

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

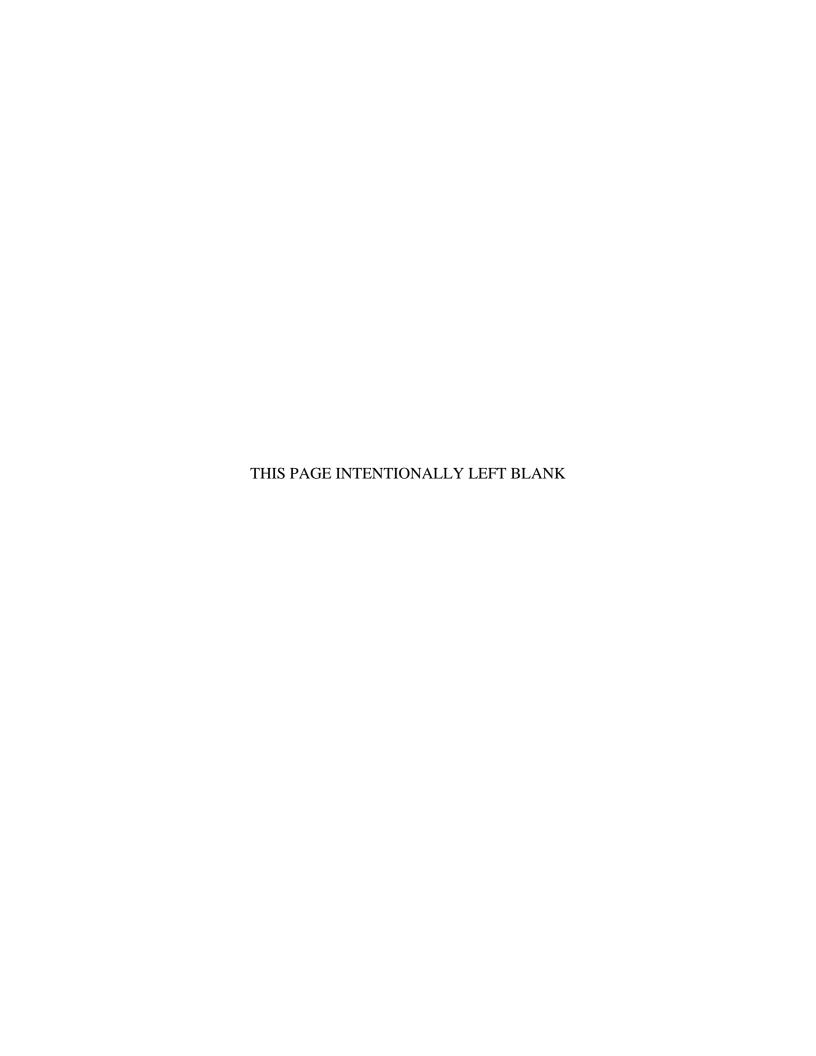
March 2007

Thesis Advisor:

Second Reader:

Dorothy Denning
Steve Iatrou

Approved for public release; distribution is unlimited.



REPORT DOCUMENTATION PAGE Form Approved 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. 3. REPORT TYPE AND DATES COVERED 1. AGENCY USE ONLY (Leave blank) 2. REPORT DATE March 2007 Master's Thesis 4. TITLE AND SUBTITLE Risk of Cyber Attack to Naval Ships Inport Naval 5. FUNDING NUMBERS Station Everett: A Model Based Project Utilizing SIAM 6. AUTHOR(S) LT Rodrick A. Tester, USN 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) 8. PERFORMING ORGANIZATION Naval Postgraduate School REPORT NUMBER Monterey, CA 93943-5000 9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) 10. SPONSORING/MONITORING AGENCY REPORT NUMBER 11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

13. ABSTRACT (maximum 200 words)

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited

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.

14. SUBJECT TERMS Cyberterrorism, information assura Assessment Module (SIAM)	15. NUMBER OF PAGES 95 16. PRICE CODE		
17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

12b. DISTRIBUTION CODE

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	RODUCTION	1
	A.	BACKGROUND AND MOTIVATION BEHIND THE RESEARC	CH1
	В.	GENERAL SCOPE OF THE THESIS	
	C.	BRIEF EXPLANATION OF METHODOLOGY	3
	D.	BENEFITS OF STUDY	
	E.	THESIS STRUCTURE:	4
II.	BAC	KGROUND INFORMATION	7
,	A.	INTRODUCTION TO INFORMATION OPERATIONS	
	В.	INFORMATION ASSURANCE	
	_,	1. Availability	
		2. Integrity	
		3. Authentication	
		4. Confidentiality	
		5. Non-repudiation	
	C.	CYBER THREATS AND THEIR MOTIVES	9
		1. Insiders	
		2. Hackers	
		3. Criminals	
		4. Corporations	
		5. Government Agencies	
		6. Terrorists	10
	D.	VULNERABILITIES	11
	E.	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	
		6. Key Logger	
		7. Logic Bomb	13
		8. Packet Sniffing	
		9. Spoofing	13
		10. Spyware	
		11. Trojan Horse	
		12. Viruses	
		13. Worms	
		14. Zombie	14
III.	SITU	UATIONAL INFLUENCE ASSESSMENT MODULE (SIAM)	15
	A.	SIAM DESCRIBED	
	В.	SIAM INFLUENCE NET SAMPLE	16
IV	MOI	DEL SET-UP	21

V.	MO	DEL DEMONSTRATION AND RESULTS	27
	A.	EXCURSION ONE	28
		1. All Security Measures Utilized	28
		2. Results	28
	В.	EXCURSION TWO	
		1. No Anti-Virus	
		2. Results:	
	С.	EXCURSION THREE	
		1. No Firewall	
		2. Results	31
VI.	REC	RECOMMENDATIONS AND CONCLUSIONS	
	A.	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	
		a. Conduct a Classified Continuation of This Thesis	34
		b. Keep the Model Current	
		c. Conduct Cost Benefit Analysis	
	В.	CONCLUSIONS	35
APP	ENDIX	X A EXPERT OPINION SURVEY	37
	1.	FIREWALL SECTION OF SURVEY	
	2.	IDS/IPS SECTION OF SURVEY	
	3.	HARDENING SECTION OF SURVEY	
	4.	TRAINING SECTION OF SURVEY	
	5.	ANTI-VIRUS SECTION OF SURVEY	54
	6.	ANTI-SPAM SECTION OF SURVEY	
	7.	ANTI-SPYWARE SECTION OF SURVEY	62
A DD	ENDIX		
AFF		RESULTS IF FIREWALL WERE USED	07 69
	1. 2.	RESULTS IF FIREWALL WERE NOT USED	
	2. 3.	RESULTS IF IDS/IPS WERE USED	
	3. 4.	RESULTS IF IDS/IPS WERE NOT USED	
	4. 5.	RESULTS IF HARDENING WAS USED	
	5. 6.	RESULTS IF HARDENING WAS USEDRESULTS IF HARDENING WAS NOT USED	
	7.	RESULTS IF ADEQUATE TRAINING WAS USED	
	8.	RESULTS IF ADEQUATE TRAINING WAS USED	/1 71
	o. 9.	RESULTS IF ANTI-VIRUS SOFTWARE WAS USED	
	9. 10.	RESULTS IF ANTI-VIRUS SOFTWARE WAS USED RESULTS IF ANTI-VIRUS SOFTWARE WAS NOT USED	
	10. 11.	RESULTS IF ANTI-VIRUS SOFTWARE WAS NOT USED	
	11. 12.	RESULTS IF SPAM FILTER WERE USED RESULTS IF SPAM FILTER WERE NOT USED	
	12. 13.	RESULTS IF SPANIFILTER WERE NOT USED RESULTS IF ANTI-SPYWARE WERE USED	
	13. 14.	RESULTS IF ANTI-SPY WARE WERE USED	
	14.	INDICATED AND AND AND INCIDENTAL TO A PARTY OF A PARTY	

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	
Figure 3.	Link Properties	
Figure 4.	Root Node and Parents	
Figure 5.	Security Tools and links	23
Figure 6.	Excursion 1 (All security measures used)	28
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, Cyber Warfare; An Analysis of the Means and Motivations of Selected Nation States (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 Institute¹ 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

¹ 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. Troian 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.

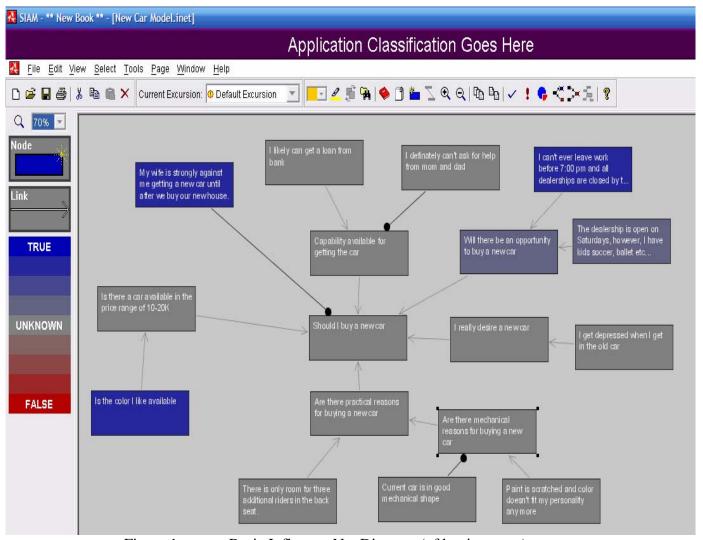


Figure 1. Basic Influence Net Diagram (of buying a car)

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.

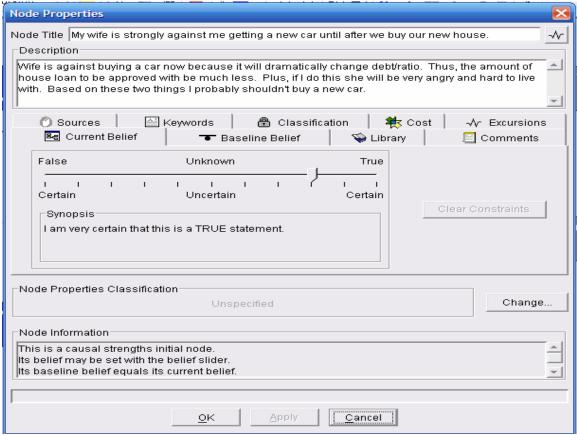


Figure 2. Node Properties

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."

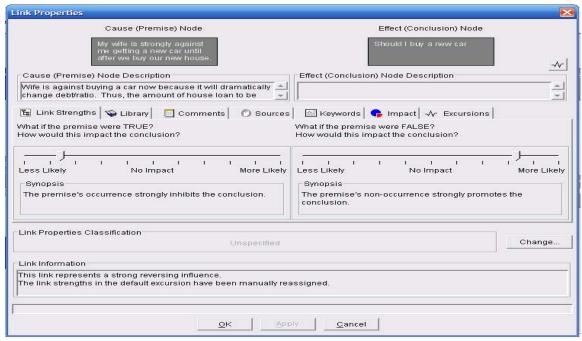


Figure 3. Link Properties

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

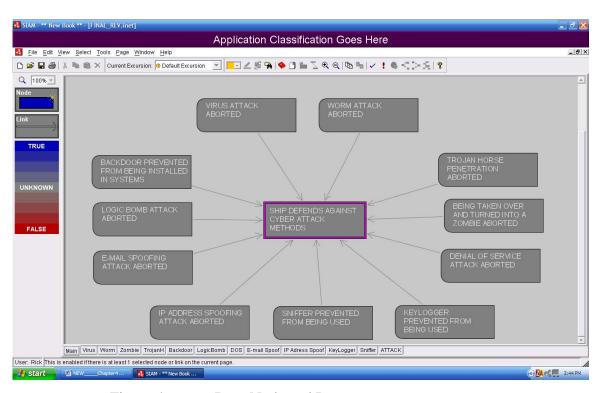


Figure 4. Root Node and Parents

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

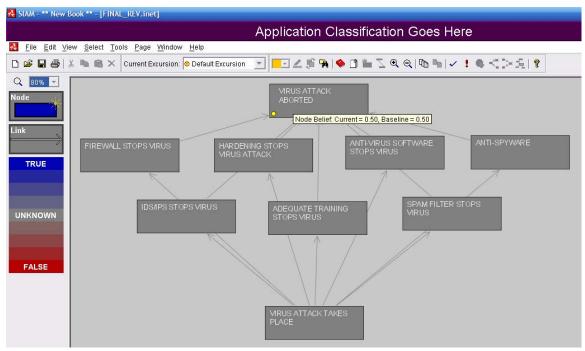


Figure 5. Security Tools and links

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:

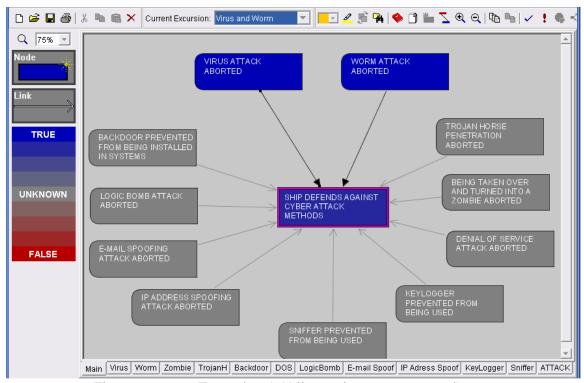


Figure 6. Excursion 1 (All security measures used)

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:

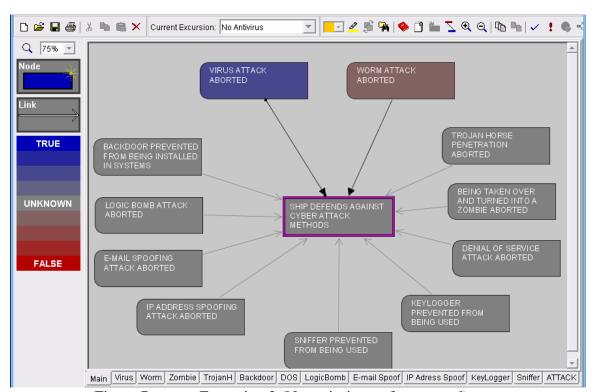


Figure 7. Excursion 2 (No anti-virus software used)

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.

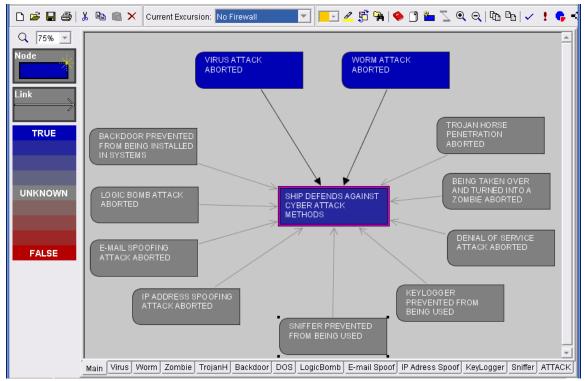


Figure 8. Excursion 3 (No firewall used)

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.

1. FIREWALL SECTION OF SURVEY

			Expert C	pinion F	Research	Tool -	FIREWAL	<u>_L</u>		
If a FIRE	WALL were	e used, ho	w likely is it t	that the sy	stem could	prevent a	VIRUS from i	nfecting th	e targeted	system?
Less likely					No Impact					More Likely
Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severel
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promote
1.	WALL were	e NOT use	d, how likely	is it that th	ne system o	ould preve	ent a VIRUS f	rom infecti	ng targeted	
Less					No Impact					More Likely
Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severel
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promote
	WALL were	e used, ho	w likely is it t	that the sy	stem could	prevent a	WORM from	infecting th	e targeted	system*
Less				01:	No Impact					Likely
Severely	Severely	Strongly	Moderately	Slightly	No loos set	Slightly	Moderately	Strongly	Severely	Severel
Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promote
If a FIRE	WALL were	e NOT use	d, how likely	is it that th	ne system o	ould preve	ent a WORM f	rom infecti	ng targete	d system
If a FIRE Less likely	WALL were	e NOT use	d, how likely	is it that th	No Impact	ould preve	enta WORM 1	from infecti	ng targete	More Likely
Less likely Severely	Severely	Strongly	Moderately	Slightly	No Impact	Slightly	ent a WORM f	Strongly	Severely	More Likely
Less likely						Slightly				More
Less likely Severely	Severely	Strongly	Moderately	Slightly	No Impact	Slightly	Moderately	Strongly	Severely	More Likely Severel
Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately	Strongly promotes	Severely promotes	More Likely Severel promote
Less likely Severely Inhibits If a FIRE	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	More Likely Severel promote
Less likely Severely Inhibits If a FIRE ZOMBIE Less	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact No Impact	Slightly promotes em could p	Moderately promotes	Strongly promotes	Severely promotes	More Likely Severel promote d into a
Less likely Severely Inhibits If a FIRE ZOMBIE I Less likely	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes em could p	Moderately promotes	Strongly promotes	Severely promotes	More Likely Severel promot d into a
Less likely Severely Inhibits If a FIRE ZOMBIE Less	Severely Inhibits WALL were by an attac	Strongly Inhibits e used, ho	Moderately Inhibits w likely is it t	Slightly Inhibits	No Impact No Impact	Slightly promotes em could p	Moderately promotes	Strongly promotes taken over	Severely promotes	More Likely Severel promote d into a More Likely Severel
Less likely Severely Inhibits If a FIRE ZOMBIE I Less likely Severely	Severely Inhibits WALL were by an attack.	Strongly Inhibits e used, ho ker?	Moderately Inhibits w likely is it to Moderately	Slightly Inhibits that the tai	No Impact No Impact No Impact	Slightly promotes em could p	Moderately promotes prevent being Moderately	Strongly promotes taken over	Severely promotes and turne Severely	More Likely Severel promote d into a
Less likely Severely Inhibits If a FIRE ZOMBIE I Less likely Severely Inhibits	Severely Inhibits WALL were by an attack Severely Inhibits WALL were	Strongly Inhibits e used, ho cker? Strongly Inhibits e NOT use	Moderately Inhibits w likely is it to Moderately Inhibits	Slightly Inhibits that the tar Slightly Inhibits	No Impact No Impact No Impact No Impact	Slightly promotes em could p Slightly promotes	Moderately promotes prevent being Moderately	Strongly promotes taken over	Severely promotes and turne Severely promotes	More Likely Severel promote d into a More Likely Severel promote
Less likely Severely Inhibits If a FIRE ZOMBIE I Less likely Severely Inhibits If a FIRE I Severely Inhibits	Severely Inhibits WALL were by an attack Severely Inhibits	Strongly Inhibits e used, ho cker? Strongly Inhibits e NOT use	Moderately Inhibits w likely is it to Moderately Inhibits	Slightly Inhibits that the tar Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact	Slightly promotes em could p Slightly promotes stem could	Moderately promotes prevent being Moderately promotes	Strongly promotes taken over	Severely promotes and turne Severely promotes	More Likely Severel promote d into a More Likely Severel promote ttacker a
Less likely Severely Inhibits If a FIRE ZOMBIE Less likely Severely Inhibits If a FIRE turned in Less likely	Severely Inhibits WALL wereby an attack Severely Inhibits WALL were to a ZOMB	Strongly Inhibits e used, hocker? Strongly Inhibits e NOT use	Moderately Inhibits w likely is it to Moderately Inhibits d, how likely	Slightly Inhibits that the tai Slightly Inhibits is it that the	No Impact No Impact No Impact No Impact	Slightly promotes em could p Slightly promotes stem could	Moderately promotes prevent being Moderately promotes d prevent bei	Strongly promotes taken over Strongly promotes ng taken over	Severely promotes and turne Severely promotes ver by an a	More Likely Severel promote d into a More Likely Severel promote ttacker More Likely
Less likely Severely Inhibits If a FIRE ZOMBIE I Less likely Severely Inhibits If a FIRE turned in Less	Severely Inhibits WALL were by an attack Severely Inhibits WALL were	Strongly Inhibits e used, ho cker? Strongly Inhibits e NOT use	Moderately Inhibits w likely is it to Moderately Inhibits	Slightly Inhibits that the tar Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact	Slightly promotes em could p Slightly promotes stem could	Moderately promotes prevent being Moderately promotes	Strongly promotes taken over	Severely promotes and turne Severely promotes	More Likely Severel promote d into a More Likely Severel promote ttacker a

	ted system?									More
Less					No Impact					Likely
Sever	ely Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
Inhibit		Inhibits	Inhibits	Inhibits	No Impact		promotes	promotes	promotes	promote
	IREWALL wer	re NOT use	d, how likely	is it that th	e system c	ould preve	ent a TROJAN	HORSE fro	om penetra	ting the
Less likely					No Impact					More Likely
Sever Inhibit		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promote:
		re used, ho	w likely is it	that the sys	tem could	prevent a	BACKDOOR fo	rom being	placed in t	he target
9 syste Less likely					No Impact					More Likely
Sever	ely Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
Inhibit		Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promote
Less likely Sever Inhibit		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly	Moderately promotes	Strongly promotes	Severely promotes	More Likely Severely promote
	IREWALL wer				tem could	prevent a	Denial Of Ser	vice (DOS	attack from	n
	, 3				No Impact					More Likely
Less likely				Climbth			Moderately	Strongly	Severely	Severely
		Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	promotes	promotes	promotes	promote
likely Sever					No Impact				promotes	promote
likely Sever Inhibit	s Inhibits	Inhibits	Inhibits	Inhibits		promotes		promotes		on the
likely Sever Inhibit If a F 2 targe Less likely	IREWALL wested system?	Inhibits re NOT use	Inhibits d, how likely	Inhibits is it that th		promotes ould preve	promotes	promotes n disruptin	ng service o	on the More Likely
likely Sever Inhibit If a F 2 targe Less	IREWALL wested system?	Inhibits	Inhibits	Inhibits	e system c	ould preve	promotes	promotes		on the
If a F Less likely Sever Inhibit If a F If a F If a F	IREWALL weited system? Severely systems Inhibits	Inhibits Te NOT use Strongly Inhibits	d, how likely Moderately Inhibits	is it that th	e system c	ould preve	ent a DOS from	n disruptin Strongly promotes	g service of Severely promotes	More Likely Severely promote
likely Sever Inhibit If a F 2 targe Less likely Sever Inhibit	IREWALL weited system? Severely systems Inhibits	Inhibits Te NOT use Strongly Inhibits	d, how likely Moderately Inhibits	is it that th	e system c	ould preve	promotes ent a DOS from Moderately promotes	n disruptin Strongly promotes	g service of Severely promotes	More Likely Severely promote

	If a FIRF\	NALL wer	e NOT use	d, how likely	is it that th	e system c	ould preve	ent a LOGIC F	BOMB attac	k against t	he targete
	system?	TALL WOL	o no ruse	a, now intoly	it that ti	ojotom t	cara prove	u LOGIO I	Joine and	ugumat t	urgott
\rightarrow	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	promote
1											
+											
+	If a FIRE\	NALL were	e used, ho	w likely is it t	that the sys	stem could	prevent a	⊥ n E-mail SPO	OFING atta	ck against	the
	targeted	system?					•				
	Less										More
	likely		0. 1		00.14	No Impact			0. 1		Likely
	Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
+	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact	promotes	promotes	promotes	promotes	promote
t											
			e NOT use	d, how likely	is it that th	ie system c	ould preve	ent an E-mail	SPOOFING	attack ag	ainst the
\rightarrow	targeted Less	system?									More
	likely					No Impact					Likely
	Severely	Severely	Strongly	Moderately	Slightly	. to impact	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact		promotes	promotes	promotes	promote
1											
4											
+	If a FIRF\	NΔII wer	e used ho	w likely is it t	that the sv	tem could	nrevent a	n IP Δddress	Spoofing a	ttack again	et the
	targeted		e useu, no	w likely is it	mat the sy.	sterii coulu	preventa	Audiess	spooning a	ttack again	ot the
	Less	ĺ									More
	likely					No Impact					Likely
	Severely	Severely	Strongly	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
	-								Strongry	Coverency	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	No Impact		promotes	promotes	promotes	_
1	Inhibits					No Impact				_	promotes
	Inhibits					No Impact				_	_
	If a FIRE\	Inhibits WALL were	Inhibits e NOT use		Inhibits	•	promotes	promotes	promotes	promotes	promotes
18	If a FIRE\	Inhibits	Inhibits e NOT use	Inhibits	Inhibits	•	promotes	promotes	promotes	promotes	promote:
18	If a FIRE\ the targe Less	Inhibits WALL were	Inhibits e NOT use	Inhibits	Inhibits	ne system c	ould preve	promotes	promotes	promotes	k against More
18	If a FIRE\ the targe Less likely	NALL were	Inhibits e NOT use	d, how likely	Inhibits	•	promotes ould preve	promotes ent an IP Add	promotes ress SPOO	promotes FING attacl	k against More Likely
8	If a FIRE\ the targe Less likely Severely	WALL were ted system	Inhibits e NOT use ? Strongly	d, how likely Moderately	is it that the Slightly	ne system c	ould preve	ent an IP Add	ress SPOO	FING attack	more Likely Severely
8	If a FIRE\ the targe Less likely	NALL were	Inhibits e NOT use	d, how likely	Inhibits	ne system c	ould preve	promotes ent an IP Add	promotes ress SPOO	promotes FING attacl	more Likely Severely
8	If a FIRE\ the targe Less likely Severely	WALL were ted system	Inhibits e NOT use ? Strongly	d, how likely Moderately	is it that the Slightly	ne system c	ould preve	ent an IP Add	ress SPOO	FING attack	more Likely Severely
18	If a FIRE\ the targe Less likely Severely Inhibits	NALL were ted system Severely Inhibits	Inhibits e NOT use ? Strongly Inhibits	d, how likely Moderately Inhibits	is it that the Slightly Inhibits	No Impact	ould preve	ent an IP Add Moderately promotes	ress SPOO Strongly promotes	FING attack	More Likely Severely promotes
18	If a FIRE\ the targe Less likely Severely Inhibits	NALL were ted system Severely Inhibits	Inhibits e NOT use ? Strongly Inhibits	d, how likely Moderately	is it that the Slightly Inhibits	No Impact	ould preve	ent an IP Add Moderately promotes	ress SPOO Strongly promotes	FING attack	More Likely Severely promotes
118	If a FIRE\ the targe Less likely Severely Inhibits	NALL were ted system Severely Inhibits	Inhibits e NOT use ? Strongly Inhibits	d, how likely Moderately Inhibits	is it that the Slightly Inhibits	No Impact	ould preve	ent an IP Add Moderately promotes	ress SPOO Strongly promotes	FING attack	more Likely Severely promotes argeting
18	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less	NALL were ted system Severely Inhibits	Inhibits e NOT use ? Strongly Inhibits	d, how likely Moderately Inhibits	is it that the Slightly Inhibits	No Impact No Impact	ould preve	ent an IP Add Moderately promotes	ress SPOO Strongly promotes	FING attack	more Likely Severely promotes argeting
8	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely	NALL were severely inhibits	Inhibits e NOT use 1? Strongly Inhibits e used, ho	d, how likely Moderately Inhibits w likely is it to	is it that the Slightly Inhibits	No Impact	ould preve	moderately promotes KEY LOGGER	ress SPOO Strongly promotes	FING attack Severely promotes g used in to	More Likely Severely promote: More Likely More Likely
9	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less Less Less Likely Severely	NALL were severely inhibits	Inhibits e NOT use 1? Strongly Inhibits e used, ho	d, how likely Moderately Inhibits w likely is it to	Inhibits is it that the Slightly Inhibits that the systematics are supported by the systematic supported by the systematic supported by the systematics are support	No Impact No Impact No Impact	ould preve	Moderately promotes KEY LOGGER	ress SPOO Strongly promotes R from bein	FING attack Severely promotes g used in to	More Likely Severely promotes More Likely Severely Severely Severely
9	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely	NALL were severely inhibits	Inhibits e NOT use 1? Strongly Inhibits e used, ho	d, how likely Moderately Inhibits w likely is it to	is it that the Slightly Inhibits	No Impact No Impact	ould preve	moderately promotes KEY LOGGER	ress SPOO Strongly promotes	FING attack Severely promotes g used in to	More Likely promotes argeting a
9	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less Less Less Likely Severely	NALL were severely inhibits	Inhibits e NOT use 1? Strongly Inhibits e used, ho	d, how likely Moderately Inhibits w likely is it to	Inhibits is it that the Slightly Inhibits that the systematics are supported by the systematic supported by the systematic supported by the systematics are support	No Impact No Impact No Impact	ould preve	Moderately promotes KEY LOGGER	ress SPOO Strongly promotes R from bein	FING attack Severely promotes g used in to	More Likely Severely promote: More Likely Severely promote: More Likely Severely
119	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely Severely Inhibits	NALL were severely Inhibits NALL were severely Inhibits	Inhibits e NOT use n? Strongly Inhibits e used, ho Strongly Inhibits	Moderately Inhibits w likely is it to Moderately Inhibits	Inhibits is it that the Slightly Inhibits that the system of the Slightly Inhibits Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact	Slightly promotes prevent a Slightly promotes	Moderately promotes KEY LOGGER Moderately promotes	strongly promotes A from bein Strongly promotes	Severely promotes g used in to	More Likely promote: More Likely promote: More Likely promote: More Likely promote:
9	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely Severely Inhibits	NALL were Severely Inhibits NALL were Severely Inhibits	Inhibits e NOT use n? Strongly Inhibits e used, ho Strongly Inhibits	d, how likely Moderately Inhibits w likely is it to	Inhibits is it that the Slightly Inhibits that the system of the Slightly Inhibits Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact	Slightly promotes prevent a Slightly promotes	Moderately promotes KEY LOGGER Moderately promotes	strongly promotes A from bein Strongly promotes	Severely promotes g used in to	More Likely promote More Likely promote More Likely promote More Likely promote
9	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely Severely Inhibits	NALL were severely Inhibits NALL were severely Inhibits	Inhibits e NOT use n? Strongly Inhibits e used, ho Strongly Inhibits	Moderately Inhibits w likely is it to Moderately Inhibits	Inhibits is it that the Slightly Inhibits that the system of the Slightly Inhibits Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact	Slightly promotes prevent a Slightly promotes	Moderately promotes KEY LOGGER Moderately promotes	strongly promotes A from bein Strongly promotes	Severely promotes g used in to	More Likely severely promote More Likely severely promote d in
9	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely Severely Inhibits If a FIRE\ targeting Less	NALL were Severely Inhibits NALL were Severely Inhibits	Inhibits e NOT use n? Strongly Inhibits e used, ho Strongly Inhibits	Moderately Inhibits w likely is it to Moderately Inhibits	Inhibits is it that the Slightly Inhibits that the system of the Slightly Inhibits Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact	ould prevent a Slightly promotes Prevent a Slightly promotes Ould prevent a	Moderately promotes KEY LOGGER Moderately promotes	strongly promotes A from bein Strongly promotes	Severely promotes g used in to	More Likely Severely promote More Likely Severely promote More Likely Severely promote More More
9	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely Severely Inhibits If a FIRE\ targeting Less likely	NALL were Severely Inhibits WALL were Severely Inhibits	Inhibits e NOT use n? Strongly Inhibits e used, ho Strongly Inhibits	Moderately Inhibits W likely is it to Moderately Inhibits Moderately Inhibits Moderately Inhibits	Inhibits is it that the Slightly Inhibits Slightly Inhibits Slightly Inhibits is it that the system of the sys	No Impact No Impact No Impact No Impact No Impact	ould prevent a Slightly promotes Prevent a Slightly promotes ould prevent a	Moderately promotes KEY LOGGER Moderately promotes	Strongly promotes R from bein Strongly promotes GGER from	Severely promotes g used in to Severely promotes being used	More Likely Severely promote: More Likely Severely promote: More Likely Severely promote:
18	If a FIRE\ the targe Less likely Severely Inhibits If a FIRE\ system? Less likely Severely Inhibits If a FIRE\ targeting Less	NALL were Severely Inhibits NALL were Severely Inhibits	Inhibits e NOT use n? Strongly Inhibits e used, ho Strongly Inhibits	Moderately Inhibits w likely is it to Moderately Inhibits	Inhibits is it that the Slightly Inhibits that the system of the Slightly Inhibits Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact	ould prevent a Slightly promotes prevent a Slightly promotes ould prevent a	Moderately promotes KEY LOGGER Moderately promotes	strongly promotes A from bein Strongly promotes	Severely promotes g used in to	more Likely Severely promote: More Likely Severely promote: More Likely Severely promote: More Likely Severely promote:

	WALL WEI	e used, ho	w likely is it	that the sy	stem could	prevent a	SNIFFER from	n being us	ed in targe	ting a
1 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 FIRE	NΔII wer	A NOT USA	d, how likely	is it that th	ne system c	ould preve	ont a SNIFFFI	2 from heir	na used in t	argeting
2 system?	WALL WOL	c HOT usc	u, now incry	is it that t	ic system c	oulu provi	one a Similar	t iioiii beii	ig asca iii i	argeting
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	promote
If a secon	nd FIREWA	LL were u	used, how like	ely is it tha	it the syster	n could pr	event one/an	y of the ab	ove attack	methods
Please e	xplain in s	pace prov	ided.	•				•		
Less							4			More
likely					No Impact		1			Likely
		0	Moderately	Slightly		Slightly	Moderately	Strongly	Severely	Severely
Severely	Severely	Strongly	woderatery	Slightly		Oligitaly	Wiodciatory	Ottorigiy	Ocverery	Severely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Inhibits		No Impact		promotes	promotes	promotes	promote
	,				No Impact				,	
Inhibits	Inhibits	Inhibits	Inhibits		No Impact				,	
Inhibits Explanation	Inhibits	Inhibits			No Impact				,	
Inhibits	Inhibits	Inhibits	Inhibits		No Impact				,	
Inhibits Explanation	Inhibits	Inhibits	Inhibits		No Impact				,	
Inhibits Explanation	Inhibits	Inhibits	Inhibits		No Impact				,	
Inhibits Explanation	Inhibits	Inhibits	Inhibits		No Impact				,	
Inhibits Explanation	Inhibits	Inhibits	Inhibits		No Impact				,	
Explanation provide:	Inhibits on of benefi	Inhibits t a second	Inhibits firewall would	Inhibits		promotes	promotes	promotes	promotes	promote
Explanation provide:	Inhibits on of benefi	Inhibits t a second	Inhibits firewall would	Inhibits		promotes	promotes	promotes	promotes	promote
Explanation provide: If a second methods	Inhibits on of benefi	Inhibits t a second	Inhibits firewall would	Inhibits		promotes	promotes	promotes	promotes	promote
Explanation provide: If a second methods: Less	Inhibits on of benefi	Inhibits t a second	Inhibits firewall would	Inhibits	t that the sy	promotes	promotes	promotes	promotes	promote ack
Explanation provide: If a second methods Less likely	Inhibits on of benefi nd FIREWA? Please	Inhibits t a second LL were i	firewall would	Inhibits / likely is ited.		promotes	promotes d prevent one	promotes	promotes	promote ack More Likely
Explanation provide: If a second methods Less likely Severely	on of benefi	Inhibits t a second LL were in explain is	firewall would not used, how space provid	/ likely is ited.	t that the sy	stem coul	d prevent one	promotes Promotes Promotes Strongly	above att	ack More Likely Severely
Explanation provide: If a second methods Less likely	Inhibits on of benefi nd FIREWA? Please	Inhibits t a second LL were i	firewall would	Inhibits / likely is ited.	t that the sy	stem coul	promotes d prevent one	promotes	promotes	promote ack
Explanation provide: If a second methods Less likely Severely	on of benefi	Inhibits t a second LL were in explain is	firewall would not used, how space provid	/ likely is ited.	t that the sy	stem coul	d prevent one	promotes Promotes Promotes Strongly	above att	promote ack More Likely Severely
Inhibits Explanation provide: If a second methods Less likely Severely Inhibits	Inhibits on of benefit and FIREWA Please of Severely Inhibits	Inhibits It a second ALL were is explain is Strongly Inhibits	firewall would not used, how space provid Moderately Inhibits	/ likely is ited.	t that the sy	stem coul	d prevent one	promotes Promotes Promotes Strongly	above att	ack More Likely Severely
Inhibits Explanation provide: If a second methods Less likely Severely Inhibits Explanation	Inhibits on of benefit and FIREWA Please of Severely Inhibits	Inhibits It a second ALL were is explain is Strongly Inhibits	firewall would not used, how space provid	/ likely is ited.	t that the sy	stem coul	d prevent one	promotes Promotes Promotes Strongly	above att	ack More Likely Severely
Inhibits Explanation provide: If a second methods Less likely Severely Inhibits	Inhibits on of benefit and FIREWA Please of Severely Inhibits	Inhibits It a second ALL were is explain is Strongly Inhibits	firewall would not used, how space provid Moderately Inhibits	/ likely is ited.	t that the sy	stem coul	d prevent one	promotes Promotes Promotes Strongly	above att	ack More Likely Severely

2. IDS/IPS SECTION OF SURVEY

+				LAPOI	СОрин	1111000	dicii iot	I - IDS/IPS	_		
	If an IDS infecting				w likely	is it tha	t the syst	em could pi	event a \	/IRUS fro	m
	Less likely		0		OF Lab	No Impa			0		More Like
	Severely Inhibits	Inhibits	Strongly Inhibits	Moderate ly Inhibits	Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
	If an IDS infecting				ed, how	likely is i	it that the	system co	uld preve	nt a VIRL	JS from
\exists	_	turgete	a system	Ī		No.					Mars Like
\exists	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impa No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	More Like Severely promotes
-											
	lf an IDS infecting				w likely	is it that	t the syst	em could pi	event a \	YORM fr	om
	Less likely					No Impa					More Like
- 1	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits		No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
+					-6	10					
	lf an IDS infecting				ed, how	likely is i	it that the	system co	uld preve	nt a V OF	RM from
	Less likelu					No Impa	ct				More Like
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
							t the targ	eted system	could p	revent be	ing taken
		turned i	nto a ∠L	MBIE by	an attac						
\exists	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderate ly Inhibits	Slightly Inhibits	No Impa No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	More Like Severely promotes
+											
				NOT use				target syst	em could	l prevent	being
_	Less likely	_				No Impa				_	More Like
	Severely Inhibits	Severely Inhibits	Strongly	Moderate lu Inhibits	Slightly	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely	Severely promotes

	from pen	etrating	the targ	eted syste	em?		t the syst	•			
	l a == lik alu					No les s					More Likel
	Less likely Severely	Severely	Strongly	Moderate	Slightly	No Impa No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ly Inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotes
8				e NOT use the targe			it that the	system co	uld preve	nt a TRO	JAN
	Less likely					No Impa	ct				More Like
	Severely	Severely	Strongly	Moderate	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ly Inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotes
	V 100	upo.					_			LOVDO	
9				e used, ho ed systen		is it that	t the syst	em could pr	event a b	SACKDU	UK From
	Less likely					No Impa	ct				More Like
	Severely	Severely	Strongly	Moderate	33	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ly Inhibits	Inhibits	Impact	promote	promotes	promote	promote	promotes
						likely is i	it that the	system co	uld preve	nt a BAC	KDOOR
10	from bei	ng place	d in the t	targeted s	stem?		-	1			
	Less likely				- 6	No Impa					More Like
	Severely	Severely	Strongly	Moderate	Slightly	No	promote	iModerately	promote	promote	Severely
	Inhibits	Inhibits	Inhibits	ly Inhibits	Inhibits	Impact	S	promotes	s	s	promotes
	Inhibits				Inhibits						
11	If an IDS	Inhibits IIPS sys	Inhibits	ly Inhibits	w likely	Impact is it that	s t the syst	promotes em could pr	S	S	promotés
11	If an IDS (DOS) at	Inhibits IIPS sys	Inhibits	ly Inhibits	w likely	is it that	s t the syst ed systen	promotes em could pr	S	S	promotés Service
11	If an IDS (DOS) at Less likely	Inhibits IIPS sys tack fro	Inhibits tem werd m disrup	ly Inhibits e used, ho ting servi	w likely ce on th	is it that	s t the syst ed system	promotes em could pr	s event a [S Denial Of	Service More Like
11	If an IDS (DOS) at	Inhibits IIPS sys	Inhibits	ly Inhibits	w likely ce on th	is it that	s t the syst ed systen	promotes em could pr	S	S	promotés Service
11	If an IDS (DOS) at Less likely Severely	Inhibits IIPS systack fro	Inhibits tem were m disrup	ly Inhibits e used, ho ting servi	ew likely ce on th	is it that the target No Impa	t the system	em could pr	event a [Denial Of Severely	Service More Likel
	If an IDS (DOS) at Less likely Severely Inhibits	Inhibits IIPS systack fro Severely Inhibits	tem werem disrup	ly Inhibits e used, ho ting servi Moderate ly Inhibits	ow likely ce on th Slightly Inhibits	is it that the target No Impact Impact	t the systed system	em could pr	event a [Strongly promote	Severely promote	Service More Like Severely promotes
	If an IDS (DOS) at Less likely Severely Inhibits	Inhibits IIPS systack fro Severely Inhibits	tem werem disrup	ly Inhibits e used, ho ting servi Moderate ly Inhibits	ow likely ce on th Slightly Inhibits	is it that the target No Impact Impact	t the systed system	em could promotes Moderately promotes	event a [Strongly promote	Severely promote	Service More Like Severely promotes
	If an IDS (DOS) at Less likely Severely Inhibits	Inhibits IIPS systack fro Severely Inhibits	tem werem disrup	ly Inhibits e used, ho ting servi Moderate ly Inhibits	ow likely ce on th Slightly Inhibits	is it that the target No Impact Impact	t the systemed systemed systemed Slightly promote	em could promotes Moderately promotes	event a [Strongly promote	Severely promote	Service More Like Severely promotes
	If an IDS (DOS) at Less likely Severely Inhibits If an IDS disruptin Less likely Severely	Inhibits /IPS systack fro Severely Inhibits /IPS systack fro Severely Service	tem were on the	y Inhibits e used, hoting servi Moderate ly Inhibits e NOT use targeted Moderate	slightly linkibits ed, how lisystem?	is it that is it that e target No Impa No Impact	t the system ct Slightly promote	em could pron? Moderately promotes system could promotes	Strongly promote	Severely promote	Service More Like Severely promotes from More Like
	If an IDS (DOS) at Less likely Severely Inhibits If an IDS disruptin Less likely	Inhibits IIPS systack fro Severely Inhibits IIPS sys	tem were strongly Inhibits	ly Inhibits e used, ho ting servi Moderate ly Inhibits e NOT use targeted	ow likely ce on th Slightly Inhibits ed, how l	is it that the target No Impact Impact No Impact No Impact	t the systemed system Slightly promote	em could promotes Moderately promotes system could	Strongly promote	Severely promote	Service More Like Severely promotes from
	If an IDS (DOS) at Less likely Severely Inhibits If an IDS disruptin Less likely Severely	Inhibits /IPS systack fro Severely Inhibits /IPS systack fro Severely Service	tem were on the	y Inhibits e used, hoting servi Moderate ly Inhibits e NOT use targeted Moderate	slightly linkibits ed, how lisystem?	is it that e target No Impa No Impact likely is i	t the system ct Slightly promote	em could pron? Moderately promotes system could promotes	Strongly promote	Severely promote	Service More Like Severely promotes from More Like
12	If an IDS (DOS) at Less likely Severely Inhibits If an IDS disruptin Less likely Severely Inhibits	Inhibits IIPS systack fro Severely Inhibits Severely Inhibits IIPS systack fro	Inhibits tem were m disrup Strongly Inhibits tem were e on the Strongly Inhibits	ly Inhibits e used, ho ting servi Moderate ly Inhibits e NOT use targeted Moderate ly Inhibits	Slightly Inhibits Slightly Inhibits Slightly Inhibits	is it that the target No Impact ikely is i	t the systemed systemed systemed Slightly promote t that the Slightly promote	em could pron? Moderately promotes system could promotes	Strongly promote Strongly promote	Severely promote	Service More Like Severely promotes More Like Severely promotes
12	If an IDS (DOS) at Less likely Severely Inhibits If an IDS disruptin Less likely Severely Inhibits	Inhibits IIPS systack fro Severely Inhibits Severely Inhibits IIPS systack fro	Inhibits tem were m disrup Strongly Inhibits tem were e on the Strongly Inhibits	ly Inhibits e used, ho ting servi Moderate ly Inhibits e NOT use targeted Moderate ly Inhibits	Slightly Inhibits Slightly Inhibits Slightly Inhibits	is it that te target No Impact No Impact No Impact No Impact ikely is it No Impact	t the system ot Slightly promote ot Slightly promote t that the	m could promotes Moderately promotes Moderately promotes	Strongly promote Strongly promote	Severely promote	Service More Like Severely promotes from More Like Severely promotes
12	If an IDS (DOS) at Less likely Severely Inhibits If an IDS disruptin Less likely Severely Inhibits	Inhibits IIPS systack fro Severely Inhibits Severely Inhibits IIPS systack fro	Inhibits tem were m disrup Strongly Inhibits tem were e on the Strongly Inhibits	ly Inhibits e used, ho ting servi Moderate ly Inhibits e NOT use targeted Moderate ly Inhibits	Slightly Inhibits ed, how I Slightly Inhibits system? Slightly Inhibits	is it that the target No Impact ikely is i	t the system ot Slightly promote ot Slightly promote t that the	m could promotes Moderately promotes Moderately promotes	Strongly promote Strongly promote	Severely promote	Service More Likel Severely promotes from More Likel Severely promotes

	BOMB a	ttack ag	ainst the			likely is ?			1	I	1
	Less likely					No Impa	et				More Likel
	Severely	Severely	Strongly	Moderat	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
_											
15	If an IDS SPOOFII						it the sys	tem could p	prevent a	n E-mail	
	Less likely					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderat	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
40							it that th	e system c	ould prev	ent an E	-mail
16	SPOOFI	VG attac	k agains	st the tar	getea sy						
	Less likely	_	_	L		No Impa					More Like
	Severely	Severely		Moderat	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
_											
17	If an IDS Spoofing						t the sys	tem could p	prevent a	n IP Add	ress
		uttuok	ugumst	Line varge			O '	3			B.A 1 3b 1
_	Less likely Severely	Couerolu	Strongly	Moderat	Slightly	No Impa No	Slightly 1	Moderately	Strongly	Severelu	More Like Severelu
	Inhibits		Inhibits	elu	Inhibits	- 1		-			-
_	IIIII II DICO	Inhibits	minores	erg	HIHIDIGS	Impact	promote	promotes	promote	promote	promotes
	minoks	Inhibits	minutes	eig	minoids	Impact	promote	promotes	promote	promote	promotes
18		/IPS sys	tem wer	e NOT us	ed, how	likely is		e system c			
18	If an IDS SPOOFII	/IPS sys	tem wer	e NOT us	ed, how	likely is stem?	it that th				Address
18	If an IDS SPOOFII Less likely	/IPS sys VG attac	tem wer k agains	e NOT us	sed, how geted sy	likely is stem? No Impa	it that th	e system c	ould prev	ent an IF	• Address
18	If an IDS SPOOFII	/IPS sys VG attac	tem wer	e NOT us	ed, how	likely is stem?	it that th				Address
18	If an IDS SPOOFII Less likely Severely	AIPS sys NG attac Severely	tem werek agains	e NOT us st the tary	sed, how geted sy Slightly	likely is stem? No Impa No	it that th	e system co	ould prev	ent an IF	Address More Likel
18	If an IDS SPOOFII Less likely Severely Inhibits	/IPS sys NG attac Severely Inhibits	tem werek agains Strongly Inhibits	e NOT us st the tar Moderat	sed, how geted sy Slightly Inhibits	likely is stem? No Impa No Impact	it that th	e system co	Strongly	Severely promote	More Likel Severely promotes
	If an IDS SPOOFII Less likely Severely Inhibits	/IPS sys NG attac Severely Inhibits	tem werek agains Strongly Inhibits	e NOT us st the tar Moderat ely e used, h	sed, how geted sy Slightly Inhibits	likely is stem? No Impa No Impact	it that th	e system co	Strongly	Severely promote	More Likel Severely promotes
	If an IDS SPOOFII Less likely Severely Inhibits	/IPS sys NG attac Severely Inhibits	tem werek agains Strongly Inhibits	e NOT us st the tar Moderat ely e used, h	sed, how geted sy Slightly Inhibits	likely is stem? No Impa No Impact	it that the	e system co	Strongly	Severely promote	More Like Severely promotes
	If an IDS SPOOFII Less likely Severely Inhibits If an IDS from bein Less likely Severely	IIPS sys NG attack Severely Inhibits IIPS sys ng used	tem wer k agains Strongly Inhibits tem wer in target	e NOT us st the tar Moderat ely e used, h	Slightly Inhibits ow likely tem?	likely is stem? No Impa No Impact	it that the ct Slightly promote at the sys	e system co	Strongly	Severely promote	More Like Severely promotes GGER More Like Severely
	If an IDS SPOOFII Less likely Severely Inhibits If an IDS from bein Less likely	AIPS sys NG attack Severely Inhibits AIPS sys ng used	tem wer k agains Strongly Inhibits tem wer in target	e NOT us st the tar Moderat ely e used, h ing a sys	ed, how geted sy Slightly Inhibits ow likely tem?	likely is stem? No Impa No Impact	it that the ct Slightly promote at the sys	e system components	Strongly promote	Severely promote	More Like Severely promotes GGER
	If an IDS SPOOFII Less likely Severely Inhibits If an IDS from bein Less likely Severely	IIPS sys NG attack Severely Inhibits IIPS sys ng used	tem wer k agains Strongly Inhibits tem wer in target	e NOT us st the tar Moderat ely e used, h ing a sys	Slightly Inhibits ow likely tem?	likely is stem? No Impact Impact is it that	it that the ct Slightly promote at the sys	e system or Moderately promotes tem could p	Strongly promote	Severely Severely	More Like Severely promotes GGER More Like Severely
19	If an IDS SPOOFII Less likely Severely Inhibits If an IDS from bein Less likely Severely Inhibits	IIPS sys WG attack Severely Inhibits IIPS sys Inhibits Severely Inhibits	tem wer k agains Strongly Inhibits tem wer in target Strongly Inhibits	e NOT us t the tar Moderat ely e used, h ing a sys Moderat ely	Slightly Inhibits Slightly Inhibits Slightly Inhibits	likely is stem? No Impact Is it that No Impact No Impact Impact	it that the state of the state	e system or Moderately promotes tem could p	Strongly promote Strongly promote	Severely promote	More Like Severely promotes GGER More Like Severely promotes
19	If an IDS SPOOFII Less likely Severely Inhibits If an IDS from bein Less likely Severely Inhibits	IIPS sys WG attack Severely Inhibits IIPS sys Inhibits Severely Inhibits	tem wer k agains Strongly Inhibits tem wer in target Strongly Inhibits	e NOT us t the tar Moderat ely e used, h ing a sys Moderat ely	Slightly Inhibits Slightly Inhibits Slightly Inhibits	likely is stem? No Impact Is it that No Impact No Impact Iikely is stem?	it that the state of the sys	e system or Moderately promotes tem could p	Strongly promote Strongly promote	Severely promote	More Like Severely promotes GGER More Like Severely promotes
19	If an IDS SPOOFII Less likely Severely Inhibits If an IDS from bein Less likely Severely Inhibits	IIPS sys WG attack Severely Inhibits IIPS sys Inhibits Severely Inhibits	tem wer k agains Strongly Inhibits tem wer in target Strongly Inhibits	e NOT us t the tar Moderat ely e used, h ing a sys Moderat ely	Slightly Inhibits Slightly Inhibits Slightly Inhibits	likely is stem? No Impact Is it that No Impact No Impact Impact	it that the state of the sys	e system or Moderately promotes tem could p	Strongly promote Strongly promote	Severely promote	More Like Severely promotes GGER More Like Severely promotes

	being us	ed in tar	geting a	system?							
	Less likelu					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderat	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
						likely is	it that th	e system co	ould prev	ent a SN	IIFFER
22	from bei	ng used	in target	ing a sys	tem?						
	Less likelu					No Impa	ct				More Likel
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderat ely	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	
_											
22								the system n in space (ent
23	Onerang	or the ai	ove att	ack mem	Ous: A	iso, piea	ise expiai	II III Space	pi Ovided.		
	Less likely					No Impa		A			More Likel
	Severely		Strongly			No	Slightly	Moderately	Strongly	Severely	
_	Inhibits	Inhibits	Inhibits	ely	Inhibits	Impact	promote	promotes	promote	promote	promotes
	Explanation	n:									
24								hat the syst	tem coul	d preven	t one/any
24	of the ab					olain in s	pace pro		tem coul	d preven	
24		ove atta	ick meth		ease exp		pace pro		t em coul	d preven i Severely	More Likel
24	of the ab Less likely	ove atta	ick meth	ods? Pl	ease exp	No Impa	p ace pro ct	vided. Moderately		Severely	More Likel Severely
24	of the ab Less likely Severely	ove atta Severely	strongly	ods? Pl Moderat	ease ezj Slightly	No Impa No	pace pro ct Slightly	vided. Moderately	Strongly	Severely	More Like
24	of the ab Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderat	Slightly Inhibits	No Impa No	pace pro ct Slightly	vided. Moderately	Strongly	Severely	More Like
24	of the ab Less likely Severely	Severely Inhibits	Strongly Inhibits	Moderat	Slightly Inhibits	No Impa No	pace pro ct Slightly	vided. Moderately	Strongly	Severely	More Like

3. HARDENING SECTION OF SURVEY

				Expert C	pinion r	\cotal(JI 1001-	Hardenin	9		
\forall											
1				tions were e targeted			d, how lik	ely is it tha	at the sys	tem coul	d preven
İ	Less likely		touing u	ic targettea	Jystem.	No Impa	et				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly	Moderately promotes	Strongly promotes	Severely promote	Severely
1	IIIIIDKS	minores	minbits	IIIIIDIO	IIIIIDKS	impacc	promotes	promotes	promotes	promote	promote
,				tions were			RDENED	, how likely	y is it tha	t the sys	tem coul
۷	Less likely	TINUS	From Inf	ecting targ	etea sysi	No Impa	et .				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly	Moderately promotes	Strongly promotes	Severely promote	Severely
1	IIIIIDKS	minbres	minbits	ininois	IIIIIDKS	impacc	promotes	promotes	promotes	promote	promote
2				tions were fecting the				likely is it	that the	system c	ould
,	Less likely			recting the	targeteu	No Impa					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact /	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely
1											
						0					
4				tions v ere fecting targ			RDENED	, how likely	y is it tha	t the sys	tem cou
	Less likely					No Impa					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promote
+											
										hatanast	cactom
5				tions were n over and						uigeteu	-
5	could pre	event be	ing take	n over and	turned in	No Impa	MBIÉ by a ct	n attacker	?	_	More Likely
5	could pre	event be				to a ZO	MBIÉ by a ct Slightly		?	Severely	More
5	could pre Less likely Severely	Severely	ing take Strongly	n over and Moderately	turned in Slightly	No Impa No	MBIÉ by a ct Slightly	n attacker Moderately	? Strongly	Severely	More Likely Severely
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	MBIE by a ct Slightly promotes ARDENED	Moderately promotes	Strongly promotes g is it that	Severely promote	More Likely Severely promote
	Less likely Severely Inhibits	Severely Inhibits stem and	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	ot Slightly promotes ARDENED	Moderately promotes	? Strongly promotes y is it that ?	Severely promote	More Likely Severely promote

	prevent a	inova	SIN FIONS	SE from per	letrating	the tary	jeteu syst	em:			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	promote
ļ											
				tions were SE from per					j is it tha	t the syst	tem coul
	Less likely				_	No Impa					More Likely
_	Severelu	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderately	Stronalu	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes	promote	promote
Ť											
				tions were om being pl					that the	system c	ould
Т	- Less likely					No Impa	_				More Likely
	Severely		Strongly	Moderately	Slightly	No	Slightly	Moderately		Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promote
+					HOT		BBENER				
				tions were om being pl					y is it tha	t the syst	
_	Less likely				22	No Impa			O		More Likely
	Severely Inhibits	Inhibits	Strongly	Moderately Inhibits	Slightly 1	No. Impact		Moderately promotes	Strongly	Severely	Severely
	IIIIIDICS	ITITIDICS	IIIIIDIGS	IIIIIIDIGS	ITITIDICS	Impact	promotes	promotes	promotes	promote	promote
Ī											
				tions were							ould
11	prevent a			tions were ce (DOS) a		m disru	pting serv				More
11	prevenť a Less likely	Denial	Of Servi	ce (DOS) a	ttack fro	m disru No Impa	pting serv ct	ice on the	targeted	system?	More Likely
11	prevent a	Denial				m disru	pting serv ct Slightly		targeted		More Likely Severely
11	prevent a Less likely Severely Inhibits	Severely Inhibits	Of Servi Strongly Inhibits	Moderately	Slightly Inhibits	M disru No Impa No Impact	pting serv ct Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	More Likely Severely promote
11	prevent a Less likely Severely Inhibits	Severely Inhibits	Of Servi Strongly Inhibits	ce (DOS) a Moderately	Slightly Inhibits	M disru No Impa No Impact	pting servict Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	More Likely Severely promote
111	prevent a Less likely Severely Inhibits If the sys prevent a Less likely	Severely Inhibits	Of Servi Strongly Inhibits I applica om disru	Moderately Inhibits tions were upting servi	Slightly Inhibits NOT pro	No Impa No Impact Impact Perly H/ e target	ot Slightly promotes ARDENED ed system ot	Moderately promotes , how likely?	Strongly promotes	Severely promote t the syst	More Likely Severely promote tem cou
2	Less likely Severely Inhibits If the sys prevent a Less likely Severely	Severely Inhibits Stem and DOS fr	Of Servi Strongly Inhibits applica om disru	Moderately Inhibits tions were upting servi	Slightly Inhibits NOT proce on the	No Impact Perly HA e target No Impa	ct Slightly promotes ARDENED ed system ct Slightly	Moderately promotes how likely?	Strongly promotes y is it that	Severely promote t the syst	More Likely Severely promote tem coul More Likely Severely
2	prevent a Less likely Severely Inhibits If the sys prevent a Less likely	Severely Inhibits	Of Servi Strongly Inhibits I applica om disru	Moderately Inhibits tions were upting servi	Slightly Inhibits NOT pro	No Impa No Impact Impact Perly H/ e target	ct Slightly promotes ARDENED ed system ct Slightly	Moderately promotes , how likely?	Strongly promotes	Severely promote t the syst	More Likely Severely promote
2	prevent a Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits	Severely Inhibits Severely Inhibits Severely Inhibits	Of Servi Strongly Inhibits applica om disru Strongly Inhibits	Moderately Inhibits tions were upting servi Moderately Inhibits	Slightly Inhibits NOT pro ce on the Slightly Inhibits	No Impact Perly H/ e target No Impact	ct Slightly promotes ARDENED ed system ct Slightly promotes	Moderately promotes , how likely? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promote Severely promote	More Likely Severely promote tem coul More Likely Severely promote
2	prevent a Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits If the sys	Severely Inhibits Severely Inhibits Severely Inhibits	Of Servi Strongly Inhibits applica om disru Strongly Inhibits	Moderately Inhibits tions were upting servi	Slightly Inhibits NOT pro ce on the	No Impact Perly H/ e target No Impact No Impact	ct Slightly promotes ARDENED ed system ot Slightly promotes	Moderately promotes , how likely? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promote Severely promote	More Likely Severely promote tem cou More Likely Severely promote
2	prevent a Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits If the sys	Severely Inhibits Severely Inhibits Severely Inhibits Severely Inhibits	Of Servi Strongly Inhibits applica om disru Strongly Inhibits	Moderately Inhibits tions were upting servi Moderately Inhibits	Slightly Inhibits NOT pro ce on the	No Impact Perly H/ e target No Impact No Impact	ot Slightly promotes ARDENED ed system ot Slightly promotes NED, how system?	Moderately promotes , how likely? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promote t the system Severely promote system c	More Likely Severely promote tem cou More Likely Severely promote
2	prevent a Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits If the sys prevent a	Severely Inhibits Severely Inhibits Severely Inhibits	Of Servi Strongly Inhibits applica om disru Strongly Inhibits	Moderately Inhibits tions were upting servi Moderately Inhibits	Slightly Inhibits NOT pro ce on the	No Impact Perly H/ e target No Impact No Impact No Impact HARDE	ct Slightly promotes ARDENED ed system ct Slightly promotes NED, how system? ct Slightly	Moderately promotes , how likely? Moderately promotes	Strongly promotes g is it that Strongly promotes that the	Severely promote Severely promote	More Likely Severely promote tem cou More Likely Severely promote ould

17	prevent a						- 3				B.4
	Less likely					No Impa	et				More Likely
	Severelu		Strongly	Moderately	Slightly	No	Slightly	Moderately	Stronglu	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes	promote	promote
1		THE TOTAL PROPERTY OF THE PARTY					promotes	promotes	p. c. m. c. c. c.	promote	p. c. iii
+											
				tions were					that the	system c	ould
9	prevent a	an E-Mai	1 52001	FING attack	against	tne targ	getea syst	em?			More
	Less likely					No Impa	et				Likely
\exists	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promote	promote
				_							
				tions were FING attack					y is it tha	t the sys	tem cou
	•										More
	Less likely Severely	Sauarelii	Strongly	Moderatelu	Slightly	No Impa No	Slightly	Moderately	Strongle	Severelu	Likely Severely
- 1	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes	promote	promote
4	HILIDICS	HIMDICS	IIIIIDIGS	IIIIIDIGS	ITITIDICS	impacc	promotes	promotes	promotes	promote	promote
- 1											
					7 -						
					20	<u> </u>	3 -	2			
				tions were					that the	system c	ould
				tions were					that the	system c	ould More
17	prevent a Less likely	an IP Ad	dress Sp	ooofing atta	ack agair	No Impa	argeted s ct	jstem?		_	More Likely
17	prevent a Less likely Severely	an IP Ad Severely	dress Sp Strongly	ooofing atta Moderately	slightly	No Impa No	argeted sy ct Slightly	stem? Moderately	Strongly	Severely	More Likely Severely
17	prevent a Less likely	an IP Ad	dress Sp	ooofing atta	ack agair	No Impa	argeted sy ct Slightly	jstem?		Severely	More
17	prevent a Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	argeted s ct Slightly promotes	stem? Moderately promotes	Strongly promotes	Severely promote	More Likely Severely promote
17	prevent a Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	ooofing atta Moderately	Slightly Inhibits	No Impa No Impact	ct Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	More Likely Severely promote
17	prevent a Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	ot Slightly promotes ARDENED	Moderately promotes	Strongly promotes	Severely promote	More Likely Severely promote
8	prevent a Less likely Severely Inhibits If the sys	Severely Inhibits Stem and	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact Perly H/ ainst the	ot Slightly promotes ARDENED	Moderately promotes	Strongly promotes g is it that	Severely promote	More Likely Severely promote tem cou
8	prevent a Less likely Severely Inhibits If the sys prevent a Less likely	Severely Inhibits Stem and	Strongly Inhibits applica dress SI	Moderately Inhibits tions were	Slightly Inhibits NOT pro	No Impa No Impact Perly H/ ainst the	ct Slightly promotes ARDENED e targeted ct Slightly	Moderately promotes , how likel system?	Strongly promotes g is it that	Severely promote t the syst	More Likely Severely promote
8	Less likely Severely Inhibits If the sys prevent a Less likely Severely	Severely Inhibits Stem and an IP Ad	Strongly Inhibits applica dress Si	Moderately Inhibits tions were POOFING a	Slightly Inhibits NOT pro ttack ag	No Impact Perly H/ ainst the	ct Slightly promotes ARDENED e targeted ct Slightly	Moderately promotes how likel system?	Strongly promotes g is it that Strongly	Severely promote t the syst	More Likely Severely promote tem cou More Likely Severely
8	prevent a Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits	Severely Inhibits Seem and P Ad Severely Inhibits	Strongly Inhibits applica dress Si Strongly Inhibits	Moderately Inhibits tions were POOFING a Moderately Inhibits	Slightly Inhibits NOT pro ttack ag Slightly Inhibits	No Impact Perly H/A ainst the No Impact No Impact	ct Slightly promotes ARDENED e targeted ct Slightly promotes	Moderately promotes how likely system? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promote t the syst Severely promote	More Likely Severely promote tem cou More Likely Severely promote
8	Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits	Severely Inhibits stem and Severely Inhibits	Strongly Inhibits Applica Aprica Strongly Inhibits Strongly Inhibits	Moderately Inhibits tions were POOFING a	Slightly Inhibits NOT pro ttack ag Slightly Inhibits	No Impact Perly H/ ainst the No Impact No Impact HARDE	ct Slightly promotes ARDENED e targeted ct Slightly promotes	Moderately promotes how likel system? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promote t the syst Severely promote	More Likely Severely promote tem cou More Likely Severely promote
18	Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits If the sys prevent a	Severely Inhibits stem and Severely Inhibits	Strongly Inhibits Applica Aprica Strongly Inhibits Strongly Inhibits	Moderately Inhibits tions were POOFING a Moderately Inhibits	Slightly Inhibits NOT pro ttack ag Slightly Inhibits	No Impact Perly H/A ainst the No Impact No Impact HARDE argeting	ct Slightly promotes ARDENED e targeted ct Slightly promotes ARDENED e targeted ct Slightly promotes ARDENED A	Moderately promotes how likel system? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promote t the syst Severely promote	More Likely Severely promote More Likely Severely promote ould
8	Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits If the sys prevent a Less likely	Severely Inhibits Severely Inhibits Severely Inhibits Severely Inhibits	Strongly Inhibits Strongly Inhibits Strongly Inhibits applica GGER 6	Moderately Inhibits tions were POOFING a Moderately Inhibits tions were rom being	Slightly Inhibits NOT pro ttack ag Slightly Inhibits	No Impact Perly H/ ainst the No Impact No Impact HARDE	ct Slightly promotes ARDENED e targeted ct Slightly promotes NED, how a system ct	Moderately promotes how likel system? Moderately promotes likely is it?	Strongly promotes g is it that Strongly promotes that the	Severely promote t the system c	More Likely Promote More Likely Severely Promote More Likely Sould More Likely
8	Less likely Severely Inhibits If the sys prevent a Less likely Severely Inhibits If the sys prevent a	Severely Inhibits Severely Inhibits Severely Inhibits Severely Inhibits	Strongly Inhibits Applica Aprica Strongly Inhibits Strongly Inhibits	Moderately Inhibits tions were POOFING a Moderately Inhibits	Slightly Inhibits NOT pro ttack ag Slightly Inhibits	No Impact Perly H/A ainst the No Impact No Impact HARDE argeting	ct Slightly promotes ARDENED e targeted ct Slightly promotes NED, how a system ct Slightly	Moderately promotes how likel system? Moderately promotes	Strongly promotes g is it that Strongly promotes that the	Severely promote t the system contents Severely promote	More Likely Severely promote More Likely Severely promote Ould

	Less likely			_		No Impa	ct				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
21				tions were being used				likely is it	that the	system c	
	Less likely			H	72	No Impa	<u>ک</u> چ	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				tions were being used				, how likel	y is it tha	t the sys	tem coul
	Less likely					No Impa					More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Stronglu	Severelu	Severely

4. TRAINING SECTION OF SURVEY

				Expert 0	pinion	Resear	ch Tool -	TRAINING			
	complimen	t other prac Protecting	ctices in a	system of def	ense in de	pth or laye	red defens	l available reso e. Essential pr ot opening or c	actices to v	vhich this q	uestion
-											
1				trained in r S infection		o essen	tial practi	ices, how lil	kely is it t	hat the s	gstem
Ė					-	No.					Mara Lika
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	More Like Severely promotes
2				properly tra of VIRUS in			to essen	tial practice	s, how lik	ely is it t	hat the
	Less likely					No Impa	ct				More Like
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
3				trained in r infect <u>ing</u>				ices, how lil	kely is it t	hat the s	ystem
	Less likely				2	No Impa	<u> </u>	1			More Like
_	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
4				properly tr DRM from i				tial practice ?	s, how lik	ely is it t	hat the
	Less likely					No Impa	ct				More Like
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
5								ices, how lil BIE by an at		hat the t	argeted
	Less likely					No Impa	ct				More Likel
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
	If sh =		Not					u			
6								tial practice od turned in			nat the
	Less likely Severely	Severelu	Strongly	Moderately	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	More Like Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes		promote	promotes

	coura pre	T	IOOAITI	HORSE from	n peneti	ating th	e targete	u system:			
	Less likely					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
8								l tial practice targeted sy		ely is it t	hat the
	Less likelu					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
_	If end-use	ers were i	oroperla	trained in r	egards t	o essen	tial practi	ices, how lil	celu is it t	hat the s	•stem
9				OR from be							1
	Less likely					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	promote	Moderately	Strongly	promote	Severely
_	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	s	promotes	promotes	s	promotes
_											
10								tial practice argeted sys		ely is it t	hat the
					11 4			1 1			
	Lacelikalıı					No Impo	et .				More Likeli
_	Less likely Severely	Severely	Strongly	Moderately	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	More Likel Severely
		Severely	Strongly	Moderately	Slightly			Moderately	Strongly	Severely	
11	Severely If end-use	ers were	properly	trained in r	egards t	No o essen	Slightly	ices, how lil	kely is it t	hat the s	Severely gstem
11	Severely If end-use could pre	ers were	properly	trained in r	egards t	o essen	Slightly tial practi disrupting		kely is it t	hat the s	Severely ystem em?
11	If end-use could pre	ers were p	properly enial Of	trained in r Service (D(egards t DS) atta	o essen	Slightly tial practi disrupting	ices, how lil g service or	tely is it to	hat the s eted syst	Severely ystem em? More Likel
11	Severely If end-use could pre	ers were	properly enial Of	trained in r	egards t DS) atta	o essen	Slightly tial practi disrupting	ices, how lil	kely is it t	hat the seted syst	Severely ystem em?
11	If end-use could pre Less likely Severely	ers were pent a Do	properly enial Of	trained in r Service (D(egards t OS) atta Slightly	o essen ck from No Impa	Slightly tial practi disrupting ct Slightly	ices, how lil g service or Moderately	tely is it to the targe	hat the seted syst	ystem em? More Likel Severely
	If end-use could pre Less likely Severely Inhibits	Severely Inhibits	properly enial Of : Strongly Inhibits	trained in r Service (DI Moderately Inhibits	egards (DS) atta Slightly Inhibits	No essen ck from No Impa No Impact	Slightly tial practi disrupting ct Slightly promote	ices, how lil g service or Moderately promotes	Strongly promotes	hat the seted sest	ystem em? More Likel Severely promotes
	If end-use could pre Less likely Severely Inhibits If the end system co	Severely Inhibits	properly enial Of : Strongly Inhibits	trained in r Service (DI Moderately Inhibits	egards (DS) atta Slightly Inhibits	O essen ck from No Impact Impact	Slightly tial practi disrupting ct Slightly promote to essen on the tar	ices, how lil g service or Moderately promotes	Strongly promotes	hat the seted sest	ystem em? More Likel Severely promotes
	If end-use could pre Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	trained in r Service (DI Moderately Inhibits properly tr OS from dis	egards t DS) atta Slightly Inhibits ained in crupting	O essenek from No Impact Impact regards service	Slightly tial pract disrupting ct Slightly promote to essenion the tar	Moderately promotes tial practice geted syste	Strongly promotes s, how like	hat the seted sest Severely promote	ystem em? More Likel Severely promotes hat the
	If end-use could pre Less likely Severely Inhibits If the end system co	Severely Inhibits	Strongly Inhibits	trained in r Service (DI Moderately Inhibits	egards (DS) atta Slightly Inhibits	O essen ck from No Impact Impact	Slightly tial practi disrupting ct Slightly promote to essen on the tar	ices, how lil g service or Moderately promotes	Strongly promotes	Severely promote	ystem em? More Likel Severely promotes
	If end-use could pre Less likely Severely Inhibits If the end system could system could system could pre	Severely Inhibits -users would prev	Strongly Inhibits	trained in r Service (Di Moderately Inhibits properly tr OS from dis	egards I DS) atta Slightly Inhibits ained in rupting	No essenick from No Impact Impact No Impact No Impact No Impa	slightly tial practidisrupting ct Slightly promote to essenion the tar ct Slightly	Moderately promotes tial practice geted syste	Strongly promotes s, how like	Severely promote	ystem em? More Likel Severely promotes hat the More Likel Severely
12	If end-use could pre Less likely Severely Inhibits If the end system co Less likely Severely Inhibits	Severely Inhibits Severely Inhibits Severely Inhibits	Strongly Inhibits ere NOT ent a DO Strongly Inhibits	trained in r Service (DI Moderately Inhibits properly tr OS from dis Moderately Inhibits	egards to Sightly Inhibits ained in crupting Slightly Inhibits	No essence from No Impact regards service No Impact No Impact	slightly tial practidisrupting ct Slightly promote to essent on the tar ct Slightly promote tial practi	Moderately promotes tial practice geted syste Moderately promotes	Strongly promotes s, how likem?	Severely promote	ystem em? More Likel Severely promotes hat the More Likel Severely promotes
12	If end-use could pre Less likely Severely Inhibits If the end system co Less likely Severely Inhibits	Severely Inhibits Severely Inhibits Severely Inhibits	Strongly Inhibits ere NOT ent a DO Strongly Inhibits	trained in r Service (DI Moderately Inhibits properly tr OS from dis Moderately Inhibits	egards to Sightly Inhibits ained in crupting Slightly Inhibits	No essence from No Impact regards service No Impact No Impact	slightly tial practi disrupting ct Slightly promote to essent on the tar ct Slightly promote tial practi eted syst	Moderately promotes tial practice geted syste Moderately promotes	Strongly promotes s, how likem?	Severely promote	stem em? More Likel Severely promotes hat the More Likel Severely promotes
12	If end-use could pre Less likely Severely Inhibits If the end system co Less likely Severely Inhibits If end-use could pre	Severely Inhibits Severely Inhibits Severely Inhibits	Strongly Inhibits Strongly Inhibits Strongly Inhibits Office of the property office BO	trained in r Service (DI Moderately Inhibits properly tr OS from dis Moderately Inhibits	egards to Sightly Inhibits ained in crupting Slightly Inhibits	o essenck from No Impact Impact No Impact No Impact No Impact No Impact No Impact	slightly tial practi disrupting ct Slightly promote to essent on the tar ct Slightly promote tial practi eted syst	Moderately promotes tial practice geted syste Moderately promotes	Strongly promotes s, how likem?	Severely promote	ystem em? More Likel Severely promotes hat the More Likel Severely promotes

•	system co	Julu pies									
	Less likely					No Impa	et				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
15	If end-users were properly could prevent an E-mail SF								cely is it t	hat the s	ystem
	Less likely					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	promotes
	If the end	-IISAIS W	ere NOT	nroneris tr	ained in	renards	to essent	tial practice	s how lik	els is it t	hat the
16								targeted sy		eig is it t	iiat the
	Less likely					No Impa	ict				More Likely
	Severely	Severely		Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promotes	promote	promotes
	lf end-use	ors were i	nroneris	trained in r	enards I	n essen	tial practi	ices how lik	els is it t	hat the s	estem
17	could pre					against	the targe	ices, how lil ted system		hat the s	-
17	could pre Less likely	vent an l	P Addre	ss Spoofin	g attack	against No Impa	the targe	ted system	?		More Likely
17	could pred Less likely Severely	vent an l Severely	P Addre	ss Spoofin Moderately	g attack Slightly	Against No Impa No	the targe ot Slightly	ted system: Moderately	Strongly	Severely	More Likely Severely
17	could pre Less likely	vent an l	P Addre	ss Spoofin	g attack	against No Impa	the targe	ted system	?	Severely	More Likely
	could pre Less likely Severely Inhibits	Severely Inhibits	P Address Strongly Inhibits	Moderately Inhibits	g attack Slightly Inhibits ained in	No Impact	ct Slightly promote	ted system: Moderately	Strongly promotes	Severely promote elg is it t	More Likely Severely promotes
	could pre Less likely Severely Inhibits	Severely Inhibits	P Address Strongly Inhibits	Moderately Inhibits	g attack Slightly Inhibits ained in	No Impact	ct Slightly promote to essented against	Moderately promotes	Strongly promotes	Severely promote elg is it t	More Likely Severely promotes hat the
	could pre Less likely Severely Inhibits If the end system co Less likely Severely	Severely Inhibits	Strongly Inhibits ere NOT ent an If	Moderately Inhibits	g attack Slightly Inhibits ained in	No Impact Impact regards NG attack	ct Slightly promote to essented against	Moderately promotes	Strongly promotes	Severely promote elg is it t	More Likely Severely promotes hat the
	could pre Less likely Severely Inhibits If the end system co	Severely Inhibits -users we	Strongly Inhibits ere NOT ent an If	Moderately Inhibits properly tr	Slightly Inhibits ained in	No Impact regards No Impact	ct Slightly promote to essenick against	Moderately promotes	Strongly promotes s, how liked system	Severely promote elg is it t?	More Likely Severely promotes hat the
18	could pre Less likely Severely Inhibits If the end- system co Less likely Severely Inhibits If end-use	Severely Inhibits -users would prev Severely Inhibits	Strongly Inhibits ere NOT ent an If Strongly Inhibits	Moderately Inhibits properly tr Address: Moderately Inhibits	Slightly Inhibits ained in SPOOFI Slightly Inhibits	No Impact regards NG attac No Impact	the targe ct Slightly promote to essent ck against ct Slightly promote tial practi	Moderately promotes the targete Moderately promotes	Strongly promotes s, how liked system Strongly promotes	Severely promote elg is it t ? Severely promote	More Likely Severely promotes hat the More Likely Severely promotes
18	Less likely Severely Inhibits If the end system co Less likely Severely Inhibits If end-use could pre-	Severely Inhibits -users would prev Severely Inhibits	Strongly Inhibits ere NOT ent an If Strongly Inhibits	Moderately Inhibits properly trop Address: Moderately Inhibits	Slightly Inhibits ained in SPOOFI Slightly Inhibits	No Impact regards NG attack No Impact No Impact or essent d in targ	the targe ct Slightly promote to esseni ck against ct Slightly promote tial practi eting a sy	Moderately promotes the targete Moderately promotes	Strongly promotes s, how liked system Strongly promotes	Severely promote elg is it t ? Severely promote	More Likely promotes hat the More Likely severely promotes
18	could pre Less likely Severely Inhibits If the end- system co Less likely Severely Inhibits If end-use	Severely Inhibits -users would prev Severely Inhibits	Strongly Inhibits ere NOT ent an If Strongly Inhibits	Moderately Inhibits properly tr Address: Moderately Inhibits	Slightly Inhibits ained in SPOOFI Slightly Inhibits	No Impact regards NG attac No Impact	the targe ct Slightly promote to esseni ck against ct Slightly promote tial practi eting a sy	Moderately promotes the targete Moderately promotes	Strongly promotes s, how liked system Strongly promotes	Severely promote elg is it t ? Severely promote	More Likely promotes hat the More Likely Severely promotes

20								tial practice ting a syste		ely is it t	hat the
	Less likely					No Impa	ct				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				trained in r from being				ices, how lil	elg is it t	hat the s	gstem
٢١	Less likely	vent a Si		Tom being	22	No Impa		1			More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
22				properly tr IIFFER fro				tial practice a system?	s, how lik	ely is it t	hat the
	Less likely					No Impa	ct				More Likely
	Severely	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely

5. ANTI-VIRUS SECTION OF SURVEY

	If undabar	A ABITI V	IDUC	·		ass likalı	in it that				ZIDLIC
1	from infe				e usea, n	iow likel	j is it tha	t the systen	n coula p	revent a	rinus
	Less likely					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotés	promotes
•						sed, how	likely is i	it that the s	ystem co	ould preve	nt a
-	TINUS IIC	m inreci	ing targ	eted syster	ne						
	Less likely		_			No Impa					More Likel
	Severely	Severely			Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
3	If updated from infe				e used, h	ow likely	is it tha	t the system	n could p	revent a \	VORM
	Less likely					No Impa	ot.				More Likel
	Severely	Severelii	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severelu	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote		promotes
_					20		2	1			
		1 ANTI-Y	IRUS so			sed, how	likely is i	it that the s	ystem co	ould preve	nt a
4	VORM fr		ting targ	jeted syste	m?						
4			ting targ	jeted syste	m?	No Impa	et				More Likel
4	Less likely Severely			j eted syste Moderately		No Impa No	et Slightly	Moderately	Strongly	Severely	More Likel Severely
4	Less likely	om infec		_	Slightly Inhibits			Moderately promotes	Strongly promote		
4	Less likely Severely	om infec Severely	Strongly	Moderately	Slightly	No	Slightly				
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote		promote	promotés	Severely promotes
	Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	promotes	promote	promotés	Severely promotes
	Less likely Severely Inhibits If updated being tak	Severely Inhibits	Strongly Inhibits IRUS so and turn	Moderately Inhibits ftware were d into a 20	Slightly Inhibits e used, h	No Impact ow likely g an atta	Slightly promote g is it that acker?	promotes t the target	promote ed system	promotés n could pr	Severely promotes revent
	Less likely Severely Inhibits If updated being tak Less likely Severely	Severely Inhibits J ANTI-V en over a	Strongly Inhibits IRUS so and turn	Moderately Inhibits ftware were d into a Zi Moderately	Slightly Inhibits used, h	No Impact ow likely g an atta No Impa	Slightly promote y is it that acker? ct	t the target	promote ed system Strongly	n could pr	Severely promotes revent More Likel Severely
	Less likely Severely Inhibits If updated being tak	Severely Inhibits	Strongly Inhibits IRUS so and turn	Moderately Inhibits ftware were d into a 20	Slightly Inhibits e used, h	No Impact ow likely g an atta	Slightly promote g is it that acker?	promotes t the target	promote ed system	n could pr	Severely promotes revent
	Less likely Severely Inhibits If updated being tak Less likely Severely Inhibits	Severely Inhibits ANTI-Ven over a Severely Inhibits	Strongly Inhibits IRUS so and turn Strongly Inhibits	Moderately Inhibits ftware were ed into a Zon Moderately Inhibits	Slightly Inhibits e used, h DMBIE b Slightly Inhibits	No Impact Ow likely an atta No Impact	Slightly promote j is it that acker? ct Slightly promote	t the targeto	ed system Strongly promote	n could promotes Severely promotes	Severely promotes revent More Like Severely promotes
5	Less likely Severely Inhibits If updated being tak Less likely Severely Inhibits If updated	Severely Inhibits ANTI-Ven over a Severely Inhibits	Strongly Inhibits IRUS so and turn Strongly Inhibits	Moderately Inhibits ftware were ed into a Zon Moderately Inhibits	Slightly Inhibits • used, h DMBIE b Slightly Inhibits	No Impact ow likely g an atta No Impa No Impa sed, how	Slightly promote j is it that acker? ct Slightly promote likely is it	t the target	ed system Strongly promote	n could promotes Severely promotes	Severely promotes revent More Likel Severely promotes
5	Less likely Severely Inhibits If updated being tak. Less likely Severely Inhibits If updated being tak.	Severely Inhibits ANTI-Ven over a Severely Inhibits	Strongly Inhibits IRUS so and turn Strongly Inhibits	Moderately Inhibits Inhibits Inhibits Moderately Inhibits Inhibits	Slightly Inhibits • used, h DMBIE b Slightly Inhibits	No Impact ow likely an atta No Impact Impact sed, how to a ZOI	Slightly promote y is it that acker? ct Slightly promote promote likely is i	t the targeto	ed system Strongly promote	n could promotes Severely promotes	Severely promotes revent More Likel Severely promotes
5	Less likely Severely Inhibits If updated being tak Less likely Severely Inhibits If updated	Severely Inhibits ANTI-Ven over a Severely Inhibits	Strongly Inhibits IRUS so and turned Strongly Inhibits IRUS so by an att	Moderately Inhibits Inhibits Inhibits Moderately Inhibits Inhibits	Slightly Inhibits e used, h DMBIE b Slightly Inhibits e NOT use	No Impact ow likely g an atta No Impa No Impa sed, how	Slightly promote g is it that acker? ct Slightly promote promote likely is in MBIE?	t the targeto	ed system Strongly promote	n could promotes Severely promotes	Severely promotes revent More Likel Severely promotes
5	Less likely Severely Inhibits If updated being take Less likely Severely Inhibits If updated being take Less likely	Severely Inhibits Severely Inhibits Severely Inhibits ANTI-Ven over I	Strongly Inhibits IRUS so and turned Strongly Inhibits IRUS so by an att	Moderately Inhibits Inhibits Moderately Inhibits Inhibits Inhibits	Slightly Inhibits • used, h DMBIE b Slightly Inhibits	No Impact No Impact No Impact No Impact No Impact No Impact No a ZOI	Slightly promote y is it that acker? ct Slightly promote promote likely is i	Moderately promotes	ed system Strongly promote	Severely promotes tem could	Severely promotes revent More Likel Severely promotes I prevent More Likel

	HURSE H	om pene	etrating	the targeted	ı system	17						
	Less likely					No Impa	ct				More Likel	
	Severely	Severely		Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely	
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes	
_												
8				 ftware were netrating th				it that the s	ystem co	ould preve	nt a	
	Less likely					No Impa	ct				More Likel	
	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 were	used, h	ow likely	is it that	t the systen	n could p	revent a		
9	BACKDO	OR from	being p	laced in the	targete	d systen	n?	_				
	Less likely	Course!	Oh '	B.d. de	Official	No Impa		B.A. dot-2	Ohan I	Consecto	More Likel	
	Severely Inhibits	Severely Inhibits	Inhibits	Moderately Inhibits	Slightly	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes	
	IIIIIDIGS	IIIIIDKS	IIIIIDKS	illinoits	IIIIIDKS	impacc	promote	promotes	promote	promotes	promotes	
-												
10	If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?											
	Less likely			Г		Nolmpa	ot				More Likel	
	Severely	Severely	Strongly	Moderately	Slightly	No	promote	Moderately	promote	Severely	Severely	
_	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	3	promotes	s	promotes	promotes	
_												
				ftware were n disrupting				t the systen system?	n could p	revent a l	Denial Of	
11		300, a.c.										
11	Less likelu	, , ,				No Impa	ct				More Likel	
11	Less likely Severely	Severely	Strongly	Moderately	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	More Likel Severely	
11			Strongly Inhibits	Moderately Inhibits	Slightly Inhibits			Moderately promotes	Strongly promote	Severely promotes	Severely	
11	Severely	Severely				No	Slightly					
	Severely Inhibits	Severely Inhibits	Inhibits	Inhibits	Inhibits	No Impact	Slightly promote		promote	promotes	Severely promotes	
	Severely Inhibits If updated from disre	Severely Inhibits	Inhibits	Inhibits	Inhibits	No Impact sed, how m?	Slightly promote likely is i	promotes	promote	promotes	promotes nt a DOS	
	Severely Inhibits If updated from disre	Severely Inhibits ANTI-V	IRUS so	Inhibits Iftware weren the target	NOT us	No Impact sed, how m?	Slightly promote likely is i	promotes t that the s	promote ystem co	promotes	promotes nt a DOS More Likel	
	Severely Inhibits If updated from disre	Severely Inhibits	IRUS so	Inhibits	Inhibits	No Impact sed, how m?	Slightly promote likely is i	promotes	promote	ould preve	Severely promotes	
	Severely Inhibits If updated from disre Less likely Severely	Severely Inhibits I ANTI-V upting se	IRUS so	Inhibits Iftware weren the target Moderately	NOT us	No Impact sed, how m? No Impa	Slightly promote likely is i	t that the s	ystem co	ould preve	severely promotes nt a DOS More Likel Severely	
	Severely Inhibits If updated from distriction Less likely Severely Inhibits	Severely Inhibits I ANTI-V upting se Severely Inhibits	IRUS so ervice or Strongly Inhibits	oftware were the target Moderately Inhibits	NOT us ed syste Slightly Inhibits	No Impact sed, how m? No Impa No Impact	Slightly promote likely is i ct Slightly promote	t that the s	gstem co Strongly promote	promotes puld preve Severely promotes	nt a DOS More Like Severely promotes	
12	Severely Inhibits If updated from disrection disrections in the severely Inhibits If updated in the severely Inhibits i	Severely Inhibits I ANTI-V upting se Severely Inhibits	IRUS so Strongly Inhibits	oftware were the target Moderately Inhibits	NOT us ed syste Slightly Inhibits	No Impact sed, how m? No Impa No Impact	Slightly promote likely is i ct Slightly promote	t that the s Moderately promotes	gstem co Strongly promote	promotes puld preve Severely promotes	nt a DOS More Like Severely promotes	
12	Severely Inhibits If updated from disrection disrections in the severely Inhibits If updated in the severely Inhibits i	Severely Inhibits I ANTI-V upting se Severely Inhibits	IRUS so Strongly Inhibits	Inhibits If ware were the target Moderately Inhibits	NOT us ed syste Slightly Inhibits	No Impact sed, how m? No Impa No Impact	Slightly promote likely is i ct Slightly promote	t that the s Moderately promotes	gstem co Strongly promote	promotes puld preve Severely promotes	nt a DOS More Likel Severely promotes	
12	Severely Inhibits If updated from disrection disrection inhibits Less likely Severely Inhibits If updated BOMB at	Severely Inhibits I ANTI-V upting se Severely Inhibits	IRUS so Strongly Inhibits IRUS so inst the	Inhibits If ware were the target Moderately Inhibits If ware were targeted sy	NOT us ed syste Slightly Inhibits	No Impact sed, how m? No Impact Impact ow likely	Slightly promote likely is i ct Slightly promote	t that the s Moderately promotes	gstem co Strongly promote	promotes puld preve Severely promotes	nt a DOS More Likel Severely promotes	

	If undated	ANTLY	IRIIS co	ftware were	NOT	ed how	likale ici	it that the s	estem co	uld preus	nt a
14				nst the targ			iikeig is i	it that the S	gstein Gu	oulu preve	TIL A
	Less likely					No Impa	a.t				More Likel
	Severelu	Sauaralu	Stronalu	Moderatelu	Slightly	No	Sliahtlu	Moderatelu	Stronalu	Severelu	Severelu
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote		promotes
\Box							promote to	promote a	p. c.iii c.ii	-	promotes.
							j is it tha	t the systen	n could p	revent an	E-mail
15	SPOOFIN	lG attack	(agains)	the target	ed syster	m?					
	Less likely					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
	IC undated	ABITI U	IDHC 50	(ture use	NOT us	ad hau	likala ici	it that the s	actom or	uld praua	nt an E
16				ainst the ta			likely is	it that the s	gstein co	ulu preve	III AII E-
	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
						100					
_						U					
	If undated		IDHS co	ftware were	used, h	o e likeli	is it tha	t the system	n could p	revent an	IP
17					targeted				-		
17				against the	targeted						
17					targeted		í?		-		More Likely
17	Address : Less likely Severely	Spoofing Severely	Strongly	against the Moderately	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	Severely
17	Address :	Spoofing	attack	against the	_	No Impa	í? ct	Moderately promotes	Strongly	Severely	
17	Address : Less likely Severely Inhibits	Spoofing Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	ct Slightly promote	promotes	promote	Severely promotes	Severely promotes
	Address : Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impa No Impact	ct Slightly promote		promote	Severely promotes	promotés
	Address S Less likely Severely Inhibits If updated Address S	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact Impact ed, howed system	ct Slightly promote likely is i	promotes	promote	Severely promotes	Severely promotes nt an IP
	Address Severely Inhibits If updated Address Sees likely	Severely Inhibits ANTI-V	Strongly Inhibits IRUS so	Moderately Inhibits Inhibits	Slightly Inhibits • NOT us he target	No Impact ed, howed system No Impact	ct Slightly promote likely is i	promotes	gstem co	Severely promotes	promotes nt an IP More Likel
	Address S Less likely Severely Inhibits If updated Address S	Severely Inhibits ANTI-V	Strongly Inhibits	Moderately Inhibits Inhibits	Slightly Inhibits	No Impact Impact ed, howed system	ct Slightly promote likely is i	promotes	promote	Severely promotes	promotes nt an IP
	Address Severely Inhibits If updated Address Severely Severely Severely Severely	Severely Inhibits ANTI-V SPOOFIF	Strongly Inhibits IRUS so VG attac	Moderately Inhibits ftware werk k against t	Slightly Inhibits NOT us he target	No Impact ed, howed system No Impact	ct Slightly promote likely is iem? ct Slightly	promotes it that the s	ystem co	Severely promotes	Severely promotes nt an IP More Likely Severely
18	Address Severely Inhibits If updated Address Severely Inhibits Less likely Severely Inhibits If updated Inhibits	Severely Inhibits Severely Inhibits Severely Inhibits	Strongly Inhibits IRUS so Strongly Inhibits IRUS so	Moderately Inhibits ftware were k against t Moderately Inhibits	Slightly Inhibits NOT us he target Slightly Inhibits	No Impa No Impact ed. how ed syste No Impa No Impact	ct Slightly promote likely is i em? ct Slightly promote	promotes it that the s	gstem co Strongly promote	Severely promotes uld preve	nt an IP More Likely Severely promotes
18	Address Severely Inhibits If updated Address Severely Inhibits Less likely Severely Inhibits If updated Inhibits	Severely Inhibits Severely Inhibits Severely Inhibits	Strongly Inhibits IRUS so Strongly Inhibits IRUS so ing used	Moderately Inhibits ftware were k against t Moderately Inhibits ftware were in targeting	Slightly Inhibits NOT us he target Slightly Inhibits	No Impa No Impact ed. how ed syste No Impa No Impact	ct Slightly promote likely is iem? ct Slightly promote	it that the s	gstem co Strongly promote	Severely promotes uld preve	nt an IP More Likely Severely promotes

20				ftware were in targetin			likely is i	it that the s	ystem co	ould preve	nt a KEY
	Less likely					No Impa	ct				More Likely
	Severely		Strongly			No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promote	promotes	promote	promotes	promotes
21				ftware were		ow likel	j is it tha	t the system	n could p	revent a S	SNIFFER
	Less likely			-	72	No Impa	ct Z	1			More Likelu
	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 NOT us	sed. how	likelu is i	it that the s	stem co	ould preve	nt a
				in targetin							
22	SNIFFER	rioiii be	_								
22	SNIFFER Less likely	rioiii be	_			No Impa	ct				More Likely
22		Severely	Strongly	Moderately	Slightly	No Impa No	ct Slightly	Moderately	Strongly	Severely	Mor Sev

6. ANTI-SPAM SECTION OF SURVEY

			Expe	rt Opinion	Resea	rch Tool	- ANTI-S	SPAM (bloc	cker/filter)	
-	If an unda	ted AN	II-SPAN	l (spam blo	cker) to	ol vere	used how	likela is it	that the s	ustem co	uld
1				cting the t				incig is it		,,5,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
	Less likely					No Impa	ot				More Likel
	Severely	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes	promotes	promotes
	minoks	minores	minores	minores	minors	impact	promotes	promotes	promotes	promotes	promotes
	1.0 . 2.1	<u> </u>									
	What if the	premise w	ere <u>False</u> '	Phow would	this impac	t the cond	lusion?				
				l (spam blo			NOT used	l, how likely	j is it that	the syste	m could
2	prevent a	VIRUS	from infe	ecting targe	ted syst	tem?					1
	Less likely					No Impa	ct				More Likel
	Severely	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes	promotes	promotes
2				(spam blo				likely is it	that the s	ystem co	uld
٦	prevenca	T TUNM	rioiii iiir	ecung the t	laryeteu	System	1				
	Less likely					No Impa	ct				More Like
	Severely		Strongly			No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
_											
				_	_	3					
				l (spam blo			NOT used		j is it that	the syste	m could
4				l (spam blo ecting targ			NOT used		j is it that	the syste	m could
4	prevent a					tem?			j is it that	the syste	
4	prevent a Less likely	VORM	from inf	ecting targ	eted sys	tem? No Impa	ct	l, how likel			More Likel
4	prevent a	VORM				tem?	ct Slightly		y is it that Strongly promotes	the syste	
4	prevent a Less likely Severely	VORM Severely	from inf Strongly	ecting targ Moderately	eted sys Slightly	No Impa No	ct Slightly	I, how likely	Strongly	Severely	More Likel Severely
4	prevent a Less likely Severely	VORM Severely	from inf Strongly	ecting targ Moderately	eted sys Slightly	No Impa No	ct Slightly	I, how likely	Strongly	Severely	More Likel Severely
	prevent a Less likely Severely Inhibits If an upda	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	ct Slightly promotes used, how	Moderately promotes	Strongly promotes	Severely promotes	More Likel Severely promotes
	prevent a Less likely Severely Inhibits If an upda	Severely Inhibits	Strongly Inhibits	ecting targ Moderately Inhibits	Slightly Inhibits	No Impact	ct Slightly promotes used, how	Moderately promotes	Strongly promotes	Severely promotes	More Likel Severely promotes
	prevent a Less likely Severely Inhibits If an upda	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	ot Slightly promotes used, how MBIE by a	Moderately promotes	Strongly promotes	Severely promotes	More Likel Severely promotes gstem
	Less likely Severely Inhibits If an updicould pre Less likely Severely	Severely Inhibits ated ANT event bei	Strongly Inhibits FI-SPAM ng taken	Moderately Inhibits (spam blo over and t	Slightly Inhibits ocker) to surned in	No Impact Impact In were to a ZOI	ot Slightly promotes used, how MBIE by a	Moderately promotes	Strongly promotes	Severely promotes	More Likel Severely promotes gstem
	Less likely Severely Inhibits If an updicould pre	Severely Inhibits ated ANI	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits cker) to	No Impact Ol were to a ZOI No Impact	st Slightly promotes used, how MBIE by a	Moderately promotes	Strongly promotes that the t	Severely promotes argeted sy	More Likel Severely promotes gstem More Likel
	Less likely Severely Inhibits If an updicould pre Less likely Severely	Severely Inhibits ated ANT event bei	Strongly Inhibits FI-SPAM ng taken	Moderately Inhibits (spam blo over and t	Slightly Inhibits ocker) to surned in	No Impact ol were to a ZOI No Impact	st Slightly promotes used, how MBIE by a	Moderately promotes	Strongly promotes that the t?	Severely promotes argeted sy	More Likel Severely promotes gstem More Likel Severely
	Less likely Severely Inhibits If an upda could pre Less likely Severely Inhibits	Severely Inhibits ated AN vent bei Severely Inhibits	Strongly Inhibits FI-SPAM ng taken Strongly Inhibits	Moderately Inhibits I (spam blo over and to Moderately Inhibits	Slightly Inhibits cker) to urned in Slightly Inhibits	No Impact No Impact ol were to a ZOI No Impact	st Slightly promotes used, how MBIE by a ct Slightly promotes	Moderately promotes I likely is it in attacker Moderately promotes	Strongly promotes that the t ? Strongly promotes	Severely promotes argeted severely promotes	More Likel Severely promotes stem More Likel Severely promotes
5	Less likely Severely Inhibits If an upda could pre Less likely Severely Inhibits	Severely Inhibits ated AN Severely Inhibits Severely Inhibits	Strongly Inhibits FI-SPAN Strongly Inhibits	Moderately Inhibits I (spam blo over and to Moderately Inhibits I (spam blo over and to Moderately Inhibits	Slightly Inhibits cker) to urned in Slightly Inhibits	No Impact No Impact ol were to a ZOI No Impact No Impact ol were	st Slightly promotes used, how MBIE by a ct Slightly promotes	Moderately promotes likely is it in attacker Moderately promotes	Strongly promotes that the t? Strongly promotes	Severely promotes argeted severely promotes	More Likel Severely promotes stem More Likel Severely promotes
5	Less likely Severely Inhibits If an upda could pre Less likely Severely Inhibits	Severely Inhibits ated AN Severely Inhibits Severely Inhibits	Strongly Inhibits FI-SPAN Strongly Inhibits	Moderately Inhibits I (spam blo over and to Moderately Inhibits	Slightly Inhibits cker) to urned in Slightly Inhibits	No Impact No Impact ol were to a ZOI No Impact No Impact ol were	st Slightly promotes used, how MBIE by a ct Slightly promotes	Moderately promotes likely is it in attacker Moderately promotes	Strongly promotes that the t? Strongly promotes	Severely promotes argeted severely promotes	More Likel Severely promotes stem More Likel Severely promotes
5	Less likely Severely Inhibits If an upda could pre Less likely Severely Inhibits	Severely Inhibits ated AN Severely Inhibits Severely Inhibits	Strongly Inhibits FI-SPAN Strongly Inhibits	Moderately Inhibits I (spam blo over and to Moderately Inhibits I (spam blo over and to Moderately Inhibits	Slightly Inhibits cker) to urned in Slightly Inhibits	No Impact No Impact ol were to a ZOI No Impact No Impact ol were	st Slightly promotes used, how MBIE by a st Slightly promotes NOT used rned into	Moderately promotes likely is it in attacker Moderately promotes	Strongly promotes that the t? Strongly promotes	Severely promotes argeted severely promotes	More Likel Severely promotes stem More Likel Severely promotes t system
5	Less likely Inhibits If an updicould pre Less likely Severely Inhibits If an updicould pre Less likely Severely Inhibits	Severely Inhibits Severely Inhibits Severely Inhibits ated AN	Strongly Inhibits FI-SPAN Strongly Inhibits	Moderately Inhibits I (spam blo over and to Moderately Inhibits I (spam blo over and to Moderately Inhibits	Slightly Inhibits cker) to urned in Slightly Inhibits	No Impact No Impact ol were to a ZOI No Impact No Impact ol were er and tu	st Slightly promotes used, how MBIE by a st Slightly promotes NOT used rned into	Moderately promotes likely is it in attacker Moderately promotes	Strongly promotes that the t? Strongly promotes	Severely promotes argeted severely promotes	More Likel Severely promotes stem More Likel Severely promotes

	picaciic u						eted syst	em:			
	Less likely					No Impa	et				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
_	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes	promotés	promotés
+											
				l (spam blo E from pen					j is it that	the syste	m could
	Less likely					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
			ri onak			_		111 -1 - 1 - 1			
				l (spam blo om being pl					that the s	system co	ula
	Less likely					No Impa	ot				More Likel
	Severely	Severely		Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
+	lf an unda	ted AN	II-SPAN	l (spam blo	cker) to	ol vere	NOT used	l how likeli	is it that	the suste	m could
				om being pl					, 15 10 01140	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	III OOGIG
	Less likely			- H		No Impa					More Likel
- 1					- I		II a				
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly /	Mo derately promotes	Strongly promotes	Severely promotes	Severely promotes
	Inhibits	Inhibits	Inhibits	Inhibits (spam blo	Inhibits	No Impact	Slightly promotes used, how	promotes	promotes	promotes	Severely promotes
11	Inhibits If an upda prevent a	Inhibits	Inhibits	Inhibits	Inhibits	ol were	Slightly promotes used, how oting serv	promotes	promotes	promotes	Severely promotes uld
11	Inhibits If an upda prevent a	Inhibits nted AN1 Denial (Inhibits FI-SPAN Of Service	Inhibits I (spam bloce (DOS) a	Inhibits ocker) to ttack fro	No Impact	Slightly promotes used, how oting serv	likely is it	that the stargeted s	promotés system co system?	promotes uld More Likel
11	Inhibits If an upda prevent a	Inhibits	Inhibits FI-SPAN Of Service	Inhibits (spam blo	Inhibits	ol were on disrup	Slightly promotes used, how oting serve	promotes	promotes	promotes	Severely promotes uld
11	Inhibits If an upda prevent a Less likely Severely Inhibits	Inhibits Ated AN Denial (Severely Inhibits	Inhibits FI-SPAN Of Service Strongly Inhibits	Inhibits I (spam bloce (DOS) at Moderately Inhibits	cker) to	ol were m disruj No Impact	Slightly promotes used, how pting serv et Slightly promotes	likely is it ice on the Moderately promotes	that the stargeted strongly promotes	system co system? Severely promotes	Severely promotes uld More Likel Severely promotes
11	If an upda prevent a Less likely Severely Inhibits	Inhibits Denial (Severely Inhibits	Inhibits II-SPAN Of Service Strongly Inhibits	Inhibits (spam bloce (DOS) at	cker) to	ol were m disruj	Slightly promotes used, howoting servest Slightly promotes	r likely is it ice on the Moderately promotes	that the stargeted strongly promotes	system co system? Severely promotes	More Likel Severely promotes
11	If an upda prevent a Less likely Severely Inhibits If an upda prevent a Less likely	Inhibits Ated AN Denial (Severely Inhibits Ated AN DOS free	Inhibits FI-SPAN Strongly Inhibits FI-SPAN om disru	I (spam bloce (DOS) at Moderately Inhibits	ocker) to ctack fro Slightly Inhibits cker) to ce on th	No Impact of were on disrup No Impact of were of the transpace of were of the transpace	Slightly promotes used, how oting servest Slightly promotes NOT used ed systemet	promotes likely is it ice on the Moderately promotes , how likely ?	that the stargeted strongly promotes	system co system? Severely promotes the syste	More Like Severely promotes More Like Severely promotes m could
111	If an upda prevent a Less likely Severely Inhibits If an upda prevent a	Inhibits Denial (Severely Inhibits	Inhibits FI-SPAN Strongly Inhibits FI-SPAN om disru	Inhibits I (spam bloce (DOS) all Moderately Inhibits I (spam blo	cker) to	No Impact Ol were on disrup No Impact Impact ol were of targete	Slightly promotes used, how oting servent Slightly promotes NOT used system ot Slightly Slightly	r likely is it ice on the Moderately promotes	that the stargeted strongly promotes	system co system? Severely promotes	More Likel Severely promotes
11	If an upda prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely	Inhibits Severely Inhibits Ated AN DOS fro	Inhibits II-SPAN Of Service Strongly Inhibits II-SPAN om disru	I (spam bloce (DOS) at Moderately Inhibits I (spam blopting service Moderately Moderately Moderately Moderately	slightly cker) to	No Impact Ol were on disrup No Impact Ol were of the control of	Slightly promotes used, how oting servent Slightly promotes NOT used system ot Slightly Slightly	promotes likely is it ice on the Moderately promotes , how likely?	that the stargeted strongly promotes	system co system? Severely promotes the syste	More Like Severely promotes m could More Like Severely
11	If an upda prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely Inhibits	sted ANI Denial (Severely Inhibits Severely Inhibits Severely Inhibits	Inhibits FI-SPAN Strongly Inhibits Strongly Inhibits Strongly Inhibits	I (spam bloce (DOS) at Moderately Inhibits I (spam block of the span block of the s	Slightly Inhibits cker) to cce on the Slightly Inhibits	No Impact Ol were on disrup No Impact Ol were of targete No Impact No Impact	slightly promotes used, howething serve states and slightly promotes states and states a	likely is it ice on the Moderately promotes how likely? Moderately promotes	that the stargeted strongly promotes Strongly promotes Strongly promotes	system co system? Severely promotes the syste Severely promotes	More Like Severely promotes More Like More Like Severely promotes
11 12 13	If an upda prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely Inhibits	sted ANI Denial (Severely Inhibits Severely Inhibits Severely Inhibits	Inhibits FI-SPAN Strongly Inhibits Strongly Inhibits Strongly Inhibits	I (spam bloce (DOS) at Moderately Inhibits I (spam blopting service Moderately Inhibits	Slightly Inhibits cker) to cce on the Slightly Inhibits	No Impact Ol were on disrup No Impact Ol were of targete No Impact No Impact	slightly promotes used, howoting servent Slightly promotes Slightly promotes Slightly promotes used, howesystem?	likely is it ice on the Moderately promotes how likely? Moderately promotes	that the stargeted strongly promotes Strongly promotes Strongly promotes	system co system? Severely promotes the syste Severely promotes	More Likel Severely promotes More Likel More Likel Severely promotes
11 12 13	If an upda prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely Inhibits	sted ANI Denial (Severely Inhibits Severely Inhibits Severely Inhibits	Inhibits II-SPAN Strongly Inhibits Strongly Inhibits Strongly Inhibits II-SPAN BOMB a	I (spam bloce (DOS) at Moderately Inhibits I (spam block of the span block of the s	Slightly Inhibits cker) to cce on the Slightly Inhibits	No Impact No Impact No Impact OI were to targete No Impact No Impact No Impact OI were to targete of were to targete	slightly promotes used, howoting servent Slightly promotes Slightly promotes Slightly promotes used, howesystem?	likely is it ice on the Moderately promotes how likely? Moderately promotes	that the stargeted strongly promotes Strongly promotes Strongly promotes	system co system? Severely promotes the syste Severely promotes	More Lik Severely promote m could More Lik Severely promote

	lf an und:	ted AN	I-SPAN	l (spam blo	cker) to	ol were	NOT used	I. how likeli	is it that	the suste	m could
				ttack again					, 13 10 01140	· · · · · · · · · · · · · · · · · · ·	ooulu
	l a a a lib abo					No.					Marca Librato
	Less likely Severely	Couerelu	Strongly	Moderately	Slightly	No Impai No	Slightly	Moderately	Strongly	Severely	More Likely Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes		promotes
	IIIIIIDICS	ITINIDICS	IIIIIDKS	IIIIIDIGS	IIIIIIIII	impact	promotes	promotes	promotes	promotes	promotes
\dashv											
				l (spam blo ING attack					that the s	ystem co	uld
	Less likely					No Impa	et				More Likel
	Severelu	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderatelu	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact		promotes	promotes		promotes
+											
=	lf an und:	ted AN	ILSPAN	l (spam blo	cker) to	ol were l	NOT used	l how likeli	is it that	the suste	m could
				ING attack					, is it that	33300	voulu
	Less likely					No Impa	ct				More Likel
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
_											
								5			
	lf an unda	ated AN	I-SPAM	(spam blo	cker) to	ol vere	used, how)	that the s	sestem co	uld
				(spam blo oofing atta				likely is it	that the s	ystem co	uld
17							argeted s	likely is it	that the s	ystem co	
17	prevent a	n IP Add		oofing atta		st the t	argeted s	likely is it		system co	
17	prevent a Less likely	n IP Add	lress Sp	oofing atta	ck agair	No Impa	argeted s y ct Slightly	likely is it jstem?		Severely	More Likely
17	prevent a Less likely Severely	n IP Add	Iress Sp Strongly	oofing atta Moderately	ck agair Slightly	No Impa No	argeted s y ct Slightly	likely is it gstem? Moderately	Strongly	Severely	More Likely Severely
17	prevent a Less likely Severely Inhibits	Severely Inhibits	Strongly Inhibits	oofing atta Moderately Inhibits	Slightly Inhibits	No Impa No Impact	ct Slightly promotes	likely is it stem? Moderately promotes	Strongly promotes	Severely promotes	More Likely Severely promotes
17	prevent a Less likely Severely Inhibits If an upda prevent a	Severely Inhibits	Strongly Inhibits	oofing atta Moderately Inhibits	Slightly Inhibits	No Impact	ot Slightly promotes NOT used	likely is it stem? Moderately promotes	Strongly promotes	Severely promotes	More Likely Severely promotes m could
17	prevent a Less likely Severely Inhibits If an upda prevent a Less likely	Severely Inhibits ated AN	Strongly Inhibits FI-SPAN Iress SP	Moderately Inhibits (spam blo	Slightly Inhibits ocker) to	No Impact Ol were ainst the	ot Slightly promotes NOT used targeted	likely is it istem? Moderately promotes , how likely system?	Strongly promotes y is it that	Severely promotes the syste	More Likel Severely promotes m could
17	prevent a Less likely Severely Inhibits If an upda prevent a	Severely Inhibits ated AN	Strongly Inhibits	Moderately Inhibits (spam blo	Slightly Inhibits	No Impact	ct Slightly promotes NOT used targeted ct Slightly	likely is it stem? Moderately promotes	Strongly promotes y is it that	Severely promotes the syste	More Likely Severely promotes m could
17	prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely	Severely Inhibits ated AN1 in IP Add	Strongly Inhibits FI-SPAN Iress SP	Moderately Inhibits I (spam blo OOFING at	Slightly Inhibits ocker) to ttack ag	No Impact ol were ainst the No Impact	ct Slightly promotes NOT used targeted ct Slightly	Moderately promotes how likely system?	Strongly promotes is it that	Severely promotes the syste	More Likely Severely promotes m could More Likely Severely
17	prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely Inhibits	Severely Inhibits ated ANT in IP Add Severely Inhibits	Strongly Inhibits I-SPAN Iress SP Strongly Inhibits	Moderately Inhibits I (spam blo OOFING at Moderately Inhibits	Slightly Inhibits cker) to ttack ag Slightly Inhibits	No Impact No Impact ol were ainst the No Impact	ct Slightly promotes NOT used targeted ct Slightly promotes	Moderately promotes Moderately promotes Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promotes the syste Severely promotes	More Likely promotes m could More Likely Severely promotes
18	prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely Inhibits If an upda	Severely Inhibits ated AN Inhibits Severely Inhibits	Strongly Inhibits I-SPAN Iress SP Strongly Inhibits	Moderately Inhibits I (spam blo OOFING at	Slightly Inhibits cker) to ttack ag Slightly Inhibits	No Impact Ol were ainst the No Impact No Impact No Impact	ct Slightly promotes NOT used targeted ct Slightly promotes	Moderately promotes how likely system? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promotes the syste Severely promotes	More Likely promotes m could More Likely Severely promotes
17	prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely Inhibits If an upda prevent a	Severely Inhibits ated AN Inhibits Severely Inhibits	Strongly Inhibits I-SPAN Iress SP Strongly Inhibits	Moderately Inhibits (spam blo OOFING at Moderately Inhibits	Slightly Inhibits cker) to ttack ag Slightly Inhibits	No Impact No Impact of were ainst the No Impact No Impact of were argeting	oct Slightly promotes NOT used targeted ct Slightly promotes used, how a system	Moderately promotes how likely system? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promotes the syste Severely promotes	More Likely promotes m could More Likely Severely promotes
18	prevent a Less likely Severely Inhibits If an upda prevent a Less likely Severely Inhibits If an upda	Severely Inhibits ated AN Inhibits Severely Inhibits	Strongly Inhibits FI-SPAN Iress SP Strongly Inhibits FI-SPAN GGER for	Moderately Inhibits (spam blo OOFING at Moderately Inhibits	Slightly Inhibits cker) to ttack ag Slightly Inhibits	No Impact Ol were ainst the No Impact No Impact No Impact	oct Slightly promotes NOT used targeted ct Slightly promotes used, how a system	Moderately promotes how likely system? Moderately promotes	Strongly promotes g is it that Strongly promotes	Severely promotes the syste Severely promotes	More Likely promotes m could More Likely Severely promotes

20				l (spam blo om being u					j is it that	the syste	m could
	Less likely					No Impac	et				More Likelu
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
21				l (spam blo being used				likely is it	that the s	ystem co	uld
	Less likely			Г		No Impad	C '	-			More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
22				l (spam blo being used				l, how likely	j is it that	the syste	m could
	Less likely					No Impac	et				More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

7. ANTI-SPYWARE SECTION OF SURVEY

from infe Less likely Severely			ARE tool v							
from infe Less likely Severely					1 Kow III	tels is it t	hat the cuct	bluos ma	nrevent a	VIRUS
Severely			d system?	reie usei	u, 110¥ 111	kei y is it ti	nat the syst	em coala	prevent a	¥II 103
			_		No Impa					More Likely
Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promote
			'ARE tool v jeted systei		used, h	ow likely i	s it that the	system c	ould prev	ent a
Less likely			_							More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promote
lC sn und	stad AM	ri epvu	ADE tool		d bass lil	ala is it t	an the cost	om aquid	nrawant s	VODIA
				rere use	ı, now III	kely is it ti	nat the syst	em coula	prevent a	WURM
Less likely										More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact			Strongly promotes	Severely promotes	Severely promote
				7						
		ri opiu			3		•	<u> </u>	<u> </u>	<u> </u>
					used, h	ow likely i	s it that the	system c	ould prev	ent a
Less likely					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 promote
ır		ri envi	ADC 1 1 -		4 6 1:1					
							nat the tary	eteu syste	in coula p	
Less likely										More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promote
lf an unda	ited AN	∏-SPY¥	ARE tool v	rere NOT	used. h	ow likels i	s it that the	target se	stem coul	d prevei
										-
Less likely				00.1						More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promote
She let Look Look Look Look	Fan upda from infe ess likely Severely nhibits Fan upda ORM fr ess likely Severely nhibits Fan upda being tak ess likely Severely nhibits	Severely Inhibits If an updated ANT From infecting the Less likely Severely Inhibits If an updated ANT From infecting the Less likely Severely Inhibits If an updated ANT Severely Inhibits	Severely Severely Strongly Inhibits Inhibits Inhibits Inhibits If an updated ANTI-SPYW Inhibits Inhib	Severely Severely Strongly Moderately Inhibits Inhibits Inhibits Inhibits Inhibits Inhibits From infecting the targeted system? Less likely Severely Strongly Moderately Inhibits Inh	Severely Severely Strongly Moderately Inhibits I	Severely Severely Strongly Moderately Inhibits I	Severely Severely Strongly Inhibits Inh	Severely Inhibits Inh	Severely Inhibits Inh	Severely Inhibits Inh

	Less likely					No Impa					More Likely
	Severely		Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
_[Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promote:
ŀ											
				ARE tool v				s it that the	system o	ould prev	ent a
	Less likely	IIOIIOE	iioiii pe	incordaing to	ic target	No Impa					More Likely
	Severelu	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promote
t											
								hat the syst	em could	prevent a	
		UK HON	n being p	laced in th	e targete						More
_	Less likely Severely	Comment'	Character's	Made	Oli -trata	No Impa		BA-de	Change -by	Comments	Likely
		Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
			1-1.3636-	I = I. (b. (c							
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promote
	Inhibits	Inhibits	TI-SPY¥	ARE tool	rere NO	used, h	ov likely i	s it that the			
0 1	If an upda BACKDO Less likely	Inhibits ated AN	TI-SPYW n being p	ARE tool v	rere NO e targete	l used, hed system	ow likely in?	s it that the	system o	ould prev	ent a More Likely
0 1	Inhibits If an upda BACKDO Less likely Severely	Inhibits ated AN OR from	TI-SPYW n being p	ARE tool volaced in the	rere NO e targete Slightly	l used, hed system No Impa	ow likely in?	s it that the	s ystem o Strongly	could prev	More Likely Severely
0 1	If an upda BACKDO Less likely	Inhibits ated AN	TI-SPYW n being p	ARE tool v	rere NO e targete	l used, hed system	ow likely in?	s it that the	system o	could prev	ent a More Likely Severely
	If an upda BACKDO Less likely Severely Inhibits	Inhibits ated AN OR from Severely Inhibits	TI-SPYW n being p Strongly Inhibits	ARE tool volaced in the Moderately Inhibits	Slightly Inhibits	No Impact	ow likely in? ct Slightly promotes	s it that the Moderately promotes	Strongly promotes	Severely promotes	ent a More Likely Severely promote
10 1	If an upda BACKDO Less likely Severely Inhibits	Inhibits ated AN OR from Severely Inhibits	TI-SPYW n being p Strongly Inhibits	ARE tool volaced in the Moderately Inhibits	Slightly Inhibits	No Impact	ow likely in? ct Slightly promotes kely is it tl targeted s	s it that the Moderately promotes	Strongly promotes	Severely promotes	ent a More Likely Severely promote
	If an upda BACKDO Less likely Severely Inhibits If an upda Service (Inhibits ated AN' OR from Severely Inhibits ated AN' DOS) at	TI-SPYW n being p Strongly Inhibits	ARE tool volaced in the Moderately Inhibits	Slightly Inhibits	No Impact	ow likely in? ct Slightly promotes kely is it tl targeted s	s it that the Moderately promotes	Strongly promotes	Severely promotes	ent a More Likely Severely promote Denial (More Likely
0 1 1 1 1 1 1 1 1 1 1 1	If an upda BACKDO Less likely Severely Inhibits If an upda Service (Less likely	Inhibits ated AN' OR from Severely Inhibits ated AN' DOS) at	TI-SPYW n being p Strongly Inhibits TI-SPYW tack from	ARE tool valued in the Moderately Inhibits	sere NO e targete Slightly Inhibits	No Impact d, how life No Impact	ov likely in? ct Slightly promotes kely is it tl targeted s	Moderately promotes hat the system?	Strongly promotes	Severely promotes	ent a More Likely Severely promote Denial (More Likely Severely
0 1 1 1 1 1 1 1 1 1 1 1	If an upda BACKDO Less likely Severely Inhibits If an upda Service (Less likely	Inhibits ated AN' OR from Severely Inhibits ated AN' DOS) at	TI-SPYW Strongly Inhibits TI-SPYW tack from	ARE tool valued in the Moderately Inhibits ARE tool value disruption	slightly Inhibits rere use g service	No Impact No Impact No Impact No Impact No Impact	ow likely in? ct Slightly promotes kely is it tl targeted s ct Slightly	Moderately promotes hat the system?	Strongly promotes em could	Severely promotes	ent a More Likely Severely promote Denial (More Likely Severely
	If an upda BACKDO Less likely Severely Inhibits If an upda Service (Less likely Severely Inhibits	Inhibits ated AN' OR from Severely Inhibits ated AN DOS) at Severely Inhibits	TI-SPYW Strongly Inhibits TI-SPYW Lack from Strongly Inhibits	ARE tool of the laced in disruption Moderately Inhibits	Slightly Inhibits rere use g service Slightly Inhibits	No Impact	ov likely in? ct Slightly promotes kely is it tl targeted s ct Slightly promotes	Moderately promotes hat the system?	Strongly promotes em could Strongly promotes	Severely promotes Prevent a Severely promotes	More Likely Severely promote Denial (More Likely Severely promote
111 :	If an upda BACKDO Less likely Severely Inhibits If an upda Service (Less likely Severely Inhibits	Inhibits ated AN' OR from Severely Inhibits ated AN DOS) at Severely Inhibits	TI-SPYW Strongly Inhibits TI-SPYW Lack from Strongly Inhibits	ARE tool value of the laced in the laced in the laced in the laced	Slightly Inhibits rere use g service Slightly Inhibits	No Impact	ct Slightly promotes kely is it tl targeted s ct Slightly promotes	Moderately promotes hat the syst gstem?	Strongly promotes em could Strongly promotes	Severely promotes Prevent a Severely promotes	More Likely Severely promote Denial (More Likely Severely promote
111 :	If an upda BACKDO Less likely Severely Inhibits If an upda Service (Less likely Severely Inhibits	Inhibits Severely Inhibits ated AN' OOS) at Severely Inhibits severely Inhibits	TI-SPYW Strongly Inhibits TI-SPYW Lack from Strongly Inhibits	ARE tool of the laced in disruption Moderately Inhibits	Slightly Inhibits rere use g service Slightly Inhibits	No Impact Impact	ct Slightly promotes kely is it tl targeted s ct Slightly promotes	Moderately promotes hat the syst gstem?	Strongly promotes em could Strongly promotes	Severely promotes Prevent a Severely promotes	More Likely Severely promote Denial (More Likely Severely promote ent a DC

											More
	Less likely	Comments	Ohana ala	B.d. d	Oli ali Ma	No Impa		B.d. deces to be	Character.	Comments	Likely
	Severely		Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
-	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
14	lf an upda LOGIC B	ated AN' OMB att	TI-SPYW ack agai	ARE tool vinst the tar	vere NO geted sy	T used, h stem?	ow likely i	s it that the	system c	ould prev	ent a
П	Less likely					No Impa	et				More Likely
	Severely	Severelu	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
	Inhibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
1						-					
#	K an und	stad AN	TI CDVU	APE tool s	HATA IICA	d hou li	kalı iç it t	hat the syst	em could	prougnt a	n E-mail
				t the target			Keig is it ti	iat the syst	em coala	prevent a	
	Less likely					No Impa	ct				More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
			Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
4	Inhibits	Inhibits	IIIIIIIIII	minores	IIIII III III	impaox	P. 51115155	promotes	promotes	promotes	pironii en
	Inhibits	Inhibits	IIIIIDICS	I I I I I I I I I I I I I I I I I I I)_		O 4	2			
	lf an upda	ated AN	TI-SPY¥	ARE tool	vere NO	T used, h	iow likely	s it that the			
16	lf an upda mail SPO	ated AN	TI-SPY¥		vere NO	T used, h	ibely	3			
16	If an upda mail SPO Less likely	ated AN	TI-SPYW attack ag	'ARE tool v	rere NO argeted	T used, h system?	now likely (s it that the	system o	ould prev	ent an E- More Likely
16	lf an upda mail SPO	ated AN	TI-SPY¥	ARE tool	vere NO	T used, I system? No Impa	ibely	3		ould prev	ent an E- More Likely Severely
16	If an upda mail SPO Less likely Severely	ated AN'	TI-SPYWattack as	ARE tool of gainst the t	rere NO argeted	T used, I system? No Impa No	ov likely i	s it that the	s ystem c Strongly	ould prev	ent an E- More Likely Severely
16	If an upda mail SPO Less likely Severely Inhibits	Severely Inhibits	TI-SPYW attack as Strongly Inhibits	ARE tool vigainst the time tool vigainst the time tool vigainst the time time tool vigainst the time time time time time time tool vigainst the time time time time time time time tim	Slightly Inhibits	I used, h system? No Impa No Impact	ct Slightly promotes	s it that the	Strongly promotes	Severely promotes	ent an E- More Likely Severely promotes
16	If an upda mail SPO Less likely Severely Inhibits	Severely Inhibits	TI-SPYW attack as Strongly Inhibits	ARE tool v gainst the t Moderately Inhibits	Slightly Inhibits	I used, h system? No Impa No Impact	ct Slightly promotes	s it that the Moderately promotes	Strongly promotes	Severely promotes	ent an E- More Likely Severely promotes
16	If an upda mail SPO Less likely Severely Inhibits If an upda Address Less likely	Severely Inhibits	TI-SPYW attack a Strongly Inhibits TI-SPYW g attack	ARE tool value of the tool val	slightly Inhibits	T used, h system? No Impact Impact d, how li	ot Slightly promotes kely is it the	Moderately promotes	Strongly promotes	Severely promotes	ent an E- More Likely Severely promotes IP More Likely
16	If an upda mail SPO Less likely Severely Inhibits If an upda Address Less likely Severely	Severely Inhibits	TI-SPYWattack as Strongly Inhibits TI-SPYW g attack	ARE tool a gainst the t Moderately Inhibits ARE tool a against the	slightly Inhibits were use a targete	T used, h system? No Impact Impact d, how li	ct Slightly promotes kely is it the	s it that the Moderately promotes	Strongly promotes	Severely promotes	ent an E- More Likely Severely promotes
16	If an upda mail SPO Less likely Severely Inhibits If an upda Address Less likely	Severely Inhibits	TI-SPYW attack a Strongly Inhibits TI-SPYW g attack	ARE tool value of the tool val	slightly Inhibits	T used, h system? No Impact Impact d, how li	ot Slightly promotes kely is it the	Moderately promotes	Strongly promotes	Severely promotes	More Likely Severely promote:
16	If an upda mail SPO Less likely Severely Inhibits If an upda Address Less likely Severely Inhibits	Severely Inhibits ated AN' Spoofin Severely Inhibits	TI-SPYWattack a Strongly Inhibits TI-SPYW g attack Strongly Inhibits	ARE tool value of the tool val	Slightly Inhibits Slightly Inhibits	T used, h system? No Impact Impact d, how li d system No Impact	ct Slightly promotes kely is it the state of the state o	Moderately promotes hat the syst	Strongly promotes em could Strongly promotes	Severely promotes Prevent all Severely promotes	More Likely Severely promote: IP More Likely Severely promote:
16	If an updanail SPO Less likely Severely Inhibits If an updanddress Less likely Severely Inhibits	Severely Inhibits ated AN' Spoofin Severely Inhibits	TI-SPYWattack as Strongly Inhibits TI-SPYWg attack Strongly Inhibits	ARE tool value of the tool val	Slightly Inhibits Slightly Inhibits	T used, h system? No Impact Impact d, how li d system No Impact	ct Slightly promotes kelly is it the state of the state o	Moderately promotes hat the syst	Strongly promotes em could Strongly promotes	Severely promotes Prevent all Severely promotes	More Likely Severely promotes IP More Likely Severely promotes
117	If an updanail SPO Less likely Severely Inhibits If an updanddress Less likely Severely Inhibits	Severely Inhibits ated AN' Spoofin Severely Inhibits	TI-SPYWattack as Strongly Inhibits TI-SPYWg attack Strongly Inhibits	ARE tool and against the transport of th	Slightly Inhibits Slightly Inhibits	No Impact d, how lited system No Impact I used, how lited system No Impact T used, heted system	ct Slightly promotes kely is it to ? ct Slightly promotes ct Slightly promotes	Moderately promotes hat the syst	Strongly promotes em could Strongly promotes	Severely promotes Prevent all Severely promotes	More Likely Severely promote: More Likely Severely promote: More Likely Severely promote:
16	If an updamail SPO Less likely Severely Inhibits If an upda Address Less likely Severely Inhibits If an upda Address	Severely Inhibits ated AN' Spoofin Severely Inhibits	TI-SPYWattack as Strongly Inhibits TI-SPYWg attack Strongly Inhibits	ARE tool and against the transport of th	Slightly Inhibits Slightly Inhibits	T used, h system? No Impact Impact d, how li d system No Impact	ct Slightly promotes kely is it to ? ct Slightly promotes ct Slightly promotes	Moderately promotes hat the syst	Strongly promotes em could Strongly promotes	Severely promotes Prevent all Severely promotes	More Likely Severely promotes IP More Likely Severely promotes

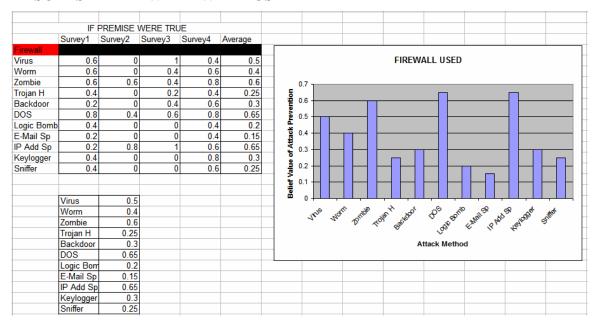
١.			_	_							More
	ess likely					No Impa					Likely
	everely	Severely		Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Int	hibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
				'ARE tool v I in targetin			ow likely i	is it that the	system o	ould prev	ent a KE'
Le	ess likely					No Impa	ot				More Likely
Se	everely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
Int	hibits	Inhibits	Inhibits	Inhibits	Inhibits	Impact	promotes	promotes	promotes	promotes	promotes
								1			
					25	HOL	2	4			
				ARE tool o		d, how lil	cely is it t	hat the syst	em could	prevent a	SNIFFEI
21 fr						d, how lill		hat the syst	em could	prevent a	SNIFFEI More Likely
21 fr Le Se	om bein esslikely everely	g used i Severely	n target i Strongly	ing a syster Moderately	n? Slightly	No Impa	ct Slightly	Moderately	Strongly	Severely	More Likely Severely
21 fr Le Se	om bein ess likely	ig used i	n targeti	ing a syster	n?	No Impa	ot				More Likely
Le Se Int	om bein ess likely everely hibits an upda	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits rere NO	No Impact	ot Slightly promotes	Moderately	Strongly promotes	Severely promotes	More Likely Severely promotes
Le Se Int	om bein ess likely everely hibits an upda	Severely Inhibits	Strongly Inhibits	ing a syster Moderately Inhibits	Slightly Inhibits rere NO	No Impact	ot Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	More Likely Severely promotes
Le Se Internation	ess likely everely hibits an upda NIFFER	Severely Inhibits ated AN	Strongly Inhibits	Moderately Inhibits 'ARE tool t	Slightly Inhibits rere NOT	No Impact Impact I used, hem?	Slightly promotes ow likely i	Moderately promotes s it that the	Strongly promotes system o	Severely promotes ould prev	More Likely Severely promote: ent a More Likely
Le Se Internation Le Internation	ess likely everely hibits an upda	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits rere NO	No Impact Impact used, h	ot Slightly promotes ow likely i	Moderately promotes	Strongly promotes	Severely promotes	More Likely Severely promote: ent a

THIS PAGE INTENTIONALLY LEFT BLANK

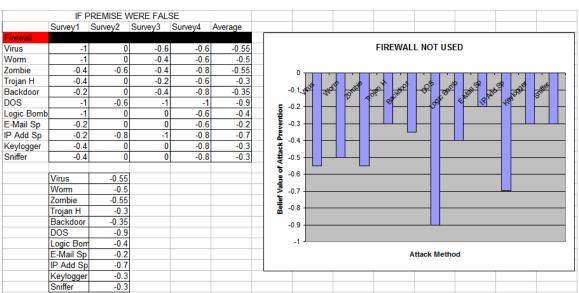
APPENDIX B EXPERT OPINION SUMMARY RESULTS

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.

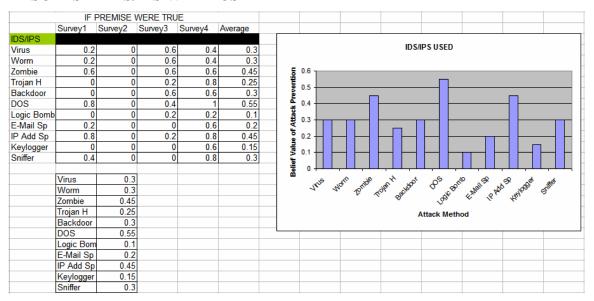
1. RESULTS IF FIREWALL WERE USED



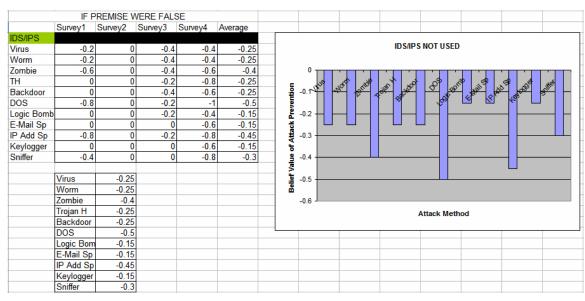
2. RESULTS IF FIREWALL WERE NOT USED



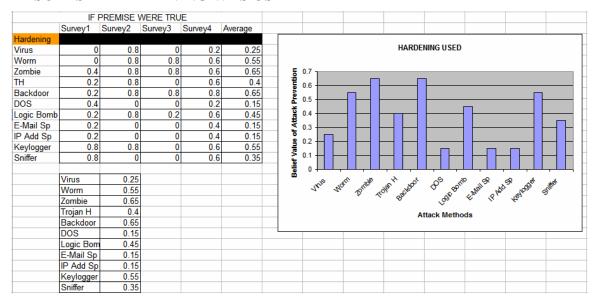
3. RESULTS IF IDS/IPS WERE USED



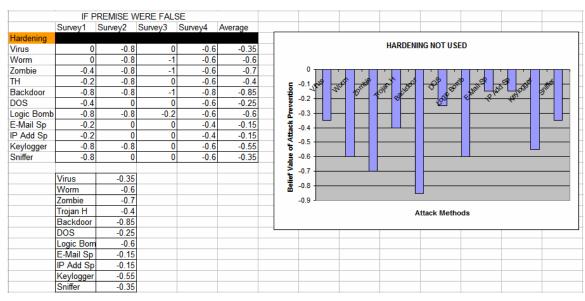
4. RESULTS IF IDS/IPS WERE NOT USED



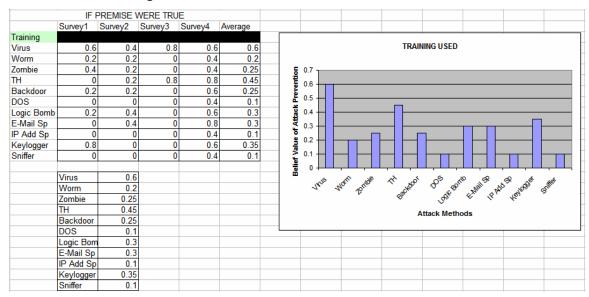
5. RESULTS IF HARDENING WAS USED



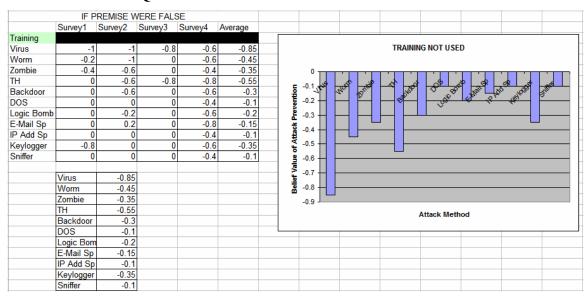
6. RESULTS IF HARDENING WAS NOT USED



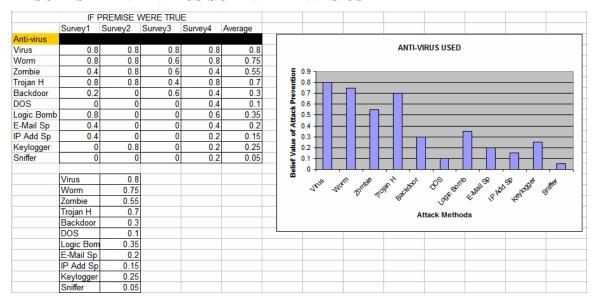
7. RESULTS IF ADEQUATE TRAINING WAS USED



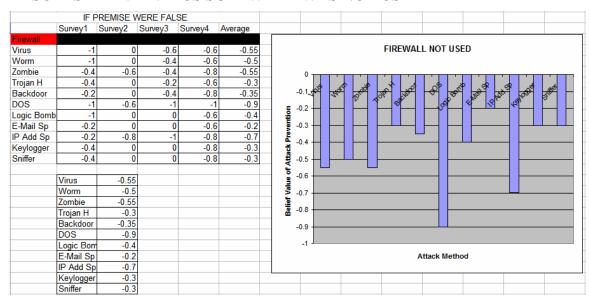
8. RESULTS IF ADEQUATE TRAINING WERE NOT USED



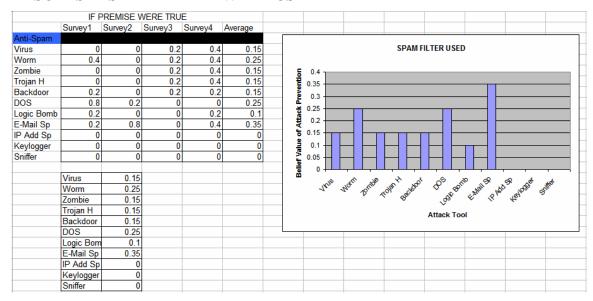
9. RESULTS IF ANTI-VIRUS SOFTWARE WAS USED



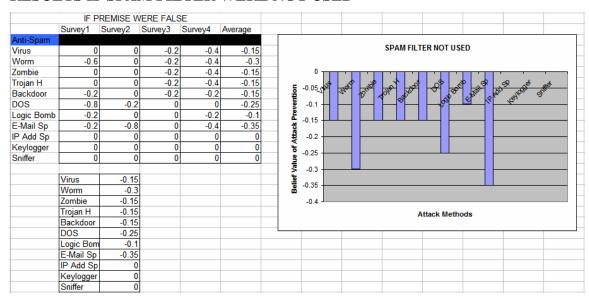
10. RESULTS IF ANTI-VIRUS SOFTWARE WAS NOT USED



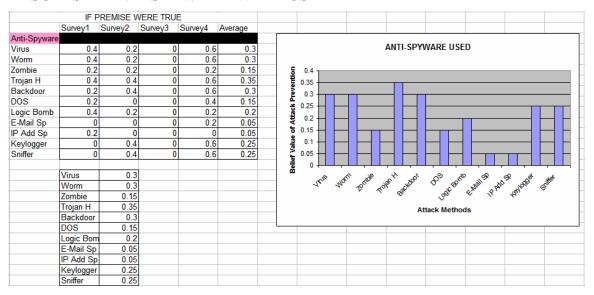
11. RESULTS IF SPAM FILTER WERE USED



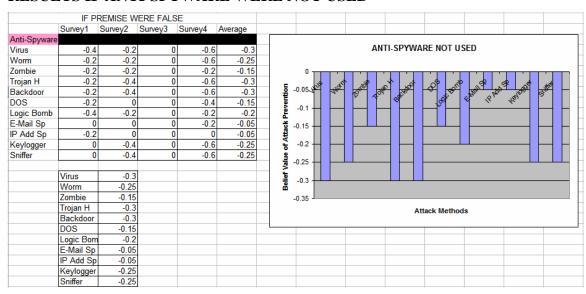
12. RESULTS IF SPAM FILTER WERE NOT USED



13. RESULTS IF ANTI-SPYWARE WERE USED



14. RESULTS IF ANTI-SPYWARE WERE NOT USED



LIST OF REFERENCES

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

Arquilla, John. Interview with FRONTLINE. <u>Cyberwar!: FRONTLINE</u>. 4 Mar. 2003. 8 Mar. 2007

http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html.

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 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 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. <u>Information Warfare and Security</u>. 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 http://www.ssrc.org/sept11/essays/denning_text_only.html>.

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 http://www.ibm.com/news/ie/en/2005/08/ie_en_news_20050804.html.

Janczewski, Lech J., and Andrew M. Colarik. <u>Managerial Guide for Handling Cyber-Terrorism and Information Warfare</u>. Hershey: Idea Group, 2005.

Lemos, Robert. "Safety: Assessing the Infrastructure Risk." CNET News. 26 Aug. 2006. 8 Mar. 2007 http://news.com/2009-1001-954780.html.

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

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

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 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> User's Manual. 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 http://www.au.af.mil/au/awc/awcgate/modeling/usesiam.doc>.

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

Serabian Jr., John A. "Cyber Threats and the U.S. Economy." Joint Economic Committee. Washington. D.C. 23 Feb. 2000. 8 Mar. 2007 http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html>.

Thomas, Douglas, and Brian D. Loader. <u>Cybercrime: Law Enforcement, Security and 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. <u>Joint Publication 3-13 Information</u> <u>Operations</u>. 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 (IA) Glossary</u>. Washington D.C.: CNSS, 2003.

United States. President of the United States. <u>The National Strategy to Secure</u> Cyberspace. Washington D.C.: The White House, 2003.

Wilson, Clay. <u>Information Warfare and Cyberwar: Capabilities and Related Policy 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 Businesses</u>. 1st ed. Arlington: Carnegie Mellon University and Internet Security Alliance, 2004. <u>Recommended Actions for Information Security</u>. 8 Mar. 2007 http://www.us-cert.gov/reading_room/CSG-small-business.pdf>.

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

- Defense Technical Information Center
 Ft. Belvoir, Virginia
- 2. Dudley Knox Library Naval Postgraduate School Monterey, California
- 3. 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