larger sample size of computer security professionals should be taken, or a workshop type forum should be used to collect the best data for incorporation into the model. A workshop consisting of the same experts would allow a forum to discuss all the particular security tools and the entire process in building the model in greater detail. A workshop would also provide a means of discussion and debate, giving experts the opportunity to convince others of their particular view which may be more correct based on experience or more thorough research – possibly coming to a consensus. However, if using the workshop method you need to be aware of "groupthink" issues which the survey style eliminates.

The expert opinion surveys were completed mainly by academic experts in the fields of computer science and information assurance. It would be prudent to conduct further research based on more opinions of those currently working as network security managers and technicians. Those personnel would see on a daily basis the summary logs and data of in-use security mechanisms (i.e., firewalls and IDS/IPS) and see first hand how many worms and viruses etc... were stopped on a given day.

#### b. Add in All Security Tools and Attack Methods

To keep this model within scope only the most popular mitigation tools and likely cyber attack methods were built into the model. However, future research should attempt to explore all security tools and threats which can then be built into future models.

#### c. Conduct More Testing of the Model

One scenario of a dual attack (worm and virus) with three variants was run to show the model's functionality and capabilities. The model should now go through an extensive series of scenarios to show its true potential and to demonstrate its usefulness to the US Naval fleet and other services. These scenarios should then be built into information assurance training which will be described next.

## 2. Recommended Applications

With a good working model constructed, the model can be used to demonstrate the effects security tools have in the prevention of attacks. The training should be designed for senior leadership and system administration personnel. With the demonstration of the model decision makers can now visualize the importance of each security measure in the prevention of various attacks. This visualization should lead to the enhanced awareness of cyber threats as well as the best practices for thwarting attacks. Additionally, with the enhanced awareness, the necessary security dollars required to buy lacking mitigation tools should come. Furthermore, the training will enhance network administrators' and technicians' knowledge as to the importance of updating anti-virus software, enforcing password policies and conducting training for anyone connected to the Internet.

#### **3.** Future Research

To further this research the following recommendations are offered:

#### a. Conduct a Classified Continuation of This Thesis

In an effort to keep this thesis unclassified no specific navy ship or its vulnerabilities were listed (i.e., what operating system and applications it uses), nor what specific security tools they have and use to counter threats. However, if a classified thesis was conducted and a model built based on a specific ship and its factual data, along with utilizing actual risk assessment data for a particular region, and then incorporating

that data to assign adversary motives, means and capabilities linkages, the user could also determine the likelihood of an attack, as well as the likelihood of a successful attack.

### b. Keep the Model Current

Each particular node and link will need to be researched periodically in order to keep the model up-to-date. Therefore, each station planning to utilize this model should evaluate all their security mechanisms and conduct a thorough product review of each mitigation tools (i.e., firewalls, IDS, anti-malware etc.). Additionally, as better and better technologies are developed the amount of protection of certain tools is likely to go up, therefore a new set of surveys or a workshop will need to be conducted to establish new link values for use in the model.

#### c. Conduct Cost Benefit Analysis

In order for the Navy to adopt such a program for service wide use, the benefits verses costs must be weighed and the actual cost determined. The SIAM program would need to be purchased from the SAIC corporation and then it would need to be approved for use by a DAA.

#### **B.** CONCLUSIONS

This thesis pointed out the prevalence of cyber attacks, as well as establishing that government computers are not necessarily safe from these attacks. This thesis considered the effects of deploying the best security tools to thwart specific attack methods. The model showed that even with all security tools in place, a ship is still susceptible to attack, however, the risk is much less with the tools in place. This thesis demonstrates a possible means of measuring that risk.

After completing and running the model it proved to be as useful as I had hoped, though a few recommendations as listed in the preceding section could make the model even more useful. Overall, the model does seem to have the key components of a good model such as adequate scope, complexity, and re-use. As far as the scope, I believe this particular model adequately modeled the system to be studied (i.e., network security) and that once populated and run could provide the user with enough information that he/she could make a good decision. Additionally the model was clear and easy to understand, yet complex enough to answer the question of interest. Lastly, the model has re-use potential. In addition to being a good training tool, the model with modification could be used to model any number of threat scenarios and provide the likelihood of their success.

## **APPENDIX A EXPERT OPINION SURVEY**

The following survey was distributed to various Naval Postgraduate School professors in the fields of Computer Science and Information Assurance as well as to technical personnel working as network security administrators. The survey was designed to gather collective experience and compiled opinions of the domain experts; they do not represent product review evaluations of network systems. The data collected was then averaged and used to assign link strength values within the SIAM model. Unfortunately only four surveys were returned. The summary results of all surveys are attached as Appendix B.

#### Expert Opinion Research Tool - FIREWALL 1 If a FIREWALL were used, how likely is it that the system could prevent a VIRUS from infecting the targeted system? More Less likely No Impact Likely Slightly Severely Severely Strongly Moderately Slightly Moderately Strongly Severely Severely Inhibits Inhibits Inhibits Inhibits Inhibits No Impact promotes promotes promotes promotes promotes 2 If a FIREWALL were NOT used, how likely is it that the system could prevent a VIRUS from infecting targeted system? More Less likely No Impact Likely Severely Severely Strongly Moderately Slightly Slightly Moderately Strongly Severely Severely Inhibits Inhibits Inhibits Inhibits Inhibits No Impact promotes promotes promotes promotes promotes 3 If a FIREWALL were used, how likely is it that the system could prevent a WORM from infecting the targeted system? Less More likely No Impact Likely Slightly Severely Severely Strongly Moderately Slightly Moderately Strongly Severely Severely Inhibits Inhibits Inhibits Inhibits Inhibits No Impact promotes promotes promotes promotes promotes . 4 If a FIREWALL were NOT used, how likely is it that the system could prevent a WORM from infecting targeted system? Less More likely No Impact Likely Slightly Severely Slightly Severely Severely Strongly Moderately Moderately Strongly Severely Inhibits Inhibits Inhibits Inhibits Inhibits No Impact promotes promotes promotes promotes promotes If a FIREWALL were used, how likely is it that the targeted system could prevent being taken over and turned into a 5 ZOMBIE by an attacker? More Less Likely likely No Impact Severely Severely Strongly Moderately Slightly Slightly Moderately Severely Strongly Severely Inhibits Inhibits Inhibits promotes Inhibits Inhibits No Impact promotes promotes promotes promotes If a FIREWALL were NOT used, how likely is it that the target system could prevent being taken over by an attacker and 6 turned into a ZOMBIE? Less More likely No Impact Likely Severely Moderately Slightly Severely Severely Strongly Slightly Moderately Strongly Severely Inhibits Inhibits Inhibits Inhibits Inhibits No Impact promotes promotes promotes promotes promotes

## 1. FIREWALL SECTION OF SURVEY

	If a FIRE\	WALL were	e used, ho	w likely is it t	that the sys	tem could	prevent a	TROJAN HOP	RSE from po	enetrating	the
7	targeted	system?									
	Less										More
	likely	0 1	0. 1		OF LH	No Impact	01.111		0. 1	0 1	Likely
	Severely	Severely	Strongly	Woderately	Slightly	No. Income	Slightly	Woderately	Strongly	Severely	Severely
	Innibits	Innibits	Innibits	Innibits	Innibits	No Impact	promotes	promotes	promotes	promotes	promotes
	If a EIREN			d how likely	ie it that th	o svetom c	ould prove	ant a TRO IAN		om nonotra	ting the
8	targeted	evetom2	e nor use	u, now neery	is it that t	ie system t	oulu pieve			nii peneua	ung me
0	Lace	ayatem.									More
	likely					No Impact					Likely
	Severely	Severely	Strongly	Moderately	Slightly	ite impuer	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
							promotoo	promotoo	promotor		
					_						
_	If a FIRE	WALL wer	e used. ho	w likelv is it t	that the sv	tem could	prevent a	BACKDOOR	from beina	placed in t	the target
9	system?			,	,						3
	Less										More
	likely					No Impact					Likelv
_	Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
							promotoo	promotoo	promotoo	promotor	
	If a FIRE	WALL wer	e NOT use	d. how likely	is it that th	e system c	ould preve	ent a BACKDO	OOR from b	eing place	d in the
0	targeted	system?		-,,							
	Less	1									More
	likely			L L		No Impact					Likely
	Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
_											
	If a FIRE\	WALL wer	e used. ho	w likely is it t	that the sv	tem could	prevent a	Denial Of Se	rvice (DOS	) attack fro	m
1	If a FIRE\	WALL were	e used, ho	w likely is it t	that the sys	tem could	prevent a	Denial Of Se	rvice (DOS)	) attack fro	m
1	If a FIRE\ disrupting	WALL were g service o	e used, ho on the targ	w likely is it t eted system?	that the sys	tem could	prevent a	Denial Of Se	rvice (DOS	) attack from	m
1	If a FIRE disrupting Less likely	WALL were g service o	e used, ho on the targ	w likely is it interest of the system?	that the sys	item could	prevent a	Denial Of Se	rvice (DOS	) attack from	m More Likely
1	If a FIRE\ disrupting Less likely Severely	WALL were g service of	e used, ho on the targ	w likely is it i eted system? Moderately	that the sys	item could	prevent a	Denial Of Se	rvice (DOS	) attack from	m More Likely Severely
1	If a FIREN disrupting Less likely Severely Inhibits	WALL were g service of Severely	e used, ho on the targ Strongly	w likely is it i eted system? Moderately	slightly	item could No Impact	prevent a Slightly	Denial Of Se Moderately	rvice (DOS)	) attack from	m More Likely Severely
1	If a FIREN disruptin Less likely Severely Inhibits	WALL were g service o Severely Inhibits	e used, ho on the targ Strongly Inhibits	w likely is it i eted system? Moderately Inhibits	that the sys	tem could No Impact No Impact	prevent a Slightly promotes	Denial Of Se Moderately promotes	rvice (DOS) Strongly promotes	attack from	m More Likely Severely promotes
1	If a FIREN disrupting Less likely Severely Inhibits	WALL were g service of Severely Inhibits	e used, ho on the targ Strongly Inhibits	w likely is it i eted system? Moderately Inhibits	Slightly	tem could No Impact No Impact	prevent a Slightly promotes	Denial Of Se Moderately promotes	rvice (DOS) Strongly promotes	attack from	m More Likely Severely promotes
1	If a FIREN disrupting Less likely Severely Inhibits	WALL were g service of Severely Inhibits	e used, ho on the targ Strongly Inhibits	w likely is it i eted system? Moderately Inhibits	Slightly	tem could No Impact No Impact	prevent a Slightly promotes	Denial Of Se Moderately promotes	rvice (DOS) Strongly promotes	attack from	m More Likely Severely promotes
1	If a FIREN disrupting Less likely Severely Inhibits	WALL were g service of Severely Inhibits	e used, ho on the targ Strongly Inhibits	w likely is it i eted system? Moderately Inhibits	Slightly Inhibits	No Impact	prevent a Slightly promotes	Denial Of Se Moderately promotes	strongly promotes	Severely promotes	m More Likely Severely promotes
2	If a FIRE\ disruptin Less likely Severely Inhibits	WALL wern g service of Severely Inhibits WALL wern system?	e used, ho on the targ Strongly Inhibits e NOT use	w likely is it i eted system? Moderately Inhibits d, how likely	Slightly Inhibits	No Impact	prevent a Slightly promotes ould preve	Denial Of Se Moderately promotes	Strongly promotes	Severely promotes	m More Likely Severely promotes
1	If a FIREL disrupting Less likely Severely Inhibits If a FIREL targeted	WALL were g service of Severely Inhibits WALL were system?	e used, ho on the targ Strongly Inhibits e NOT use	w likely is it i eted system? Moderately Inhibits d, how likely	Slightly Inhibits	item could No Impact No Impact	prevent a Slightly promotes ould preve	Denial Of Se Moderately promotes ent a DOS fro	Strongly promotes	Severely promotes	m More Likely Severely promotes on the
2	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely	WALL wern g service of Severely Inhibits WALL wern system?	e used, ho on the targ Strongly Inhibits e NOT use	w likely is it t eted system? Moderately Inhibits d, how likely	Slightly Inhibits	tem could No Impact No Impact	prevent a Slightly promotes ould preve	Denial Of Se Moderately promotes ent a DOS fro	Strongly promotes	Severely promotes	m More Likely Severely promotes on the More
2	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely Severely	WALL were g service of Severely Inhibits WALL were system?	e used, ho on the targ Strongly Inhibits e NOT use	Moderately Moderately Inhibits	Slightly is it that the	tem could No Impact No Impact e system c	prevent a Slightly promotes ould preve	Denial Of Se Moderately promotes ent a DOS fro	Strongly promotes	attack from Severely promotes	m More Likely Severely promotes on the More Likely Severely
1	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely Severely Inhibits	WALL were g service of Severely Inhibits WALL were system?	e used, ho on the targ Strongly Inhibits e NOT use Strongly	Moderately d, how likely Moderately	Slightly Inhibits is it that the Slightly	No Impact No Impact	prevent a Slightly promotes ould preve	Denial Of Se Moderately promotes ent a DOS fro Moderately	strongly promotes m disruptin	attack from Severely promotes	m More Likely Severely promotes on the More Likely Severely promotor
2	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely Severely Inhibits	WALL were g service of Severely Inhibits WALL were system? Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits	Moderately Inhibits Moderately Inhibits d, how likely Moderately Inhibits	Slightly Inhibits is it that the Slightly	tem could No Impact No Impact e system c No Impact No Impact	prevent a Slightly promotes ould preve Slightly promotes	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes	strongly promotes m disruptin	attack from Severely promotes	m More Likely Severely promotes on the More Likely Severely promotes
2	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely Severely Inhibits	WALL were g service of Severely Inhibits WALL were system? Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits	Slightly Inhibits is it that the Slightly Inhibits	tem could No Impact No Impact e system c No Impact	prevent a Slightly promotes ould preve Slightly promotes	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes	strongly promotes m disruptin Strongly promotes	) attack from Severely promotes	m More Likely Severely promotes on the More Likely Severely promotes
2	If a FIREL disruption Less likely Severely Inhibits If a FIREL targeted Less likely Severely Inhibits	WALL were g service of Severely Inhibits WALL were system? Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits	Slightly Inhibits is it that the Slightly Inhibits	tem could No Impact No Impact e system c No Impact	prevent a Slightly promotes ould preve	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes	strongly promotes m disruptin Strongly promotes	attack from Severely promotes	m More Likely Severely promotes Dn the More Likely Severely promotes
2	If a FIREL disrupting Less likely Severely Inhibits If a FIREL targeted Less likely Severely Inhibits	WALL were g service of Severely Inhibits WALL were system? Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits	Slightly Inhibits is it that the Slightly Inhibits	tem could No Impact No Impact e system c No Impact	prevent a Slightly promotes ould preve	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes	strongly promotes m disruptin Strongly promotes	attack from Severely promotes	m More Likely Severely promotes on the More Likely Severely promotes
2	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely Severely Inhibits	WALL were g service of Severely Inhibits WALL were Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits e used, ho	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits w likely is it i	Slightly Inhibits is it that the Slightly Inhibits	tem could No Impact No Impact No Impact No Impact No Impact	prevent a Slightly promotes ould preve Slightly promotes prevent a	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes LOGIC BOME	strongly promotes m disruptin Strongly promotes 3 attack aga	attack from Severely promotes severely promotes Severely promotes	m More Likely Severely promotes on the More Likely Severely promotes rgeted
2	If a FIREL disrupting Less likely Severely Inhibits If a FIREL Severely Inhibits If a FIREL System?	WALL were g service of Severely Inhibits WALL were Severely Inhibits WALL were	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits e used, ho	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits	Slightly Inhibits is it that the Slightly Inhibits that the system	tem could No Impact No Impact No Impact No Impact No Impact	prevent a Slightly promotes ould preve Slightly promotes prevent a	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes LOGIC BOME	strongly promotes m disruptin Strongly promotes 3 attack aga	attack from Severely promotes severely promotes Severely promotes	m More Likely Severely promotes on the More Likely Severely promotes rgeted
2	If a FIRE\ disruptiny Less likely Severely Inhibits If a FIRE\ targeted Less likely Severely Inhibits If a FIRE\ system? Less	WALL were g service of Severely Inhibits WALL were Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits e used, ho	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits	Slightly Inhibits is it that the Slightly Inhibits	tem could No Impact No Impact No Impact No Impact No Impact	prevent a Slightly promotes ould preve Slightly promotes prevent a	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes LOGIC BOME	Strongly promotes m disruptin Strongly promotes 3 attack aga	attack from Severely promotes ag service of Severely promotes	m More Likely Severely promotes on the More Likely Severely promotes rgeted
12	If a FIREV disruptiny Less likely Severely Inhibits If a FIREV targeted Less likely Severely Inhibits If a FIREV system? Less likely	WALL were g service of Severely Inhibits WALL were system? Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits e used, ho	Moderately Inhibits Moderately Inhibits d, how likely Moderately Inhibits	Slightly Inhibits is it that the Slightly Inhibits that the system	No Impact No Impact No Impact No Impact No Impact No Impact	prevent a Slightly promotes ould preve Slightly promotes prevent a	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes	strongly promotes m disruptin Strongly promotes 3 attack age	attack from Severely promotes g service of Severely promotes ainst the ta	m More Likely Severely promotes on the More Likely Severely promotes rgeted
2	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely Severely Inhibits If a FIREV system? Less likely Severely	WALL were g service of Severely Inhibits WALL were system? Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits e used, ho	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits w likely is it i	Slightly Inhibits Slightly Inhibits Slightly Inhibits Slightly	tem could No Impact No Impact No Impact No Impact No Impact tem could No Impact	prevent a Slightly promotes ould preve Slightly promotes prevent a Slightly	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes LOGIC BOME	strongly promotes m disruptin Strongly promotes 3 attack aga Strongly	attack from Severely promotes g service of Severely promotes ainst the ta	More Likely Severely promotes on the More Likely Severely promotes rgeted More Likely Severely Severely
2	If a FIREV disrupting Less likely Severely Inhibits If a FIREV targeted Less likely Severely Inhibits If a FIREV system? Less likely Severely Inhibits	WALL were g service of Severely Inhibits WALL were system? Severely Inhibits WALL were Severely Inhibits	e used, ho on the targ Strongly Inhibits e NOT use Strongly Inhibits e used, ho Strongly Inhibits	w likely is it i eted system? Moderately Inhibits d, how likely Moderately Inhibits w likely is it i Moderately Inhibits	Slightly Inhibits is it that the Slightly Inhibits Slightly Inhibits Slightly Inhibits	tem could No Impact No Impact No Impact No Impact No Impact tem could No Impact	prevent a Slightly promotes ould preve Slightly promotes prevent a Slightly promotes	Denial Of Se Moderately promotes ent a DOS fro Moderately promotes LOGIC BOME Moderately promotes	strongly promotes m disruptin Strongly promotes attack aga Strongly promotes	attack from Severely promotes g service of Severely promotes ainst the ta Severely promotes	m More Likely Severely promotes Don the More Likely Severely promotes rgeted More Likely Severely promotes

If a FIRE 4 system?	WALL wer	e NOT use	d, how likely	is it that th	e system c	ould preve	ent a LOGIC E	SOMB attac	k against tl	ne targeted
Less likely					No Impact					More Likely
Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
							5			•
If a FIRE	WALL wer	e used, ho	w likely is it t	hat the sys	tem could	prevent a	n E-mail SPO	OFING atta	ck against i	the
Less										More
likely	Courseha	Changely	Madaastah	Climbal	No Impact	Olizabelia	Madaatak	Changeles	Coursely	Likely
Severely	Severely Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
If a FIRE	WALL wer	e NOT use	d, how likely	is it that th	e system c	ould preve	ent an E-mail	SPOOFING	attack aga	ainst the
6 targeted	system?		· ·		,					
Less					No Import					More
Severely	Severely	Stronaly	Moderately	Slightly	по тпраст	Slightly	Moderately	Stronaly	Severely	Severely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
If a FIRE	WALL wer	e used, ho	w likely is it t	hat the sys	tem could	prevent a	n IP Address	Spoofing a	ttack again	st the
7 targeted	system?									14
likelv			- F	22	No Impact	· <b>۲</b>	K			Likely
Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
If a FIRE	WALL were	e NOT use	d, how likely	is it that th	ie system o	ould preve	ent an IP Add	ress SPOO	FING attack	against
Less	ieu systen	1:								More
likely					No Impact					Likely
Severely	Severely	Strongly	Moderately	Slightly	No. Inc.	Slightly	Moderately	Strongly	Severely	Severely
Innibits	Innibits	Inhibits	Infilbits	Innibits	No impact	promotes	promotes	promotes	promotes	promotes
								6		
9 system?	WALL Wer	e usea, no	w likely is it t	nat the sys	tem could	prevent a	NET LUGGER	from bein	g used in ta	argeting a
Less										More
likely	Coursely	Chronoliu	Mederately	Clinhthy	No Impact	Oliobthy	Madaratak	Changles	Coursely	Likely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
If a FIRE	WALL wer	e NOT use	d, how likely	is it that th	e system c	ould preve	ent a KEY LOC	GGER from	being used	1 in
Less	a system									More
likely					No Impact					Likely
Severely	Severely Inhibite	Strongly	Moderately Inhibits	Slightly	No Impact	Slightly	Moderately	Strongly	Severely	Severely
innibits	minutes	innoits	initial s	minutes	No impact	promotes	promotes	promotes	promotes	promotes

	If a FIREV	VALL were	e used, ho	w likely is it t	hat the sys	tem could	prevent a	SNIFFER fron	n being use	ed in target	ing a
21	system?										0
	Less										More
	likely					No Impact					Likely
	Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
	If a FIREV	VALL were	e NOT use	d, how likely i	is it that th	e system o	ould preve	ent a SNIFFEF	l from bein	g used in t	argeting a
22	system?										
	Less										More
	likely					No Impact					Likely
	Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
	If a secon	nd FIREWA	LL were u	ised, how like	ly is it tha	t the syster	n could pr	event one/an	y of the ab	ove attack	methods?
23	Please ex	cplain in s	pace provi	ided.							
	Less										More
	likely					No Impact					Likely
	Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits 📕	Inhibits	No Impact	promotes	promotes	promotes	promotes	promotes
	Explanation	on of benefit	a second t	firewall would							
	provide:										
					1	1		1			
								• •		• • •	·
~	If a secon		LL were n	ot used, how	likely is it	that the sy	stem could	d prevent one	any of the	above atta	ack
24	methods	Please e	explain is s	space provide	a.						14
	Less					Ne leans -t					iviore
	likely Causalu	Coursel	Channels	Madaatab	Olimbali	ivo impact	Olivebal	Madaastati	Channelle	Courselui	Causalu
	Severely	Severely	Strongly	woderately	Slightly	Nie Immerst	Slightly	woderately	Strongly	Severely	Severely
	Innibits	Innibits	Innibits	Innibits	Innibits	INO IMPACT	promotes	promotes	promotes	promotes	promotes
	Evolopetic	n of honofi	a cocord	frowall would							
	Explanatio	in or benefit	a second i	mewan would							
	provide.										

# 2. IDS/IPS SECTION OF SURVEY

If an IDS/IPS system were used, how likely is it that the system could prevent a VIRUS from         1       If an IDS/IPS system were used, how likely is it that the system could prevent a VIRUS from         2       Severely       Severely       Strongly       Moderate       Sightly       Moderate       Strongly       Severely       Moderate       Sightly       Moderate       Sightly       Moderate       Severely       Severely       Severely       More Likely         2       If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VIRUS from       More Likely       Severely					Exper	t Opinio	on Rese	arch Too	ol - IDS/IPS			
If an ID5/IPS system were used, how likely is it that the system could prevent a VIRUS from       More Likely         Less likely       Severely       Strongly       Moderate       Sighty       Moderately       promotes       promotes         If an ID5/IPS system were NOT used, how likely is it that the system could prevent a VIRUS from       If an ID5/IPS system vere NOT used, how likely is it that the system could prevent a VIRUS from         If an ID5/IPS system vere NOT used, how likely is it that the system could prevent a VIRUS from       More Likely       More Likely         Severely       Severely       Strongly       Moderate       Sighty       No         If an ID5/IPS system vere used, how likely is it that the system could prevent a VORM from       Inhibits       More Likely         Severely       Severely       Strongly       Moderate       Sighty       No         If an ID5/IPS system vere used, how likely is it that the system could prevent a VORM from       Strongly       More Likely         If an ID5/IPS system vere used, how likely is it that the system could prevent a VORM from       Storngly       More Likely         Severely       Severely       Strongly       More Likely       Strongly       More Likely         Severely       Severely       Strongly       More Likely       More Likely       Strongly       More Likely         Less likely												
1       infecting the targeted system?       No Impact       Moderately promote       Severely severely severely promote         2       Less likely severely inhibits       Inhibits       Inhibits       Severely inhibits       Moderately promote       Severely promote         2       If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VIRUS from infecting targeted system?       More Likely inhibits       More Likely inhibits         2       Eess likely severely inhibits       Strongly Moderate Slightly inhibits       More Likely inhibits       More Likely inhibits         2       Eess likely severely Strongly Inhibits       Inhibits       Inhibits       More Likely inhibits         3       Inhibits       Inhibits       Inhibits       Inhibits       More Likely inhibits         4       Inhibits       Inhibits       Inhibits       More Likely inhibits       Strongly informate         4       Inhibits       Inhibits       Inhibits       Inhibits       More Likely inhibits       Strongly informate       Strongly informate         4       Inhibits       Inhibits       Inhibits       Inhibits       More Likely inhibits       Strongly inhibits       Strongly inhibits         5       Severely Severely Strongly inhibits       Moderatel Sightly inhibits       More Likely inhibits       Strongly i	_	lf an IDS	JIPS car	tom More	a usad br	u litale	is it that	the cast	em could n	ouent a l	l IBUS 6r	
Less likely       Severely       Strongly       Moderate       Strongly       Moderate       Strongly       More Likely         Severely       Severely       Strongly       Inhibits       Inhibits       Strongly       Severely       Moderate       Sightly       Moderately       Severely       <	1	infecting	the targ	eted sys	tem?	/ incerg	13 14 414	e <b>33</b> 3.	em ooala pi	event a t	1100 110	
Severely       No Impact       Moderately       Severely       More Likely         Severely       Severely       Severely       Severely       Severely       Severely       More Likely         Severely       Severely       Severely       Severely       Severely       More Likely         Severely       Severely       Severely       Severely       More Likely       Severely       Severely <td< th=""><th></th><th>Less likely</th><th></th><th></th><th></th><th></th><th>No Impa</th><th>ct</th><th></th><th></th><th></th><th>More Likely</th></td<>		Less likely					No Impa	ct				More Likely
Inhibits       Inhibits <th< th=""><th></th><th>Severely</th><th>Severely</th><th>Strongly</th><th>Moderate</th><th>Slightly</th><th>No</th><th>Slightly</th><th>Moderately</th><th>Strongly</th><th>Severely</th><th>Severely</th></th<>		Severely	Severely	Strongly	Moderate	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VIRUS from       More Likely         Less likely       Severely       Strongly       Moderate       Slightly       No Impact       More Likely         Severely       Severely       Strongly       Inhibits       Inhibits       Slightly       Moderately       Strongly       Severely       More Likely         Severely	_	Inhibits	Inhibits	Inhibits	ly inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotes
If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VIRUS from         2       Less likely       Severely       Strongly       Moderate Sightly       No Impact       Moderately       Strongly       Promote       promote       promote       promote       promote       More Likely         Severely       Severely       Strongly       Inhibits       Inhibits       Inhibits       No Impact       Moderately       Strongly       promote       promote       promote       promote       Severely       Severely       Severely       Severely       Severely       promote       promote       promote       promote       More Likely         3       If an IDS/IPS system were used, how likely is it that the system could prevent a WORM from       If an IDS/IPS system were NOT used, how likely is it that the system could prevent a WORM from       If an IDS/IPS system were NOT used, how likely is it that the system could prevent a WORM from         4       If an IDS/IPS system were used, how likely is it that the system could prevent a WORM from       If an IDS/IPS system were used, how likely is it that the system could prevent a WORM from         4       If an IDS/IPS system were used, how likely is it that the target dynamic promote       Strongly       More Likely         Severely       Severely       Strongly       Moderate Sightly       No       More Likely	_											
If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VIRUS from         2 infecting targeted system?         Less likely       Severely         Severely       Strongly         Inhibits       Severely         If an IDS/IPS system were used, how likely is it that the system could prevent a VORM from         3       Severely         Severely       Severely         Inhibits       Inhibits         Inhibits       Severely         Severely       Severely         Inhibits       Inhibits         Inhibits       In	_											
2       infecting targeted system?       No Impact       More Likely         Severely       Severely       Strongly       Moderate       Slightly       No Impact       Severely         Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       More Likely         Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Severely         If an IDS/IPS system were used, how likely is it that the system could prevent a VORM from         3       infecting the targeted system?         Less likely       Severely       Strongly       Moderate       Slightly       Moderately       Strongly       Severely         Severely       Severely       Strongly       Moderate       Slightly       No Impact       Moderately       Strongly       Severely         Severely       Severely       Severely       Strongly       Moderate       Slightly       No Impact       Moderately       Strongly       Severely       Severely         Inhibits       Inhibits       Inhibits       No Impact       Moderately       Strongly       Severely       Severely         Inhibits       Inhibits       Inhibits       Inhibits       No Impact       More Likely       Severely       Severely <th></th> <th>lf an IDS</th> <th>/IPS sys</th> <th>tem wer</th> <th>e NOT us</th> <th>ed, how</th> <th>likely is i</th> <th>t that the</th> <th>system co</th> <th>uld preve</th> <th>nt a ¥IRl</th> <th>JS from</th>		lf an IDS	/IPS sys	tem wer	e NOT us	ed, how	likely is i	t that the	system co	uld preve	nt a ¥IRl	JS from
Less likely       Severely       Strongly       Moderate       Slightly       No Impact       Moderately       Strongly       Severely       Moderate       Sightly       Moderate       Sightly       Moderate       More Likely         Severely       <	2	infecting	targete	d system	1?				1			
Severely Inhibits       Strongly Inhibits       Moderate Inhibits       Strongly Inhibits       More Likely Inhibits         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from infecting targeted system?       Moderate Inhibits       Moderate Inhibits       Strongly Inhibits       Strongly Inhibits       Strongly Inhibits       More Likely Inhibits         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from infecting targeted system?       Moderate Inhibits       Moderate Inhibits       Moderate Inhibits       Strongly Inhibits       Strongly Inhibits       Severely Inhibits       Moderate Inhibits       Moderate Inhibits       Moderate Inhibits       Strongly Inhibits       Severely Inhibits       Strongly Inhibits       Severely Inhibits       Moderate Inhibits       Strongly Inhibits       Severely Inhibits       Severely Inhibits       Strongly Inhibits       Severely Inhibits       Severely Inhibits       Severely Inhibits       Severely Inhibits       Severely Inhibits       Severely Inhib		Localikolu					Nolma	ct.				More Likelu
Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Impact       promote       promote <td>_</td> <td>Severelu</td> <td>Severelu</td> <td>Stronglu</td> <td>Moderate</td> <td>Sliahtlu</td> <td>No</td> <td>Slightlu</td> <td>Moderatelu</td> <td>Stronglu</td> <td>Severelu</td> <td>Severelu</td>	_	Severelu	Severelu	Stronglu	Moderate	Sliahtlu	No	Slightlu	Moderatelu	Stronglu	Severelu	Severelu
If an IDS/IPS system were used, how likely is it that the system could prevent a VORM from         3 infecting the targeted system?         Less likely         Severely         Inhibits         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         4 infecting targeted system?         Less likely         Severely         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         4 infecting targeted system?         Less likely         Severely         Severely         Severely         Inhibits         Inhibits         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         4         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         5       over and turned into a ZOMBIE by an attacker?         Less likely       Severely         Severely       Inhibits         Inhibits       Inhibits         Inhibits       No Impact         No Impact       Moderately         Severely       Severely         Inhibits       No Impact         No Impact       Moderately         Severely		Inhibits	Inhibits	Inhibits	lu Inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotes
If an IDS/IPS system were used, how likely is it that the system could prevent a WORM from         3 infecting the targeted system?         Less likely         Severely       Severely         Inhibits       Inhibits         Inhibits       Inhibits         Inhibits       Noderate         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a WORM from         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a WORM from         4 infecting targeted system?         Less likely         Severely       Inhibits         Inhibits       No Impact         More Likely         Severely       Severely         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a WORM from         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         5       Severely         Inhibits       Inhibits         Inhibits       Inhibits         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         5       Over and turned into a 20MBIE by an attacker?         Less likely       No Impact         Severely       Severely         Inhibits       Inhibits         S					1							
If an IDS/IPS system vere used, how likely is it that the system could prevent a VORM from         3         1         2       Less likely         Severely       Severely         1       Inhibits         1       Inhibits         1       Inhibits         2       Less likely         Severely       Severely         1       Inhibits         1       Inhibits <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>												
an IDSRPS system were used, now likely is it that the system could prevent a VORM from         3 infecting the targeted system?         Less likely       Severely         Severely       Inhibits         Inhibits       Wolf and the system?         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         If an IDS/IPS system were used, how likely is it that the targeted system?         Less likely       Strongly         Inhibits       Inhibits         Inhibits       Inhibits         Inhibits       Inhibits         Inhibits       Strongly         Inhibits       Inhibits         Inhibits       Inhibits         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         5 over and turned into a ZOMBIE by an attacker?         Less likely       Severely         Severely       Inhibits         Inhibits       Inhibits         Inhibits       Inhibits         Isseerely       Mo		K IDC	UDC				in it that					
Simeoting the daycete system:       No Impact       More Likely         Severely       Severely       Strongly       Moderate Slightly       No       Impact       Moderately       Strongly       Severely       Severely       Severely       promote       promote       promote       Severely       Severely       Severely       promote       promote       promote       promote       Severely       Severely       promote	3	infecting	rir ə sys i the tare	iotod ceo	e usea, na :tom?	ow likely	is it that	t the syst	em coula pi	event a i	PURM IN	om
Less likely       Moderately       More Likely       More Likely       More Likely         Severely       Inhibits       Inhibits       Inhibits       Inhibits       Strongly       More Likely       Severely       More Likely       More Likely       More Likely       Severely       More Likely       More Likely       More Likely       More Likely       More Likely       Severely       Severely <td>-</td> <td>meeting</td> <td>the targ</td> <td>eteu sys</td> <td>,</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	-	meeting	the targ	eteu sys	,							
Severely Inhibits       Severely Inhibits       Strongly Inhibits       Moderate Stightly Inhibits       No       Slightly promote       Moderately promote       Strongly promote       Severely promote       More Likely         4       If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       No Impact       More Likely       Severely promote       Severely promote       Severely promote       More Likely         5       If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       No Impact       More Likely       More Likely         5       If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?       More Likely       Severely promote       Severely promote       More Likely Severely promote         6       If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into		Less likely					No Impa	ct				More Likely
Inhibits       Inhibits       Inhibits       Inhibits       Impact       promote       promotes       promote       promote <td></td> <td>Severely</td> <td>Severely</td> <td>Strongly</td> <td>Moderate</td> <td>Slightly</td> <td>No</td> <td>Slightly</td> <td>Moderately</td> <td>Strongly</td> <td>Severely</td> <td>Severely</td>		Severely	Severely	Strongly	Moderate	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         Is a IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from         Is a IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         Severely       Severely       No Impact         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken       More Likely         Severely       Severely       Strongly       Moderate       Slightly       More Likely         Severely       Severely       Inhibits       Inhibits       No Impact       More Likely       More Likely         Severely       Severely       Severely       Moderate       Slightly       Moderate       Slightly       More Likely         Severely       Inhibits       Inhibits       Inhibits       Inhibits       No Impact       More Likely       More Likely         Severely       Inhibits		Inhibits	Inhibits	Inhibits	ly Inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotes
If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VORM from infecting targeted system?       Mo Impact       More Likely         Less likely       Severely       Severely       Severely       Severely       Moderate       Slightly       Moderately       promote       Severely       Severely       Severely       Severely       Severely       Inhibits       Inhibits       Inhibits       Inhibits       No Impact       Moderately       Strongly       Severely       Severely       Severely       Severely       Severely       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Strongly       Severely       More Likely       More Likely         5       If an IDS/IPS system were used, how likely is it that the target system could prevent being taken       Severely									1			
If an IDS/IPS system vere NOT used, how likely is it that the system could prevent a VORM from infecting targeted system?       More Likely severely is it that the system could prevent a VORM from More Likely severely inhibits         Less likely       Severely inhibits       More Likely is it that the targeted system could prevent a VORM from Slightly inhibits       More Likely severely promote         If an IDS/IPS system vere used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       More Likely is it that the targeted system could prevent being taken         If an IDS/IPS system vere used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       More Likely is it that the targeted system could prevent being taken         If an IDS/IPS system vere used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       More Likely is it that the target system could prevent being taken         If an IDS/IPS system vere NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?       More Likely is it that the target system could prevent being is it taken over by an attacker and turned into a ZOMBIE?         If an IDS/IPS system vere NOT used, how likely is it that the target system could prevent being is it taken over by an attacker and turned into a ZOMBIE?       More Likely is it that the target system could prevent being is it taken over by an attacker and turned into a ZOMBIE?         If an IDS/IPS system vere NOT used, how likely is it that the target system could prevent be	_					C	44					
4       infecting targeted system?       No Impact       More Likely         Less likely       Severely       Severely       Strongly       Moderate       Slightly       Moderately       promote       Severely       Severely       Severely       Inhibits       Inhibits       Inhibits       No Impact       Moderately       Severely       Severely       Severely       Severely       Inhibits       Inhib	_	lf an IDS	/IPS sus	tem ver	e NOT use	ed. how	likelu is i	t that the	sustem co	uld preve	nt a VOF	SM from
Less likely       Severely Inhibits       Severely Inhibits       Noderate Sightly Inhibits       No Impact Moderate Inhibits       Moderate Sightly Impact       Moderate Sightly Impact       Moderately Promote       Strongly Promote       Severely Promote       More Likely Severely Promote         If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       No Impact       Impact       More Likely       More Likely         Severely Inhibits       Severely Inhibits       Moderate Impact       No Impact       Impact       More Likely       More Likely         Severely Inhibits       Severely Inhibits       Moderate Impact       No Impact       Impact       Impact       More Likely         Severely Inhibits       Severely Inhibits       Moderate Imhibits       No Impact       Impact       Impact       More Likely         If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?       Impact	4	infecting	targete	d system	1?		····,··		-,			
Less likely       No impact       Moderately       No impact       Moderately       Strongly       Severely       Severely       Severely       Severely       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       No       Inhibits       Inhibits       Severely       Severely       Severely       Severely       Promote       Promote       Promote       Promote       Promote       Severely       Severely       Severely       Promote       Promote       Promote       Promote       Promote       Promote       Severely       Severely       Promote												
Severeing Inhibits       Severeing Inhibits       Severeing Inhibits       Severeing Inhibits       Severeing Impact       Severeing promote       More Likely         5       Severeing Inhibits       Strongly Inhibits       Strongly Inhibits       Moderate Sightly Inhibits       No Impact       Moderately promote       Strongly promote       Severeing promote       Severeing promote       More Likely promote         6       If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?       More Likely promote       More Likely promote       Severeing promote       More Likely promote       Severeing promote       Severeing promote       Severeing promote       Severeing promote       Severeing promote       Severeing promote       Severeing promote       Severeing promote	_	Less likely Coursely	Courselu	Chronolu	Madarata	Clinktle	No Impa No	Clinialation	Madaratalu	Chronolu	Coursela	More Likely Severals
Impose		lohibite	Inhibits	Inhibits	In Inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotes
If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       No Impact       More Likely         Less likely       No Impact       Severely       Severely       No Impact       More Likely         Severely       Inhibits       Inhibits       No Impact       Severely       Severely         Inhibits       Inhibits       Inhibits       No Impact       Moderately       Severely         Inhibits       Inhibits       Inhibits       No Impact       No       Severely         Inhibits       Inhibits       Inhibits       No Impact       No       Severely         Inhibits       Inhibits       Inhibits       No Impact       No       No       Severely         Inhibits       Inhibits       No Impact       No       No       No       No       No         If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being       Moderately       No       More Likely         It as in this       No       Impact       No Impact       More Likely       More Likely         Severely       Inhibits       Inhibits       No Impact       No       More Likely         Severely       Inhibits       Inhibits       No		in indico	in indico	in indico	ig minores	IIIIIBK9	Impdox	promote	promoteo	promote	promote	promoteo
If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?       No Impact       No Impact       More Likely Severely inhibits       More Likely Severely inhibits       Severely inhibits       Strongly inhibits       Severely inhibits       More Likely Severely inhibits       More Likely inhibits </td <td></td>												
If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken         5       over and turned into a ZOMBIE by an attacker?       More Likely       More Likely         2       Less likely       Inhibits       No Impact       Inhibits       More Likely         2       Severely       Severely       Inhibits       Inhibits       Moderate       Slightly       Moderately       Strongly       Severely       Severely       Severely       Inhibits       Inhibits       Inhibits       Severely       Inhibits       Severely       Inhibits       Inhibits       Inhibits       No       Severely       Inhibits       Severely       Severely       Severely       Severely       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Severely       Severely       Severely       Severely       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       More Likely         6       If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being       More Likely       More Likely       More Likely         6       taken over by an attacker and turned into a ZOMBIE?       No Impact       Inhibits       More Likely       Severely       Severely       Severely       Severely       Severely       Seve												
5       over and turned into a 2UMBIE by an attacker?         Less likely	_	If an IDS	/IPS sys	tem wer	e used, ha	ow likely	is it that	t the targ	eted system	i could pi	event be	ing taken
Less likely	5	over and	turned i	nto a ZL	IMBIE DY	an attac	xer?		1	1	1	1
Severely Inhibits       Severely Inhibits       Severely Inhibits       Strongly Inhibits       Strongly Inhibits       Severely Inhibits       Moderatel Impact       Strongly Promote       Severely Promote       More Likely Promote         6       If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being       More Likely       More Likely       More Likely         6       Less likely       Image: Severely Inhibits       Moderate       Sightly Inhibits       Moderate       Sightly Promote       More Likely         8       Severely Inhibits       Inhibits       Moderate       Sightly Inhibits       No       Sightly Promote       Moderately Promote       Strongly Promote       Severely Promote       Severely Promote       Severely Promote       Severely Promote       Severely Promote       Severely Promote       Severely Promote       Severely Promote         1       Inhibits		Less likelu					No Impa	ct				More Likelu
Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Imhibits       Imhibits <td< td=""><td>_</td><td>Severelu</td><td>Severelu</td><td>Strongly</td><td>Moderate</td><td>Slightly</td><td>No</td><td>Slightly</td><td>Moderately</td><td>Strongly</td><td>Severelu</td><td>Severelu</td></td<>	_	Severelu	Severelu	Strongly	Moderate	Slightly	No	Slightly	Moderately	Strongly	Severelu	Severelu
If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being         6 taken over by an attacker and turned into a ZOMBIE?         Less likely       No Impact         Severely       Severely         Inhibits       Moderate         Sightly       No         Severely       Inhibits         Inhibits       Inhibits         Less likely       No         Severely       Severely         Inhibits       Inhibits		Inhibits	Inhibits	Inhibits	ly Inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotés
If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMBIE?         Is specify taken over by an attacker and turned into a ZOMER												
If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?         Less likely       No Impact       More Likely         Severely       Severely       Nhibits       No Impact       More Likely         Inhibits       Inhibits       Inhibits       No Impact       Strongly       Severely         Inhibits       Inhibits       Inhibits       Inhibits       No Impact       Strongly       Severely         Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits												
6       taken over by an attacker and turned into a ZOMBIE?         Less likely       No Impact       More Likely         Severely       Severely       Inhibits       Inhibits       Inhibits       Severely         Inhibits       Inhibits       Inhibits       Inhibits       Severely			11DC	tom	• NOT	ad ker	likal- is i		barach er-1	om could	l provert	haing
Less likely       No Impact       More Likely         Severely       Severely       Strongly       Moderate         Inhibits       Inhibits       Inhibits       Strongly         Inhibits       Inhibits       Inhibits       Strongly         Inhibits       Inhibits       Inhibits       Inhibits	6	taken ov	er by an	attacke	r and turn	ea, no <del>u</del> ed into a	a ZOMBI	E?	arget syst	em could	i prevenc	being
Less likely     No Impact     Moderately     More Likely       Severely     Severely     Strongly     Moderate     Slightly     No     Slightly     Moderately     Strongly     Severely     Severely       Inhibits     Inhibits     Inhibits     Inhibits     Inhibits     Inhibits     Strongly     Severely     promote     promote     promote     promote     promote       Inhibits     Inhi			-									
Severeig       Severeig       Strongly       Moderate       Slightly       Moderately       Strongly       Severely       Severely         Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Inhibits       Impact       Promote       Pr		Less likely		0	R.A. Jacob	Official	No Impa	et Lon-tate		Observed.	0	More Likely
influxes influxes influxes influxes influxes influxes influxes influxes promote promotes promotes promote promote promotes influxes influx		Severely Inhibite	Severely	Strongly	IVIODErate	Slightly	NO	Slightly	woderately	strongly	Severely	Severely
		nihidits	innibits	innibits	ig innibits	innibits	impact	promote	promotes	promote	promote	promotes
	_											
	_											

7	lf an IDS from per	/IPS sys etrating	tem were the targ	e used, ho eted syst	ow likely em?	is it that	the syst	em could pi	revent a 1	ROJAN	HORSE
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impac No Impact	st Slightly promote	Moderately promotes	Strongly promote	Severely promote	More Likely Severely promotes
8	lf an IDS HORSE (	/IPS sys from pen	tem were etrating	e NOT use the targe	ed, how l ted syst	likely is i em?	t that the	system co	uld preve	nt a TRO	JAN
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impac No Impact	st Slightly promote	Moderately promotes	Strongly promote	Severely promote	More Likely Severely promotes
	lf an IDS	/IPS sys	tem wer	e used, ha	ow likely	is it that	the syst	em could pi	revent a E	BACKDO	OR from
9	being pla	ced in t	he target	ed syster	n? -		-				
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impac No Impact	st Slightly promote	Moderately promotes	Strongly promote	Severely promote	More Likely Severely promotes
	lf an IDS	/IPS sys	tem vere	NOT use	ed, how l	likely is i	t that the	system co	uld preve	nt a BAC	KDOOR
10	from bei	ng place	d in the l	argeted	astem?	-		<u> </u>	-		
	Less likely	Causada	Chanada	5 de		No Impa	<u>e</u> :	2			More Likely
	Inhibits	Inhibits	Inhibits	ly Inhibits	Inhibits	Impact	s	promotes	s	s	promotes
11	lf an IDS (DOS) at	/IPS sys tack fro	tem were m disrup	e used, ho ting servi	ow likely ice on th	is it that e target	the system ed system	em could pi n?	revent a [	Denial Of	Service
	Less likelu					No Impa	st				More Likelu
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
12	lf an IDS disruptin	/IPS sys g servic	tem were e on the	e NOT use targeted	ed, how l system?	ikely is i	t that the	system co	uld preve	nt a DOS	from
	Less likely					No Impac	ot				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
13	lf an IDS attack ag	/IPS sys gainst th	tem were e targete	e used, ho ed system	w likely ?	is it that	the syst	em could pi	revent a L	OGIC BO	мв
	Less likely Severely Inhibits	Severely Inhibite	Strongly	Moderate Julokibito	Slightly	No Impac No	st Slightly	Moderately	Strongly	Severely	More Likely Severely
	minutes	annotes	annoits	ig minibit(S	annoits	anpace	promote	promotes	promote	promote	promotes

14	lf an IDS BOMB a	/IPS sys ttack ag	tem wer ainst the	e NOT us e targete	ed, how d system	likely is ?	it that th	e system c	ould prev	rent a LO	GIC
	Less likely Severely	Severely	Strongly	Moderat	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	More Likely Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
15	lf an IDS	/IPS sys	tem ver	e used, h	ow likely	is it tha	t the sys	tem could	prevent a	n E-mail	
	Less likely		k again.		geteu 39	No Impa	ct				More Likely
	Severely Inhibits	Severely Inhibits	Strongly	Moderat ely	Slightly	NO Impact	Slightly promote	Moderately promotes	Strongly promote	promote	Severely promotes
16	If an IDS	/IPS sys	tem ver	e NOT us	ed, how	likely is	it that th	e system c	ould prev	rent an E	-mail
10	Less likely		k agams	st the tar	geteu sy	No Impa	ct				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderat ely	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
17	lf an IDS Spoofing	/IPS sys 1 attack	tem ver against	e used, h the targe	ow likely ted syst	j is it tha em?	at the sys	tem could	prevent a	n IP Add	ress
	Less likely Severely	Severely	Strongly	Moderat	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	More Likely Severely
	Inhibits	Inhibits	Inhibits	eiy	Inhibits	Impact	promote	promotes	promote	promote	promotes
18	lf an IDS SPOOFII	/IPS sys NG attao	tem wer k again:	e NOT us st the tar	ed, how geted sy	likely is stem?	it that th	ie system c	ould prev	rent an IF	P Address
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderat ely	Slightly Inhibits	No Impa No Impact	ct Slightly promote	Moderately promotes	Strongly promote	Severely promote	More Likely Severely promotes
19	lf an IDS from bei	/IPS sys ng used	tem wer in targel	e used, h ting a sys	ov likely tem?	j is it tha	t the sys	tem could	prevent a	KEY LO	GGER
	Less likely Severely	Severelu	Stronglu	Moderat	Slightlu	No Impa No	et Slightlu	Moderatelu	Strongly	Seuerelu	More Likely Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
200	If an IDS	/IPS sys	tem wer	e NOT us	ed, how	likely is	it that th	e system c	ould prev	rent a KE	Y
20	Less likely	Coursely	eng use	u m carge	Slightly	No Impa	et Slightle	Moderately	Chronale	Soucroli	More Likely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes

21	lf an IDS being us	/IPS sys ed in tar	tem wer geting a	e used, h system?	o <b>v</b> likely	j is it tha	at the sys	tem could	prevent a	SNIFFE	R from
	Less likelu					No Impa	ct				More Likelu
	Severely	Severely	Strongly	Moderat	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
22	lf an IDS from bei	/IPS sys ng used	tem wer in targel	e NOT us ting a sys	sed, how tem?	likely is	it that th	ie system c	ould prev	ent a SN	IIFFER
	Less likelu					No Impa	ct				More Likelu
	Severelu	Severelu	Stronalu	Moderat	Sliahtlu	No	Slightlu	Moderatelu	Stronalu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	elų	Inhibits	Impact	promote	promotes	promote	promote	promotes
				- <b>-</b>							
23	lf a seco one/an∎	nd IDS/I of the al	PS systemeters bove att	em were : ack meth	used, ho ods? A	w likely i Iso, plea	is it that ise e <b>x</b> olai	the system in in space	could be provided	tter prev	ent
	,										
	Less likely					No Impa	ct	4			More Likelu
	Severely	Severely	Strongly	Moderat	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
							<u> </u>	-			
	Explanatio	n:									
	16 > 6000	ad IDGJI	DC cach		not ucod	l hay lik	als is it t	hat the cos	tom ooul	d prouon	
24	of the ab	ove atta	no syst ack meth	ods? Pl	ease e <b>z</b> j	plain in s	space pro	vided.	tem cour	u preven	t onerany
	Less likelu					Nolmoa	ct				More Likelı
	Severelu	Severelu	Stronalu	Moderat	Slightlu	No	Slightlu	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	elu	Inhibits	Impact	promote	promotes	promote	promote	promotes
	Explanatio	n of benef	it a secon	d firewall w	ould						-
	provide:										

# 3. HARDENING SECTION OF SURVEY

				Expert O	pinion F	Researd	ch Tool -	Hardenin	g		
	K	-									
1	a VIRUS	stem and from inf	l applica ecting th	tions were ne targeted	properly system?	hardene	d, how lik	ely is it th	at the sys	tem coul	d prevent
	Less likely					No Impa	ot				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
	If sha and		Lenglige				DOCHED	) b a se lib a l	- :- :• •• •		
2	prevent a	a ¥IRUS	from inf	ecting targ	eted sys	periy HA tem?	RUENEL	, no <b>v</b> likel	y is ic cna	t the syst	em coula
	Less likely					No Impa	ot				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
_	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
_											
_	If the sys	stem and	applica	tions were	properly	HARDE	NED, how	likely is it	that the	system c	ould
3	prevent a	a VORM	from in	fecting the	targeted	system	?	-		-	
	Less likely					No Impa	ot				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly 🏒	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact /	promotes	promotes	promotes	promote	promotes
							,			-	
						3					
_	lf the sus	tem and	Lannlica	tions were	NOT pro	nerla HA		) how likel	n is it tha	t the sust	em could
4	prevent a	VORM	from in	fecting targ	eted sys	tem?		, no <b>-</b> nkci	<b>y</b> 13 it tha		
	- Less likelu					Nolmpa	et.				More Likelu
_	Severelu	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderatelu	Strongly	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	If the cas	tom and	Lannlina		n e e e e e e e e e e e e e e e e e e e		NED hav	likala is it	that the		
5	could pre	ovent he	i applica ina take	n over and	property turned in	to a 20	MRIF he :	n nkeng is n an attacke	nacine 12	targeteu	system
Ť	Less likelu					Nolmpa	et		-		More Likelu
_	Severelu	Severelu	Stronalu	Moderatelu	Slightlu	No	Slightly	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	Kaba				NOT -		DOCUSE				
c	ir the sys	stem and	i applica	tions were	NUT pro	perly HA ar and to	INDENED	> ZOMPIC	y is it tha :2	t the targ	et system
6	coura pre	event De	ing cake	n over by a	n attacki	er and Cu	inea inco	a ZUMBIE	ſ		More
	Less likelu					No Impa	ot				Likelu
	Severely	Severely	Stronglu	Moderatelu	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotés

7	If the sys prevent a	stem and a TROJ/	l applica N HOR	tions were SE from pe	properly netrating	HARDE the targ	NED, how jeted syst	likely is it em?	that the	system c	ould
	Less likely					No Impa	ct				More Likely
	Severely Jobibite	Severely	Strongly	Moderately Inhibite	Slightly	NO Imposet	Slightly	Moderately	Strongly	Severely	Severely
	Innibits	innibits	Innibits	innibits	Innibits	impact	promotes	promotes	promotes	promote	promotes
8	if the sys	stem and a TROJ/	1 applica \N HOR!	tions were SE from pei	NOT pro netrating	perly HA the targ	RDENED	), how likel :em?	y is it tha	t the sys	tem could
	Less likelu					No Impa	ct				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	If the sus	stem and	l applica	tions were	properly	HARDE	NED, how	likel <b>u</b> is it	that the	sustem c	ould
9	prevent a	a BACK	DOOR fr	om being p	laced in	the targe	eted syste	m?			
	- Less likely					No Impa	ct -				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	If the sus	stem and	l applica	tions were	NOT pro	perla HA		hov likel	∎ is it tha	t the sus	tem could
10	prevent a	BACK	DOOR fr	om being p	laced in I	the targe	ted syste	m?	<b>,</b>		
	-							)			More
	Less likely		-			No Impa	ot		-		Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Innibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	If the sys	stem and	l applica	tions were	properly	HARDE	NED, how	likely is it	that the	system c	ould
11	prevent a	a Denial	Of Servi	ice (DOS) a	ttack fro	om disru	pting serv	rice on the	targeted	system?	
	Logg likolu					Nolmes	~*				iviore Likolu
	Severelu	Severelu	Stronglu	Moderatelu	Slightlu	No	Slightlu	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	K the cas	tom and	Lanaliaa	Nices		n a sin LLA	DDENED	hav likel	n in it that		am aguld
12	nrevent :	scem and s DOS G	i applica om disri	uons vere Intina serui	NUT pro	o targeti	A CECTOR	, now likel 2	y is it tha	t the syst	em coula
12	prevent			pung servi		e target	eu systen				More
	Less likely					No Impa	ct				Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	lf the sec	tem and	l annlina	tions ware	properie		NED her	likol= iz is	that the	castem e	ould
13	prevent a	a LOGIC	BOMB	attack agai	nst the t	argeted	system?	incerg is to	that the	system c	Marc
	المجج انلامات					Nolmes	et				l ik ele
	Severelu	Severelu	Stronglu	Moderatelu	Slightly	No	Slightlu	Moderatelu	Strongly	Severelu	Severela
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes

14	lf the sys prevent a	tem and LOGIC	l applica BOMB	tions were attack agai	NOT pro nst the t	perly HA argeted	\RDENED system?	), ho <b>v</b> likel	y is it tha	t the sys	tem could
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
15	lf the sys prevent a	tem and an E-mai	İ applica il SPOOI	tions were FING attacl	properly Lagainst	HARDE the targ	NED, how leted syst	likely is it tem?	that the	system c	ould
	Less likely					No Impa	ct -				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	lf the sys	tem and	l applica	tions were	NOT pro	perly HA	RDENED	), ho <b>v</b> likel	y is it tha	t the sys	tem could
16	prevent a	an E-mai	il SPOOI	FING attacl	k against	the targ	jeted syst	tem?			
	Less likely		~ .		OF LU	No Impa	ot Lon Lui		~ .		Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
				_							
						01		2			
17	lf the sys prevent a	tem and an IP Ad	l applica dress Sj	tions were poofing att	properly ack again	HARDE	NED, how argeted s	likely is it stem?	that the	system c	ould
	- Less likely					No Impa	ct -				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	lf the sus	tem and	1 annlica	tions were	NOT pro	nerls HA		) how likel	∎ is it tha	t the sast	huoo mat
18	prevent a	an IP Ad	dress SI	POOFING a	ttack au	ainst the	e targeted	sustem?	<b>,</b>		
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes
	14 - 1	-			-					_	
19	If the sys	a KEY LO	i applica DGGER (	tions were from being	properly used in t	argeting	a system	ikely is it ?	that the	system c	ould
	Less likely	_				No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promotes

20	If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?												
	Less likely					No Impa	ot				More Likely		
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes		
21	lf the sys prevent a	tem and SNIFFI	l applica ER from	tions were being used	properly in targe	HARDE	NED, how stem?	likely is it	that the :	system c	ould		
	Less likely				2A	No Impa	ך ב	L			More Likely		
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes		
22	If the sys prevent a	tem and SNIFFI	l applica ER from	tions were being used	NOT pro in targe	perly HA ting a sy	RDENED	, how likel	y is it that	t the syst	em could		
	Less likely				_	No Impa	ot				More Likely		
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes		

# 4. TRAINING SECTION OF SURVEY

				Expert C	pinion l	Resear	ch Tool -	TRAINING			
Acc com refei ema	ording t opliment rs are: F ails or ic	o CiSR, es : other prac Protecting ons.	sential pra tices in a user IDs a	actices are the system of def nd Password	ose that ar ense in de s, utilizing j	iyone can pth or laye proper pas	do utilizing red defens sswords, no	available reso e. Essential pr ot opening or c	urces, are 81 actices to w licking on u	0% effectiv /hich this q nknown or	e, and uestion unexpected
lf ei	nd-use	ers were j	properly of VIDU	trained in r S infection	egards t	o essen	tial pract	ices, ho <b>v</b> lil	cely is it t	hat the s	ystem
TTO	uu ren	iam riee		5 mrection	f 						
Less	s likely orolu	Souerelu	Stronglu	Moderatelu	Sliabtlu	No Impa No	et Slightlu	Moderatelu	Stronglu	Souorolu	More Likely Severelu
Inhib	oits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
lf th 2 sys	tem w	-users we ould rem	ere NOT ain free	properly tr of ¥IRUS in	ained in fection?	regards	to essen	tial practice	s, ho <b>v</b> lik	ely is it t.	hat the
Less	s likely					No Impa	ct				More Likely
Sev	erely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhib	oits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
If er 3 cou	nd-use Ild pre	ers were j vent a V	properly ORM fro	trained in r m infecting	egards t 1.the tar	o esseni aeted su:	tial practi stem?	ices, how lil	cely is it t	hat the s	ystem
							<u> </u>	1			
Less	s likely erelu	Severelu	Stronalu	Moderatelu	Slightlu	No impa	et Slightlu	Moderatelu	Stronalu	Severelu	More Likely Severelu
Inhib	oits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
lf th 4 sys	he end tem co	users we	ere NOT ent a V(	properly tr DRM from i	ained in infecting	regards targete	to essen d system	tial practice ?	s, ho <b>v</b> lik	ely is it t	hat the
Loca	e likolu					Nolmes	et.				More Likelı
Sev	erely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhib	oits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
lf ei	nd-use	IS WATA I	nroneria	trained in r	enards t	n essen	tial practi	ices how lil	els is it t	hat the ta	heted
5 <b>sys</b>	tem co	ould prev	ent bein	g taken ov	er and tu	rned inte	o a ZOME	BIE by an at	tacker?		ingereu
less	slikelu					Nolmea	ct.				More Likelu
Sev	erely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhib	oits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
K al	ha en 1			proporte te	ainad in	roand c	to occa-	tial prostice	e heulik	ala in it t	
6 targ	ne end get sys	tem cou	id preve	nt being tal	aineo in cen over	by an at	tacker ar	nd turned in	s, nov lik to a ZOM	BIE?	nat the
Less	s likelu					No Impa	ct				More Likelu
Sev	erely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhib	oits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes

7	lf end-use could pre	ers were j vent a Ti	properly ROJAN I	trained in r IORSE froi	egards t m penetr	o essent ating the	tial practi e targeteo	ices, how lil I system?	cely is it t	hat the s	ystem
	Loss likolu					Nolmpa					More Likelu
_	Severelu	Severelu	Stronalu	Moderatelu	Slightlu	No	Sliahtlu	Moderatelu	Stronalu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
			NOT.								
	If the end	-users ¥(	ere NUI	property tr	ained in DGE (ror	regards   n nonotri	to essent	tial practice	s, how lik stom?	ely is it t	hat the
•	system of	Julu prev	enta ir		ISE NUI	n penetra	acing the	targeteu sy	stem		
	Less likelu					No Impac	et				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotés
	K										
9	could pre	vent a B	ACKDO(	Crained in r DR from bei	egaros ( ing place	o essent ed in the	targeted	ices, nov ill system?	cely is it t	nac (ne s	yscem
	Less likely					No Impa	ət				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	promote	Moderately	Strongly	promote	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	s	promotes	promotes	s	promotes
_											
_											
_	lf the end	UCOIC M	ara NOT	nroneris tr	ainad in	rogarde l	to accan	tial practice	s how lik	als is it t	hat the
10	sestem co	-users w nuld nrev	ent a B/		ameu m fr <b>o</b> m hei	na niace	d in the <b>f</b>	arneted sus	tem?	eig is it t	nactie
	5,500.00										
	Less likely					No Impac	at 📕 🥖				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
_											
_	If and use			trained in r	a a sed a b	o occord	isl sesse	aac hay lil	als is it t		
11	could pre	uont a Dr	property anial Of	Gameu in i Garuica (Dí	egarus ( NG) attai	o esseni et from d	liar pracu dicrunting	ices, no <b>v</b> ili I seruice or	the targe	nal line S stad cect	ystem om2
	could pre-	vent a Di		001310100	Jojalla		usiuping	J SELVICE OF	i the targe	icu syst	
	Less likely					No Impac	st				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
_	If the end			neonarla te	ain a d in	reaseda		tial aractica	a hau lik	ala ia it t	
12	sestem co	-users we	ere NOT lant a Dí	property tr 19 from dis	ameu m runtina (	regarus : cornico c	io esseni in the tar	natad sesta	-s, now iik .m2	ery is ic c	nacine
16	system of	Julu prev			aupung :	SELVICE C	n the tai	geteu syste			
	Less likelu					No Impac	st				More Likelu
_	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
13	lf end-use could pre	ers were j vent a LO	properly DGIC BO	trained in r MB attack	egards t against	o essent the targe	tial practi eted syst	ices, how lil em?	tely is it t	hat the s	ystem
	l ess likelu					Nolmos	st.				More Likela
_	Severelu	Severelu	Stronalu	Moderatelu	Slightlu	No	Slightlu	Moderatelu	Stronalu	Severela	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes

lf the ei 14 system	nd-users ¥ could prev	ere NOT ent a LC	properly tr GIC BOME	ained in 3 attack	regards against	to essen the targe	tial practice ted system?	s, how lik	ely is it t.	hat the
Localika	lu l				Nolmos	et.				Mora Likalu
Severelu	Severelu	Stronglu	Moderatelu	Slightlu	No	Slightlu	Moderatelu	Stronglu	Severelu	Severelu
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
If end-u	isers were	properly	trained in r	egards t	to essen	tial practi	ices, how lil	kely is it t	hat the s	ystem
io coulu p	nevent an c	-man ər		ILLACK A <u>y</u>	janist tr	e targetei	u system?			
Less like	ly 🛛				No Impa	ct				More Likely
Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
If the ei 16 sustem	nd-users ¥ could prev	ere NOT vent an E	properly tr -mail SPO	ained in DFING a	regards ttack au	to essen ainst the	tial practice targeted su	es, how lik stem?	ely is it t	hat the
Less like	ly .				No Impa	ct				More Likely
Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
	_		_							
						<u> </u>				
lf end-u 17 could p	isers were revent an l	properly P Addre	trained in r ss Spoofin	egards ( g attack	to essen against	tial practi the targe	ices, how lil ted system	kely is it t ?	hat the s	ystem
Less like	lu				No Impa	et				More Likelu
Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotés
If the er	nd-users W	ere NOT	properiy tr P Address '	ained in SPOOFI	regards NG atta	to essent	tial practice t the target	es, how lik	ely is it t 2	hat the
io system	could pres	ent an n	Autess			/k ayams	c the target	eu system		
Less like	ly 🛛				No Impa	ct				More Likely
Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
							<u> </u>			
19 could p	isers were j revent a Kl	properiy EY LOGO	crained in r iER from b	eing use	o essen d in targ	cial practi jeting a sy	ices, nov ill Istem?	cely is it t	nat the s	ystem
	I			_	N					Marris
Less like	<sup>19</sup>	Ohan a chi	B.d., dasabala	Officialistic	INO Impa	CC	Man danah - Iu	Ohan alt	Coursels	IVIOre Likely
I WOLLOFAM			LINNOGOL STOLL	LOUGHTU	LINO	Silantiu	Invioderatelu	i stronalu	i beverelų	Libevereill
Jok bits	Severely	Strongly Jokibite	Inhibite	Inhibito	Imposit	DIOT OF	nometer	Diamatra	DIOP	promotor
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
Inhibits	Severely Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promoté	promotes

20	If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?												
	Less likely					No Impa	ot				More Likely		
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes		
21	If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?												
	Less likely				22	No Impa	2	1			More Likely		
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slig <b>htly</b> Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes		
_													
22	If the end-users were NOT properly trained in regards to essential practices, how likely is it that the 22 system could prevent a SNIFFER from being used in targeting a system?												
	Less likely					No Impa	at				More Likely		
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly	Moderately promotes	Strongly promotes	Severely promote	Severely promotes		
							p. c. nore						

# 5. ANTI-VIRUS SECTION OF SURVEY

			E	Expert Opir	nion Res	search s	oftware	- ANTI-VIF	US		
	lf undater	I ANTI-V	IBUS so	ftware wer	e used b	ov likeli	is it that	t the susten	n could n	revent a 1	/IBUS
1	from infe	cting the	targete	d system?					, ooala p		
	Less likelu					No Impa	et				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
	lf undater	I ANTI-V	IBUS so	ftware wer	» NOT из	ed how	likolu is i	it that the s	estem co	uld preve	nt a
2	VIRUS fro	om infect	ing targ	eted syster	n?		incerg is i	it that the s	ystem oc	ala preve	iii a
	Loss likolu					Nolmoa	-t				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
				-							
3	from infe	cting the	targete	ntware were d system?	e usea, n	ow likely	is it that	t the system	n coula p	revent a v	URM
				_							
	Less likely Severelii	Severelu	Stronglu	Moderatelu	Slightlu	No Impa No	et Sliahtlu	Moderatelu	Stronglu	Severelu	More Likely Severelii
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
					$D_{\cap}$	$\sim$		-			
4	lf updated VORM fr	i ANTI-V om infec	IRUS so ting targ	ftware were leted syste	e NOT us m?	ed, how	Tikely is i	it that the s	ystem co	ould preve	nt a
	Less likelu					No Impa	ct				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
	lí undator	4 ANTI V		ftuara uar	ucad b	ou litalı	ic it that	the target	ad castor	n aguld n	auant
5	being tak	en over a	and turn	ed into a Z	DMBIE b	y an atta	icker?	t the target	eu syster	n coala pi	event
	Loss likolu					Nolmos	~t				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
			IDUIC		NOT						
6	lf updated being tak	en over l	iRUS so by an att	acker and t	e NOT us turned in	ed, how to a ZON	likely is i 4BIE?	it that the t	arget sys	tem coulo	1 prevent
	Less likelu					No Impa	ot				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes

7	lf updated HORSE fi	i ANTI-V rom pene	IRUS so etrating	ftware were the targete	e used, h d system	ow likely ?	is it tha	t the systen	n could p	revent a 1	rojan
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	ct Slightly promote	Moderately promotes	Strongly	Severely promotes	More Likely Severely promotes
	lf updated		IRUS so	ftware were	e NOT us	ed, how	likely is i	t that the s	ystem co	ould preve	nt a
•	Less likelu	HUNGE	riom per	netrating th	ie targett	No Impa	et				More Likelu
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
•	lf updated	I ANTI-V	'IRUS so	ftware were	e used, h	ow likely	is it that	t the system	n could p	revent a	
3	Localikalu		being p	laceu în îne	e cargece	Nolmon	1 <i>f</i>				Moro Likolu
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
10	lf updated BACKDO	i ANTI-V OR from	IRUS so being p	ftware were laced in the	e NOT us e targete	ed, how d system	likely is i 1?	t that the s	ystem ca	uld preve	nt a
	Less likely				Da	NoImpact		)			More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	promote s	Moderately promotes	promote s	Severely promotes	Severely promotes
11	lf updated Service (I	I ANTI-V DOS) att	'IRUS so ack from	ftware were disrupting	e used, h 1 service	ov likely on the t	is it that argeted s	t the system	n could p	revent a [	Denial Of
	Loss likelu					Nolma	ot				More Likelu
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
10	lf updated	I ANTI-V	'IRUS so	ftware were	e NOT us	ed, how	likely is i	t that the s	ystem ca	uld preve	nt a DOS
12		upting st	ervice of	i the target	eu syste						
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	ct Slightly promote	Moderately promotes	Strongly promote	Severely promotes	More Likely Severely promotes
13	lf updated BOMB at	I ANTI-V tack aga	IRUS so inst the	ftware were targeted sy	e used, h stem?	o <b>v</b> likely	is it tha	t the system	n could p	revent a l	.OGIC
	Less likely Severals	Seucrali	Strengte	Moderately	Slightle	No Impa No	ct Slightle	Moderately	Strongle	Souerole	More Likely Severals
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
	lf undated	I ANTI-V	'IBUS so	ftware wer	e NOT us	sed, how	likelu is i	it that the s	astem co	uld preve	nta
----	-------------------------	--------------------	---------------------	----------------	----------------------	-----------------------	-------------------	---------------	-----------	------------	-------------------------
14	LOGIC B	DMB atta	ack agai	nst the targ	jeted sy	stem?			<b>,</b>	<b>F</b>	
	Less likelu					No Impa	et				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotés
	If updated	ANTI-V	IRUS so	ftware wer	e used, h	ov likele	is it tha	t the suster	n could p	revent an	E-mail
15	SPOOFIN	IG attack	agains	t the target	ed syste	m? .					
	Less likely Severale	Courselu	Chanada	5 An decetator	Clinkslu	No Impa No	ot Defension	Mandasatalu	Changela	Courselu	More Likely
	Severely Inhibite	Inhibite	Inhibite	Invioderately	Inhibits	Impact	promote	promotes	strongly	promotes	promotes
	mmbros	mindics	mindits	minoits	mindits	impace	promote	promotes	promote	promotes	promotes
10	If updated	d ANTI-V	IRUS so	ftware wer	e NOT us	sed, how	likely is i	it that the s	ystem ca	ould preve	nt an E-
10	mail 5PU		ссаск ад	ainst the G	argeceu s	system?					
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
					$\boldsymbol{\nu}$	n a		<u> </u>			
							5 3				
	If updated	ANTI-V	'IRUS so	ftware wer	e used, h	ow likely	is it tha	t the system	n could p	revent an	IP
17	Address	Spoofing	attack	against the	targete	d system	?	-	•		
	Less likely Severely	Couerelu	Strongly	Moderatelu	Clicktlu	No Impa No	Ct Cliabelu	Moderatelu	Strongly	Couerelu	More Likely Soucroly
	Severely Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
	in the test		in the loss	in indice	in in its its	Inpact	promote	promotes	promote	promoteo	promoteo
					NOT						
12	It updated	I ANTI-¥ SPOOFI	IRUS SO NG attac	tware were	e NUT US Ko targo	sed, now tod custo	likely is i m2	it that the s	ystem co	ula preve	nt an IP
10	Autess			k ayamse e	ne targe	leu syste					
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
	If updated	ANTI-V	'IRUS so	ftware wer	e used, h	ow likely	is it tha	t the system	n could p	revent a l	(EY
19	LOGGER	from bei	ing used	in targetin	g a syste	•m?		-			
	1					N - 1					Marris 1 Mart
	Less likely Severale	Seuerola	Strongle	Moderately	Sliaktlu	No Impa No	ot Sliaktlu	Moderately	Strongly	Seuerole	Nore Likely Severals
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
						and a second	provinore	promotes	promote	promotes	promotes

	lf updated	ANTI-Y	IRUS so	ftware were	e NOT us	ed, how	likely is i	t that the s	ystem co	uld preve	nt a KEY
20	LOGGER	from bei	ng used	in targeting	g a syste	m?		1			
	Less likely					No Impa	ot		-		More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Infilbits	InfilDits	Infilblics	Infilblics	TITIDICS	impact	promote	promotes	promote	promotes	promotes
-											
	lf updated	ANTI-Y	IRUS so	ftware were	e used. h	ov likelu	is it that	the susten	n could p	revent a S	NIFFER
21	from bein	q used i	n targeti	ng a sys <mark>ten</mark>	n?			<b>A</b>			
	Less likely		_		23	No Impa					More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
				-							
	If updated	ANTI-Y	IRUS so	ftware were	e NOT us	ed, how	likely is i	t that the s	ystem co	uld preve	nt a
22	SNIFFER	rrom be	ing usea	in cargetin	g a syste	?m?		1	1	1	1
	Less likely					No Impa	ot				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes

## 6. ANTI-SPAM SECTION OF SURVEY

lf a 1 pre	an upda revent a	ted AN1 VIRUS f									
1 pre	event a	VIRUS A	1-3F AM	fenam bla	akar) ta			likola is it	that the c	nctom oo	uld
Les			rom infe	cting the t	argeted :	system?	usea, nov	nkely is it	(nat the s	ystem co	uia
Les											Marca I Stark
Col	iss likely Wordu	Couorolu	Strongly	Moderately	Sliabtlu	No impai	St Sliaktlu	Moderatelu	Strongly	Souorolu	Nore Likely Severely
lohi	hibits	lohibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
	ile Ko	in the Ko	IIII DRD	IIII DIO	in indice	mpaos	promoteo	promoteo	promotes	promotes	promoteo
Wh	hat IF the p	premise we	ere <u>False</u> '	Pow would	this impac	t the cond	lusion?				
lf a	an upda	ted AN1	I-SPAM	l (spam blo	cker) to	ol were l	NOT used	l, ho <b>v</b> likely	, is it that	the syste	m could
2 pre	event a	<b>VIRUS</b> A	rom infe	ecting targe	ted syst	em?					
1.00	ce likolu					Nolmey					Moro Likoly
Sei	ssaralı	Severelu	Stronglu	Moderatelu	Slightlu	No	Sliahtlu	Moderatelu	Stronglu	Severelu	Souerelu
Inhi	hibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
								promoto		promoto	
lf a	an upda	ted AN1	I-SPAM	l (spam blo	cker) to	ol were i	used, how	likely is it	that the s	system co	uld
3 pre	event a	VURM	III MON	ecting the t	cargeced	system	f				1
Les	sslikelu					No Impai	t:				More Likelu
Set	everelu	Severelu	Stronalu	Moderatelu	Slightlu	No	Sliahtlu	Moderatelu	Stronalu	Severelu	Severelu
Inhi	nibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
						$\sim$					
4 nre	an upda revent a	VORM	I-SPAM	l (spam blo ecting targ	ckerj to eted ses	ol were i tem?	NUT used	i, how likeli	j is it that	the syste	m could
1 10	C I C II C II C II			coung ung							
Les	ss likely					No Impa	st				More Likely
Sev	everely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Inhi	nibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
_											
lf a	an upda	ted AN1	I-SPAM	l (spam blo	cker) to	ol were i	used, how	likely is it	that the t	argeted s	stem
5 <b>co</b>	ould pre	vent bei	ng taken	over and t	urned in	to a ZOI	MBIE by a	in attacker	?		
1.00	aa lik olu					Nolmes					Moro Likolu
Sei	ss interg	Souaralu	Strongly	Moderatelu	Slightlu	No	a Sliahtlu	Moderatelu	Strongly	Severelu	Severelu
Inhi	hihits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	nromotes	promotes	promotes	promotes	promotes
	i bito	in the loss	IIII DRD	in the test		in pass	promoto	promoteo	promotes	promotes	promoteo
							UST				
e lf a	an upda	ted AN1	I-SPAN	i (spam blo	cker) to	ol were i	NUT used	i, how likely	j is it that 2	the targe	t system
0 00	oula pre	vent bei	ng taken	over by an	attacke	er and tu	mea into		f		
Les	sslikelu					No Impai	st				More Likelu
Set	everelu	Severelu	Stronalu	Moderatelu	Slightlu	No	Slightlu	Moderatelu	Stronalu	Severelu	Severelu
Inhi	nibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes

58

7	lf an upda prevent a	ated AN TROJA	TI-SPAN N HORS	l (spam blo E from per	ocker) to etrating	ol were the targ	used, hov eted syst	r likely is it em?	that the s	system co	uld
	Less likely Severelu	Severelu	Stronglu	Moderatelu	Sliahtlu	No Impa No	ct Sliahtlu	Moderatelu	Stronglu	Severelu	More Likely Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
							UCT				
8	ir an upda prevent a	TROJA	N HORS	E from per	etrating	the targ	NUT used eted syst	i, now likely em?	j is it that	the syste	m could
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
0	lf an upda	ated AN		l (spam blo	cker) to	ol were i	used, how	likely is it	that the s	system co	uld
3	prevent a			in venig pi	aceu m i	ine targe	teu syste				
	Less likelu					No Impa	ct				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
	K		TLODAN		-						
10	It an upd	ALEG AN	11-5PAN	1 (spam bio sm baing bl	ockerj to	ol vere l	NUT used	i, nov likelj m2	j is it that	the syste	m could
10	preventa		Joon m	in being p	aceum	ine targe	area syste				
	Less likely			l P		No Impa	<b>.</b>				More Likely
	Severelu	Severelu	Stronalu	Moderatelu	Slightlu	No	Slightly /	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotés
	K an and			l fan en bla	ak as l ba	-	unad has	, likala ia it	bh ab bh a a		
11	prevent a	Denial	Of Servi	ce (DOS) a	ttack fro	m disruj	usea, nov pting serv	rice on the	targeted s	system co system?	
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
	lf an upda	ated AN	TI-SPAN	l íspam blo	cker) to	ol vere	NOT used	l. ho <b>v</b> likely	is it that	the suste	m could
12	prevent a	DOS fr	om disru	pting servi	ce on th	e targete	ed system	?			
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Innibits	Innibits	Innibits	Innibits	Impact	promotes	promotes	promotes	promotes	promotes
	lf an upda	ated AN	TI-SPAN	l (spam blo	cker) to	ol were	used, hov	likely is it	that the ≤	system co	uld
13	prevent a	LOGIC	BOMB a	ittack agair	ist the ta	argeted :	system?		1	1	
	Loce likely					Nolmer	~*				More Likely
	Severely	Severelu	Strongly	Moderatelu	Slightle	No impa	Slightlu	Moderatelu	Strongle	Severela	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
								Pression and a	pressione a	pressione a	pression and a

	lf an upd	ated AN	TI-SPAN	l (spam blo	ocker) to	ol were	NOT used	l, ho <b>v</b> likelj	y is it that	the syste	m could
14	prevent a	LOGIC	BOMB a	ittack agair	ist the ta	argeted :	system?				
	Less likelu					No Impa	ct				More Likelu
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
_											
	lf an upd	ated AN	TI-SPAN	l (spam blo	ocker) to	ol were	used, hov	likely is it	that the s	system co	uld
15	prevent a	in E-mail	SPOOF	ING attack	against	the targ	eted syst	em?			
	Loce likolu					Nolmea	ot				More Likelu
_	Severelu	Severelu	Stronalu	Moderatelu	Sliahtlu	No	Slightlu	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
_	lf an und	atod ÖN'	TLSPAN	l (snam blo	eker) to	ol wara l	ΝΟΤ μερι	l how likel	ic it that	the caste	m could
16	prevent a	in E-mail	SPOOF	ING attack	against	the targ	eted sust	em?	y 15 IC Cliac	the syste	
	Less likely					No Impa	ct			-	More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
_	Inhibits	Inhibits	Inhibits	Inhibits	innibits	Impact	promotes	promotes	promotes	promotes	promotes
_								$\mathbf{O}$			
					~~	5		-			
	lf an upd	ated AN	TI-SPAN	l (spam blo	ocker) to	ol vere	used, hor	likely is it	that the s	system co	uld
17	prevent a	in IP Add	dress Sp	oofing atta	ick agair	nst the t	argeted s	stem?			
	Less likelu					No Impa	ct				More Likelu
_	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
_											
-	lf an upd	ated AN	TI-SPAN	l (spam blo	ocker) to	ol were	NOT used	l, how likel	is it that	the syste	m could
18	prevent a	in IP Ade	dress SF	OOFING a	ttack ag	ainst the	e targeted	system?			
	Less likely Souorolu	Souaralu	Strongly	Moderatelu	Sliabtlu	No Impa No	Ct Sliaktlu	Moderatelu	Strongly	Souorolu	More Likely Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
						-					
19	It an upd	ALEG AN	II-SPAN IGGER (	i (spam bio com being i	ickerj to	ol vere l	used, nov	/ likely is it 2	that the s	system co	ula
10	preventa			om being t	iseu m c	argeting	a system	-			
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes

200	lf an upda	ated AN1		l (spam blo	ocker) to	ol were l	NOT used	l, how likely	y is it that	the syste	m could
20	prevent a	KETLU	GGER N	rom being u	isea in c	argeting	a system	f	1		
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
L_											
21	prevent a	SNIFFE	R from	i (spam bio being us <mark>e</mark> d	in targe	ting a sy	usea, nov stem?	inkely is it	(nat the s	system co	ula
	Less likely				6	No Impa					More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
							LIGT		L		
200	If an upda	ated ANI	II-SPAN	1 (spam bio	ckerj to	ol were l	NUT used	i, how likely	j is it that	the syste	m could
22	prevent a	SNIFFE	.R from	being usea	in carge	cing a sy	stem?	1	1	1	1
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes

## 7. ANTI-SPYWARE SECTION OF SURVEY

				Expert Op	inion Re	esearch	Tool - Al	NTI-SPYWA	RE		
1	lf an upd from infe	ated AN ecting the	 TI-SPY₩ e targete	ARE tool v	rere use	d, ho <b>v</b> lil	kely is it t	hat the syst	em could	prevent a	VIRUS
	Less likely		e targett	u system:		No Impa	ct				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
2	lf an upd VIBUS fr	ated AN om infec	TI-SPYW ting targ	ARE tool v	rere NOT m?	í used, h	ov likely i	is it that the	system o	ould prev	ent a
-	l ess likelu					Nolma	et				More Likelu
_	Severelu	Severelu	Stronalu	Moderatelu	Slightly	No	Sliahtlu	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
3	lf an upd from infe	ated AN	TI-SPY₩ e targete	ARE tool v	rere use	d, ho <b>v</b> lil	kely is it t	hat the syst	em could	prevent a	VORM
Ť	Lesslikelu					Nolma	et				More Likelu
_	Severelu	Severelu	Stronalu	Moderatelu	Sliahtlu	No	Sliahtlu	Moderatelu	Stronalu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
				-							
							_	-			
	IF an upd	ated AN	II-SPY¥	ARE tool	rere NUI	used, h	ow likely i	is it that the	system o	ould prev	ent a
4		om mret	cung car	gerea sysre	2002						More
	Less likelu					No Impa	t:				Likelu
_	Severelu	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotés	promotes
F	If an upd	ated AN	II-SPYW	ARE tool	ere use	d, how lil	kely is it t	hat the targ	eted syste	em could p	prevent
9	being tak	en over	and turn	ed into a Z		iy an acca	acker?	1			Moro
	Less likelu					Nolmos	et				Likelu
_	Severelu	Severelu	Stronglu	Moderatelu	Slightlu	No	Slightlu	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
	lf an upd	ated AN	TI-SPYW	ARE tool	rere NO1	í used, h	ov likely i	is it that the	target sy	stem cou	ld prevent
6	being tak	en over	by an at	tacker and	turned in	to a ZOI	MBIE?	1			
	المحج انلامات					Nolmer	~t				iviore Likola
_	Severalu	Severale	Strongle	Moderately	Slightly	No impa	Slightly	Moderatele	Stropalu	Severalu	Severalu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
						angeov	promotes	promotes	promotes	promotes	promotes

7	lf an upda HORSE f	ated AN rom pen	TI-SPY¥ etrating	ARE tool when the targete	vere use d systen	d, ho <b>v li</b> l n?	kely is it t	hat the syst	em could	prevent a	TROJAN
	Less likely Severely	Severelu	Strongly	Moderatelu	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	More Likely Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
•	lf an upda TPO IAN	ated AN	TI-SPYV	ARE tool	ere NOT	f used, h	ov likely i m2	is it that the	e system o	ould prev	ent a
Ŭ	Loss likolu		nom pe	netrating ti	ie target	Nolmoa					More Likolu
	Severelu	Severelu	Stronglu	Moderatelu	Slightlu	No	Slightlu	Moderatelu	Stronglu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Imnact	promotes	promotes	promotes	promotes	promotes
						in pass	promotes	promotes	promotes	promotes	promotes
9	lf an upda BACKDO	ated AN OR from	TI-SPY¥ n beina c	ARE tool v	ere use e targete	d, how lil d susten	kely is it t n?	hat the syst	em could	prevent a	
	Less likelu					No Impa	ct				More Likelu
	Severelu	Severelu	Stronalu	Moderately	Slightly	No	Slightly	Moderatelu	Strongly	Severely	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
						-	-				
10	lf an upda BACKDO	ated AN OR from	TI-SPYW n being p	ARE tool v laced in the	rere NO) e targete	f used, h d system	ov likely n?	is it that the	e system o	ould prev	ent a
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
-11	lf an upda Service (	ated AN DOC) an	TI-SPYV	ARE tool 1	ere use	d, how lil	kely is it t	hat the syst	em could	prevent a	Denial Of
	Service	DOSJ at	LACK NU	n uisruptin	y service		targeteu s	system?			More
	Couerely Couerely	Couerelu	Chronolu	Madaratalu	Cliabelo	No impai	C( Cliabelo	Madaratalu	Chronalu	Courselu	Likely
	Jobibite	Jobibite	Inhibite	Inhibite	Inhibite	Impact	promotes	promotes	promotes	promotes	promotes
	Infibits	TITIDICS	Infindics	Infibits	Infilblics	impact	promotes	promotes	promotes	promotes	promotes
12	lf an upda from disr	ated AN upting s	TI-SPY¥ ervice o	ARE tool v n the targe	ere NOT	r used, h m?	ow likely	is it that the	e system o	ould prev	ent a DOS
	Less likelu			<b>_</b> _		No Impa	ct				More Likelu
	Severelu	Severelu	Stronalu	Moderatelu	Slightlu	No	Slightlu	Moderatelu	Stronalu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes

13	lf an upda BOMB at	ated AN <sup>°</sup> ttack aga	TI-SPYW ainst the	ARE tool v targeted s	vere use: ystem?	d, ho <b>v</b> lil	kely is it t	hat the syst	em could	prevent a	LOGIC
	Localikolu					Nolmos	~*				More Likolu
-	Sauaralu	Souorolu	Stronglu	Moderatelu	Slightlu	No	Sliabtlu	Moderatelu	Strongly	Souaralu	Sauaralu
	Inhibite	Inhibite	lohibite	Inhibite	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
-	minoks	nniidits	nniidits	mindics	minores	impace	promotes	promotes	promotes	promotes	promotes
14	lf an upda LOGIC B	ated AN OMB att	TI-SPYW ack agai	ARE tool v	ere NOT aeted su:	r used, h stem?	ov likely i	is it that the	e system o	ould prev	ent a
<u> </u>											More
	Less likely	<u> </u>	<u>.</u>			No Impa	ot				Likely
	Severely	Severely	Strongly	Moderately	Slightly	NO	Slightly	Moderately	Strongly	Severely	Severely
L	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
L											
	lf an upda	ated AN	TI-SPYW	ARE tool <b>1</b>	rere use	d, how lil	kely is it t	hat the syst	em could	prevent a	n E-mail
15	SPOOFI	IG attac	k agains	t the target	ted syste	-m?					
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
								~			
16	lf an upda mail SPO	ated AN OFING a	TI-SPYW attack a	'ARE too <mark>l</mark> v nainst the t	rere NO) argeted :	i used, h sustem?	ov likely	is it that the	e system o	ould prev	ent an E-
-				1							More
	Less likely					No Impa	ot				Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
17	lf an upda Address	ated AN Spoofin	FI-SPYW g attack	ARE tool v against the	rere use e targete	d, how lil d systen	kely is it t 1?	hat the syst	em could	prevent a	n IP
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
18	lf an upda Address	ated AN SPOOFI	TI-SPY¥ NG atta	'ARE tool v ck against (	vere NO1 the targe	í used, h ted syst	ow likely i em?	is it that the	e system o	ould prev	ent an IP
	Lesslikelu			-		Nolmoa	et				More Likela
	Severela	Severelu	Strongly	Moderatelu	Slightle	No	Slightlu	Moderatelu	Strongly	Severela	Severela
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
						angeov	promotes	promoteo	promotes	promotes	promotes

19	lf an upda LOGGER	ated AN from be	II-SPY¥ ing used	ARE tool <b>v</b> in targetin	rere useo g a syste	l, how lil m?	tely is it t	hat the syst	em could	prevent a	KEY
	Less likely		-			No Impa	ot				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
											-
	lf an und:	Nă hat	ILSPYN	ABE tool N	ιοτο ΝΠΤ	ucad b	ou litels i	c it that the	cectom c	ould preu	ont a KFY
20	LOGGER	from be	ina used	in targetin	a a suste	m?	ow likely i	s it that the	system o	ouiu prev	
	Less likelu					No Impa	ot				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
						~	_	<u>/</u>			
	lf an unda	ted AN	I-SPYV	ABE tool y	ere used	t hoy lit	elu is it t	hat the sust	em could	prevent a	SNIFFEB
21	from bein	ig used i	n targeti	ing a syster	n?						
	Less likely		-			No Impa	ot				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
	lf an unde	bad AN				ucad b	au likala i	a it that the	carcham a	ould prov	
22	SNIFFER	from be	ing use	d in targetin	ig a syste	usea, n em?	ow likely i	is it that the	system c	ouia prev	enc a
	Less likely					No Impa	ot				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

THIS PAGE INTENTIONALLY LEFT BLANK

#### **APPENDIX B EXPERT OPINION SUMMARY RESULTS**

The following results are comprised from the seven sets of questions which madeup the expert opinion survey. As you may remember from Chapter 2 the survey questions came in pairs. The first question was designed to capture the survey takers judgment of the security measures impact on attack prevention if the measure is employed; the second question was designed to reflect the survey taker's judgment of the impact on not using the security measure. Each question had an eleven category range, spanning from "severely inhibits" to "severely promotes," which matches up with SIAM's measurement techniques for assigning linkage values between nodes. Each of the eleven possible selections has a corresponding numerical value for use in the influence net model, with +1 being severely promoting and a -1 corresponding to severely inhibiting.

### 1. **RESULTS IF FIREWALL WERE USED**

	IF	PREMISE	WERE TRU	JE	1	
	Survey1	Survey2	Survey3	Survey4	Average	
Firewall						
Virus	0.6	0	1	0.4	0.5	FIREWALL USED
Worm	0.6	0	0.4	0.6	0.4	
Zombie	0.6	0.6	0.4	0.8	0.6	0.7
Trojan H	0.4	0	0.2	0.4	0.25	
Backdoor	0.2	0	0.4	0.6	0.3	
DOS	0.8	0.4	0.6	0.8	0.65	<b>≧</b> 0.5
Logic Bomb	0.4	0	0	0.4	0.2	
E-Mail Sp	0.2	0	0	0.4	0.15	
IP Add Sp	0.2	0.8	1	0.6	0.65	
Keylogger	0.4	0	0	0.8	0.3	
Sniffer	0.4	0	0	0.6	0.25	
	Virus	0.5				
	Worm	0.4				the son Rel Par and De con the star the son the
	Zombie	0.6				1 10" HOT BOTH THE LAND ON BIT
	Trojan H	0.25				
	Backdoor	0.3				Attack Method
	DOS	0.65				
	Logic Borr	0.2				
	E-Mail Sp	0.15				
	IP Add Sp	0.65				
	Keylogger	0.3				
	Sniffer	0.25				

## 2. **RESULTS IF FIREWALL WERE NOT USED**

	IF F	REMISE V	VERE FAL	SE			
	Survey1	Survey2	Survey3	Survey4	Average		
Firewall							
Virus	-1	0	-0.6	-0.6	-0.55	FIREWALL NOT USED	
Worm	-1	0	-0.4	-0.6	-0.5		
Zombie	-0.4	-0.6	-0.4	-0.8	-0.55	0	
Trojan H	-0.4	0	-0.2	-0.6	-0.3		
Backdoor	-0.2	0	-0.4	-0.8	-0.35	-0.1 4 20 50 50 50 00 00 50 50 50 50 50 50 50 50	1990 - H
DOS	-1	-0.6	-1	-1	-0.9		
Logic Bomb	-1	0	0	-0.6	-0.4		
E-Mail Sp	-0.2	0	0	-0.6	-0.2		
IP Add Sp	-0.2	-0.8	-1	-0.8	-0.7		
Keylogger	-0.4	0	0	-0.8	-0.3	ž -0.4 T	
Sniffer	-0.4	0	0	-0.8	-0.3		
	Virus	-0.55				g -0.6	
	Worm	-0.5				-0.7	
	Zombie	-0.55					
	Trojan H	-0.3				₿ -0.8	
	Backdoor	-0.35				-0.9	
	DOS	-0.9					
	Logic Borr	-0.4				-1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -	
	E-Mail Sp	-0.2				Attack Method	
	IP Add Sp	-0.7					
	Keylogger	-0.3					
	Sniffer	-0.3					

## 3. **RESULTS IF IDS/IPS WERE USED**

	IF	PREMISE	NERE TRU	E															
	Survey1	Survey2	Survey3	Survey4	Average														
IDS/IPS																			
Virus	0.2	0	0.6	0.4	0.3							IDS	IPS U	SED					
Worm	0.2	0	0.6	0.4	0.3														
Zombie	0.6	0	0.6	0.6	0.45	5	0.6											_	
Trojan H	0	0	0.2	0.8	0.25	Ë	0.5												
Backdoor	0	0	0.6	0.6	0.3	- Mai	0.5												
DOS	0.8	0	0.4	1	0.55	Ē	0.4			┥┟				{ ⊢			$\neg$		
Logic Bomb	0	0	0.2	0.2	0.1	Ę	03												
E-Mail Sp	0.2	0	0	0.6	0.2	FAt	V.3 T			ר ר	_	_							
IP Add Sp	0.8	0	0.2	0.8	0.45	6	0.2		+	┥┟	_			┥┝─		_			
Keylogger	0	0	0	0.6	0.15	ale	01												
Sniffer	0.4	0	0	0.8	0.3	۴.	·' T			ר ר									
						eli.	0 🖵	<b>_</b>	<u> </u>		_		<b>_</b>	<u> </u>		<u> </u>			
	Virus	0.3					wis		n ,	æ	~	¢	ó	P - 5	(P)	۶.	জ ুর্ব	. 3	**
	Worm	0.3					7	20	125	بر	ð.	actor	$\mathcal{Q}$	୍କ୍ୟୁ	Main	2 Par	NOSS	୍ରେ	R.
	Zombie	0.45										5		Ŷ.	*	*	Æ.		
	Trojan H	0.25											Attacl	k Meth	od				
	Backdoor	0.3																	
	DOS	0.55																	
	Logic Borr	0.1																	
	E-Mail Sp	0.2																	
	IP Add Sp	0.45																	
	Keylogger	0.15																	
	Sniffer	0.3																	

### 4. **RESULTS IF IDS/IPS WERE NOT USED**

	IF F	REMISE V	VERE FALS	SE							
	Survey1	Survey2	Survey3	Survey4	Average						
IDS/IPS											
Virus	-0.2	0	-0.4	-0.4	-0.25		IDS/IPS	NOT USED			
Worm	-0.2	0	-0.4	-0.4	-0.25						
Zombie	-0.6	0	-0.4	-0.6	-0.4	0					
TH	0	0	-0.2	-0.8	-0.25	- 39 A	k. K. k.	a Pa	\$. <del>\$</del> .	A .4	40
Backdoor	0	0	-0.4	-0.6	-0.25	ੂਊ -0.1° 🖓 🖓		2 8.	AND A	익세액	5 <sup>111</sup> -
DOS	-0.8	0	-0.2	-1	-0.5	Les les	I M I	1		K. □	
Logic Bomb	0	0	-0.2	-0.4	-0.15	<b>E</b> -0.2	-			_	
E-Mail Sp	0	0	0	-0.6	-0.15						
IP Add Sp	-0.8	0	-0.2	-0.8	-0.45	-0.3				_	
Keylogger	0	0	0	-0.6	-0.15	÷ l					
Sniffer	-0.4	0	0	-0.8	-0.3	<u>9</u> -0.4				_	
						2					
	Virus	-0.25				🧧 -0.5 -					
	Worm	-0.25				ä					
	Zombie	-0.4				-0.6					
	Trojan H	-0.25						Attack Meth	od		
	Backdoor	-0.25									
	DOS	-0.5									
	Logic Borr	-0.15									
	E-Mail Sp	-0.15									
	IP Add Sp	-0.45									
	Keylogger	-0.15									
	Sniffer	-0.3									

## 5. **RESULTS IF HARDENING WAS USED**

	IF	PREMISE	WERE TRU	ΙE			
	Survey1	Survey2	Survey3	Survey4	Average		
Hardening							
Virus	0	0.8	0	0.2	0.25	HARDENING USED	
Worm	0	0.8	0.8	0.6	0.55		
Zombie	0.4	0.8	0.8	0.6	0.65	<b>5</b> 0.7	
TH	0.2	0.8	0	0.6	0.4		
Backdoor	0.2	0.8	0.8	0.8	0.65		1
DOS	0.4	0	0	0.2	0.15		
Logic Bomb	0.2	0.8	0.2	0.6	0.45		<u> </u>
E-Mail Sp	0.2	0	0	0.4	0.15		
IP Add Sp	0.2	0	0	0.4	0.15		
Keylogger	0.8	0.8	0	0.6	0.55		
Sniffer	0.8	0	0	0.6	0.35		H H
						┋╻┼┷┹┯┺┹┯┺┹┯┺┹┯┺┹┯┺┹┯┺┹┯┺	
	Virus	0.25					ъđ
	Worm	0.55				- In we prin role seed to so and we	SUIT
	Zombie	0.65				, & <sup>Q</sup> , & 4, 16,	
	Trojan H	0.4				Attack Methods	
	Backdoor	0.65					
	DOS	0.15					
	Logic Borr	0.45					
	E-Mail Sp	0.15					
	IP Add Sp	0.15					
	Keylogger	0.55					
	Sniffer	0.35					

## 6. **RESULTS IF HARDENING WAS NOT USED**

	IF F	REMISE V	VERE FAL	SE		
	Survey1	Survey2	Survey3	Survey4	Average	
Hardening						
Virus	0	-0.8	0	-0.6	-0.35	HARDENING NOT USED
Worm	0	-0.8	-1	-0.6	-0.6	3
Zombie	-0.4	-0.8	-1	-0.6	-0.7	
TH	-0.2	-0.8	0	-0.6	-0.4	
Backdoor	-0.8	-0.8	-1	-0.8	-0.85	
DOS	-0.4	0	0	-0.6	-0.25	
Logic Bomb	-0.8	-0.8	-0.2	-0.6	-0.6	3 <b>£</b> -0.3 <b>+ + + + + + + + +</b>
E-Mail Sp	-0.2	0	0	-0.4	-0.15	j ž _0,4
IP Add Sp	-0.2	0	0	-0.4	-0.15	
Keylogger	-0.8	-0.8	0	-0.6	-0.55	j <b>v</b> -0.5
Sniffer	-0.8	0	0	-0.6	-0.35	j <u>9</u> -0.6
						-0.7
	Virus	-0.35				
	Worm	-0.6				<b>a</b> -0.8
	Zombie	-0.7				-0.9 _
	Trojan H	-0.4				Attack Methods
	Backdoor	-0.85				
	DOS	-0.25				
	Logic Borr	-0.6				
	E-Mail Sp	-0.15				
	IP Add Sp	-0.15				
	Keylogger	-0.55				
	Sniffer	-0.35				

# 7. **RESULTS IF ADEQUATE TRAINING WAS USED**

	IF I	PREMISE \	NERE TRU	E															
	Survey1	Survey2	Survey3	Survey4	Average														
Training																			
Virus	0.6	0.4	0.8	0.6	0.6								TRAI	NING USE	D				
Worm	0.2	0.2	0	0.4	0.2														
Zombie	0.4	0.2	0	0.4	0.25		5	0.7											
TH	0	0.2	0.8	0.8	0.45		Ē	0.6											
Backdoor	0.2	0.2	0	0.6	0.25		- A	0.5											
DOS	0	0	0	0.4	0.1		Ē	0.5				_	_						
Logic Bomb	0.2	0.4	0	0.6	0.3		tac.	0.4	┥┝				-						
E-Mail Sp	0	0.4	0	0.8	0.3		¥.	0.3	┥┝								_		
IP Add Sp	0	0	0	0.4	0.1		6	0.2											
Keylogger	0.8	0	0	0.6	0.35		- ale	0.2											
Sniffer	0	0	0	0.4	0.1		ž	0.1				$\square$							
							elie	0		<b>,</b>	Ļ				-		┯┻		
	Virus	0.6					-	~~~~		- m	S.	×	. ¢	S	-Ch	ୁ କ	, A	at the second	and the
	Worm	0.2						20	4	A0.	Dun		- acter	5	°,	Main	20	NOSS .	Super
	Zombie	0.25											ଙ	্ 🖓		* *	4	S	
	TH	0.45											A	ttack Me	etho	ds			
	Backdoor	0.25																	
	DOS	0.1				L L													
	Logic Borr	0.3																	
	E-Mail Sp	0.3																	
	IP Add Sp	0.1																	
	Keylogger	0.35																	
	Sniffer	0.1																	

# 8. **RESULTS IF ADEQUATE TRAINING WERE NOT USED**

	IF F	REMISE V	VERE FAL	SE									
	Survey1	Survey2	Survey3	Survey4	Average								
Training													
Virus	-1	-1	-0.8	-0.6	-0.85				TRAINI	NG NOT USE	D		
Worm	-0.2	-1	0	-0.6	-0.45								
Zombie	-0.4	-0.6	0	-0.4	-0.35		0						
TH	0	-0.6	-0.8	-0.8	-0.55		1	1 10			8 9	a a	400
Backdoor	0	-0.6	0	-0.6	-0.3		-0.1.4	No Dun	- Jer	\$ \$	Non D	S. JOB	Sille
DOS	0	0	0	-0.4	-0.1		-0.2	—		100 to	<u>&amp;</u>	<del>- &amp;</del> ,	
Logic Bomb	0	-0.2	0	-0.6	-0.2		-0.3						
E-Mail Sp	0	0.2	0	-0.8	-0.15								
IP Add Sp	0	0	0	-0.4	-0.1		-0.4						
Keylogger	-0.8	0	0	-0.6	-0.35		-0.5						
Sniffer	0	0	0	-0.4	-0.1		-0.6						
							0.7						
	Virus	-0.85					-0.7						
	Worm	-0.45				i i i i i i i i i i i i i i i i i i i	-0.8						
	Zombie	-0.35					-0.9						
	TH	-0.55								Attack Meth	bou		
	Backdoor	-0.3								Attaok mou			
	DOS	-0.1											
	Logic Borr	-0.2											
	E-Mail Sp	-0.15											
	IP Add Sp	-0.1											
	Keylogger	-0.35											
	Sniffer	-0.1											

### 9. RESULTS IF ANTI-VIRUS SOFTWARE WAS USED

	IF	PREMISE	WERE TRU	E																
	Survey1	Survey2	Survey3	Survey4	Average															
Anti-virus																				٦
Virus	0.8	0.8	0.8	0.8	0.8							ANTI-V	IRUS US	ED						
Worm	0.8	0.8	0.6	0.8	0.75															
Zombie	0.4	0.8	0.6	0.4	0.55	5	0.9													
Trojan H	0.8	0.8	0.4	0.8	0.7	Ē	0.8	-											_	
Backdoor	0.2	2 0	0.6	0.4	0.3	Na.	0.7												_	
DOS	0	0	0	0.4	0.1	<u> </u>	0.6		┥┝		_	<u> </u>							_	
Logic Bomb	0.8	0	0	0.6	0.35	ţ	0.5		┥┝	$-\Box$	_								_	
E-Mail Sp	0.4	0	0	0.4	0.2	₹.	0.4		┥┝										_	
IP Add Sp	0.4	. 0	0	0.2	0.15		0.3		┥┝	-	_			_				_	_	
Keylogger	0	0.8	0	0.2	0.25	alu	0.2		┥┝	-	_	$\mathbf{H}$		_		<u> </u>	_			
Sniffer	0	0 0	0	0.2	0.05	٩ <sup>2</sup>	0.1		┥┝	-	_	$\mathbf{H}$							_	
						<u>Seli</u>	0 +	<b>.</b>		,	-			-		<b>_</b>	<b>.</b>	<b>_</b>		
	Virus	0.8					NS		¢ .	de la	~*	set.	S	mp	୍କ	.9	€®	+ 4	ø	
	Worm	0.75					-2-	-240	10	· 🖈	ð.	actor.		æ	Man	, pào	- Aloge	et.	(	
	Zombie	0.55									~	5	2º.		× 1	¢	Æ.			
	Trojan H	0.7										A	ttack Me	thod	Is					
	Backdoor	0.3																		
	DOS	0.1																_		_
	Logic Bon	n 0.35																		
	E-Mail Sp	0.2																		
	IP Add Sp	0.15																		
	Keylogger	0.25																		
	Sniffer	0.05																		

#### 10. RESULTS IF ANTI-VIRUS SOFTWARE WAS NOT USED

	IF F	REMISE V	VERE FAL	SE			
	Survey1	Survey2	Survey3	Survey4	Average		
Firewall							
Virus	-1	0	-0.6	-0.6	-0.55	FIREWALL NOT USED	
Worm	-1	0	-0.4	-0.6	-0.5		
Zombie	-0.4	-0.6	-0.4	-0.8	-0.55	0	
Trojan H	-0.4	0	-0.2	-0.6	-0.3		*
Backdoor	-0.2	0	-0.4	-0.8	-0.35	-0.1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	4 H
DOS	-1	-0.6	-1	-1	-0.9		
Logic Bomb	-1	0	0	-0.6	-0.4		
E-Mail Sp	-0.2	0	0	-0.6	-0.2		
IP Add Sp	-0.2	-0.8	-1	-0.8	-0.7		
Keylogger	-0.4	0	0	-0.8	-0.3	¥ ***	
Sniffer	-0.4	0	0	-0.8	-0.3	₽ -0.5 + + + + + + + + + + + + + + + + + + +	
	Virus	-0.55				<u>9</u> -0.0	
	Worm	-0.5				-0.7	_
	Zombie	-0.55					
	Trojan H	-0.3				<b>B</b> -0.8	
	Backdoor	-0.35				-0.9	
	DOS	-0.9					
	Logic Borr	-0.4				-1 J	
	E-Mail Sp	-0.2				Attack Method	
	IP Add Sp	-0.7					
	Keylogger	-0.3					
	Sniffer	-0.3					

### 11. RESULTS IF SPAM FILTER WERE USED

	IFI	PREMISE \	VERE TRU	E		
	Survey1	Survey2	Survey3	Survey4	Average	
Anti-Spam						
Virus	0	0	0.2	0.4	0.15	SPAM FILTER USED
Worm	0.4	. 0	0.2	0.4	0.25	
Zombie	0	0	0.2	0.4	0.15	5 0.4
Trojan H	0	0	0.2	0.4	0.15	E 0.35
Backdoor	0.2	0	0.2	0.2	0.15	2 0.3
DOS	0.8	0.2	0	0	0.25	▲ ★ 0.25
Logic Bomb	0.2	0	0	0.2	0.1	
E-Mail Sp	0.2	0.8	0	0.4	0.35	
IP Add Sp	0	0	0	0	0	
Keylogger	0	0	0	0	0	
Sniffer	0	0	0	0	0	
	N.C.	0.45				
	Virus	0.15				we share the the top of the set in the set
	VVorm	0.25				- V. W. D. rol see . ret in a plu and an
	Zombie	0.15				
	Trojan H	0.15				Attack Tool
	Dackdoor	0.15				
	Logic Deg	0.25				
	E Mail Sn	0.1	-			
	E-Iviali Sp	0.35				
	Kovloggor					
	Spiffor	0				
	Sniner	U U				

## 12. RESULTS IF SPAM FILTER WERE NOT USED

	IF P	REMISE W	ERE FALS	E																
	Survey1	Survey2	Survey3	Survey4	Average															
Anti-Spam																				
Virus	0	0	-0.2	-0.4	-0.15							SPAN	I FILT	ER NO	TUS	ED				
Worm	-0.6	0	-0.2	-0.4	-0.3															
Zombie	0	0	-0.2	-0.4	-0.15		0 т			<b>_</b>			<b>'</b> ''			<b>_</b>				
Trojan H	0	0	-0.2	-0.4	-0.15	=			A.		3 <b>8</b>	1		0	1 di	० ्व	2	A 2	40	
Backdoor	-0.2	0	-0.2	-0.2	-0.15	ē -0.1	24		20	Pr	أړ[	8	Sec.		J.S.	Mor	200	all the second	SUL	
DOS	-0.8	-0.2	0	0	-0.25	- R	.1 -	┥┝	_	-	- 1-	<b>—</b> °			*₽—	<u>v</u>	~_	4°.	_	
Logic Bomb	-0.2	0	0	-0.2	-0.1	Ê.	16													
E-Mail Sp	-0.2	-0.8	0	-0.4	-0.35	월 -0.	'° T													
IP Add Sp	0	0	0	0	0	∰ -0	.2 +		_										_	
Keylogger	0	0	0	0	0	÷.,	26													
Sniffer	0	0	0	0	0	_≘ <sup>-0.4</sup>	° T													
						- R	.3 -												_	
	Virus	-0.15				ie .														
	Worm	-0.3				å -0	° T													
	Zombie	-0.15				-0	. <u>4</u> JII													
	Trojan H	-0.15											A	ttack I	Metho	ods				
	Backdoor	-0.15																		
	DOS	-0.25																		 -
	Logic Borr	-0.1																		
	E-Mail Sp	-0.35																		
	IP Add Sp	0																		
	Keylogger	0																		
	Sniffer	0																		

### 13. RESULTS IF ANTI-SPYWARE WERE USED

	IF F	REMISE V	VERE TRU	Ē		
	Survey1	Survey2	Survey3	Survey4	Average	
Anti-Spyware						
Virus	0.4	0.2	0	0.6	0.3	ANTI-SPYWARE USED
Worm	0.4	0.2	0	0.6	0.3	
Zombie	0.2	0.2	0	0.2	2 0.15	5 0.4
Trojan H	0.4	0.4	0	0.6	0.35	0.35
Backdoor	0.2	0.4	0	0.6	0.3	0.3
DOS	0.2	0	0	0.4	0.15	
Logic Bomb	0.4	0.2	0	0.2	2 0.2	
E-Mail Sp	0	0	0	0.2	2 0.05	
IP Add Sp	0.2	0	0	C	0.05	
Keylogger	0	0.4	0	0.6	0.25	
Sniffer	0	0.4	0	0.6	0.25	
						▁▏      ┋॒
	Virus	0.3				the the the the the the the the the
	Worm	0.3				IN THE DOLL HOLE SHOW I FOR THEM AND HOLE GUT
	Zombie	0.15				, & <sup>Q</sup> o, & 1 th.
	Trojan H	0.35				Attack Methods
	Backdoor	0.3				
	DOS	0.15				
	Logic Born	0.2				
	E-Mail Sp	0.05				
	IP Add Sp	0.05				
	Keylogger	0.25				
	Sniffer	0.25				

### 14. RESULTS IF ANTI-SPYWARE WERE NOT USED

	IF P	REMISE W	ERE FALS	SE									
	Survey1	Survey2	Survey3	Survey4	Average								
Anti-Spyware													
Virus	-0.4	-0.2	0	-0.6	-0.3			AN	TI-SPYWA	RE NOT US	SED		
Worm	-0.2	-0.2	0	-0.6	-0.25								
Zombie	-0.2	-0.2	0	-0.2	-0.15		0						
Trojan H	-0.2	-0.4	0	-0.6	-0.3		A CONSTRUCTION	× 138	1 .		S. 4 .	\$	
Backdoor	-0.2	-0.4	0	-0.6	-0.3	- i - j - j - j - j - j - j - j - j - j	0.05 9 38	10 A	Charles -		ANOL O POO	all	580
DOS	-0.2	0	0	-0.4	-0.15	Ver	-01				× 14	Æ.	
Logic Bomb	-0.4	-0.2	0	-0.2	-0.2		-0.1						
E-Mail Sp	0	0	0	-0.2	-0.05	걸.	.0.15						
IP Add Sp	-0.2	0	0	0	-0.05	Att .							
Keylogger	0	-0.4	0	-0.6	-0.25		-0.2		+ $+$ $+$ $+$ $+$ $+$ $+$ $+$ $+$ $+$				
Sniffer	0	-0.4	0	-0.6	-0.25		0.25						
						S	-0.23						
	Virus	-0.3					-0.3						
	Worm	-0.25				ă							
	Zombie	-0.15					0.35						
	Trojan H	-0.3							At	tack Method	s		
	Backdoor	-0.3											
	DOS	-0.15											
	Logic Borr	-0.2											
	E-Mail Sp	-0.05											
	IP Add Sp	-0.05											
	Keylogger	-0.25											
	Sniffer	-0.25											

## LIST OF REFERENCES

Adams, James. <u>The Next World War: Computers are the Weapons & the Front Line is</u> <u>Everywhere</u>. New York: Simon and Schuster, 1998.

Arquilla, John. Interview with FRONTLINE. <u>Cyberwar!: FRONTLINE</u>. 4 Mar. 2003. 8 Mar. 2007 <a href="http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html">http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html</a>.

Billo, Charles G., and Welton Chang. <u>Cyber Warfare: an Analysis of the Means and Motivations of Selected Nation States</u>. Institute for Security Technology Studies, Dartmouth College. Hanover: Trustees of Dartmouth College, 2004.

Brodhun III, Carl P. <u>Prioritization of Information Assurance (IA) Technology in a</u> <u>Resource Constrained Environment</u>. Thesis. Naval Postgraduate School, 2001. Monterey: Naval Postgraduate School, 2001.

Cragin, Kim, and Sara A. Daly. <u>The Dynamic Terrorist Threat: an Assessment of Group</u> <u>Motivations and Capabilities in a Changing World</u>. RAND Corporation. Santa Monica: RAND Corporation, 2004.

Denning, Dorothy E. Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, Washington. D.C. 23 May 2000. 8 Mar. 2007 <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

Denning, Dorothy E. Information Warfare and Security. New York: Addison-Wesley, 1999.

Denning, Dorothy E. <u>Is Cyber Terror Next</u>. Social Science Research Council. Georgetown: Social Science Research Council / After Sept 11. 8 Mar. 2007 <<u>http://www.ssrc.org/sept11/essays/denning\_text\_only.html></u>.

Gross, Grant. "U.S. DHS Completes Large-Scale Cyber Exercise: Cyber Storm Simulates Attack on Computer Systems At an Electric Utility, Cybersecurity Vendors Kick of Analysis of Results." <u>InfoWorld</u> (2006). 8 Mar. 2007.

"IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005." IBM News. 4 Aug. 2005. 22 Feb. 2007 <a href="http://www.ibm.com/news/ie/en/2005/08/ie\_en\_news\_20050804.html">http://www.ibm.com/news/ie/en/2005/08/ie\_en\_news\_20050804.html</a>>.

Janczewski, Lech J., and Andrew M. Colarik. <u>Managerial Guide for Handling Cyber-</u> <u>Terrorism and Information Warfare</u>. Hershey: Idea Group, 2005. Lemos, Robert. "Safety: Assessing the Infrastructure Risk." CNET News. 26 Aug. 2006. 8 Mar. 2007 <a href="http://news.com/2009-1001-954780.html">http://news.com/2009-1001-954780.html</a>>.

Lewis, Ted G. <u>Critical Infrastructure Protection in Homeland Security: Defending a</u> <u>Networked System</u>. New Jersey: John Wiley & Sons Inc., 2006.

Libicki, Martin C. "Information Dominance." <u>Strategic Forum</u> (1997). 8 Mar. 2007 <<u>http://www.ndu.edu/inss/strforum/SF132/forum132.html></u>.

Peltier, Thomas R. <u>Information Security Risk Analysis</u>. Second ed. Boca Raton: Auerbach Publications, 2005.

Rollins, John, and Clay Wilson. <u>Terrorist Capabilities for Cyberattack: Overview and</u> <u>Policy Issues</u>. CRS Report for Congress. Washington, D.C.: Congressional Research Service - the Library of Congress, 2005.

Rosen, Julie A., and Wayne L. Smith. <u>Situational Influence Assessment Module (SIAM)</u> <u>User's Manual</u>. 6th ed. San Diego: Science Applications International Corporation, 2006.

Sands, Jeffrey I., and Bradd C. Hayes, comps. <u>Understanding and Using SIAM</u>. Naval War College, Center for Naval Warfare Studies, Decision Support Department. 15 Jan. 2007 <a href="http://www.au.af.mil/au/awc/awcgate/modeling/usesiam.doc">http://www.au.af.mil/au/awc/awcgate/modeling/usesiam.doc</a>.

"SANS Top 20-Internet Security Attack Targets." <u>SANS</u>. 8 Mar. 2007. Escal Institute of Advanced Technologies. 8 Mar. 2007 <a href="http://www.sans.org/top20/>">http://www.sans.org/top20/</a>.

Serabian Jr., John A. "Cyber Threats and the U.S. Economy." Joint Economic Committee. Washington. D.C. 23 Feb. 2000. 8 Mar. 2007 <a href="http://www.cia.gov/cia/public\_affairs/speeches/2000/cyberthreats\_022300.html">http://www.cia.gov/cia/public\_affairs/speeches/2000/cyberthreats\_022300.html</a>>.

Thomas, Douglas, and Brian D. Loader. <u>Cybercrime: Law Enforcement, Security and</u> <u>Surveillance in the Information Age</u>. New York: Routledge, 2000.

United States. Assistant Secretary of Defense for Command, Control, Communications and Intelligence. Department of Defense. <u>DoD Directive 8500.1 Information Assurance</u> (IA). Washington D.C.: DoD, 2002.

United States. Chairman. Joint Chiefs of Staff. Joint Publication 3-13 Information Operations. Washington D.C.: Joint Chiefs of Staff, 2006.

United States. Department of Defense. <u>DoD Directive 8500.2 Information Assurance</u> (IA) Implementation. Washington D.C.: DoD, 2003.

United States. National Manager, Committee on National Security Systems (CNSS). National Security Agency. <u>CNSS Instruction No. 4009 National Information Assurance</u> (IA) Glossary. Washington D.C.: CNSS, 2003. United States. President of the United States. <u>The National Strategy to Secure</u> <u>Cyberspace</u>. Washington D.C.: The White House, 2003.

Wilson, Clay. <u>Information Warfare and Cyberwar: Capabilities and Related Policy</u> <u>Issues</u>. CRS Report for Congress. Washington, D.C.: Congressional Research Service the Library of Congress, 2004.

Woody, Carol, and Larry Clinton. <u>Common Sense Guide to Cyber Security for Small</u> <u>Businesses</u>. 1st ed. Arlington: Carnegie Mellon University and Internet Security Alliance, 2004. <u>Recommended Actions for Information Security</u>. 8 Mar. 2007 <a href="http://www.us-cert.gov/reading\_room/CSG-small-business.pdf">http://www.uscert.gov/reading\_room/CSG-small-business.pdf</a>>.

Verton, Dan. <u>Black Ice: the Invisible Threat of Cyber-Terrorism</u>. New York: McGraw-Hill/Osborne, 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

## **INITIAL DISTRIBUTION LIST**

- 1. Defense Technical Information Center Ft. Belvoir, Virginia
- 2. Dudley Knox Library Naval Postgraduate School Monterey, California
- Dr. Dan C. Boger Naval Postgraduate School Monterey, California
- 4. Dr. Dorothy E. Denning Naval Postgraduate School Monterey, California
- 5. Mr. Steve Iatrou Naval Postgraduate School Monterey, California