11-12-2004

A novel neural network based system for assessing risks associated with information technology security breaches

Monica DeZulueta
Florida International University

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

A NOVEL NEURAL NETWORK BASED SYSTEM FOR ASSESSING RISKS ASSOCIATED WITH INFORMATION TECHNOLOGY SECURITY BREACHES

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

by

Monica DeZulueta

2004

To: Dean Vish Prasad
College of Engineering

This dissertation, written by Monica DeZulueta, and entitled A Novel Neural Network Based System for Assessing Risks Associated with Information Technology Security Breaches, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved

Melvin Ayala

Tadeusz Babij

Malcolm Heimer

Robert Oikawa

Ana Pasztor

Naphtali Rishe

Malek Adjouadi, Major Professor

Date of Defense: November 12, 2004

The dissertation of Monica DeZulueta is approved.

Dean Vish Prasad
College of Engineering

Dean Douglas Wartzok
University Graduate School

Florida International University, 2004

DEDICATION

To my family, Julian, Elizabeth, Julian Alexander, Concepcion, Luis Alberto, Eugenia, Isabel, and Luis Alberto, Jr..

ACKNOWLEDGMENTS

I wish to acknowledge my sincere appreciation and thanks to my advisor Dr. Malek Adjouadi who has patiently guided me for so many years. My deepest thanks go to Dr. Melvin Ayala whose contribution with Neural Studio was invaluable. Many thanks go to Dr. Robert Oikawa for his assistance and knowledge of security principles. I would also like to thank my committee members Dr. Malcom Heimer, Dr. Naphtali Rishe, Dr. Tadeusz Babij and Dr. Ana Pasztor for their extra support and attention.

I am very thankful to have had the opportunity to have worked with some of the very best graduates from the Center for Advanced Technology and Education (CATE). I am also very thankful for the expertise and assistance that several of my Microsoft colleagues such as Greg Roberts and Kimberly Matlock offered.

Most importantly, I wish to extend my sincere gratitude and love to my family for their undying support for my work and studies. Their love and patience has been immense.

This work has been supported by Microsoft that generously supplied the access to data that was used to evaluate the analysis approaches and to the National Science Foundation and Office of Naval Research for their invaluable support provided under grants EIA-9906600 and N-00014-99-1-0952.

ABSTRACT OF THE DISSERTATION

A NOVEL NEURAL NETWORK BASED SYSTEM FOR ASSESSING RISKS ASSOCIATED WITH INFORMATION TECHNOLOGY SECURITY BREACHES

by

Monica DeZulueta

Florida International University, 2004

Miami, Florida

Professor Malek Adjouadi, Major Professor

Security remains a top priority for organizations as their information systems continue to be plagued by security breaches. This dissertation developed a unique approach to assess the security risks associated with information systems based on dynamic neural network architecture. The risks that are considered encompass the production computing environment and the client machine environment. The risks are established as metrics that define how susceptible each of the computing environments is to security breaches.

The merit of the approach developed in this dissertation is based on the design and implementation of Artificial Neural Networks to assess the risks in the computing and client machine environments. The datasets that were utilized in the implementation and validation of the model were obtained from business organizations using a web survey tool hosted by Microsoft. This site was designed as a host site for anonymous surveys that were devised specifically as part of this dissertation. Microsoft customers can login to the website and submit their responses to the questionnaire.

This work asserted that security in information systems is not dependent exclusively on technology but rather on the triumvirate people, process and technology. The questionnaire and consequently the developed neural network architecture accounted for all three key factors that impact information systems security.

As part of the study, a methodology on how to develop, train and validate such a predictive model was devised and successfully deployed. This methodology prescribed how to determine the optimal topology, activation function, and associated parameters for this security based scenario. The assessment of the effects of security breaches to the information systems has traditionally been post-mortem whereas this dissertation provided a predictive solution where organizations can determine how susceptible their environments are to security breaches in a proactive way.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

CHAPTER 1

Introduction

There have been great strides and innovations in the field of information technology as in the case of the increases in computing power as well as the proliferation of computing power. Over the past decades, the access to computers has changed the way people do business and even interact with each other as can be seen in the extensive usage of email and instant messaging. The increased usage of computers in people's daily life has led to an increased dependency on computers. This means that if there are problems encountered with the information technology, people's lives are disrupted. Security breaches have been a great source of these disruptions to the computing world.

Security is still very reactive, and this study proposes more proactive measures when dealing with security. Examples of the reactive nature of security measures are the facts that most companies do not implement security countermeasures until they have suffered an attack and that companies sometimes fail to apply patches let alone test the patches in a timely manner. Sometimes a patch to a security breach is available six months prior to the release of a virus that exploits the vulnerability, and the computer personnel fail to install the patch the removes the vulnerability. One reason that companies do not deploy patches in a timely manner is that they feel overwhelmed with the number of patches that are being released.

Before detailing the proactive or even reactive measures, it is best to have an understanding of what the various security breaches are. It can often be seen in the media that the attacks such as viruses, worms, or Trojan horses have affected organizations, but there is a failure to really differentiate between the attacks. For example, a virus is an attack that requires a host to propagate or to even be active. Common examples of viruses are the ILOVEYOU virus which is a Visual Basic Script (VBS) that is sent as an e-mail attachment. [1] This virus required that an individual run the vbs script by means of clicking on the attachment. Since the attachment is a VBS script, the operating system would make the association that the VBS scripts are invoked and executed using the script engine. This association was done when a user opened the attachment; thereby, executing the script which in turn would iterate through the user's mailing list contacts and email itself to all the contacts in the mailing list. In addition to this, it would overwrite each graphic file that it found on the user's machine with the copy of the script.

As opposed to a virus which requires the use of a host, the worm is a stand alone attack, thereby, not requiring the use of a host. This malicious code self-propagates itself across the networks. A common example of a worm is the Blaster attack which exploited a buffer overflow vulnerability in Microsoft's implementation of the Distributed Common Object Model (DCOM) Remote Procedure Call (RPC) interface within the operating system. [2]

Another type of attack that is common is known as the Trojan horse. A Trojan horse refers to a program that is placed on the computer without being detected. The Trojan horse gives the attacker who placed the malicious code on the computer unrestricted access to data. Trojan horses have been known to access confidential data and transmit it back to the attacker. Back Orifice is an example of a Trojan horse which installs its server piece on a unsuspecting victim's object and is controlled by its client piece on an attacker's machine. [3] Unfortunately, most anti-virus software applications fail to detect the Trojan horse because the anti-virus engine is primarily focused on the scanning for viruses.

Three different classes of malware based attacks have been mentioned, but a key factor is that these attacks could have been controlled and not have had an impact on the victimized corporations had certain security measures been present. Security relies on three key important factors: people, process, and technology. Although the attacks that were discussed earlier are directed toward software, technology is not the only way to mitigate against such attacks. In fact, 70% of attacks can be prevented by having the people and process in place, meaning that the use of technology accounts for only 30% of mitigating against a security attack. For instance, the ILOVEYOU virus relied on the host running with administrator privileges. If a corporation had the policy of least privilege in place meaning that users are not allowed to use administrative privileges to run applications, the virus would not have been able to iterate through the contacts in mailing list or overwrite the graphic files. Most of the users that were not affected by the ILOVEYOU virus were spared because the user did not click on the attachment rather than because they had the right policy in place.

Information security breaches have cost organizations in the upwards of 200 millions of dollars in the US alone. This cost encompasses physical attacks such as theft as well as software security attacks. The cost associated with property theft is roughly 7 million dollars while the software attacks has costs of over 65 million dollars. It is evident that these are staggering costs, yet there are a great deal of costs that do not even get reported. [4] The costs listed apply to US firms. Organizations in other countries are also plagued by security breaches. In fact, the Department of Trade and Industry reported that security breaches have cost businesses in the United Kingdom losses in the billions of pounds. [5]

Currently, there is no easy way to gauge how susceptible a corporation is to a security attack. In this study, a way of determining an organization's susceptibility to a virus attack is proposed, implemented, and detailed. The study includes determining which are key parameters in establishing and maintaining a secure system. People, process and technology are the three important aspects, and there are parameters associated with each of these areas. In order to discern what are the key parameters that have an affect on the outcome which is a secure system, a sensitivity analysis was performed. The study also undertook the effort of determining the relationship between the parameters in the areas of people, process, and technology to security. In essence, this study has three goals which are to determine what is the relationship between people, process, and technology to security, to perform a sensitivity analysis to discern what are the key inputs needed to have a secure system, and to build a predictive model that can determine the degree of risk to a virus attack an organization has.

Although part of the study is focused on assessing the degree of vulnerability that an organization may be susceptible to a virus, the results of the study can be utilized to assess a corporation's vulnerability to security breaches such as Trojan horses and worms. These security breaches can be passive or active. Passive attacks refer to an attack that does not change the state of the information system and is designed only to gain access to the system whereas active attacks do result in unauthorized changes to the state of the information system. This study is focused on the active attacks, namely, worms, but the assessment results can be utilized to determine how vulnerable an organization is to a passive attack.

The motivation to pursue this course of study was the fact that there is no way to properly assess the degree of risk that an organization may be facing when a security breach takes place. It is most astounding that there is no predictive or proactive methodology considering the exorbitant amount of money that a security breach costs an organization. Sometimes, the security breaches not only affect the cost, but they also affect the branding and the perceived good will of the organization. There have a been documented attacks in which the attacker obtained confidential information such as the social security numbers of customers or credit card numbers and the attacker published the confidential information. The public loses faith in the company to safeguard the confidential information. This loss of faith usually results in lost business. An example of this is Wells Fargo case where customers' security numbers were released. [6]

It is important to note that there is no efficient or automated proactive methodology to assess the risk; in fact there is on going research that centers on monitoring network traffic patterns and determine if a passive attack is being attempted. This type of research is centered on reactive measures. An expert system monitors network traffic for load assessments and attempts to discern patterns to see if an attack is being performed. Modern day intrusion detection systems work in a similar fashion. An intrusion detection system (IDS) is defined as a defense mechanism that attempts to discern network activity. By its very definition, an IDS is a defense mechanism meaning it is entirely reactive. Another flawed aspect of an IDS in terms of its ability to be proactive is that it only addresses the technological aspects of security. It is imperative to emphasize that technology is only an element of security. In fact, it only constitutes about 30% of security. [8]

Because of the necessity of security especially in these days of post September 11 and the fact that security is often viewed in a reactive manner, this is why the study was proposed in order to view security in a more proactive manner. Since a more proactive methodology was the goal of the project, a model that serves as a predictor was developed. It was determined that an artificial neural network (ANN) is a viable fit in this endeavor because ANNs can provide a predictor value given the proper training. The development and training of the model requires much data. In this study, the data addressed the three key facets of security: people, process, and technology. A critical factor of the innovation of this study was that it took into account other facets of security beyond the normal scope of previous studies which just focus on the technological aspect of security.

Using data that was collected detailing the current environments of Microsoft's customers globally, a neural network was developed, trained, and validated. The neural network was developed using a tool, Neural Studio, developed at the Center for Advanced Technology and Education at Florida International University. The data were obtained with the customers' consent in fact, a website was established so customers would voluntarily submit profiles about their environments. The data were voluntarily submitted by customers who were eager to see a study of this magnitude be successful. The customers filled a survey which would give the research an understanding of the people, process, and technology that was in place at the customer site. The survey consisted of over forty questions. Since the answers to some of the questions were qualitative in nature, answers were quantified. Prior to feeding the data into the Neural Studio, the answers were also normalized meaning they were adjusted to values ranging from 0 to 1.

In order to better communicate the contribution of this work, this dissertation has the following structure:

- Chapter 1 provides an introduction of the current problem of being reactive with respect to security and why there is a need to make improvements in security. In addition, it provides a brief overview of what are different types of security breaches.

- Chapter 2 introduces the three key factors of security which are people, process and technology. It details what contributions each factor provides in ensuring a secure environment. This chapter also establishes the security terminology that are used throughout this dissertation.

- Chapter 3 focuses on the approach that was utilized to build the predictor model. It provides reasons as why an artificial neural network (ANN) was chosen to develop the predictor model. A background on artificial neuron networks is furnished in order to provide a foundation of knowledge for the subsequent chapters.

- Chapter 4 details the how the predictor model was designed, trained, and validated. In this chapter, the methodology was validated using generated data. This chapter discusses the selection of the neural network topology, the activation functions, and the activation function parameters.

- Chapter 5 builds upon the knowledge gained by implementing the model using generated data, and it applies such insight to building a model based on actual customer furnished data. This chapter discusses the collection of data and the normalization procedures that were applied to the data, in addition to detailing the selection of the topology, activation functions, and the associated parameters.

- Chapter 6 provides a discussion of the results. The results associated with the model that was built using generated data are discussed as well as providing a detailed discussion and analysis of the results pertaining to the model that was implemented using actual collected data

- Chapter 7 consists of concluding remarks as well as listing future enhancements to this already significant body of work.

CHAPTER 2

Security Principles

Before there is an attempt to address the security problems that plague companies, it is imperative that the overall security principles be well understood. There is a tendency to attack security problems from a technology perspective only instead of taking a holistic stance. In this study, security was viewed from three key sides: people, process and technology. Before delving into the implementation details of this study, the key security principles will be discussed and some key security terminology will be defined.

2.1 Security Terminology

The goal of security professionals is to ensure that an information system meets the following requirements:

- Availability
- Integrity
- Confidentiality

These requirements are the most basic ones that need to be met, and ensuring that there are controls to certify that three requirements have been addressed is fundamental. Availability centers around the information systems being able to be used and accessed. For instance, if there is a security breach that causes the database server to be down, the information stored on that server is rendered unavailable. With availability, there are usually two associated topics of discussions, denial of services and loss due to a natural disaster. Denial of services often refers to an intruder whose actions burden a computing system so much that valid users cannot utilize the system. Controls that authenticate and authorize only valid users to perform duties can be useful to ensure availability. Loss of computing services due to a natural disaster is address by contingency planning and disaster recovery methods.

Integrity refers to protecting the state of the information and ensuring that the information has not been tampered with. Systems where integrity is of the utmost importance are government systems such as air traffic control systems and military weapons systems. Controls associated with the integrity of data are:

- Least privilege
- Separation of duties
- Rotation of duties

Least privilege refers to granting access to only what is needed to perform the job duties. Users are often given administrative access when their job function does not deem it necessary. This is often the case in the type of access that a user has to his/her own computer. It is important to note that users should only modify data through well-formed transactions that are well documented to ensure and maintain data integrity. Separation of duties is targeted at ensuring that no one individual is given control of a transaction from the beginning to the end. Control is segmented, and control of each segment is assigned to different individuals. This control is to ensure that personal gain cannot be achieved by having access to the entire transaction. The rotation of duties refers to periodically changing job assignments to avoid users from collaborating in order to gain access to the entire transaction.

Confidentiality refers to keeping information private and not disclosing that information. Privacy is critical to industries such as the healthcare and financial industries where patient information or credit information needs to be kept confidential and its access closely guarded. These industries are subject to governmental oversight. Controls focused on authentication and authorization can help address the confidentiality concerns so that only authenticated and authorized users can have access to data.

In order to meet the three requirements of availability, integrity and confidentially, technical controls are usually put in place to address the three key requirements. These controls often center on the following:

- Authentication
- Authorization
- Auditing
- Non-repudiation

Authentication refers to validating that the user is who he/she says he/she is whereas authorization is giving permission to the validated user to do what he/she needs to do. The first thing to do is validate the user before allowing the user to carry out any actions. Auditing is the ability to track the user's activities. This can be accessing a file or attempting to access a server or even attempting to enter a physical location such as the server room. Non-repudiation is the ability to ensure that a transferred message was received or sent by parties claiming that they did perform said actions. For instance, a user may deny sending an email. If the email was signed, it can easily be verified that he indeed sent that email.

Other key terms that are often associated with security breaches also need to be reviewed. These key security terms are:

- Threat
- Safeguard
- Vulnerability
- Attack
- Patch

A threat represents a potential danger to business assets. All threats should be calculated in terms of business risk. For instance, a threat can be the unauthorized access to a customer's credit information. A threat can manifest itself in the loss of privacy, availability, and/or data integrity. A safeguard is a measure that counters the threat. This measure can be technology, people, or process. An example of a safeguard may be the process of requiring employees to use a badge to gain entrance to a facility so the threat of non-badge personnel accessing the facility is lessened. A vulnerability is a weakness in a safeguard or an absence of a safeguard that can be exploited. Leaving ports open in a firewall is classified as a vulnerability. An attack refers to a threat that was carried out by exploiting the vulnerability. The various viruses that have penetrated information systems and corrupted files such as the ILOVEYOU virus are considered examples of attacks. Patches are designed to eliminate the vulnerabilities that may exist. Usually upon the discovery of a vulnerability, platform vendors will release a software update which is referred to as a patch to address the vulnerability before an attack can be made to exploit it.

2.2 People and Process

Although people and process are two distinct factors in security, they are closely tied together in that the processes are created by people and implemented for people to follow. This section will detail how people and process can impact security.

People and their behavior play a pivotal and critical role in maintaining a strong security. Social engineering demonstrates how attacks on computer information systems may be successfully carried out by exploiting weaknesses in humans. An example of this is where unassuming individuals have pretended to be government officials and have been given access to secured areas because the security guards thought that the visiting personnel were federal officers. [9] One way to guard against people being the weakest link is having processes and policies encompassing training and awareness in place to ensure that people become the best defense instead of the weakest link.

A key person that can assist in ensuring that processes are in place is the security officer. Companies should invest in a qualified chief security officer that can provide the needed guidance and set the overall security policy for the company. The security officer would create the overall security policy and ensure that the guidelines, standards, baselines and procedures adhere to the policy.

The security policy refers to the overall corporate policy. In essence, it establishes the company's attitude toward security. Standards are needed to detail the mandatory actions or rules that support the corporate policy that every employee must adhere to. For instance, a standard may dictate that all computers in a corporation must run a specific anti-virus software. In addition to standards, companies also need baselines which provide mandatory descriptions how to implement security packages in order to ensure a consistent deployment. The guidelines refers to recommendations on how to deal with security issues whereas the procedures are the step by step instructions on how to handle security issues. If an organization wishes to have an environment that exhibits security awareness, it needs to establish a corporate security policy, standards, baselines, guidelines, and procedures. It is not enough to just have these documents created. [10] Employees need to live by them and use them. Ironically, some organizations have these documents, but they do not enforce them which renders them useless. For instance, there may be procedures when an employee is terminated. The procedure may dictate that all access, whether it be physical or remote, to network resources be terminated as well as having the employee escorted by security guards. If this procedure is not followed, the terminated employee may implant a virus or erase data on an application server.

2.3 Physical Security

An often overlooked factor of security is physical security. Theft of computer property has cost US companies an excess of 7 million dollars [4]. Physical security should be considered a fundamental part of security. When securing physical equipment, servers should be the first priority. Most if not all, software technical controls can be defeated easily if an attacker has physical access to a machine. For instance, a malicious user could boot a machine using another operating system running off a CD, grab the password file and crack it. This demonstrates how physical access trumps software technical controls. There should be guidelines and procedures in place that detail the secured physical access to the server rooms. Access to information needs to be restricted whether it is technological restrictions and/or physical restriction.

As part of physical security, the use of escorting terminated employees should be considered as well as escorting guests. These circumstances needed to be addressed in the guidelines and standards.

Theft is not the only consideration of physical security; environmental concerns should also be considered as part of physical security. For instance, redundant network connections, fire suppression, and power connections should also be part of the physical security plan because of their impact on availability. [10]

2.4 Training

Before the policies, guidelines, and procedures can be enforced, they need to be shared and communicated to the employees. Training is how an organization can effectively communicate the security policies, the guidelines, and the procedures. Security awareness training is needed for all employees and should be done periodically so that security becomes foremost in people's minds. Those individuals in the information technology (IT) and security departments should have specialized training focused on technologies that safeguard information. Since technology changes at a staggering pace, those in IT and security need access to current training, periodically.

Training is only part of the story. In order to achieve the goal of a secure organization, security needs to be foremost in the employees' minds so that it becomes just second nature. This means that even the development of software should also incorporate security best practices as well as the physical access should incorporate best practices.

In addition to offering security awareness training and specialized security training, it is important to ensure that personnel are well versed in security practices. Key security personnel should be experienced professionals with experience in establishing security policies, guidelines, standards, baselines and procedures in addition to having experience in enforcing them as well.

2.5 Privileges

Other processes that need to be in place revolve around *least privilege*. This refers to running resources using non-administrative privileges. There is a tendency to run applications with administrative privileges even if the application does not require such privileges. For instance, many employees run as local administrator on their Windows machines when all they wish to do is use a word processor. Malware may run at a privilege level equal to that of the logged-on user, and thus gain the same ability to control and administer the computer as the local administrator. By enforcing the use of least privilege, the company may reduce the damage that a security breach can do.

Another facet of privileges is ensuring that no one employee has control over an entire transaction of work. If one employee is given that much power, there may be an opportunity to violate or bypass any controls that exist in the transaction. This type of opportunity can be avoided by applying separation of duties where no one individual has control of an entire process. For instance, an enforcement of separation of duties would require two separate parties to approve expenditures and release the monies instead of having just one person approve the money and having physical access to the money. It would be too easy for the person to make fake approvals and keep the cash.

Rotation of duties refers to the recommendation that duties should be routinely rotated so collaboration can be avoided. In an environment where there is separation of duties, collaboration is needed to gain control over an entire transaction. Too much time on the same assignment may lead to complacency and lend itself to employees collaborating, thereby making the separation of duties ineffectual.

2.6 Patch Management Process

Companies need to have a patch management process. This process should detail the procedures for testing patches targeted for both client and server computers and the procedures for deploying patches to both clients and servers. Along with the procedures, there should be deadlines as to when the patches will be fully deployed across the enterprise.

There have been instances where software vendors have released patches six months prior to the creation of a virus that can exploit the vulnerability, and organizations have not deployed the patch in a timely manner. Deploying is only one aspect of the patch management process; testing of the patch needs to occur before any roll out is done. For instance, a patch may somehow affect a third-party or in-house developed application. Thorough testing of a patch needs to occur before any deployment is performed to ensure that the patch does not affect the operating applications. Figure 2-1 depicts a flow of the patch management process that can be utilized to roll out patches to production servers. A similar process can be done with client machines. [11] There are software packages such as Microsoft's System Management Software that can perform the deployment to clients machines without requiring physical access to a client machine. Such tools also provide auditing features that detail if the deployment was successful and when it was performed.

2.7 Password Policy

Passwords are useful and common tools for validating users. Because they are so common, it is necessary to ensure that they are not shared. There needs to be a policy that enforces the uses of password. Using passwords is not enough; there needs to be a requirement that the password be a strong password. Strong passwords impose minimum limits on size and the characters that can be used and how often a portion of the password can be reused. There is a tendency for users to use an easy-to-remember password such as their name and then change a portion of it periodically in a predictable fashion such as adding "1" and "2" to remain within the company policy for changing passwords. to devise a password and just simply change a portion of it periodically. This means that the passwords could be obtained with greater ease, thereby making the company more at risk to a security breach. Since passwords are susceptible to dictionary attacks, there needs to an enforceable policy that requires strong passwords. Dictionary attacks refers to finding password using a words that can be found in a pre-defined list of words such as a dictionary.

2.8 Software Development Process

When an organization opts for developing application software in-house, security needs to be included in the design phase and not considered at the end of the development process. [12]

One of the reasons that security is often overlooked in the design phase is that security is often considered inversely proportional to usability. Many users and even developers tend to find that a very secure system is not very user friendly. A user friendly system having no passwords may not be available because of security attacks. People need to recognize the value of security and include it in their design. The goal should be secured by design. In fact, about 50% of the security bugs are often associated to design errors. [13] Processes that reduce security flaws need to be established.

2.9 Threat Modeling

A useful methodology in assessing threats and vulnerabilities is known as threat modeling. It is a detailed process that should be incorporated early in the product life and should be

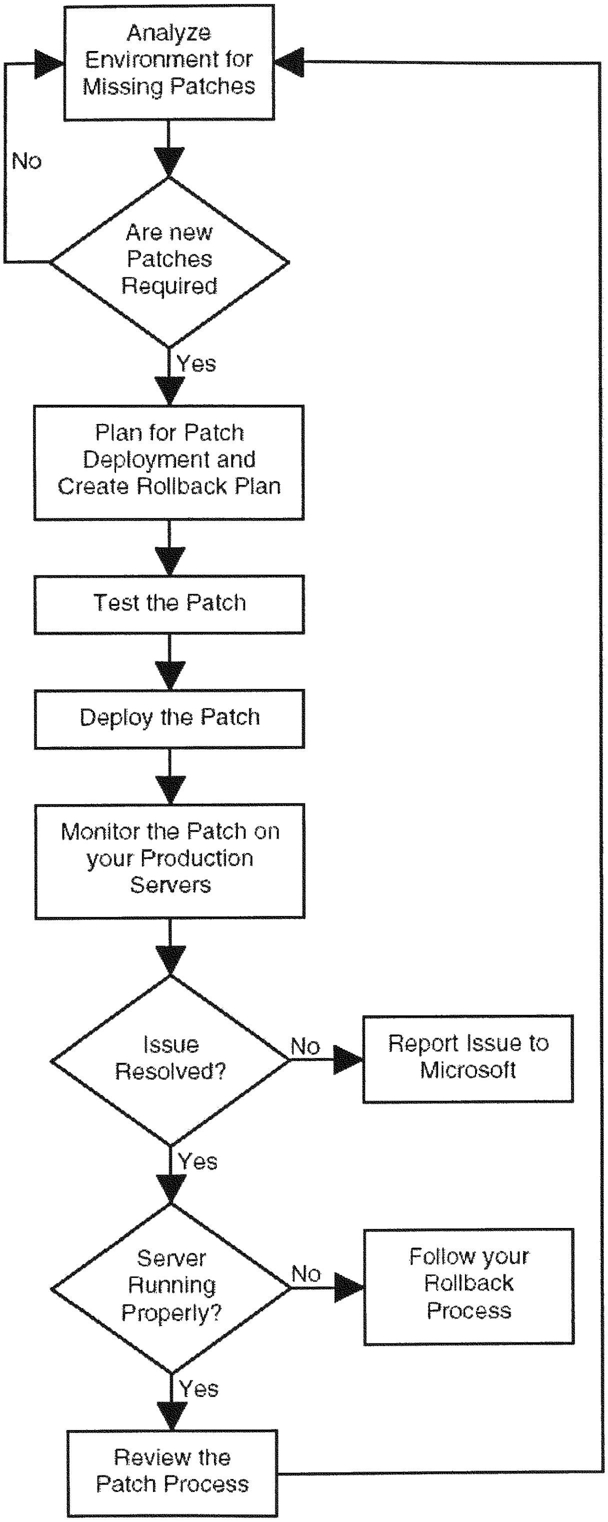

Analyze Environment for Missing Patches
No
Are new Patches Required
Yes
Plan for Patch Deployment and Create Rollback Plan
Test the Patch
Deploy the Patch
Monitor the Patch on your Production Servers
Issue Resolved?
No
Report Issue to Microsoft
Yes
Server Running Properly?
No
Follow your Rollback Process
Yes
Review the Patch Process

Figure 2.1: Patch Management Process

maintained throughout the product's life cycle. The process of threat modeling can be defined by the following set of steps:

- Create a team to perform the threat modeling
- Decompose the healthcare application into its key components
- Ascertain the potential threats to the system and its components
- Rank the threats
- Decide on effective ways to address the threats
- Evaluate which techniques may be applied to address the risks
- Establish which technologies are suitable to implement the chosen techniques

Threat modeling by its indefinite and encompassing nature is not a simple task. The team needs to include a security analyst as well as having representation from the disciplines that are involved in the solution life as well as those disciplines associated with the solution functions. Paradoxically, hackers are well suited for the role of security analyst because there is a tendency in hackers to search for the vulnerabilities. The project life cycle related disciplines may include networking, developers, operations, training, and testing; whereas the functional disciplines may include users such as clinicians and insurance representatives in the healthcare landscape.

The next step is to identify the subsystems (components) that constitute the solution. For software-based solutions, common decomposition tools can be UML (unified modeling language) diagrams or the DFD (data flow diagrams). For the hardware-based systems, block diagrams can be used. The key part of this step is to identify the boundaries on the subsystems and not the functionalities. This means that software lines of code or schematics are not the object of the analysis at this junction, but it is rather the study of boundaries of the subsystems that are at the core of the analysis. As part of the decomposition it is recommended to study the interfaces and interactions among the subsystems. The interfaces and interactions may include events, triggers, requests, and responses the subsystems will generate or respond to. During this phase, the decomposition of the system should not typically go beyond four levels [13].

2.10 Classifying Threats

The threats can be classified using the STRIDE categorization [13] developed by Microsoft. Although it is usually applied in a software based scenario, it can be applied to classify threats in general. STRIDE is an acronym which stands for six classifications:

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

The spoofing of identity refers to an attacker impersonating a known user or server. The tampering of data means when data are maliciously altered. Repudiation refers to a user denying that he/she performed an act, yet there is evidence that the act was committed by that user. A denial of service refers to the valid user being unable to access a system because a maliciously attack has consumed the system resources. The elevation of privilege refers to an attacker obtaining privileged access giving him/her access to the system. The different classes of threats can be interrelated. For instance, spoofing of identity may result in the elevation of privilege. Another important fact to retain is that an asset may be the target of more than one class of threat.

2.11 Identifying Threats and Vulnerabilities

Once the system has been decomposed into components, it is necessary to determine what the system's vulnerabilities are and which threats can exploit those vulnerabilities. Threat trees can be used in identifying those vulnerabilities. Threat trees refer to applying the concept of fault trees to security. The use of fault trees is a common way of identifying failure modes in hardware. Threat trees show how an attack can manifest itself and how a system can be compromised by showing the decision-making process that an attacker may apply to attack the key components. As the components are attacked, the entire system is getting compromised. The listing of threats should contain several details in addition to just the threat title and the type threat. The list of threats should include:

- Threat – a description of the threat

- Threat target – key component that is susceptible to attack

- Threat type – STRIDE classification

- Risk – calculated consistently according to desired method

- Attack tree – tree showing how an attack will manifest itself

2.12 Ranking Threats

Risk assessments are useful for assessing the risks and vulnerabilities of protected information. After the threats have been identified, the ranking of the threats is done. Such ranking is based on the risk associated with each threat. There are various methods of calculating risk. One method is called DREAD. [13] Calculating risk and its pre-requisites are an analysis process essential in the identification of threats and vulnerabilities that the healthcare system faces. In the complexity spectrum, DREAD is considered to be somewhat moderate in complexity in that it takes into account more factors than an overly simplified methodology which will account for a minimal of two factors such as criticality and likelihood. A very complex method will instead involve complex calculations such as regression analysis. DREAD is an acronym that stands for:

- Damage potential

- Reproducibility

- Exploitability

- Affected users

- Discoverability

Damage potential refers to the criticality of the vulnerability. Reproducibility signifies if the threat can exploit its target in a predictable manner with respect to time. Exploitability metric measures how much effort or how easily the asset can be exploited. The value assigned to affected users would reflect how many users would be affected by the threat. The discoverability factor refers to how easily the vulnerability will be discovered. After each metric has been assigned a value between 1 and 10 with 10 having the highest impact, the risk associated with each threat is determined by summing each metric's assigned value and dividing by the number of metrics which in this case is 5.

2.13 Mitigating Threats

Table 2-1 showcases a sampling of techniques that can be used to mitigate the risks associated with the different threat types.

To determine which mitigation technology should be applied, it becomes necessary when designing the system to see what are the implementations associated with the technique. Examples of software authentication technologies are forms-based authentication, Windows authentication, and Kerberos authentication. Authorization technologies that are found in software implementations are access control lists, privileges, IP restrictions, and server-specific permissions. These technologies have been used to address denial of service threats, information disclosure threats, spoofing identity threats, and tampering with data threats. The use of logging in both operating systems and application server systems are useful technologies associated with the mitigation technique known as audit trails which addresses the threat of non-repudiation.

Table 2.1: Mitigation Techniques Associated with Threat Types

Threat Type	Mitigation Technique
Spoofing identity	Appropriate authentication Protect secret data Don't store secrets
Tampering with data	Appropriate authorization Hashes Message authentication codes Digital signatures Tamper-resistant protocols
Repudiation	Digital signatures Timestamps Audit trails
Information disclosure	Authorization Privacy-enhanced protocols Encryption Protect secrets Don't store secrets
Denial of service	Appropriate authentication Appropriate authorization Filtering Throttling Quality of service
Elevation of Privilege	Run with least with privilege

2.14 Technology

The technologies that are detailed in this section can be applied to the software development process as well as technologies that can be applied in general for securing information technology systems.

To ensure that a system exhibits the characteristic of a secured system, certain technologies can be implemented where it is deemed appropriate. This section will provide an overview of the various technologies and what security features they implement.

One technology that companies often treat as the proverbial *silver bullet* that will protect them from any attacks is the anti-virus software. Although anti-virus software is important to implement across the enterprise, it is only one step and by no means the only step. Installing anti-virus software is only a start; ensuring that the virus signatures are always up to date is the critical factor with regards to using anti-virus software.

Firewalls are another technology that many companies tend to use. A firewall is a hardware or software defense mechanism that monitors traffic going through and determines if it adheres to a security policy. For instance, a firewall can block traffic on designated ports. Firewalls are usually placed to separate the Internet from the corporate network. These firewalls usually should block all ports with the exception of the ports that handle standard internet protocols such as HTTP and HTTPs. Too further protect the corporate information assets, companies tend to separate their web servers from their *backend* systems. The *backend* systems are usually the databases or mainframes that house business data. The firewall that separates the *backend* systems should block all unnecessary ports. The zone that lies between two firewalls is called the perimeter network. The perimeter network is the area where web servers are placed. There is a tendency to think that by having firewalls the company is free of problems. Again, firewalls are only one very small way of protecting the corporate resources. There are also different types of firewalls some of which are better than others at inspecting the traffic. Another important fact is that upgrades to firewall software should always be current. Along with firewalls there is a technology that monitors the traffic and makes decisions based on the traffic patterns. These systems are referred to Intrusion Detection Systems (IDS). IDS systems usually are based on a rules-type engine such as an expert system. They monitor the traffic to see if an Internet Protocol (IP)-based attack such as SYN Flood is being done. The SYN Flood attack is when a machine continually initiates TCP/IP connections forcing the receiving machine to continually allocate memory and allocate resources to handle the connection requests. This ties up the receiving machine so that it cannot handle valid connection requests, thereby resulting in a denial of service attack.

2.15 Authentication and Authorization

Some key requirements for a secure system are authentication and authorization. Mechanisms such as directory services can be utilized for authentication and authorization. Directory services can determine if the user is a valid user. Based on the access control lists (ACL), directory services can determine if the validated user should be given access to system resources. Access Control Lists detail what capabilities a principal has on a resource. These capabilities may be read, write, and execute. When an authenticated principal wishes to access a resource, the system checks in the ACL to see what can the principal do on the resource. The system will grant access according to the ACL. Examples of system resources can be a file share repository and a printer. The use of both directory services and ACLs can address authentication and authorization concerns. Directory services are not always suitable for authentication as in the case of an internet web application, but it may be suitable for an intranet application and to some extent an extranet web application. An authentication mechanism which would verify users against account information stored in a database server is a more suitable mechanism for an internet web application. [14]

In essence, authentication requires that proof also called credentials be supplied to certify that the user is a valid user. Credentials can be:

- Something that is known as in the case of a password or Personal Identification Number (PIN)
- Something that is owned such as a smart-card
- Something that is unique about the user such as a bio-metric possibly a fingerprint

With respect to authentication, the use of two-factor authentication is considered far superior than simply using one factor authentication such as a password. Two-factor authentication utilizes two types of credentials. For example, two-factor authentication can be implemented as something that is known such as a password and something that is owned such as smart-card.

2.16 Non-repudiation

Analyzing the characteristics of a secure system, the ability to have non-repudiation is key in that it provides a guarantee that the sender did in fact send the message as well as the recipient received the message. Non-repudiation is usually accomplished by means of digital signatures. Digital signatures rely on a private and public key infrastructure. A message having passed through a cryptographic function is said to be hashed. The hash is then encrypted with the sender's private key and sent. The recipient will decrypt the message with the sender's public key. This message is said to have been digitally signed; therefore, the recipient can verify that the sender was indeed a trusted party.

2.17 Auditing

Auditing refers to tracking system activities and having a trail of the recorded activities. These activities can be successful and unsuccessful attempts to access a resource. Collecting the system activities is critical in the review and analysis of how secure a system is. The auditing activity is entirely reactive.

There are different types of trail or logs that are associated with auditing. For instance, platform vendors offer an event log that lists the tracked system related events. Some of the events that can be monitored are:

- Accessing system resources such as printers or file shares
- Analyzing network traffic and connections
- Attempts to logon
- Modifying records

Other types of logs are the web server logs and the database server logs. All the different types of logs need to be reviewed regularly. Another consideration is to have an alert mechanism that would notify operational personnel if certain critical events occur. These events can be high CPU utilization or extensive memory utilization for an extended period of time.

2.18 Internet Protocol Security (IPSEC)

Since the Transport Control Protocol/Internet Protocol (TCP/IP) was not designed to be a secure protocol but rather a reliable protocol, packets associated with the TCP/IP stack can be easily faked. TCP/IP offers no authentication, authorization, privacy, and data integrity. IPSEC attempts to address the security problems associated with the TCP/IP stack by relying on a key exchange to offer the much needed authentication, authorization, privacy, and integrity. All traffic that is exchanged between IPSEC-secured servers is encrypted and integrity-checked.

2.19 Secure Sockets Layer (SSL) or Transport Layer Security (TLS)

SSL was invented by vendors, Concencus and Netscape, whereas TLS is a product of the Internet Engineering Task Force (IETF). SSL uses Message Authentication Code (MAC) algorithms to ensure data integrity. Data packets are encrypted as they travel between a client and server and vice versa. The sender and receiver obtain message integrity assurances by using a secret key and the message to obtain a MAC or sometimes called a hash. The sender sends the message and the hash to the receiver. The receiver will calculate a hash and compare with the hash that was received. If the two hashes are the same, then both the receiver and sender are assured that the message was not tampered with during the transit.

The technologies, SSL/TLS, are often used in web sites to provide encryption for confidential information such as credit information or login passwords on web sites. It also used for encrypted logins.

Both IPSEC and SSL/TLS can be used to address many privacy or data integrity concerns. Both technologies use cryptography to encrypt network traffic. Encrypted traffic increases the difficulty to sniff the traffic, hence keeping the data confidential and private. Data integrity is ensured by the use of MAC algorithms which certify that data are not tampered with.

This section has detailed the different security principles that encompass people, process, and technology. This has been an overview of the various technologies that can be utilized.

CHAPTER 3

Approach Proposed for Risk Assessment

After reviewing that the affects that security breaches have on organization, a course of study that would be yield a predictor for these security breaches was undertaken. The goal was to build a model that given a profile of an organization's information system environment would generate the degree of risk of being impacted by a virus.

This section will discuss the proposed approach that was developed for assessing risk in an organization. Two risks will be analyzed: one for the production server environment and the other for the environment composed of client machines. This chapter will detail the methodology that was designed for building the predictive model. This chapter begins with a discussion of the universal theorems for developing approximators and progresses to the selection of the type of model based on the universal theorems. The methodology developed for building the model is defined. The dataset collection and its preparation are also discussed in this chapter.

3.1 Universal Approximators

There are various methodologies that could have been utilized to build the model. The artificial neural network was selected as the methodology because neural networks are well suited for building universal approximators. Other methodologies that were considered were support vectors. Support vectors are better suited for classification scenarios. In this study, the goal was to build a predictor or approximator given certain environmental conditions.

Multilayer networks can be utilized in approximating multi-dimensional functions. This is supported by several key theorems that are universally accepted. [15-21] Some of the theorems that support that selection of an artificial neural network for the model:

- Kolmogorov's Theorem
- Sprecher Theorem
- Hecht-Nielsen Theorem

Kolmogorov's Theorem states that any continuous function defined on a closed multi-dimensional cube can be rewritten as a summation of applications of continuous function on one variable. This means that for all functions $f(x_1, \ldots, x_n)$ with $x_i \in [0,1]$ there are continuous functions ψ_i and φ_{ij} on one variable such that:

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{2n+1} \psi_i \left(\sum_{i=1}^{n} \varphi_{ij} (x_i) \right)$$

This theorem only states that the function exists meaning it is only an existence theorem. It provides no assistance in finding the functions. The functions ψ_i and φ_{ij} are dependent on the mapping function, *f*. This theorem refers to the mapping for multi-dimensional functions with *n* inputs and *1* output.

The Hecht-Nielsen Theorem is based on Kolmogorov's Theorem, and it shows that any continuous function can be approximated by a feed forward network with n inputs, 2n+1 hidden neurons, and m output nodes. Unlike Kolmogorov's Theorem and Sprecher's Theorem, both of which refer to having only one output, the Hecht-Nielsen Theorem states that any continuous multi-dimensional function with *n* inputs and *m* outputs can be rewritten.

All these theorems state that an appropriate network exists for such a multi-dimensional problem, but they offer no guidance on how to find the appropriate network. In particular, they give no indication of a method to find the appropriate weights and biases. A key contribution of this study is the development of an appropriate network to determine the risks in the security space.

3.2 Conception of the Methodology

The methodology used in building model for predicting the risk in a company's production server environment and client machine environment consists of:

- Selecting the appropriate type of model for a predictor
- Determining the artificial neural network topology
- Selecting the training methods best suited for the predictive model
- Collecting datasets
- Preprocessing the datasets
- Training the model
- Validating the model

Analyzing suitable strategies for creating a predictive model resulted in the selection of an artificial neural network (ANN) since the ANNs are very suitable for creating predictors given historical data. This selection is further validated by the universal approximators theorems presented earlier.

Before discussing the proposed approach, a review of artificial neural networks will be performed. This review will define what an artificial neural network is , how it works, and where it is being used. In addition, a brief history and the foundation of artificial neural networks will be provided.

3.3 Artificial Neural Network Fundamentals

An artificial neural network is a system that models the structure of the brain. It uses general mathematical functions to model the functions of neurons in the brain. A multitude of layers consisting of simple processing elements called neurons are used to simulate the brain. Each processing element or neuron is connected to certain neighboring elements. With each connection there are coefficients that represent the strength of the connection. The coefficient of strength is called the weight, and it usually is multiplied by the input signal. A learning phase is needed in order to adjust these strengths to cause the overall network to output appropriate results. This learning phase is often called training the network.

Artificial neural networks have been used in many industries. In the financial services, ANNs are used for predict stock market fluctuations. The military has made extensive use of ANNs because of its ability to facilitate pattern recognition. The power utility companies often leverage ANNs for fault detection.

3.4 Artificial Neural Network Overview

Similarly to biological neuron network, the artificial neural network has as its basic element, the neuron. This artificial neuron has four basic elements, which accepts inputs, applies weights, and applies an operation, and outputs the results. The figure below shows an artificial neuron and its four basic functions. [22] The inputs to the network are referred to as x(n) and are multiplied by weights, w_n. There may also be a bias which lets the output be biased without accounting for the inputs. In this simplified case, the products of inputs and weights are just summed. The summation is processed through a transfer function also called an activation function and outputted.

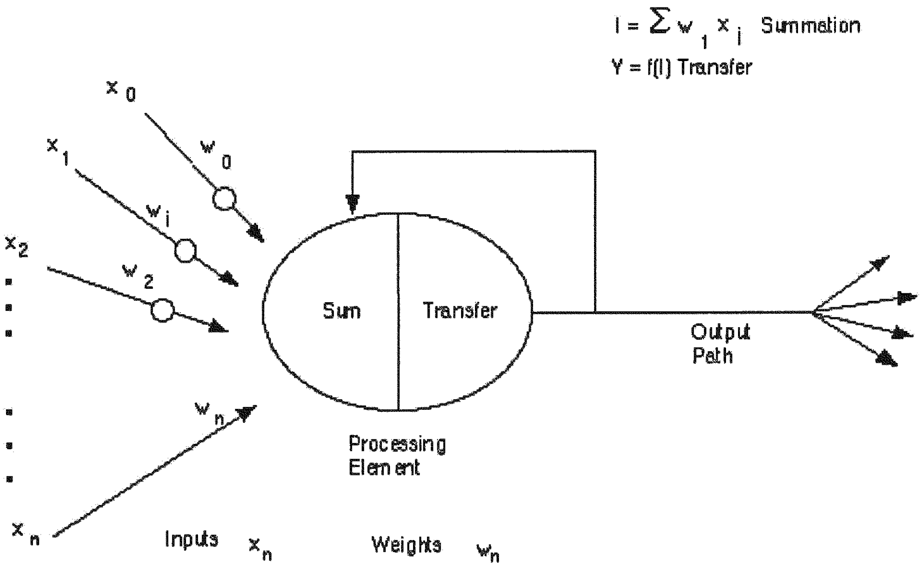


Figure 3.1. Simplified Artificial Neuron

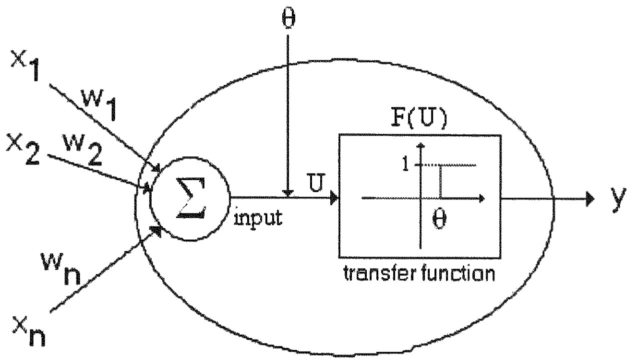


Figure 3.2 McCulloch-Pitts Model

The Hebb net is considered to be the first supervised training neural network. In this type of network, the weights change according to the training and are not fixed like its predecessor, the McCulloch-Pitts model. [22] In the Hebb model, the weights are initialized to zero and are updated as the network is trained. The Hebb model uses the following rule:

$$w_i(\text{new}) = w_i(\text{old}) + x_i t$$

where w_i is the weight associated with the input, x_i, and t is the target output. The Hebb model accepts either binary or bipolar inputs. The problem with using binary is the model will not learn if the target is 0.

The Perceptron builds upon the Hebb model. The Perceptron uses an iterative learning procedure to converge to the correct weights. The correct weights are defined as the ones that will yield the correct output for all input training patterns. There is the assumption that such weights do exist. The output of the Perceptron is defined as:

$$y = f(y_{in})$$

where

$$y_{in} = b + \Sigma\, x_i w_i$$

The activation function is

$$f(y_{in}) = 1 \qquad \text{if } y_{in} > \theta$$

$$= 0 \qquad \text{if } -\theta \leq y_{in} \leq \theta$$

$$= -1 \qquad \text{if } y_{in} < -\theta$$

It should be noted that there two thresholds, θ, and,-θ. These two thresholds define two decision boundaries and the three output spaces. In the Perceptron, the weights and the bias are adjusted when an error occurs. An error refers to the output not matching the target function. The weights are adjusted by using the following:

$$w_i(\text{new}) = w_i(\text{old}) + \alpha x_i t$$

where α denotes the learning rate and lies in the range between 0 and 1.

With the Perceptron as more training patterns yield the correct response, the learning is lessen since the weights are adjusted when errors occur.

The Adaptive Linear Neuron (Adaline) has much similarity to the Perceptron. In fact, the net input, y_{in}, is calculated in the same way. The activation function for Adaline is different and is defined as:

$$f(y_{in}) = 1 \quad \text{if} \quad y_{in} \geq 0$$

$$= -1 \quad \text{if} \quad y_{in} < 0$$

The weights are calculated using:

$$w_i(new) = w_i(old) + \alpha(t - y_{in})x_i$$

A major difference between the Perceptron and the Adaline is in the way the weight is calculated. In Adaline, the weight is proportional to the delta or difference between the target and the actual output whereas in the Perceptron the weight is the target output.

The Madaline model is simply an extension of the Adaline. The Madaline applies the Adaline algorithm to multiple layers. [23]

3.5 Design

The design of a neural network can be complex and is often iterative until a satisfactory design is developed. The following steps are considered typical of any artificial neural network:

- Determining how many layers are necessary
- Arranging the neurons in the various layers
- Selecting the type of connections between the layers as well as within a layer
- Deciding the strength of the connection by permitting the network to learn what are the suitable weights for the connection

- Determining how the neurons receive their inputs and yield their output
- Selecting what is the most suitable training method

3.6 Layers

Biological neural networks are constructed in a three dimensional way capable of a multitude of connections. Such complexity is not true of the artificial neural network. ANN are simple clustering of artificial neurons. The clustering is accomplished by creating inter-connected and intra-connected layers. The connections between layers and within layers vary. Artificial neural networks have at least three layers: an input layer, one or more hidden layers, and an output layer. The input layer accepts real world inputs, and the output layer delivers the network's output to the real world. The number of hidden layers vary. Unfortunately, determining the number of hidden layers is usually accomplished via trial and error. If the number of hidden neurons is too large, the neural net will have difficultly generalizing which is also known as an over fit. The training set will then be memorized and the network will not work with new data sets. The figure below shows the typical topology of an artificial neural network. [22]

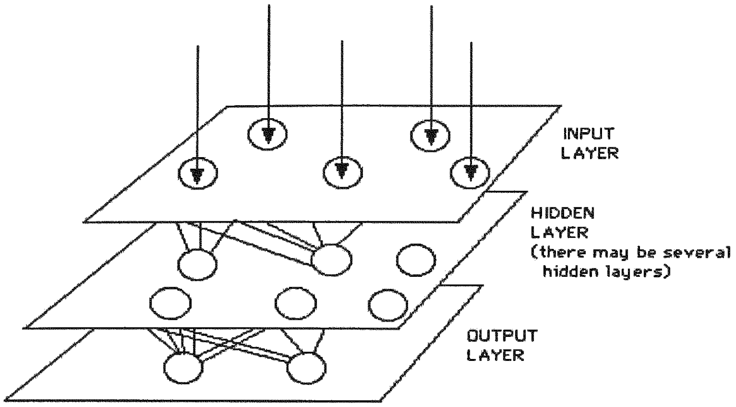


Figure 3.3. Layering Structure of an Artificial Neuron

3.7 Communications and Connections

In order for the communications to exist between the layers, there needs to be connections between the neurons. The way neurons communicate is the output of one neuron feeds the input of another. This usually reflects uni-directional communications. If bi-directional communications is desired, the output of one neuron is connected to the input of another and a separate connection going the opposite direction also exists between the neurons.

The connections between neurons can be either inhibitory or excitatory. If the connection is inhibitory, the output of the neuron causes the activity of the receiving neuron to reduce whereas in an excitatory connection the output of the neuron causes the activity to increase. In other words, the excitatory connection causes the summing mechanism to add unlike the inhibitory connection which causes the mechanism to subtract.

The neurons are usually organized in at least three layers: an input layer, one or more hidden layers, and one output layer. The connections between neurons can be across the layers which is referred to as inter-layer connections and within a layer which is known as intra-layer connectivity. There are various types of inter-layers and intra-layers connections.

The connections between layers can either be fully connected or partially connected. A fully-connected inter-layer connection refers to having every neuron in one layer connected to every neuron in the other layer. In a partially connected inter-layer connection, not all neurons in a layer have to be connected to all neurons in another layer. Another characteristic of inter-layer connections is whether the output of the second layer is fed back to the input of the first layer. In a feed forward network, the neurons of the first layer send their output to the neurons in the subsequent layer, but the first layer neurons do not receive any input back from the neurons on the subsequent layer. Unlike the feed forward network, in a bi-directional network, the subsequent layer does provide input back to the first layer. Feed forward networks as well as bi-directional connected networks can be either fully connected or partially connected.

Communications between layers can reflect a hierarchical structure in which the neurons in one layer can only communicate with neurons in the subsequent layer. Other times, communications may require bi-direction where messages are sent continuously between neurons until a certain condition is achieved. This format of bi-directional communications is called resonance.

More complex neural network have connections not only between layers but also within layers. The connections of neurons within a layer is referred to as intra-layer. The two types of intra-layer connections are recurrent and on-center/off surround. In the recurrent intra-layer, neurons receive inputs from another layer and will communicate their outputs with other neurons in the same layer until some condition is achieved and signals others to communicate their outputs of the layer to another layer. In the on-center/off surround model, a neuron has excitatory connections with itself and its neighbors and inhibitory connections with the other non-neighboring neurons. After an exchange among the group of neurons, the output is released.

3.8 Learning

The learning done in the artificial neuron network is analogous to the learning done in a human brain in that learning is accomplished through experience. Such learning is accomplished via the adjustment of the weights on the connections. The weights reflect the strength of the connection between the neurons. A neural network's learning ability is influenced by its architecture and the training methodology.

The three types of training methodologies that are associated with neural networks are as follows:

- Unsupervised
- Reinforcement
- Back propagation

In the unsupervised learning, the neurons in the hidden layer or layers do not need any outside assistance in organizing themselves. This means that no sample outputs are provided for a given set of inputs. The neurons do not have a sample to measure against. In the unsupervised training scenario, the neurons simply learn by doing.

The reinforcement learning method is a type of supervised learning. This learning method relies on reinforcement from the outside meaning that a teacher is involved. This teacher can either be a training set of data or an observer that grades the network. During the reinforcement training, the connections are continually reshuffled as the network is informed on its progress on solving the problem.

The unsupervised and reinforcement training are plagued by the inefficiency in obtaining the proper connection weights. The back propagation method attempts to address the inefficiencies of the other methodologies. In the back propagation method, the errors are filtered back, and the information about the errors is used to adjust the connections of the neurons between the layers. Back propagation is also considered a form of supervised learning. It has significant performance improvements over the other methods.

Aside from the three different, learning methodologies, learning is also characterized in one of two modes: on-line or offline. If a neural network is in the off-line mode, it is not in operating mode nor it is being used for decision-making. During the off-line mode, the neural network is adjusting the weights as it learns. Once the off-line neural network changes to operational, the weights are fixed. Most neural networks learn in off-line mode. As opposed to off-line networks which learn while the network is not operational, on-line neural networks are those that continually learn while it being used as a decision tool.

3.9 Learning Algorithms

There are various learning algorithms. These algorithms are mathematically-based algorithms that are used to adjust the weights associated with the connections. The oldest learning algorithm is Hebb's Rule. Most of the subsequent learning algorithms are simply variations of Hebb's Rule. The current learning algorithms are simplifications of the complex process of learning. Although there is on-going research into learning algorithms, in this study the following the algorithms will be reviewed:

- Hebbian Learning Law
- Hopfield Law
- Delta Rule
- Kohonen's Learning Law

The Hebbian Learning Law was introduced by Donald Hebb in his book, *The Organization of Behavior*, in 1949. [24] The rule states that the weight of a connection between two neurons is strengthened if the two connected neuron mathematically have the same sign.

Building upon the Hebbian Learning Law, Hopfield Law denotes the magnitude of strength or weakness of connection. Hopfield Law states "if the desired output and the input are both active or both inactive, increment the connection weight by the learning rate, otherwise decrement the weight by the learning rate." [22] The learning rate is usually a learning constant between 0 and 1.

One of the most commonly used algorithms is the Delta Rule. The weights are adjusted to reduce the delta or difference between the desired output and the actual output. This delta or error is propagated back from the output layer through the hidden layers. With this algorithm the least squared error is minimized. This algorithm is also called the Windrow-Hoff or the Least Means Square Learning Rule. Neural networks that utilize this algorithm are called feed forward back propagation networks.

Another learning rule is Kohonen's Learning Law. This algorithm searches for the neuron with largest output. This neuron is declared the winner. It will excite its neighbors while inhibiting its competitors. Since the Kohonen's Learning Law does not rely on the desired output, it can be used for unsupervised learning.

3.10 Sensitivity Analysis

Determining the number of inputs is critical to the modeling process. The number of inputs has a direct bearing on the amount of data that is needed during training. Since the training process as well as the data collection can be costly in terms of money and time, only relevant inputs should be used to avoid redundant, irrelevant, or misleading data. The two types of selection procedures to discern what are the relevant inputs are:

- Model-independent approach
- Model-dependent approach

In the model-independent approach, the statistical merits of the input variables affecting outcomes are directly evaluated using data. In the model-dependent approach, the inputs are evaluated in conjunction with the learning algorithms. This means that the leaning algorithm is applied to the data and the subset of inputs that yields the best result for the algorithms is utilized in the modeling. Sensitivity analysis is an example of a model-dependent approach. Its goal is to remove any irrelevant or misleading inputs from a trained neural network.

Sensitivity analysis can be viewed as a procedure to determine how sensitive an output is to changes in an input. The analysis would check if a small change in the input can cause a significant change in the output. This would signal that the outcome is sensitive to the input. An input that has a significant affect on an outcome needs to be assessed very accurately. If the analysis shows that a large change in an output has little or no affect on an outcome, the input would be classified as having low sensitivity.

Sensitivity analysis can be applied to the entire set of data or to individual patterns. The following measures can be applied to the entire set:

- Delta Error Sensitivity
- Average Gradient Sensitivity
- Average Absolute Gradient Sensitivity
- Gradient Variance Sensitivity

The Delta Error Sensitivity, $S_{DE,\,i}$, defines a delta error measure in terms of the increase of the average square error of the network, TotalError_{ANN}, when an existing variable x_i (p) for any pattern p is replaced by its mean $\overline{x_i}$ computed from all N_p patterns. This is given by:

$$\bar{x}_i = \frac{1}{N_p}\sum_{p=1}^{Np} x_i(p)$$

The delta error sensitivity $S_{DE,i}$ of the input variable x_i is defined as:

$$S_{DE,i} = \frac{1}{N_p}\sum_{p=1}^{Np} S_{DE,i}(p)$$

where

$$S_{DE,i}(p) = TotalError_{ANN}(\bar{x}_i) - TotalError_{ANN}(x_i(p))$$

The first summand of the above expression is the total square error when the training set is applied to the network.

If $S_{DE,i}$, is large, the input feature is sensible. In the case that $S_{DE,i}$ is small., the three additional sensitivity measures should be computed in order to determine if the input variable is useful.

The Average Gradient Sensitivity, $S_{AG,\,i}$, uses the average gradient of the artificial neural network's output, y, with respect to the specified input variable, x_i. This equation below denotes how $S_{AG,\,i}$ is calculated.

$$S_{AG,i} = \frac{1}{N_p}\sum_{p=1}^{Np} \frac{\partial\, y(p)}{\partial x_i}$$

The Average Absolute Gradient Sensitivity, $S_{AAG,\,i}$, uses the absolute value of the average gradient of the ANN's output, y, with respect to the specified input, x_i. The Average Absolute Gradient Sensitivity can be calculated using the following equation:

$$S_{AAG,i} = \frac{1}{N_p} \sum_{p=1}^{Np} \left| \frac{\partial y(p)}{\partial x_i} \right|$$

The Gradient Variance Sensitivity $S_{GV,\,i}$, is calculated using the variance of the gradient of the output of the neural network to the specified input variable, $x_{i.}$ This sensitivity measure is calculated using the following equation.

$$S_{GV,i} = \sqrt{\frac{1}{N_p} \sum_{p=1}^{Np} \left[\frac{\partial y(p)}{\partial x_i} \right]^2}$$

If sensitivity analysis is done for an individual pattern as opposed to applying the analysis to an entire set, the recommended measures are:

- Delta Output Sensitivity
- Output Gradient Sensitivity

If either measure is large for the given individual pattern, this shows that the output is greatly affected by changes in the input. In this case, the input variable plays an important role in the neural network's output.

The Delta Output Sensitivity $S_{DO,\,i}$, calculates the sensitivity of the an input variable to the an individual pattern by simply taking the difference or the delta of the two. The following equation denotes the calculation for the Delta Output Sensitivity:

$$S_{DO,i}(p) = y(x_1(p), x_2(p), \ldots, x_i(p), \ldots, x_n(p)) - y(x_1(p), x_2(p), \ldots, \bar{x}_i(p), \ldots, x_n(p))$$

The Output Gradient Sensitivity $S_{OG,\,i}$, uses the gradient of the individual pattern to the specified input variable, x_i. This measure is determined using the following:

$$S_{OG,i}(p) = \frac{\partial y(p)}{\partial x_i}$$

Since the goal of sensitivity analysis is to find the inputs that are relevant to the output, it is important to ensure that irrelevant inputs and misleading are removed as well as eliminating redundancy. The sensitivity measures that have been discussed earlier address this well but are not suitable in identifying redundant inputs. Redundancy is present when there is a well defined relationship between two or more input variables. In such cases, only one of the inputs is necessary. Statistical methods such as the least means square method (LMS) are useful in finding if there is relationship between two variables.

3.11 Implementing the Risk Prediction Model

Building on the knowledge gained from studying the artificial neural network fundamentals and reviewing the sensitivity analysis techniques, the risk prediction model was designed based on the methodology that was discussed earlier.

Based on the theorems for universal approximators, the risk predictor model is an artificial neural network. The number of inputs is 46 parameters and the number of outputs is two. The number of inputs is based key parameters identified by the security experts at Microsoft. The team of experts are Certified Information Systems Security Professionals that are part of the Microsoft Security Team, Microsoft Technical Systems Engineering Team, Microsoft Circle of Excellence in Security Team, and the Microsoft Premier Support Services Team. The team agreed that the parameters that affect security are not only based on technology but need to include people and process as well. The sensitivity analysis is designed to ensure that the number of input parameters are relevant and not redundant. The number of outputs is two. One output identifies the risk associated with the production server environment while the other output is the risk associated with the client machine environment.

In this scenario there is no feed back so the model was designed as a feed forward network. Feedback refers to situations where the output affects the input. Feedback is very suitable for control systems as in the case of closed loop control systems where the feedback changes the input of the plant. In feedback systems, the input is partly affected by the output. In this study of work, the model is a black box where the security risks are the outputs and where these outputs do not affect the inputs.

3.12 Training

Although the network inputs are not affected by the outputs, the errors in the outputs are propagated back to best establish the weights and the biases during the training phase. This type of training is the back propagation method which refers to the error being propagated back through the network to adjust the weights and biases. In this study the error is defined as (Target-Output)^2.

The training process relied on k-fold cross validation which is useful in estimating the generalization error based on *resampling.* [25-30] K-fold cross validation consists of dividing the data into *k* subsets of approximately equal size. The network is the then trained *k* times using *k-1* subsets. The weights and biases are obtained after each training. The averages for both the weights and biases are calculated after the network has been trained *k* times. The subset that is excluded is used for computing the error criteria. In this study, the number of folds was five so the network was trained 5 times using 4 datasets each time.

3.13 Data Collection

An essential part of building an approximator is the data collection because it is used to build, test and train the approximator. The collection of data was two fold: one set consisted of data generated by TableLab, a data generation tool developed at the Center for Advanced Technology and Education at Florida International University, and the other set was collected using a Microsoft website. The reasoning for doing this is to first validate the methodology with generated data before applying it to the actual data.

Using the TableLab application, the datasets were randomly generated, yet they were purposely created to exhibit statistical dependencies amongst certain columns within the matrix of data. The columns are comparable to the parameters in the questions and the number of rows would reflect customer responses. The number of rows that were generated using TableLab was 1000. The generated data contained the same number of inputs and outputs as the datasets that were collected via a secure website hosted by Microsoft for interacting with customers. This site is hosting an anonymous security questionnaire, and a copy of the questionnaire can be found in Appendix A.

The survey included questions regarding an organization's environment such as people, process and technology as well as if the organization was impacted by the Sasser worm and to what extent was the organization impacted. This refers to impacts to the production servers and the client machines. This information was obtained via an anonymous questionnaire that Microsoft's customers filled out.

The reason that the Sasser worm was selected for this study was that it impacted a sufficient number of customers as well as having been in the past year so customers could more easily recollect its impact. In addition to this, its impact was defined as critical which means a vulnerability whose exploitation could allow an Internet worm to be propagated without user action. The Sasser worm and its variants exploits the Local Security Authority Subsystem Service (LSASS). The Sasser worm has the potential of affecting the Microsoft Windows XP client machine and the Microsoft Windows 2000 Server and the Microsoft Windows 2003 Server machines. LSASS is responsible for the security mechanisms in the Microsoft Windows operating systems. The service verifies that the user logons to the computer or sever are valid. LSASS is specifically responsible for generating the process that authenticates users for the Winlogon service. The worm is capable of exploiting a buffer overrun vulnerability. A buffer overrun refers to passing data to a memory buffer which is smaller than the amount of data that are being passed to it. The data that can be passed to the buffer can be malicious code. A successful exploitation of a buffer run could allow an attacker to execute malicious code. In the case of the Sasser worm, the exploit of the buffer overrun vulnerability can be accomplished remotely and can compromise the system. Depending on the version of the operating system, there is a difference on who can exploit the vulnerability. For example, the vulnerability can be exploited by an anonymous user on the Microsoft Windows 2000 and XP operating systems. If the operating system is Microsoft Server 2003 or Microsoft Windows XP 64-bit Edition 2003, the vulnerability can be exploited by local, authenticated users. Microsoft released a patch to address the vulnerability on April 13, 2004.

The survey contained questions pertaining to key security parameters such as people, process and technology which correspond to the inputs of the network. The survey also queried customers on the effects that the Sasser worm had on the production servers and on client machines. The responses to these questions corresponded to the outputs. The number of columns in the matrix data are 48 with 46 columns reflecting inputs and the last two reflected the outputs. The matrix of the raw data showing the actual responses can be found in Appendix B. Although there are more than 48 columns, some columns were actually compounded questions that were combined. They were merely separated to ease the querying of the customers. The data exhibited in Appendix B is the actual raw data whereas Appendix C displays the normalized data. The data were normalized so that all data would be between 0 and 1, inclusive. The number of columns in the matrix corresponded to the questions in the survey. The rows in the matrix of data refer to the companies' responses to the questionnaire.

CHAPTER 4

Implementation of the Prediction Model

In this chapter, the implementation of the prediction model will be discussed. The focus of this chapter is the implementation of the prediction model utilizing the dataset generated by the TableLab application. The design and development of a neural network can be complex and is often iterative until a satisfactory design is developed. The following steps are typical of any artificial neural network implementation and were utilized in this study:

- Determining how many layers are necessary
- Arranging the neurons in the various layers
- Selecting the type of connections between the layers as well as within a layer
- Deciding the strength of each connection by permitting the network to learn what are the suitable weights for each connection
- Determining how the neurons receive inputs and yield the outputs
- Selecting what is the most suitable training method

This chapter will detail how the artificial neural network was built, implemented, trained and tested using the generated data with TableLab. All models were built, trained and tested using the Neural Studio application. The analysis and comparisons were charted using Microsoft Excel. The discussion begins with the initial ANN configuration and it evolves to how the final and optimal configuration was achieved.

4.1 Determining of the Starting Configuration

Although the design process is generally based on trial and error, rules of thumb were considered. When designing the model, the two givens were the number of inputs and the number of outputs. The number of neurons in the input and output layers were equated to the number of input parameters and the number of output parameters, respectively. In this study, there were 46 inputs and 2 outputs.

The first effort was determining how many layers are needed. In this case, the number of layers was set to three: an input layer, one hidden layer, and an output layer. Since there were over 40 input parameters, the number of layers was kept to the minimum. Having such a large number of input parameters was already adding a level of computational complexity.

The rules of thumb were applied with respect to the recommended number of neurons in the hidden layer. The rules of thumb as offered by Hecht-Nielsen recommended using 2N+1 neurons where N is the number of neurons in the input layer [17]. Applying the rules of the thumbs and using the fact that number of neurons in the input layer is forty-six, the recommended number of neurons in the hidden layer would be 93 neurons. This yielded a topology of 46-93-2.

The use of the rules of thumb was considered a good starting point, but the application of the rules of thumb needs to be verified and validation for this specific scenario and data. The rules of thumbs simply offer guidance, and there are counterexamples. [17] That is why there was much effort spent on verifying and testing the topologies to determine which offered the optimal solution. The tests that were performed in this investigation revolved around the speed with which model can process and the speed with which the model yielded a testing error of less than 5%. The reason for selecting 5% as the error level is that 5% is a statistically accepted error value. In this case, the speed of processing refers to speed of training. This factor gave an measure of the computational complexity the model encountered. Throughout this study, the error is defined by the following equation:

$$\text{Error} = (\text{Target} - \text{Output})^2$$

One thing to note is that the Neural Studio application provides a straight error value, but they can be treated as percentages since the datasets have been normalized.

When the 46-93-2 topology was tested for its ability to converge in a timely manner, it failed to do so. In fact during the testing phase, the topology was given over 90 minutes to converge, and it never yielded an error less than 90%. The testing consisted of letting the model run until an error of less than 5% was achieved or giving the model at least 90 minutes of running time to see how fast it would converge. In the 90+ minutes it had processed 191 iterations, yet the error was reduced from 113.95% to 90.92%. The other test was to check its processing speed. The model was checked to see how fast it can process 15 iterations. The 46-93-2 topology processed 15 iterations in 6 minutes and 17 seconds. Since this model did not produced a timely convergence, the number of neurons in the hidden layer were reduced to 80. The same testing criteria was applied to the new topology. Like its predecessor, the 46-80-2 topology did not produce an error of less than 5%. This topology yielded errors that were worse than its predecessor. After 1 hour and 42 minutes and 325 iterations, the error was at 223.25%. The reduction in the number of neurons did lower the time it took to process 15 iterations from over six minutes to under five minutes.

As part of the iterative process to determine the optimal topology, the number of neurons in the hidden layer was reduced by ten, thereby yielding a 46-70-2 topology. With this topology, an error of less than 5% was achieved in approximately 9.5 minutes and after 38 iterations. The 46-70-2 topology was able to process 15 iterations in 4 minutes. The number were again reduced in the hope of improving the speed with which the model would converge without impacting its ability to deliver within the error guidelines of less than 5%. After the reduction in the number of neurons in the hidden layer, the resulting topology was 46-60-2. This one achieved the targeted error range in 7 minutes and 22 seconds using 36 iterations. The 46-60-2 topology was able to process 15 iterations in 3 minutes and 16 seconds. The process of removing 10 neurons from the hidden layer continued until there were only 20 neurons in the hidden layer. The reduction of neurons did result in improvements in the speed with which the model would process 15 iterations. For example, the 46-50-2 topology was capable of processing 15 iterations in 2 minutes and 29 seconds as opposed to the 46-20-2 topology that processed the same number of iterations in 54 seconds. When the rate with which the topology was able to achieve the targeted error range was analyzed, it showed that the 46-30-2 topology reached the error rate better than the 46-40-2 or 46-20-2 topology. The topology with 30 neurons produced less than 5% error after 16 iterations whereas the 46-20-2 topology needed 29 iterations. The 46-20-2 topology did offer the ability to process an iteration faster. The hidden layer was altered by 5 neurons resulting in a 46-25-2 topology. The analysis of this topology showed that it was the optimal one. This topology achieved the error goal of less than 5% in 1 iteration. In addition to its ability to achieve the necessary error rate, it also demonstrated its ability to process 15 iterations in 66 seconds. The analysis with which the various topologies achieved the targeted error range is captured in Table 4.1 and graphically displayed in Figure 4.1. Table 4.2 shows the speed with which each topology was able to process 15 iterations. Figure 4.2 provides a graphical representation comparing how fast each topology processed the 15 iterations. Figure 4.3 showcases the optimal artificial neural network topology that resulted.

Table 4.1 Iterations needed to achieve an error ≤ 5%

Topology	Iterations	Start Error (%)	Stop Error (%)	Error Difference Stop-Start Error (%)	Delta Time Stop – Start Time (sec)
46-93-2	191	113.95	90.92	23.03	5733
46-80-2	325	237.27	223.25	14.01	6139
46-70-2	38	246.48	4.95	241.53	576
46-60-2	36	107.84	4.96	102.88	442
46-50-2	25	11.48	4.96	6.51	238
46-40-2	19	6.89	4.95	1.93	136
46-30-2	16	12.14	4.93	7.21	79
46-25-2	1	4.84	4.84	0	4
46-20-2	29	22.97	4.98	17.99	91

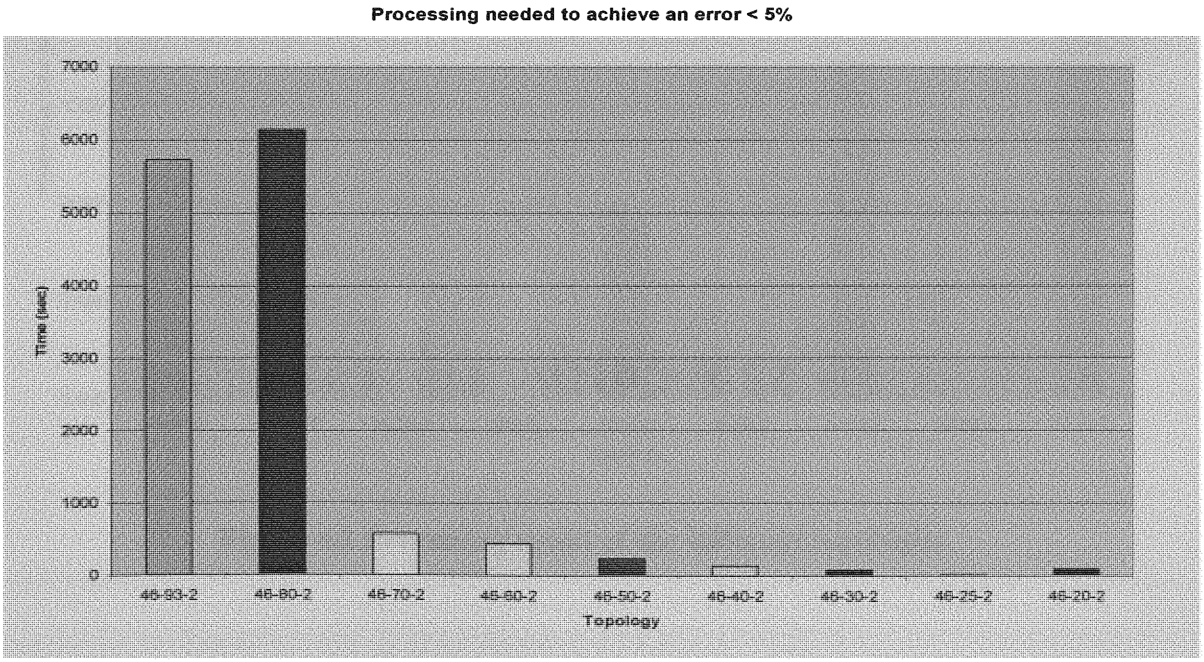


Figure 4.1 Iterations needed to achieve an error ≤ 5%

Table 4.2 Processing speed of the different topologies

Topology	Start Error (%)	Stop Error (%)	Error Difference Stop-Start Error (%)	Delta Time Stop – Start Time (sec)	Processing Speed 15/Delta Time (Iterations/sec)
46-93-2	113.95	93.29	20.66	377	0.04
46-80-2	237.27	224.70	12.56	291	0.02
46-70-2	246.48	9.42	237.06	240	0.06
46-60-2	107.84	7.43	100.41	196	0.08
46-50-2	11.48	5.81	5.67	149	0.10
46-40-2	6.89	5.28	1.61	113	0.13
46-30-2	12.14	5.01	7.13	87	0.17
46-25-2	4.84	4.50	0.34	66	0.23
46-20-2	22.97	5.85	17.13	54	0.28

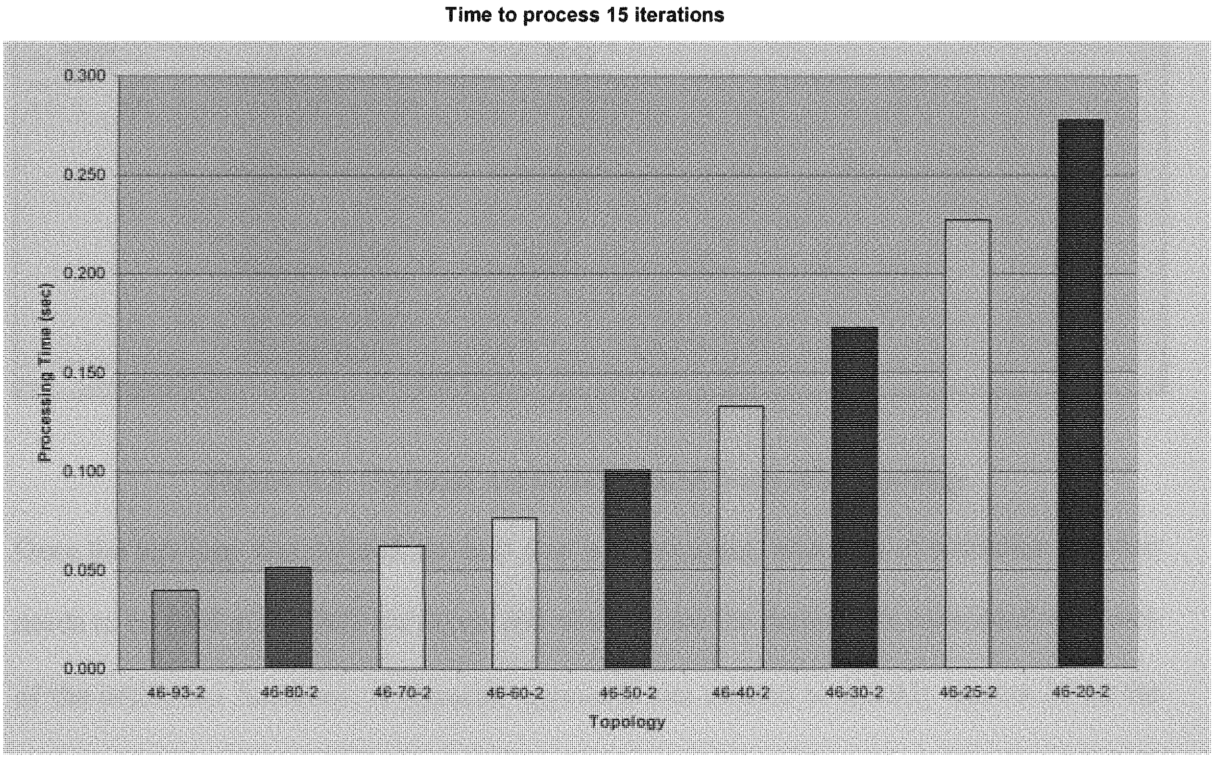
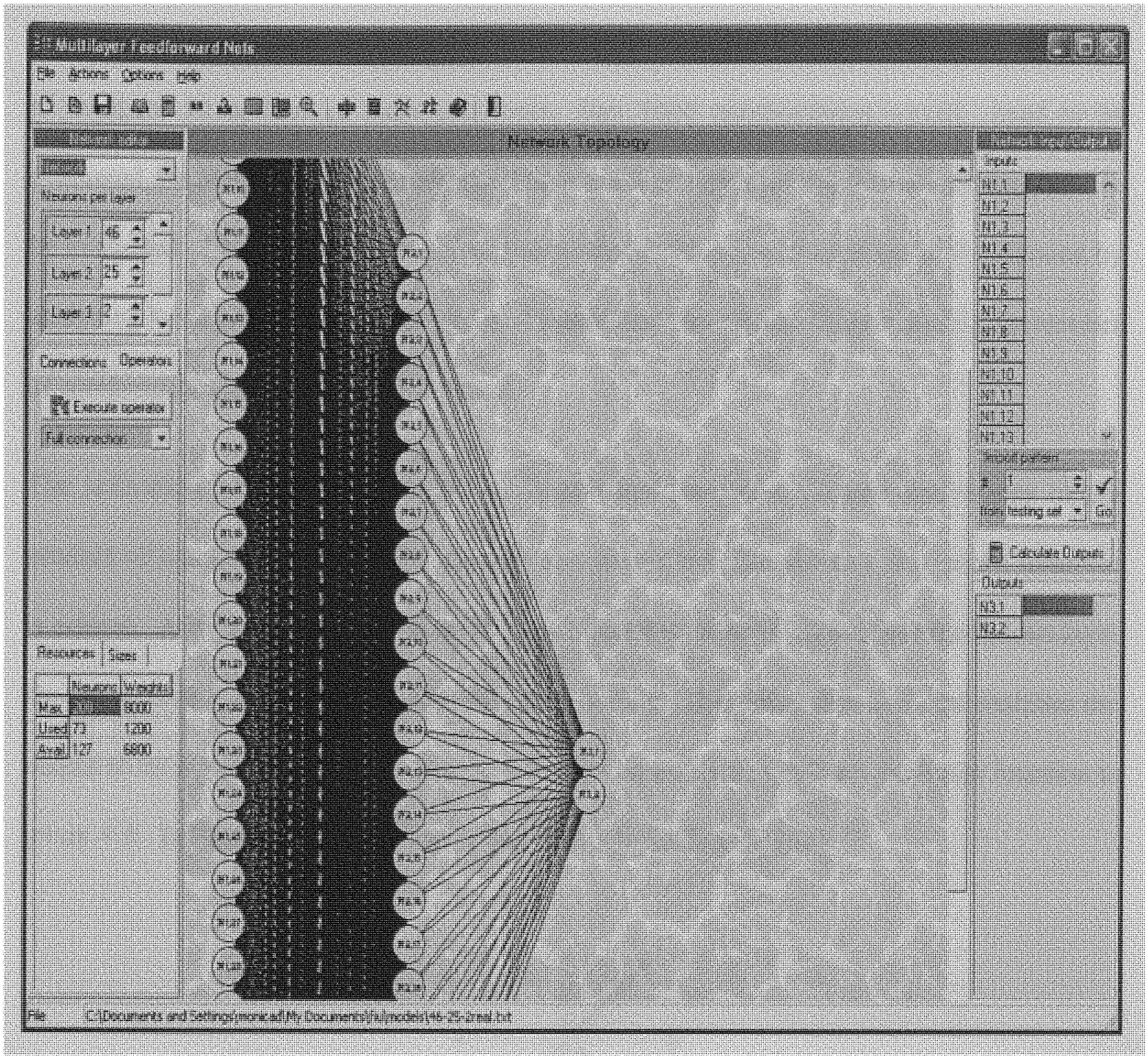


Figure 4.2 Processing speed of the different topologies



Layer 1 46
Layer 2 25
Layer 3 2

	Neurons	Weights
Max	200	8000
Used	73	1200
Avail	127	6800

Figure 4.3 Optimal Artificial Neural Network Topology

Once the topology was defined, the next step is determining what type of activation function needs to be used at the different layers and what the are the parameters associated with each of the activation functions. A dynamic approach was created to quickly narrow in on the optimal transfer function configuration and its parameters. The reason why the dynamic approach was developed was due to the number of combinations that would need to be reviewed to determine the optimal transfer function and its parameters. For instance, a Gaussian transfer function has two parameters that need to be evaluated. If the hidden and output layers both utilize the Gaussian activation function and the evaluation process needed to evaluate 10 options of each parameter, then 1000 combinations would need to be evaluated for one configuration alone. There are four types of configurations that need to be evaluated. This approach first determines what is the optimal configuration followed by analyzing what parameter settings are best suited, thereby substantially reducing the number of combinations that need to be reviewed.

The activation function is the transfer function that processes the cumulative sum of the product of input values to a node and the connections weights; thereby, its correct selection is critical. Analyzing the input layer, the linear function is selected because the hidden layer should receive the input values without any filtering. The linear function best matches the output to its input as depicted in Figure 4.4. The equation that defines the linear function is y= *a*x + *b*. In Figure 4.4, *a* and *b* are 1 and 0 which yields y=x. [31]

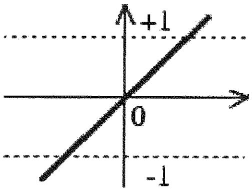


Figure 4.4 Linear function where y = x

For the hidden layer and the output layer, the desired feature for the transfer function is an ability to differentiate. The reasoning for selecting an activation function that is differential is to fully satisfy the complexity of the dataset. Activation functions such as the logistical sigmoidal and the Gaussian functions are considered good differentiable functions. In fact, the logistic sigmoid is often used in non-input layers for networks that rely on backpropagation. [32] An important consideration with respect to the output layer is selecting an activation function that provides smoothing. The differentiable functions such as the sigmoid have the ability to do smoothing.

The logistic sigmoidal function is defined by the following equation and depicted in Figure 4.5: [31]

$$y = \frac{1}{1 + e^{-a(x-b)}}$$

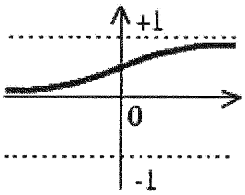


Figure 4.5 Logistic sigmoidal function

A graph of the Gaussian function can be found in Figure 4.6. [31] This differentiable function is defined by the following equation:

$$y = e^{-\frac{(x-b)^2}{2a^2}}$$

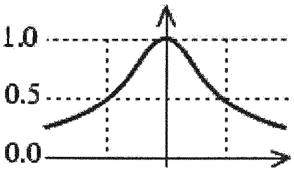


Figure 4.6 Gaussian function

The next step in the process is to determine which activation function configuration is best suited for the risk predictor model. It is necessary to determine what differentiable function is optimal for the hidden layer and for output layer. The configurations for the input – hidden – output layers that were analyzed are:

- Linear - Gaussian - Gaussian
- Linear - Gaussian - Logistic Sigmoidal
- Linear - Logistic Sigmoidal - Gaussian
- Linear - Logistic Sigmoidal- Logistic Sigmoidal

The analysis associated with the selection of the transfer function consists of studying the errors after each iteration for the first ten iterations. The error after 100 iterations was also reviewed. In essence, the model's ability to converge using the four different configuration was studied. Each configuration that was analyzed had the same topology, 46-25-2, that was defined earlier as optimal.

After 10 and 100 iterations, the first configuration, Linear - Gaussian – Gaussian, exhibited an error of 91.84% down from 92.40% after just two iterations. After 100 iterations the error was still at 91.84%. The error associated with the Linear - Gaussian - Logistic Sigmoidal configuration stayed relatively the same. After 1 iteration the error was 65.94%, but it increased to 65.96% after 2 iterations. The error remained at 65.96% for the remainder of the 100 iterations. The configuration, Linear - Logistic Sigmoidal – Gaussian, never converged. Throughout the 100 iterations the error was 1218.01%, and it did not change. The last configuration, Linear - Logistic Sigmoidal- Logistic Sigmoidal, exhibited the best convergence. The error was 4.84% after 1 iteration; by the end of the test the error was down to 3.38%. The configuration, Linear - Logistic Sigmoidal- Logistic Sigmoidal, was deemed the optimum activation function configuration for the input-hidden-output layers. Table 4.3 lists the errors associated with the different activation function configurations. Figure 4.7 graphically depicts how well the models with the different configurations converged.

Table 4.3 Errors associated with the different activation function configurations

		Activation Functions			
		linear-gaussian-gaussian	linear-gaussian-logsig	linear-logsig-gaussian	linear-logsig-logsig
Iterations	1	92.40%	65.94%	1218.01%	4.84%
	2	89.91%	65.96%	1218.01%	4.81%
	3	91.84%	65.96%	1218.01%	4.78%
	4	91.84%	65.96%	1218.01%	4.75%
	5	91.84%	65.96%	1218.01%	4.73%
	6	91.84%	65.96%	1218.01%	4.70%
	7	91.84%	65.96%	1218.01%	4.67%
	8	91.84%	65.96%	1218.01%	4.64%
	9	91.84%	65.96%	1218.01%	4.62%
	10	91.84%	65.96%	1218.01%	4.59%
	100	91.84%	65.96%	1218.01%	3.38%

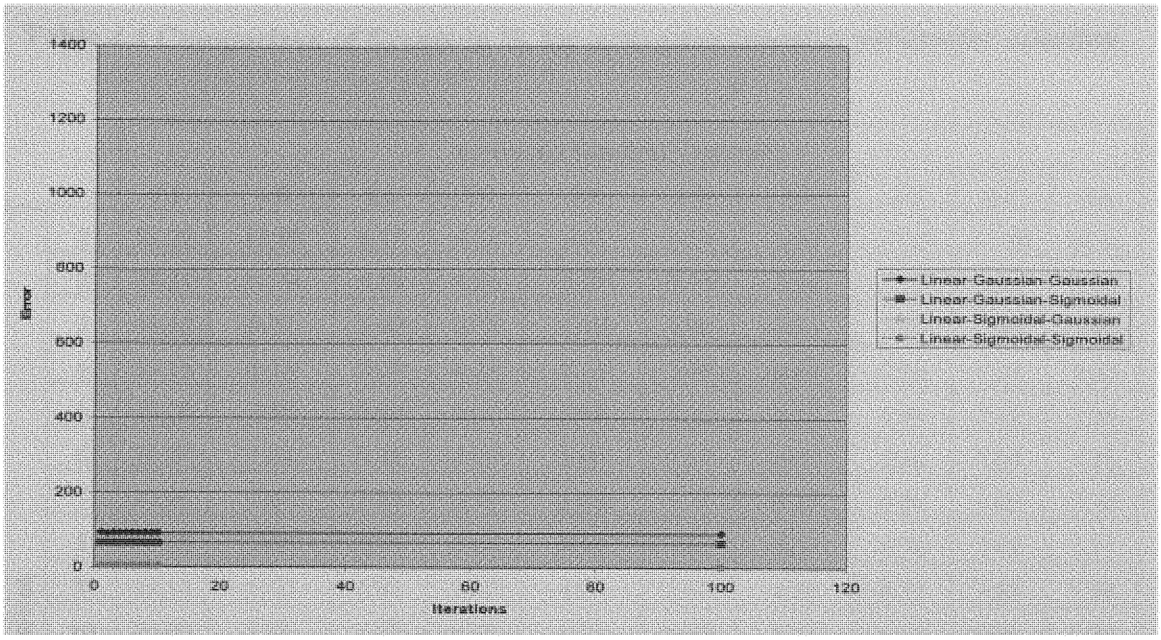


Figure 4.7 Errors associated with the different activation function configurations. The error is defined as (Target-Output)^2

Once the optimal transfer function configuration has been obtained, the next step is to select what are the parameters that are optimal for this study. Reviewing the equation associated with the logistic sigmoid, there are two parameters, *a* and *b*, that are configurable. Upon closer inspection, it can be noted that the parameter, *b*, only provides translation across the x-axis. Such translation is compensated via the weights and the biases. This means that parameter, *b*, can be set to 0 and that parameter, *a*, is the parameter that needs to be under investigation. In this study, the parameter was varied from 0.5 to 5 in increments of 0.5. If the value is greater than 5, the function practically becomes a step function and is not differentiating as well. Table 4.4 showcases the errors, that were measured as the parameter is varied, after the marked iterations. A graphical depiction of the full set of measurements can be found in Figure 4.8. Evaluating the table and graph leads to the selection of parameter, $a = 2.0$. This setting yields the lowest error for the already optimal configuration.

Table 4.4 Comparison of Errors in % for activation function parameter selection

		Activation Function Parameter, a									
		0.5	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0
Iterations	1	53.22	17.89	6.15	4.84	5.43	6.74	8.40	10.20	11.90	14.11
	2	48.21	11.74	5.59	4.81	5.25	6.19	7.24	8.10	8.64	9.00
	3	43.52	9.27	5.40	4.78	5.18	6.00	6.83	7.32	7.49	7.62
	4	39.15	8.15	5.29	4.75	5.13	5.90	6.64	7.06	7.23	7.42
	5	35.09	7.58	5.20	4.73	5.09	5.83	6.53	6.94	7.13	7.36
	6	31.37	7.24	5.12	4.70	5.05	5.77	6.45	6.86	7.08	7.35
	7	27.99	7.01	5.06	4.67	5.02	5.72	6.39	6.81	7.05	7.36
	8	24.98	6.84	5.00	4.64	4.98	5.67	6.35	6.76	7.04	7.37
	9	22.34	6.70	4.95	4.62	4.95	5.63	6.30	6.72	7.03	7.38
	10	20.05	6.59	4.90	4.59	4.92	5.59	6.26	6.69	7.02	7.38
	20	10.23	5.93	4.54	4.37	4.66	5.26	5.96	6.42	6.67	6.87
	30	8.56	5.51	4.31	4.18	4.43	4.96	5.67	6.24	6.25	6.13
	40	8.01	5.18	4.14	4.03	4.25	4.71	5.33	5.86	6.22	6.05
	50	7.67	4.90	4.00	3.89	4.09	4.53	5.04	5.11	5.29	5.40
	60	7.43	4.68	3.89	3.77	3.96	4.36	4.84	4.71	4.86	4.95
	70	7.23	4.49	3.79	3.66	3.84	4.19	4.63	4.43	4.56	4.63
	80	7.07	4.34	3.70	3.56	3.72	4.03	4.44	4.22	4.33	4.39
	90	6.92	4.21	3.62	3.47	3.60	3.89	4.28	4.05	4.14	4.20
	100	6.79	4.10	3.54	3.38	3.50	3.76	4.14	3.91	3.97	4.04

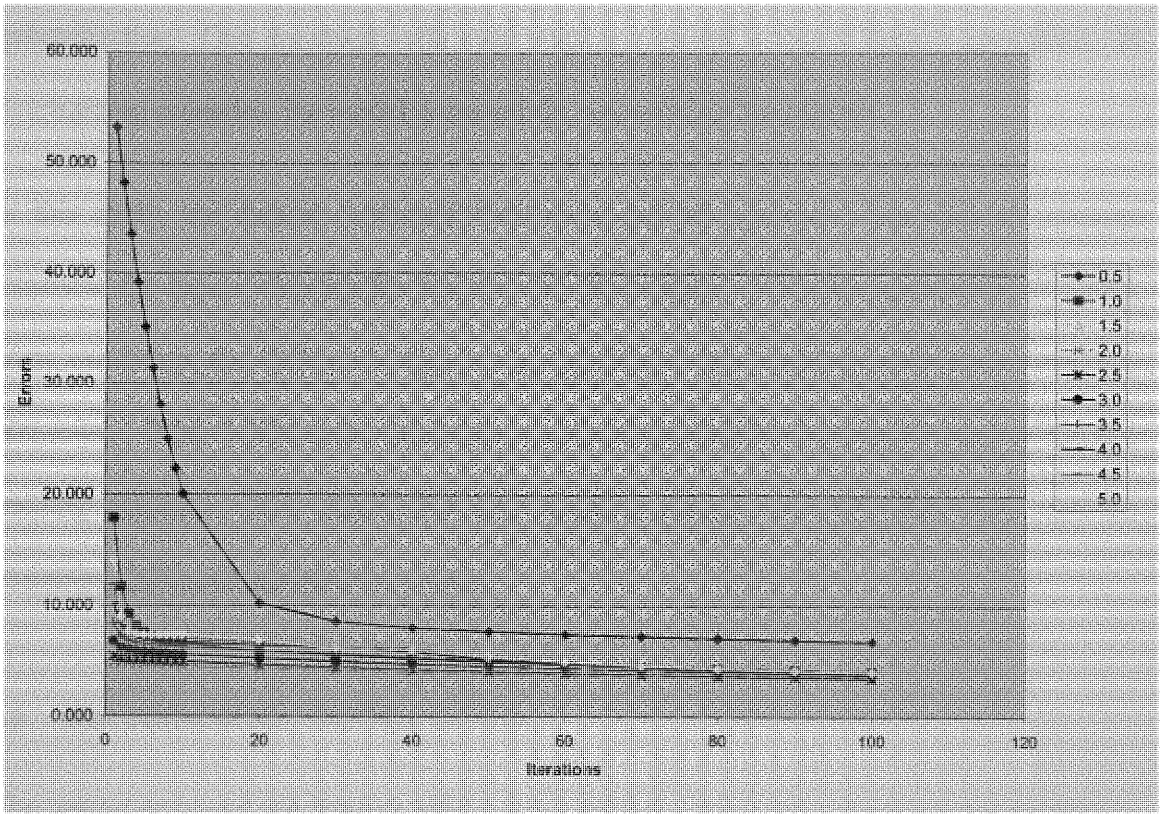


Figure 4.8 Comparison of errors for activation function parameter selection

4.2 Determination of the Optimum Predictor Configuration

The optimum predictor configuration is a three layer network consisting of 46 inputs, 25 neurons in the hidden layer and 2 outputs. The activation functions for the input layer, the hidden layer and the output layer are linear, logistic sigmoid and logistic sigmoid respectively. The key parameter in the activation function is set at 2.0.

After the optimum predictor configuration was obtained, the model was validated using 5-fold cross validation. Cross validation refers to dividing the dataset into *k* subsets and using the *k-1* subsets to train the model *k* times. The reason why k-fold cross validation was selected for this study is that it is designed to avoid over training and improve generalization. One drawback with over training a model is that it fails to generalize. In overtraining scenarios, the model is essentially memorizing the patterns.

In this study, the dataset contained 1000 rows and 48 columns. The first 46 columns represent the inputs whereas the last two are the outputs. With the application of 5-fold, cross validation, the 1000 rows dataset was subdivided into 5 subsets with each containing 200 rows. With 5-fold cross validation, 4 subsets are used for training for each of the five training sessions. This means that each training session uses 800 data rows, and the remaining 200 rows are used for testing.

4.3 Discussion of the Training Errors

The testing error and the training error were constantly monitored and compared in order to avoid over training. The training was stopped when the testing error was at a minimum. Each session has a set of biases and weights that are evaluated and recalculated throughout the training. When the training was stopped at each session, the weights and biases were recorded. This resulted in 5 sets of biases and weights which were then inputted into Microsoft Excel, and the averages for both the biases and weights were calculated and recorded. A listing of the weights and biases can be found in Appendix D. The average weights and average biases were then inputted into the Neural Studio application.

Table 4.5 denotes the training and testing errors that were recorded for each fold during the cross validation testing. The table clearly indicates that the training error was always below the targeted maximum of 5% and that the testing error was well below the desired maximum value. As noted from inspecting Table 4.5, the errors indicate that the model was capable of generalizing and did not have the over fitting problem.

Table 4.5 Errors associated with Cross Validation

Training Set	Training Error (%)	Testing Error (%)	Iterations
1	4.641	0.673	2
2	4.585	0.800	2
3	4.385	0.828	9
4	3.980	0.763	24
5	3.649	0.569	2

CHAPTER 5

Implementation of the Practical Predictor Model

This chapter is dedicated to the analysis and discussion on how the predictor model was implemented using real data. The chapter discusses how the real data was obtained, how the normalization procedures were applied to the datasets, as well how the predictor model was implemented, trained and validated.

The knowledge that was gained from building a model based on the data generated from TableLab was leveraged in this effort. Key insights that were gained from this implementation of the model, that was built using the generated data, were applied in the practical application. Some of these key insights include:

the number of layers were set to three: one input layer, one hidden layer, and one output layer

- the use of a linear function for the input layer's transfer function
- the use of differentiable functions in the hidden and output layers' activation functions
- the dynamic approach for discerning the activation functions' parameters
- the application of k-fold cross validation
- the need for a generalization test

5.1 Data Collection and Processing

Since collection of the data is an instrumental part of implementing a practical prediction model, the first endeavor was to determine how to best collect data. In this study, it was necessary to provide a mechanism that would let companies candidly share their experiences with security breaches. Although there is much in the media about security breaches such as the computer viruses and worms that have attacked the information systems of businesses globally, there is no formal collection of the data that showcases the extent and impact of the attacks or even profiles the information technology infrastructure of the impacted businesses. The survey which can be found in Appendix A was devised for this study and is the first step in collecting such information. The creation of the survey was the result of a multitude of activities which ranged from reviewing forms that queried the technical controls that customer implement in their environments to interviewing security professionals as to what they saw were key factors to having a secure information system. The survey was hosted on a Microsoft web site and was designed to be anonymous so customers could comfortably furnish information without divulging any association with their specific company. Another thing to note when inspecting the survey is that the questions regarding impacts associated with a security breach only focused on the impact of the Sasser worm. The Sasser worm was specifically picked because of its critical nature and its relevant recent activity making it easier on the customer filling out the questionnaire. The responses were posted to a database and a spreadsheet was used to access the database. Appendix B details the raw responses that the customers furnished. When the responses of the survey are reviewed, intra subject inconsistency was observed. For instance, a customer replied having an elevated maturity level in the security personnel, yet the company did not have security personnel with any certifications or provided security training to its employees.

After reviewing the survey questions, it can be noted that some questions exhibited certain dependencies on other questions. For instance, the question which queried whether the customer performed software code reviews is dependent upon the question that determines if the customer developed any in-house applications. Questions such as these were treated as compounds questions. The following topics were treated as compound questions which are dependent upon the company developing in-house applications:

- the requirement of software code reviews
- the testing of software by a quality assurance department
- the strict validation of input
- the handling of error messages
- the use of threat modeling

Another compound parameter is whether the anti-virus signatures are up to date. This parameter is dependent upon the use of anti-virus software. Likewise the questions that pertain to having the firewalls which block unnecessary ports are dependent upon the use of firewalls.

This compounding affected the normalization procedure and the number of parameters in the input layer of the predictor model. After compounding was applied, essentially, the number of questions in the survey pertaining to the information system technical infrastructure, people, and process corresponded to the number of inputs in the model and the number of questions pertaining to the extent of the impact that the Sasser worm effected in terms of percentage denoted the number of outputs in the model. The final result was 46 inputs and 2 outputs.

The normalization of the data was key in the development of the model. Since the desired outputs are risks, and risks are best denoted as percentages, the input data was also normalized to fall between 0 and 1, inclusively. This normalization process was designed to simplify any internal mathematical processing as in the case of applying the transfer functions. When inspecting the customer responses in Appendix B, it can be noted that certain responses were in days as in the case of how often are passwords reused. This resulted in utilizing the following normalization equations:

$$\begin{array}{ll} 1-\dfrac{x}{worst} & \text{if } x \leq \text{worst} \\ 0 & \text{if } x > \text{worst} \end{array}$$

where x is the customer response and worst is the industry accepted worst case value for the security parameter. For instance, patches to virus are often released 6 months prior to the release of a virus that exploits the vulnerability. If for some reason, the company exceeds the industry worse case value, the result is capped at 0 and is not allowed to go less than 0. In this study, a value of *0* in the input parameter signifies the worst case scenario and a value of *1* indicates the best possible response. In this study, the *yes* responses were given a value of *1* during the normalization process, and the *no* responses were assigned a value of *0*. If the customer fail to answer a question associated with an input parameter, the response to the question was treated as a *0*. With respect to questions that reflect the impact of the virus, the customer would only furnish percentages and did not give specifics on the actual number of machines that were hit. The percentages was used in the analysis and not the other number. It was asked to ascertain the size of the company from an infrastructure perspective.

Parameters related to the pay scales of the security personnel and the IT professionals were affected during the normalization and compounding. For instance, customers that classified the scale as according to industry standard were issued a value of 0.5. If the customer defined the pay scale as below industry standard, a value of 0 was assigned as opposed to issuing a value of 1 to companies paying above the industry standard. Another parameter that was effected by the compounding and normalization procedures was the desktop manageability. Two customers did provide a response to having a managed desktop environment, but they failed to provide a provide a percentage indicating how many desktops are managed. In this case where there is a compounding effect, those two customers were each assigned a value of 0.50 for management desktop since they answered half of the two compounded questions.

During the normalization process, if a customer responded that they had deploy a technology as in the case of digital rights management but were in the midst of testing, a value of 0.5 was assigned. These questions expected a yes or no answer which translates to a 1 or 0 so a testing response was given to signify the middle value. This same process was applied to responses pertaining to people and process as in the question on whether the passwords are changed on domain accounts when an IT administrator is terminated. One customer responded *sometimes* so a value of 0.5 was given.

The analysis that took effect as a result of the compounding process and the results of the normalization process can be found in Appendix C.

5.2 Development of Practical Predictor

The methodology that was validated with the generated data was then utilized to build the practical predictor model using the customer responses after the normalization procedures were applied to the dataset collection. In this scenario, certain givens are noted. These givens are the number of neurons in the input layer being 46 and the output layer having 2 outputs. The number of layers were kept to three meaning that there is only one hidden layer. Once these givens have been identified, the methodology focuses on determining the optimum topology by determining how many neurons should be in the hidden layer.

In search of the topology that best suits this specific scenario, the rule of thumb concerning the number of neurons in the hidden layer was first applied. Such an application resulted in the 46-93-2 topology.

The process of verifying the topology consisted of analyzing how fast the topology would achieve an error less than or equal to 5% and how fast the topology can process 15 iterations of data. The latter measure denotes how fast the model is trained, yet it can be used as an indication of the computational complexity of the model. Table 5.1 showcases how quickly the topologies achieved the desired error level, and the Figure 5.1 provides a graphical view of this measure. To compare the different topologies in terms on how fast the topologies are capable of processing data, Table 5.2 and its graphical counterpart, Figure 5.2, are provided.

Inspecting the values associated with the 46-93-2 topology, it can be noted that it only took one second to achieve the desired error level, yet the processing speed is 2.14 iterations/sec. Since the number of inputs and outputs are given values, the only factor that can be changed is the number of neurons in the hidden layer. Reducing the number of neurons in the hidden layer to 80 resulted in the 46-80-2 topology. This topology did not converge. Even after 1000 iterations, the error reduced only marginally from 22.50% to 22.27%. The processing associated with the topology did improve to 2.50 iterations/sec. The topology was again changed to 46-70-2. This configuration was able to converge, but it took 4 iterations and 30 seconds to achieved this as opposed to the 46-90-2 topology which required only 2 iterations and 1 second. The processing speed of the new topology increased to 3 iterations/sec. A new topology having 60 neurons in the hidden layer was analyzed. This one required 7 iterations to reach the targeted error level. The processing speed improved by 25%. The 46-50-2 topology displayed more reduction in terms of the number of iterations needed to meet the desired error level, yet its processing speed stayed on par with 46-60-2 topology. The 46-40-2 topology required only one iteration to achieve the 5% error level, and its processing speed jumped to 5 iterations/sec. Reducing the number of neurons in the hidden layer to 30 resulted in an increase in the number of iterations needed to meet the targeted error level. This time it took 2 iterations to get to an error of 3.53%. The associated processing speed is 7.50 iterations/sec. The reduction of 10 neurons in the hidden layer yielded the 46-20-2 topology. This one required 3 iterations to reach the desired error level. The processing speed of 15 iterations/sec is 100% better than its predecessor. A 46-25-2 configuration was created and analyzed to see how well it addressed each metric. This configuration required only 1 iteration to achieve an error of 2.80%, and at the same time its processing speed was 15 iterations/sec. Since this topology excelled at each metric, it was deemed the optimal one. The optimal model can be seen in Figure 5.3. One thing to note is that this configuration had an error of only 2.80%, yet the 46-40-2 configuration had a 2.04% error.

Table 5.1 Iterations needed to achieve an error ≤ 5%

Topology	Iterations	Start Error (%)	Stop Error (%)	Error Difference Stop-Start Error (%)	Delta Time Stop – Start Time (sec)
46-93-2	2	18.26	3.05	15.21	1
46-80-2	1000	22.50	22.27	0.23	422
46-70-2	4	46.85	3.18	43.67	30
46-60-2	7	46.00	3.21	42.79	0
46-50-2	2	5.16	2.88	2.28	0
46-40-2	1	2.04	2.04	0.00	0
46-30-2	2	10.10	3.53	6.56	1
46-25-2	1	2.80	2.80	0.00	0
46-20-2	3	19.10	2.71	16.38	1

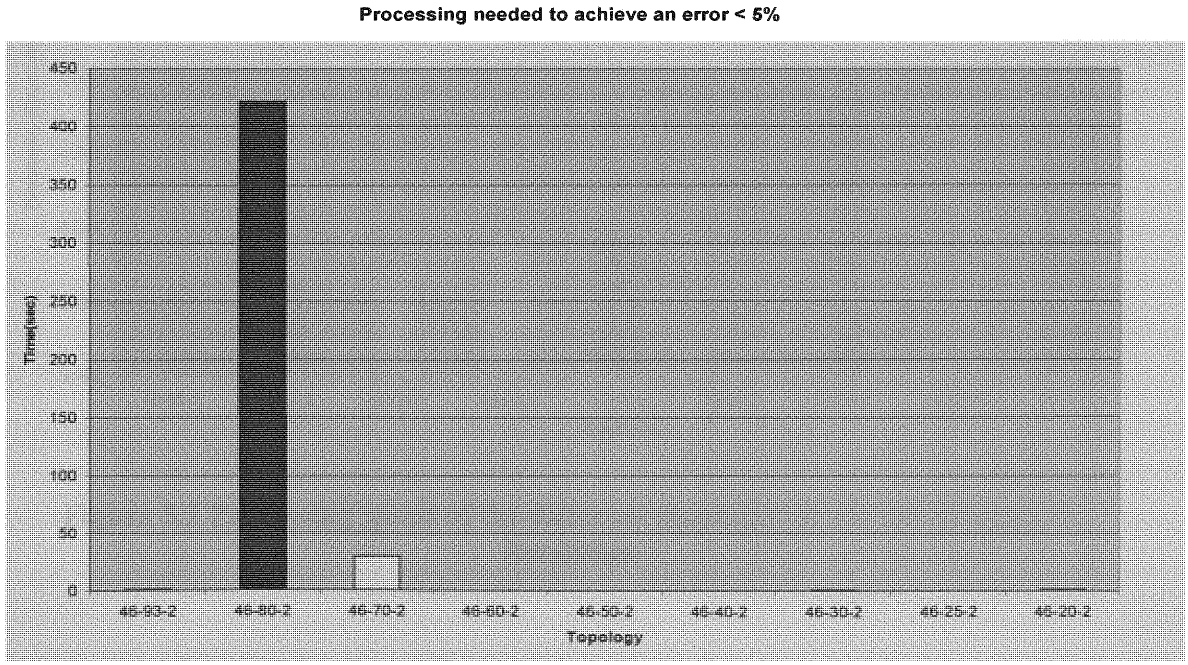


Figure 5.1 Iterations needed to achieve an error ≤ 5%

Table 5.2 Processing speed of the different topologies to iterate through 15 iterations

Topology	Start Error (%)	Stop Error (%)	Error Difference Stop-Start Error (%)	Delta Time Stop – Start Time (sec)	Processing Speed 15/Delta Time (Iterations/sec)
46-93-2	113.95	93.29	20.66	377	2.14
46-80-2	237.27	224.70	12.56	291	2.50
46-70-2	246.48	9.42	237.06	240	3.00
46-60-2	107.84	7.43	100.41	196	3.75
46-50-2	11.48	5.81	5.67	149	3.75
46-40-2	6.89	5.28	1.61	113	5.00
46-30-2	12.14	5.01	7.13	87	7.50
46-25-2	4.84	4.50	0.34	66	15.00
46-20-2	22.97	5.85	17.13	54	15.00

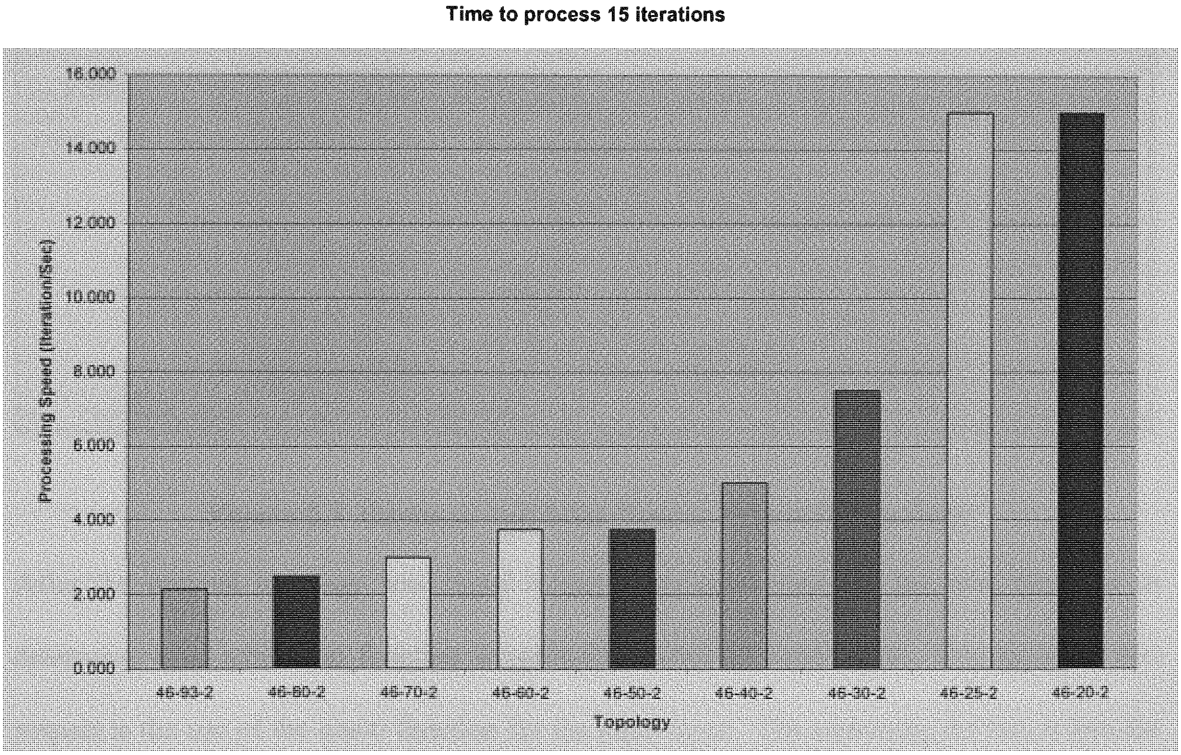
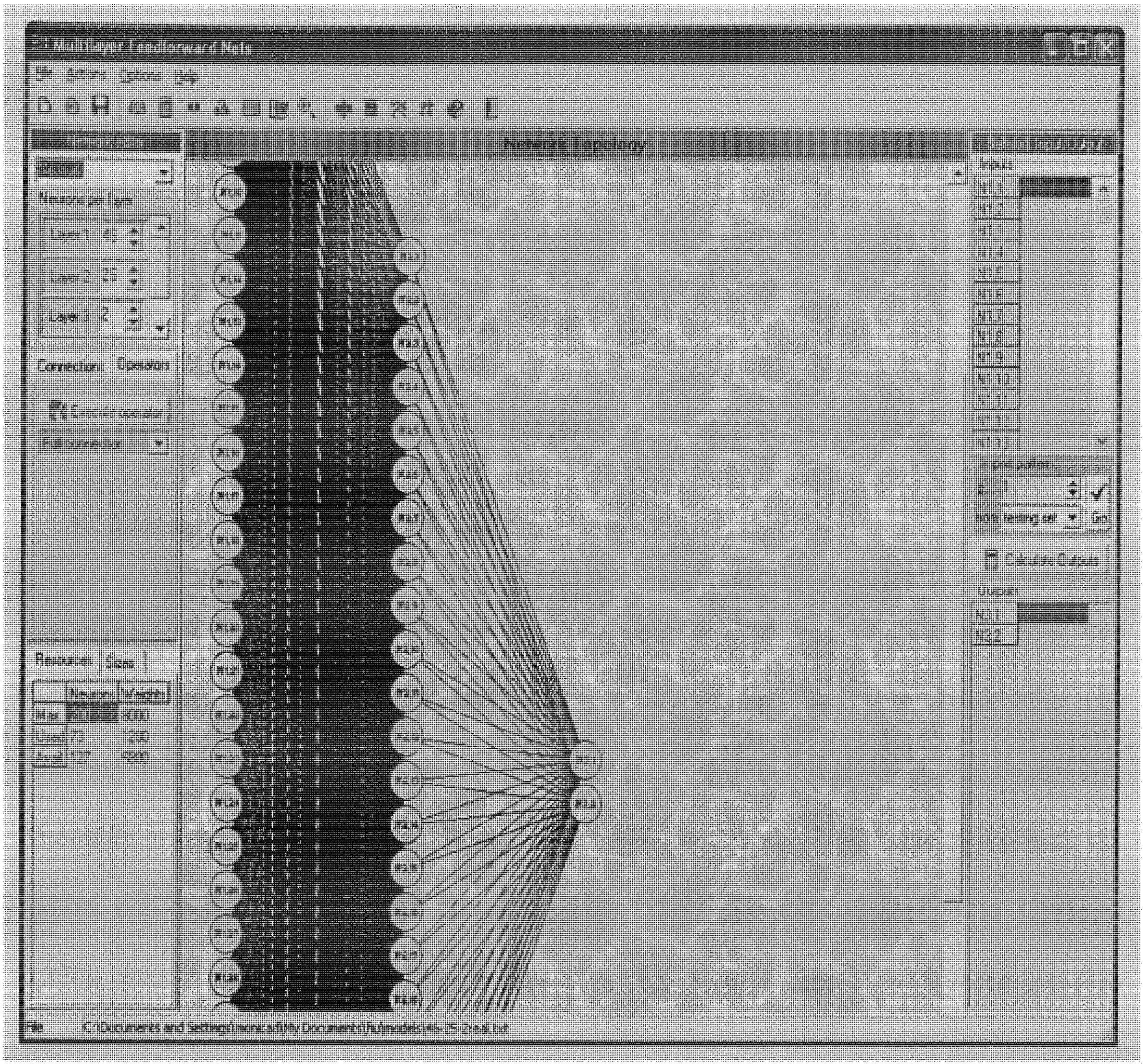


Figure 5.2 Processing speed of the different topologies to iterate through 15 iterations.



Layer 1 46
Layer 2 25
Layer 3 2

	Neurons	Weights
Max	200	8000
Used	73	1200
Avail	127	6800

Inputs: N1.1 N1.2 N1.3 N1.4 N1.5 N1.6 N1.7 N1.8 N1.9 N1.10 N1.11 N1.12 N1.13

Input pattern #: 1

Outputs: N3.1 N3.2

File C:\Documents and Settings\[illegible]\My Documents\[illegible]\models\46-25-2real.txt

Figure 5.3 Optimal Artificial Neural Network Topology

After the optimal topology was found through empirical analysis, the next step was to determine what activation function is optimally suited for each layer. One given in this respect is the use of the linear function for the input layer. The reasoning for this is that the use of a linear function in the input layer provides the entire input to the hidden layer. The configurations in question are what type of differentiable function should be used in the hidden and output layers. The reasoning for using a differentiable function is that they are best suited for models that rely on back propagation for training. The configurations for the input – hidden – output layers that were analyzed are:

- Linear - Gaussian - Gaussian
- Linear - Gaussian - Logistic Sigmoidal
- Linear - Logistic Sigmoidal - Gaussian
- Linear - Logistic Sigmoidal- Logistic Sigmoidal

The analysis consisted on monitoring each of the first ten iterations to determine how well the model was capable of reducing the error. The model was again check after 100 iterations to see what the error was. This is charted in Table 5.3 and graphed in Figure 5.4. The table and graph denote that the use of the logistic sigmoidal function in the both the hidden and output layers yielded the best results. The error was reduced from 1.71% to 0.37% over the course of 100 iterations. The linear-logistic sigmoidal-gaussian configuration had a lower error, 1.36%, at the start of the test, yet this error did not reduce through the course of the test. The other two configurations did indicate reductions in error, but the errors were larger at the beginning and at the end of the test when comparing with linear-logistic sigmoidal-logistic sigmodal configuration.

Table 5.3 Errors associated with the different activation function configurations

		Activation Functions			
		Linear-gaussian-gaussian	linear-gaussian-logsig	linear-logsig-gaussian	linear-logsig-logsig
Iterations	1	1.98%	3.43%	1.36%	1.71%
	2	1.09%	2.82%	1.36%	1.68%
	3	1.08%	2.52%	1.36%	1.64%
	4	1.07%	2.31%	1.36%	1.61%
	5	1.07%	2.11%	1.36%	1.59%
	6	1.07%	1.94%	1.36%	1.57%
	7	1.06%	1.81%	1.36%	1.56%
	8	1.17%	1.73%	1.36%	1.55%
	9	1.08%	1.65%	1.36%	1.54%
	10	1.07%	1.59%	1.36%	1.53%
	100	1.06%	1.06%	1.36%	0.37%

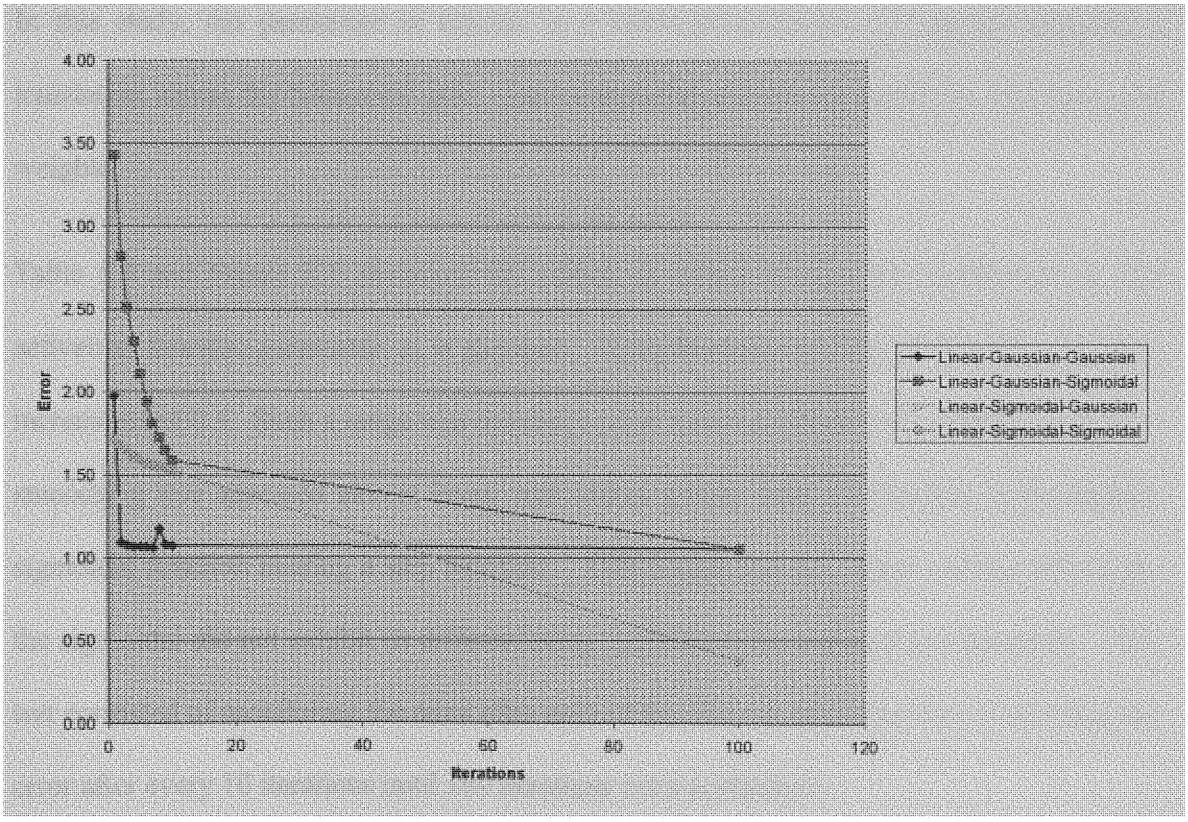


Figure 5.5 Errors associated with the different activation function configurations. The error is defined as (Target-Output)^2

Once the optimal topology and transfer function configuration were determined, the methodology called upon the dynamic approach to determine what was the value of the activation function parameter that best suited the dataset. The dynamic approach consisted of determining the activation function first and then narrowing in on the value of the activation parameter without having to review thousands on configurations. By doing so the combinations in this case is reduced to 10 different values of the activation parameter.

Recalling that the logistic sigmoidal function is defined using the equation:

$$y = \frac{1}{1 + e^{-a(x-b)}}$$

In this study, the parameter of interest is *a* since the parameter, *b*, simply provides a translation across the horizontal axis. Such translation can be accounted by the biases and weights.

Table 5.4 and Figure 5.5 showcase the effects in terms of error that model has as the activation function parameter, *a*, is changed This parameter is changed from 0.5 to 5.0 in increments of 0.5. Such a range was suitable in that values of a below 0.5 yielded very little smoothing and appeared almost linear and values greater than 5.0 resulted in the logistic sigmoidal function nearing a step function. This means that for values outside this range, the sigmoidal did not exhibit its differentiating qualities as necessitated by this study. The test consisted of monitoring the error after each of the first ten iterations then monitoring the error after every 10 iterations until 100 iterations were performed.

Reviewing Table 5.4 and its corresponding graph, Figure 5.5, it can be noted that the model having an activation parameter equal to 3.5 exhibit the smallest error throughout the test. The error at the start of the test was 0.13% and at the end it was measured at 0.07%.

Table 5.4 Comparison of errors in % for activation function parameter selection

		Activation Function Parameter, a									
		0.5	1.0	1.5	2.0	2.5	3.0	3.5	4.0	4.5	5.0
Iterations	1	4.13	1.35	0.61	0.37	0.30	0.18	0.13	0.45	0.51	0.56
	2	3.51	1.11	0.57	0.37	0.29	0.16	0.13	0.41	0.48	0.54
	3	3.04	0.99	0.55	0.36	0.28	0.15	0.13	0.36	0.45	0.52
	4	2.67	0.92	0.54	0.36	0.27	0.15	0.12	0.32	0.41	0.50
	5	2.39	0.88	0.53	0.35	0.26	0.15	0.12	0.28	0.38	0.47
	6	2.17	0.85	0.52	0.35	0.26	0.14	0.12	0.25	0.33	0.45
	7	2.00	0.83	0.52	0.35	0.25	0.14	0.12	0.23	0.29	0.42
	8	1.86	0.82	0.51	0.34	0.25	0.14	0.12	0.22	0.27	0.38
	9	1.74	0.81	0.51	0.34	0.25	0.14	0.12	0.21	0.25	0.33
	10	1.65	0.80	0.50	0.34	0.24	0.14	0.12	0.21	0.24	0.30
	20	1.21	0.75	0.47	0.30	0.22	0.12	0.11	0.18	0.20	0.23
	30	1.10	0.72	0.44	0.27	0.19	0.11	0.11	0.17	0.18	0.21
	40	1.06	0.70	0.41	0.25	0.18	0.11	0.10	0.16	0.17	0.18
	50	1.04	0.67	0.38	0.23	0.16	0.10	0.09	0.15	0.16	0.17
	60	1.02	0.65	0.36	0.21	0.15	0.09	0.09	0.15	0.15	0.16
	70	1.01	0.63	0.34	0.19	0.14	0.09	0.08	0.14	0.15	0.15
	80	1.01	0.62	0.32	0.18	0.14	0.09	0.08	0.13	0.14	0.15
	90	1.00	0.60	0.30	0.17	0.13	0.08	0.08	0.13	0.13	0.14
	100	1.00	0.58	0.28	0.16	0.12	0.08	0.07	0.12	0.13	0.13

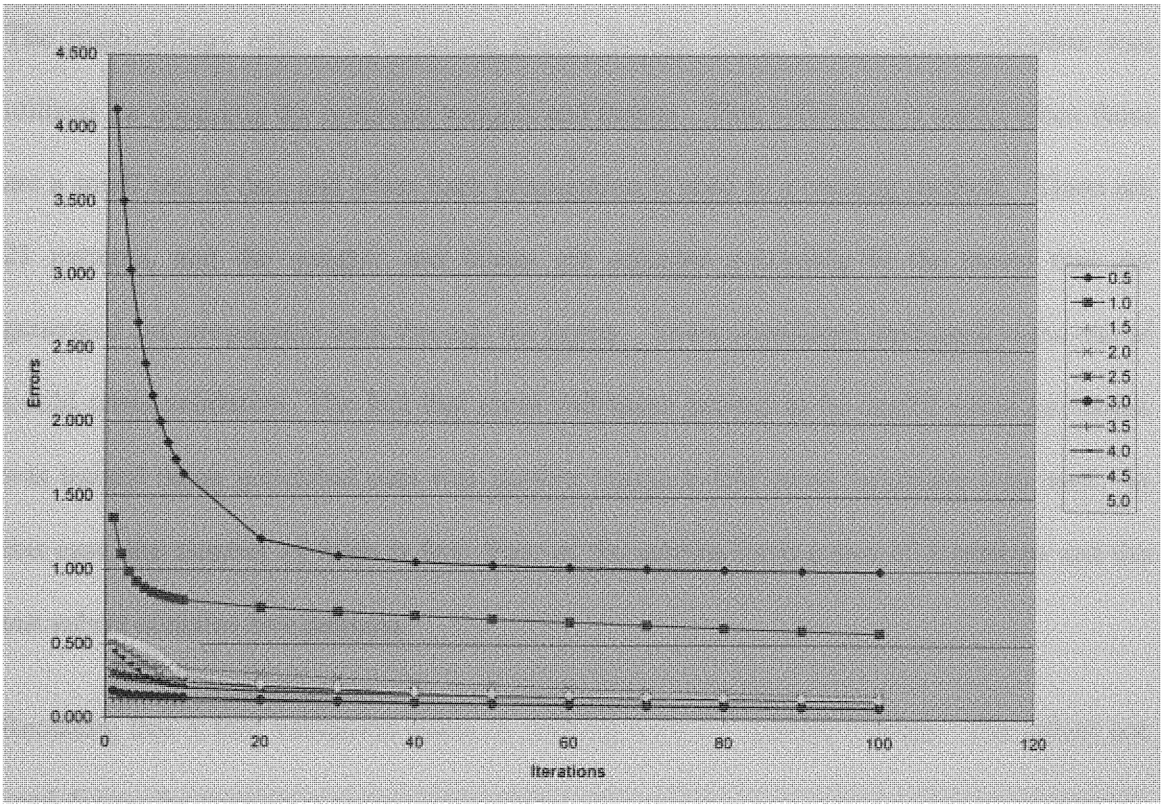


Figure 5.5 Comparison of errors for activation function parameter selection

5.3 Determining the Optimum Configuration

The resulting configuration of the development phase is a model that consists of three layers:

- an input layer containing 46 neurons and using a linear function, y=x for its transfer function
- a hidden layer containing 25 neurons and relying on the logistic sigmoidal function for the activation function where *a*=3.5
- and an output layer containing 2 neurons and utilizing the logistic sigmoid for a transfer function where *a*=3.5

The methodology calls for a training phase. In this study, k-fold cross-validation was utilized for obtaining the optimum weights and biases. This validation is useful when there are a small sets of data and when back propagation is used as a training method. There are 21 patterns, and the weights and biases are adjusted according to the errors that are generated and propagated back through the layers. These conditions lend itself to the use of k-fold cross validation. The fact that cross-validation proved to be useful when the model was trained using generated data was another reason k-fold cross validation was used. In this case, the number of folds is five. Four of the subsets have a size of 4 patterns and the last subset contains five patterns.

Recalling that k-fold validation refers to training with *k-1* subsets *k* times. The subset not used during the training is reserved for testing. The testing and training errors are compared. In this test, the training continued as the training errors reduced when testing error would increase, the training was stopped. The reason for stopping at this point was to avoid over training a network which results in the network unable to generalize and tends to simply memorize the patterns. Table 5.5 contains the testing and training errors associated with each of the 5 times that the network was trained. When the training was stopped, the biases and weights were recorded. The biases and weights from the five sessions were averaged. The average of the biases and weights can be found in Appendix E.

Table 5.5 Errors associated with cross validation

Training Set	Training Error (%)	Testing Error (%)	Iterations
1	0.13	0.03	2
2	0.13	0.36	4
3	0.42	0.18	2
4	0.37	0.20	2
5	0.43	0.28	2

CHAPTER 6

Discussion of Results

The focus of this chapter is a detailed discussion of the results. In this dissertation two models were built. The first model was to built to validated the methodology and built with generated data, and the latter model was built upon the validation of the methodology using the datasets that were collected using the Microsoft hosted website. This chapter is dedicated to the discussion of both implementations.

6.1 Validation of the Prediction Model

A generalization test was then run to determine how capable was the final model of generalizing. The sum of the errors as determined by the generalization test are 1.91 for the risk associated with the production server environment and 2.26 for the risk pertaining to client machine environment. The averages of the these errors, as calculated by the sum of the errors divide by the total number of patterns in the testing test which is 1000, are 0.0019 and 0.0023, respectively. The minimum of the errors and the maximum of the errors across all outputs is 0.00 and 0.10. The average error across outputs was calculated to be 0.004.

To validate the predictor, different patterns was randomly selected from the dataset and applied to the ANN. For each pattern, the prediction of the associated risks for each one of the categories was computed as the output of the two last nodes of the ANN. Those outputs were compared with the targets. The analysis with respect to the risk associated with the production environment are shown in Table 6.1, and the analysis of the errors associated with the risk to client machine environment can be found in Table 6.2.

Table 6.1 Errors associated with the production environment risk analysis

Pattern Number	Production Risk Target (%)	Production Risk Computed (%)	Production Risk Error (%)
37	82.79	86.76	0.08
119	90.16	90.61	0.00
246	88.52	88.55	0.03
313	87.70	88.95	0.00
432	85.25	89.08	0.07
561	82.80	82.80	0.00
681	91.80	89.58	0.02
749	50.00	76.71	0.04
824	82.79	79.80	0.04
938	86.89	88.59	0.00

Table 6.2 Errors associated with the client machine environment risk analysis

Pattern Number	Client Risk Target (%)	Client Risk Computed (%)	Client Risk Error (%)
37	78.69	78.67	0.00
119	88.52	90.00	0.01
246	77.87	84.72	0.20
313	82.79	84.94	0.02
432	81.15	83.36	0.02
561	34.43	38.70	0.09
681	93.44	86.03	0.27
749	45.90	54.46	0.37
824	37.70	42.10	0.10
938	80.33	83.27	0.04

6.2 Validation of the Practical Predictor

A model was built using the average of the weights and biases that were obtained during the k-fold cross validation. As part of the validation of this newly built model, a generalization test was performed. This generalization test was designed to ensure that the model was capable of generalizing and that it had not been overtrained. The sum of the errors as calculated during the generalization test was 12.68% for the risk associated with the production environment and the 17.34% for the risk pertaining to the client machines. The average of the errors was also obtained by dividing the sum of the errors by the number of patterns, 21. The averages of the errors are 6.04% for the production environment related risk and 8.26% for the risk associated with the client environment. The average of the errors across all outputs was found to be 1.43%. The minimum error across all of the outputs was 0.00% as opposed to the maximum which was calculated to be 7.94% .

Table 6.3 Errors associated with the production environment risk analysis

Pattern Number	Production Risk Target (%)	Production Risk Computed (%)	Production Risk Error (%)
1	5.00	0.00	0.63
2	0.00	0.00	0.04
3	0.00	0.00	0.49
4	0.00	0.00	0.89
5	0.00	0.00	0.20
6	0.00	0.00	0.03
7	0.00	0.00	0.13
8	0.00	0.00	0.86
9	0.00	0.00	0.75
10	10.00	0.00	1.48
11	0.00	0.00	0.06
12	0.00	0.00	0.12
13	1.00	0.00	0.19
14	0.00	0.00	0.07
15	0.00	0.00	0.11
16	15.00	000	3.49
17	5.00	0.00	0.47
18	10.00	0.00	72.54
19	0.00	0.00	0.04
20	0.00	0.00	0.04
21	0.00	0.00	0.05

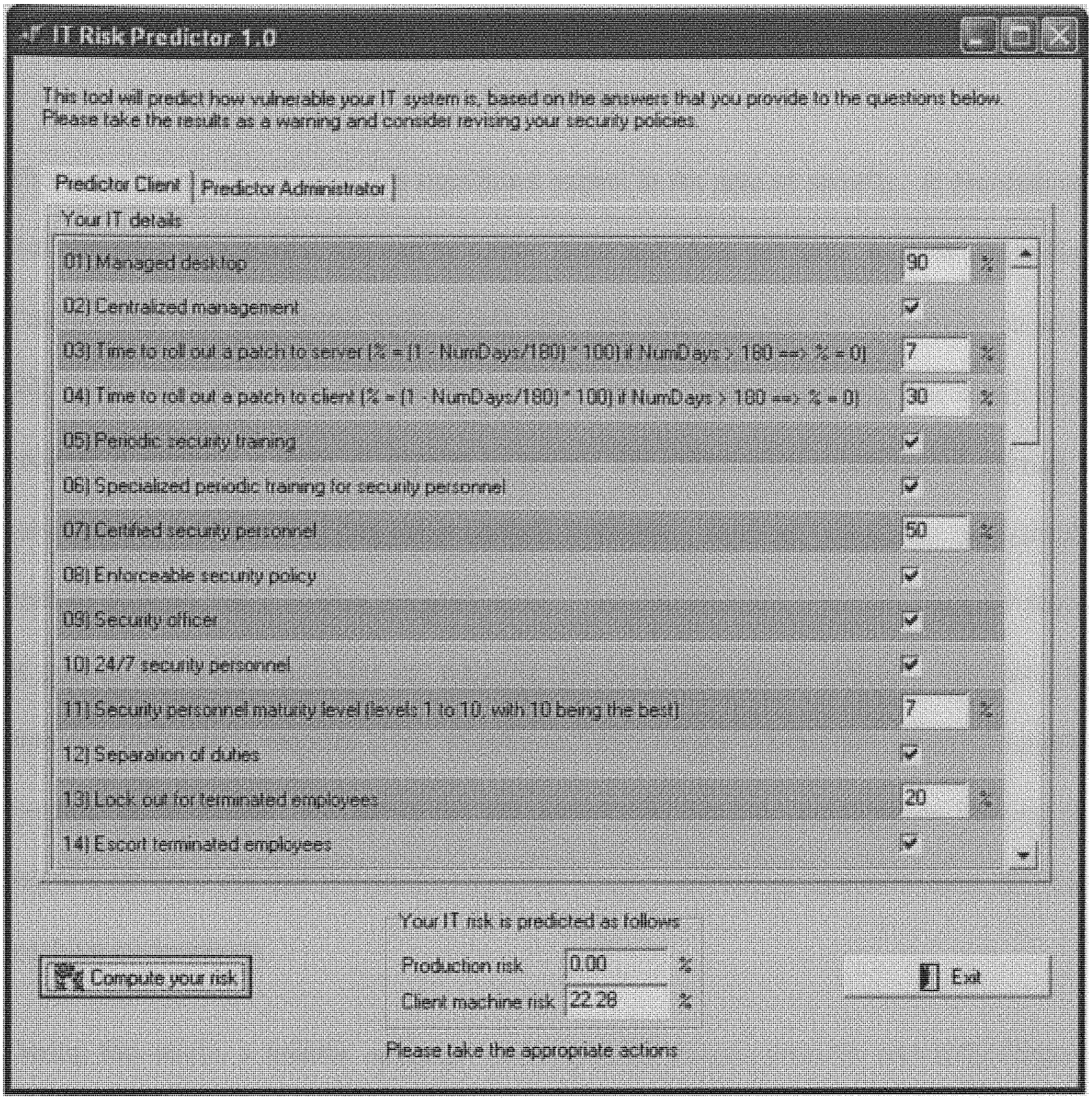
Another part of the validation of the predictor is to see how well the model would predict the risk to the production environment and to the client machine environment. The patterns used in the training were again submitted. The outputs obtained from the ANN were compared against the targets as defined in the datasets. Table 6.3 contains the risk to the production environment as computed by the model and furnished by the pattern. Likewise risk to the client environment was computed and compared with the target risk value furnished by client. This comparison is detailed in Table 6.4.

Table 6.4 Errors associated with the client machine environment risk analysis

Pattern Number	Production Risk Target (%)	Production Risk Computed (%)	Production Risk Error (%)
1	5.00	0.00	0.50
2	1.00	0.00	0.10
3	1.00	0.00	0.04
4	0.00	0.00	0.59
5	0.00	0.00	0.07
6	0.00	0.00	0.04
7	0.00	0.00	0.58
8	0.00	0.00	0.54
9	0.00	0.00	0.46
10	10.00	0.00	1.50
11	3.00	0.00	0.12
12	0.00	0.35	0.00
13	1.00	0.00	0.31
14	7.00	0.00	0.95
15	1.00	0.00	0.97
16	80.00	51.82	7.94
17	5.00	0.00	0.48
18	80.00	2.54	0.56
19	0.00	0.00	0.04
20	10.00	0.00	1.48
21	0.00	0.00	0.06

6.3 Risk Predictor Tool

After analyzing the results of the risk predictor model in terms of how well did the model predict the risk to the client and production companies, a risk predictor was built based on the final artificial neural network model. This tool is graphical user interface (GUI) that allows users to input characteristics of their production and client environments. Based on these inputs, the tool will normalize the inputted data to values between 0 and 1 and provide two results, the risk to the production environment and the risk to the client environment. The following figure is a screen shot of the tool.



This tool will predict how vulnerable your IT system is, based on the answers that you provide to the questions below.
Please take the results as a warning and consider revising your security policies.

Your IT details

01) Managed desktop 90 %

02) Centralized management ☑

03) Time to roll out a patch to server (% = (1 - NumDays/180) * 100) if NumDays > 180 ==> % = 0) 7 %

04) Time to roll out a patch to client (% = (1 - NumDays/180) * 100) if NumDays > 180 ==> % = 0) 30 %

05) Periodic security training ☑

06) Specialized periodic training for security personnel ☑

07) Certified security personnel 50 %

08) Enforceable security policy ☑

09) Security officer ☑

10) 24/7 security personnel ☑

11) Security personnel maturity level (levels 1 to 10, with 10 being the best) 7 %

12) Separation of duties ☑

13) Lock out for terminated employees 20 %

14) Escort terminated employees ☑

Your IT risk is predicted as follows

Production risk 0.00 %

Client machine risk 22.28 %

Please take the appropriate actions

Figure 6.1 Risk Predictor Tool

CHAPTER 7

Conclusion

The contribution of this work has significant impact in the area of security. It demonstrates that obtaining an actuarial risk can be easily done and does not have be time consuming. Traditionally, risk assessment tools simply rank and order risk and do not provide an actual risk. Obtaining an actual risk has been customarily a time consuming and costly effort because it requires a team of experts to review the information systems and attempt to calculate the cost of not having these systems available. Such an assessment has typically been so difficult that it is often not performed. The risk assessment tool that was developed as part of this study provides an actuarial risk in a very timely manner. In fact, the predictor tool simply requires a few minutes of time to input information about information systems' environment. As part of the risk assessment, the tool distinguishes between the risk to a environment that is a production ready mission critical environment from the client machine environment.

During this study, a holistic approach encompassing people, process, and technology to security was undertaken. Historically, security issues related to information systems have been focused only on technology. In this study, the technology was only factor. This work accounted for people and process in addition to technology. Although this work used data from customers using Microsoft technology, the model can assess risk to the environments regardless of the platform vendor. In fact, the customers were queried with respect to technology but at no time was a vendor specific query made.

Another significant result of this work is the methodology that was provided to build the security risk predictive model. The methodology provided a step by step approach on how to build, implement, and validate a predictor. As part of the methodology, much emphasis was placed on the collection of the data. Since the predictor was designed for assessing security risks, there was great apprehension with the obtaining data. Customers were repeatedly assured of the confidentially of the data., and an anonymous website was created for data capture.

As the model was built, this work at first relied on the recommendations that the rules of thumb provided. The rules of thumb are a good starting point, but they do not take into account the number of training sets or the complexity of the data. Rules of thumb tend to focus on the simplicity and the quantitative accuracy of the data. In this case, the rules of thumb recommended using a 46-93-2 topology, but this model was not suitable in this work. This study empirically revealed that a 46-25-2 topology was optimal.

When selecting the appropriate activation function for the hidden and output layers in this study, the empirical process revealed that the logistic sigmoid was a better fit than the Guassian function even though they are both differentiable functions. Gaussian functions are traditionally suited for clusters of data and classification scenarios. Clusters are mostly used when trying to classify data. In this study of work, the goal was to build an approximator, and it did not involve looking at clusters of data. This is why it was not surprising that the Gaussian function was proven that it was not the optimal activation function for the datasets. In this study, the Gaussian function was not a good choice for either of the two approximators that were built as evidenced by the results. The logistic sigmoidal function proved to be a better choice for the models that were built.

Although this work has made great strides in taking a proactive stance towards security, there are future enhancements that can be made. For instance, much of the responses to the survey were yes or no answers. At times, customers did respond with *sometimes*, *almost*, *mostly* instead of a blanket yes or no. These answers were mapped to values, yet the application of fuzzy logic could be used to better capture such responses. In the survey, the format for responding was free format instead of a simple binary selection in order to give customers the flexibility to provide such answers. The reasoning for this was to best capture the customer information without provide any filtering.

References

1. "ILOVEYOU virus", http://searchsecurity.techtarget.com/sDefinition/0,,sid14 gci214542,00.html, May 10, 2000.

2. Knowles, D. Perriot, F. and Szor, P., "W32.Blaster.Worm", http://security response.symantec.com/avcenter/venc/data/w32.blaster.worm.html, Symantec, February 26, 2004.

3. Shimonski, Robert J.,"Trojan Horse Primer", http://www.windowsecurity.com /articles/Trojan_Horse_Primer.html, July 23, 2004.

4. Richardson, Robert, "2003 CSI/FBI Computer Crime and Security Survey", http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf, Computer Security Institute, July 2003.

5. Norah, Laurence, "Security Attacks Cost Business Billions", http://itvibe.com /default.aspx?NewsID=2494, I.T. Vibe, April 28, 2004.

6. Lazarus, David, "Wells in a World of Woe after Theft", http://www.sfgate.com/ cgi-bin/article.cgi?file=/chronicle/archive/2003/11/21/MNGLT37MH71.DTL, San Francisco Chronicle, November 21,2003.

7. Debar, H., Becker, M., and Siboni, D., "A Neural Network Component for an Intrusion Detection System", *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA, pp. 240-258, May 1992..

8. Andress, Amanda, "Surviving Security: How to Integrate People, Process, and Technology", Second Edition. Auerbach Publications, December 2003.

9. McDowell, Mindi, "Avoid Social Engineering and Phishing Attacks" http://www.us-cert.gov/cas/tips/ST04-014.html, United States Computer Emergency Readiness Team, July 28, 2004.

10. CISSP book C. M., "Discrete Fourier Transforms when the Number of Data Samples Is Prime," *Proceedings of the IEEE*, Vol. 56, June 1968, pp. 1107-1108.

11. Patterns and Practices. "Security Operations for Microsoft Windows Server". Redmond, Washington: MS Press, 2002.

12. DeZulueta, M., Adjouadi, M., "Using Threat Modeling When Architecting a Healthcare System", *Proceedings of the 8th World Multi-Conference on Systematics, Cybernetics and Informatics* (Orlando, Florida, July 18-21, 2004).

13. Howard, Michael and LeBlanc, David. "Writing Secure Code". Redmond, Washington: MS Press, 2003.

14. Meier, J. D. and etal, “Building Secure Microsoft ASP.NET Applications”. Redmond, Washington: MS Press, 2003.

15. Funahashi, K.. “On the approximate realization of continuous mappings by neural networks”. Neural Networks, 2:183-192, 1989.

16. Hecht-Nielsen, R., “Kolmogorov's mapping neural network existence theorem”. *Proceedings of the International Conference on Neural Networks*, Volume 3, pages 11-14, New York, 1987. IEEE Press..

17. Hecht-Nielsen, R.,. “Theory of the back-propagation neural network”. *Proceedings of the International Joint Conference on Neural Networks*, Volume 1, pages 593-608, New York, 1989. IEEE Press.

18. Hornik, K., “Approximation capabilities of multilayer feedforward networks”. *Neural Networks*, 4:251-257, 1991.

19. Kurkova, V., “Kolmogorov's Theorem and multilayer neural networks”. Neural Networks, 5:501-506, 1992.

20. Hornik, K., Stinchcombe, M., and White, H.,. “Multi-layer feedforward networks are universal approximators”. *Neural Networks*, 2:359--366, 1989.

21. Sprecher, D. A., “One the structure of continuous functions of several variables”. *Transactions of the American Mathematical Society*, 115:340- 355, 1965.

22. Shalvi, Doron, “An Introduction to Artificial Neural Networks”, http://www.ee.umd.edu/medlab/papers/nnsumm/nnsumm.html, September 30, 1997.

23. Fausett, Laurene. “Fundamentals of Neural Networks. Architectures, Algorithms, and Applications”. Englewood Cliffs New Jersey: Prentice-Hall Inc., 1994.

24. Hebb, Donald, “The Organization of Behavior”. John Wiley & Sons, Inc., 1949.

25. Weiss, S.M. and Kulikowski, C.A., “Computer Systems That Learn”, Morgan Kaufmann. 1991.

26. Efron, B. and Tibshirani, R.J. “An Introduction to the Bootstrap”, London: Chapman & Hall. 1993.

27. Efron, B. and Tibshirani, R.J. (1997), “Improvements on cross-validation: The .632+ bootstrap method”, *Journal of the American Statistical Association*, 92, 548-560.

28. Shao, J., "Linear model selection by cross-validation," *Journal of the American Statistical Association*, 88, 486-494. 1993.

29. Cowan, J.D., Tesauro, G., and Alspector, J. (eds.) "Advances in Neural Information Processing Systems", San Mateo, CA: Morgan Kaufman, pp. 391-398. 1994.

30. Hjorth, J.S.U., "Computer Intensive Statistical Methods Validation, Model Selection, and Bootstrap", London: Chapman & Hall. 1994

31. The Math Works, Inc. "Neural Network Toolbox", http://www.mathworks.com /access /helpdesk/help/toolbox/nnet/, 1994 2004.

32. Spencer-Smith, Richard, "Neural Networks", http://www.mdx.ac.uk/www/psychology/cog/psy3250/Index.htm, 1996.

APPENDICES

Appendix A

Security Questionnaire

This questionnaire is designed to provide data to train a neural network that predicts the level of risk to virus attack.

1. Was your organization impacted by the Sasser worm? Yes or No

2. How many servers were hit? Percentage of server hit to total number of servers

3. How many clients were hit? Percentage of clients hit to total number of clients

4. How long was your organization working to address the impact of the virus after detecting being hit by the virus? Number of days spent patching, testing, etc.

Environment questions

1. Does your organization have a managed desktop environment?
Yes or No If yes, what percentage

2. Do your organization have a centralized management/administration of Information Technology services? Yes or No

3. Are patches tested before being deployed on a server? Yes or No

4. Time to roll out a patch to server? Days between a patch is announced and it is deployed. This may be an average number of days

5. Are patches tested before being deployed on a client? Yes or No

6. Time to roll out a patch to client? Days between a patch is announced and it is deployed. This may be an average number of days

7. Is there security awareness training for employees?
Yes or No If yes, is training done periodically? Yes or No

8. Is there specialized security training for security professionals?
Yes or No If yes, is the training done periodically? Yes or No

9. The percentage of security professionals that hold a security related certification?

10. Is there a security policy? Yes or No If yes, is it enforced?

11. Do you have security officer? Yes or No

12. Is the security personnel 24/7? Yes or No

13. What is the average maturity level (proficiency of security procedures) of the security personnel? Rate 1 to 10 with 10 being the highest level of maturity level

14.Is there a clear separation of duties among the employees? Yes or No

15. When an employee is terminated, what is delay between the termination and the locking out of the employee's access to system resources? Time in days or fraction of day

16. When an employee is terminated, is the employee escorted out by security?
Yes or No

17.The percentage of employees that run applications with non-administrative privileges?

18.Is there secured physical access to the production servers? Yes or No

19. Is there a firewall separating the internet from the web servers? Yes or No
If yes, are all ports other than internet ports (HTTP and HTTPS) blocked? Yes or No

20. Is there a firewall separating the web servers from the backend servers? Yes or No
If yes, are all ports other than necessary ports blocked? Yes or No

21.Does your organization use a anti-virus software? Yes or No
If yes, how often are the anti-virus signatures updated? Interval in days (eg daily = 1, weekly = 7, etc.)

22. Does your organization have a password policy? Yes or No
If yes, are client computers tested to ensure that they meet password policy? Yes or No

23. Does your organization require strong passwords? Yes or No If yes, is this tested? Yes or No

24. Does your company allow the reuse of passwords? Yes or No If yes, what is the period before a password or portion of a password can be reused? Period in days

25. Does your organization utilizes directory services for authentication? Yes or No

26.Does your organization make use of group policy? Yes or No

27. Does your organization use access control lists? Yes or No

28. Does your organization use the encrypted file system? Yes or No If yes, what percentage of the field machines use encrypted file system?

29.Does your organization have an Intrusion Detection System? Yes or No

30. Are there IP restrictions? Yes or No

31. Are there DNS restrictions? Yes or No

32.Does your organization use 2 token authentication (eg, biometric and password, smart card and password)? Yes or No

33. Is encrypted login used? Yes or No

34. Is Digital Rights Management utilized? Yes or No

35. Is Instant Messaging allowed? Yes or No

36. Are email attachments that are executables or scripts blocked? Yes or No

37. Are there email quotas? Yes or No

38. Does your organization utilize digital certificates? Yes or No

39. Are domain accounts changed when an IT pro is terminated? Yes or No

40. Does your organization use IPSEC? Yes or No

41. Does your organization develop any applications? Yes or No
a. If yes, are software code reviews required? Yes or No
b. If yes to 41, is software tested by a quality department? Yes or No
c. If yes to 41, is there a strict validation of input? Yes or No
d. If yes to 41, are error messages filtered? Yes or No
d. If yes to 41, is threat modeling performed? Yes or No

42. Are servers routinely backed up? Yes or No If yes, what is period in days?

43. Does your organization pay its security professionals according to industry standard? Yes or No If no, is it above or below? Above or Below

44. Does your organization pay its information technology professionals according to industry standard? Yes or No If no, is it above or below? Above or Below

Appendix B

Customer Responses

Was your organization impacted by the Sasser virus	How many servers were hit	Percentage of server hit to total number of servers	How many clients were hit	Percentage of clients hit to total number of clients
Yes	2-3	005%	250	5%
Yes	0	0	<50	Less than 1%
Yes	0	0	100	.01
No	0	0	7	.001
No	0	0	0	0
No	0	0	0	0
No	0	0	0	0
No	0	0	0	0
No	0	0	0	0
Yes	10	.1	100	.1
No	0	0	10	.03%
No	0	0	0	0
No	I think 0 managed servers. Unknown # for rogue servers.	< 1%	I think 0 managed clients. Unknown # for rogue clients.	< 1%
Yes	0	0	400	7
Yes	0	0	1	1
Yes	5	15%	Many	80%
Yes	10	5%	150	5%
Yes		10%		80%
no		0		0
yes		0		10%
no				

How long was your organization working to address the impact of the virus after detecting being hit by the virus	Number of days spent patching, testing, etc
2 DAYS	5 days
Had resources focused on Sasser for about 4 days	Most patching was done in less than 4 days
2 weeks	approximately 2 weeks
2 days	10 days
0	0
0	0
0	5
0	10
0	1
7 days	21
We were patched	7
0	0
2 weeks, primarily reporting on patch status, mitigating steps (sw restriciton GPO)	30 or so. Began deploy w/in 48 hours of release. Checked compliance numbers when FullDisclosure started indicating Sasser was coming. Found 1 SUS server misconfigured (https), result ~30% of clients not patched. Fixed 48 hours or so before Sasser. Clients at +95% patched by mid-week after Sasser. Servers patched for Sasser by 1st weekend after Sasser. Servers fully patched around 2nd/3rd weekend after Sasser. Distributed servers (not data center) now using SUS.
4 days	You mean patching after being hit? 4 Or testing before being deploying? 7 Or after deploying before being hit? 30
4 hours	2
3 days	7
12 hours	5
	16 hours
	2
	2

Does your organization have a managed desktop environment	If yes, what percentage	Does your organization have a centralized management/administration of Information Technology services
Yes	90%	Yes
Yes	Almost 100%	Yes
No		Yes
No		No
Yes		Yes
Yes	100	Yes
Yes	80	Yes
Yes	75	Yes
Yes	100	Yes
Yes	90	Yes
Yes	90%	Yes
Yes		Yes
Yes	Good question. %age of what? ~90% of company owned desktops are managed (probably higher). Contractor/consultant desktop count is ~25% of company owned(?).	Yes
Yes	95	Yes
Yes	100	Yes
Yes	100	Yes
Yes	90	Yes
yes	80%	Yes
yes	100%	Yes
yes	98%	yes
yes	85%	yes

Are patches tested before being deployed on a server	**Time to roll out a patch to server? Days between a patch is announced and it is deployed**	**Are patches tested before being deployed on a client**	**Time to roll out a patch to client? Days between a patch is announced and it is deployed**
Yes	30	Yes	14
Yes	14	Yes	5
Yes	10	Yes	5
No	10	Yes	21
Yes		Yes	5
Yes	2	Yes	1
Yes		Yes	5
Yes	3	Yes	5
Yes	4	Yes	4
Yes	21	Yes	21
Yes	14	Yes	14
Yes	5	Yes	2
Yes	3	Yes	2
Yes	7	Yes	7
Yes	14	Yes	5
Yes	2	Yes	2
Yes	4	Yes	5
Yes, no formal process	5	Yes but no formal process	3
Yes, formal process	critical patch 24 hours, non-critical 1 month	yes, formal	critical patch 24 hours, non-critical 1 month
yes	2 days	yes	2 days
yes no formal process	5 days	yes	5 days

Is there security awareness training for employees	If yes, is training done periodically	Is there specialized security training for security professionals	If yes, is the training done periodically
No	No	Yes	Yes
No	No	Yes	Yes
No	No	No	No
No		Yes	No
No	No		No
Yes	Yes	No	
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
Yes	No	Yes	Yes
Yes	Yes	Yes	No
Yes	No	Yes	Yes
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
No	No	No	No
Yes	Yes	No	No
No		Yes	yes
yes	Yes	Yes	yes
no		yes	yes
yes		yes	yes

The percentage of security professionals that hold a security related certification	Is there a security policy	If yes, is it enforced	Do you have a security officer
100	Yes	Yes	Yes
50%	Yes	No	No
0	Yes	No	No
0	Yes	Yes	Yes
0	Yes	Yes	No
0	Yes	No	No
0	Yes	Yes	Yes
	Yes	Yes	Yes
100	Yes	Yes	No
5	Yes	Yes	Yes
100%	Yes	Yes	Yes
	Yes	Yes	Yes
0% ? I only know 1 person & the cert is IDS.	Yes	Yes	Yes
30	Yes	Yes	Yes
1	Yes	Yes	Yes
100%	Yes	Yes	No
	Yes	Yes	Yes
	Yes	no	yes
100%	Yes	yes	yes
100%	Yes	yes	yes
	Yes	yes	no

Is the security personnel 24/7	What is the average maturity level of the security personnel	Is there a clear separation of duties among the employees	what is delay between the termination and the locking out of the employees access to system resources
No	8	Yes	.25
No	7	Yes	Same day
Yes	4	No	Depends best .1, worst NEVER
Yes	8	No	15 minutes
Yes	7	Yes	0.5
No		Yes	
No	7	No	0
Yes	5	Yes	2
	8	No	1
Yes	7	Yes	.5
Yes	9	Yes	1
Yes	8	Yes	1
Yes	9	No	less than a day (8 hours).
Yes	8	No	1
Yes	7	No	1
Yes	5	No	0
No	6	No	1
yes	8	no	1 day
yes	9	yes	< 1 day
yes	7	yes	within 2 days
yes	8	no	1 day

When an employee is terminated, is the employee escorted out by security	What percentage of employees run applications using non-administrative privileges	Is there secured physical access to the production servers
No	95	Yes
No		Yes
No	90	Yes
Yes	10	Yes
No	80	No
No		Yes
Yes	50-50	Yes
No		Yes
No	5	Yes
Yes	25	Yes
Yes	0%	Yes
No	10	Yes
Yes	~80%, probably higher	Yes
Yes	20	Yes
No	50	Yes
No	90	Yes
Yes	90	Yes
yes	85%	yes
yes		yes
yes	90%	yes
yes		Yes

Is there a firewall separating the internet from the web servers	If yes, are all ports other than internet ports (HTTP and HTTPS) blocked	Is there a firewall separating the web servers from the backend servers	If yes, are all ports other than necessary ports blocked
Yes	No	Yes	Yes
Yes	No	Yes	Yes
Yes	Yes	Yes	Yes
Yes	No	Yes	No
Yes	Yes	No	No
Yes	Yes	Yes	Yes
Yes	No	No	No
Yes	Yes	Yes	Yes
Yes	No	No	No
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes
Yes	No	Yes	No
Yes	No	Yes	Yes
Yes	Yes	Yes	Yes
yes	yes	yes	yes
yes	yes	yes	yes
yes	yes	yes	yes
yes	yes	yes	yes

Does your organization use a anti-virus software	If yes, how often are the anti-virus signatures updated	Does your organization have a password policy	If yes, are client computers tested to ensure that they meet the password policy
Yes	7	No	No
Yes	SMTP and Exchange Servers are updated in realtime (15 mins). File/Print and workstations weekly, or more frequently depending on the severity of the DAT.	Yes	Yes
Yes	.1	Yes	No
Yes	1	Yes	No
No	1	Yes	No
Yes	1	Yes	Yes
Yes	1	Yes	Yes
Yes	1	Yes	Yes
Yes	1	Yes	Yes
Yes	1	Yes	Yes
Yes	7	Yes	Yes
Yes	2		No
Yes	1	Yes	No
Yes	1	Yes	No
Yes	7	Yes	Yes
Yes	7	Yes	Yes
Yes	Daily	Yes	Yes
yes		yes	yes
yes	1	yes	yes
yes	1	yes	yes
yes	1	yes	yes

Does your organization require strong passwords	If yes, is this tested	Does your company allow the reuse of passwords	If yes, what is the period before a password or portion of a password can be reused
No	No	No	
Yes	Yes	Yes	5
Yes	No	Yes	30
Yes	Yes	No	
Yes	Yes	No	180
Yes	Yes	Yes	120
Yes	Yes	No	
Yes	Yes	No	
Yes	Yes	No	
Yes	Yes	Yes	730
No	No	No	
No	No	No	
Yes	Yes	Yes	1
Yes	Yes	No	400
Yes	Yes	No	
Yes	Yes	No	
Yes	Yes	No	
yes	no	yes	
yes	yes	yes	
yes	yes	yes	90 days
yes	yes	yes	

Does your organization utilize directory services for authentication	Does your organization make use of group policy	Does your organization use access control lists	Does your organization use the encrypted file system	If yes, what percentage of the field machines use encrypted file system
No	No	Yes	No	
Yes	Yes	Yes	No	
Yes	Yes	Yes	No	
Yes	No	Yes	No	
Yes	Yes	Yes	No	
Yes	Yes	Yes	No	
Yes	Yes	Yes	No	
Yes	Yes	Yes	No	
Yes	Yes	Yes	Yes	20
Yes	Yes	Yes	Yes	10
Yes	Yes	Yes	No	
Yes	Yes	Yes	Yes	10
Yes	Yes	Yes	No	< 1 %
Yes	Yes	Yes	No	
Yes	Yes	Yes	No	
Yes	Yes	Yes	No	
Yes	Yes	Yes	No	
yes	yes	Yes	yes	
yes	yes	Yes	yes	
yes	yes	Yes	no	
yes	yes	Yes	yes	

Does your organization have an Intrusion Detection System	Are there IP restrictions	Are there DNS restrictions	Does your organization use 2 token authentication
Yes	Yes	Yes	No
Yes	No	Yes	Yes
Yes	Yes	Yes	Yes
No	No	No	No
Yes	Yes	Yes	No
No			No
Yes	Yes	Yes	Yes
Yes	No	No	Yes
Yes	Yes	Yes	No
Yes	Yes	Yes	No
Yes	Yes	Yes	No
Yes	Yes	Yes	Yes
Yes	Yes	Yes	No
Yes	No	No	No
Yes	Yes	Yes	No
Yes	Yes	No	No
Yes	Yes	Yes	No
yes	yes	Yes	no
yes	yes	Yes	no
yes	yes	Yes	yes
yes	yes	yes	yes

Is encrypted login used	Is Digital Rights Management utilized	Is Instant Messaging allowed	Are email attachments that are executables or scripts blocked	Are there email quotas
Yes	Yes	No	Yes	Yes
Yes	No	Yes	Yes	Yes
Yes	No	Yes	Yes	No
No	No	Yes	Yes	Yes
No	No	Yes	Yes	No
		Yes	Yes	No
No	Yes	No	Yes	Yes
No	No	No	Yes	Yes
No	No	Yes	Yes	Yes
Yes	No	Yes	No	Yes
Yes	No	No	Yes	Yes
Yes	No	Yes	Yes	No
Yes	No	Yes	Yes	Yes
Yes	No	Yes	Yes	Yes
Yes	No	No	Yes	Yes
Yes	No	Yes	Yes	Yes
No	No	No	Yes	Yes
no	no	no	yes	yes
yes	testing	yes	yes	yes
yes	no	yes	yes	no
yes	yes	no	yes	yes

Does your organization utilize digital certificates	Are domain accounts changed when an IT pro is terminated	Does your organization use IPSEC	Does your organization develop any applications
No	No	No	No
Yes	Yes	Yes	Yes
No	No	No	Yes
Yes	Yes	No	Yes
No	Yes	No	Yes
Yes	No	No	Yes
No	No		Yes
No	Yes	No	Yes
Yes	No	No	No
Yes	Yes	No	Yes
Yes	No	Yes	No
No	No	Yes	Yes
Yes	No	Yes	Yes
No	Yes	No	Yes
Yes	No	No	Yes
Yes	No	Yes	No
No	Yes	No	Yes
no	sometimes	yes	yes
yes	yes	yes	yes
no	yes	yes	no
yes	yes	yes	yes

If yes to developing in-house applications, are software code reviews required	If yes to developing in-house applications, is software tested by a quality department	If yes to developing in-house applications, is there a strict validation of input	If yes to developing in-house applications, are error messages filtered	If yes to developing in-house applications, is threat modeling performed
Yes	Yes	Yes	Yes	Yes
No	No	No	No	No
No	No	No	No	No
No	No	Yes	Yes	Yes
Yes	Yes	Yes	Yes	Yes
Yes	Yes	No	No	No
Yes	Yes	No	No	No
No	No	No	No	No
Yes	Yes	Yes	Yes	No
Yes	No	No	Yes	No
Yes	Yes	Yes	Yes	Yes
No	No	No	No	No
Yes	Yes	No	No	No
Yes	Yes	Yes	Yes	Yes
sometimes	yes			
yes	yes	yes	yes	yes
no	no	no	yes	no

Are servers routinely backed up	If yes, what is period in days	Does your organization pay its security professionals according to industry standard	Security Professionals: If no, is it above or below
Yes	1	Yes	
Yes	1	Yes	
Yes	1	No	Below
Yes	1	Yes	
Yes	1	Yes	Above
Yes	1	No	Above
Yes	7	No	Above
Yes		Yes	
Yes	1	Yes	
Yes	1	Yes	
Yes		No	Above
Yes	1	Yes	
Yes	1	No	Below
Yes	1	Yes	
Yes	1	Yes	
Yes	1	No	Below
Yes	1	Yes	Above
yes	some daily some weekly	yes	
yes	most daily	yes	
yes	most daily	yes	
yes	some daily	yes	

Does your organization pay its information technology professionals according to industry standard	If no, is it above or below
Yes	
Yes	
No	Below
Yes	
No	Below
Yes	
Yes	Above
Yes	
Yes	
Yes	
Yes	
Yes	
No	Below
Yes	
Yes	
Yes	
Yes	Above
yes	
yes	
yes	
yes	

Appendix C

Normalized Customer Responses

Managed desktop percentage	Centralized management	Time to roll out a patch to server	Time to roll out a patch to client
0.9	1	0.83	0.92
0.95	1	0.92	0.97
0	1	0.94	0.97
0	0	0.94	0.88
0.5	1	0.00	0.97
1	1	0.99	0.99
0.8	1	0.00	0.97
0.75	1	0.98	0.97
1	1	0.98	0.98
0.9	1	0.88	0.88
0.9	1	0.92	0.92
0.5	1	0.97	0.99
0.9	1	0.98	0.99
0.95	1	0.96	0.96
1	1	0.92	0.97
1	1	0.99	0.99
0.9	1	0.98	0.97
0.8	1	0.97	0.98
1	1	0.99	0.99
0.98	1	0.99	0.99
0.85	1	0.97	0.97

Periodic security training	Specialized Periodic Training for Security Personnel	Certified Security Personnel	Enforceable Security Policy
0	1	1	1
0	1	0.5	0
0	0	0	0
0	0	0	1
0	0	0	1
1	0	0	0
1	1	0	1
1	1	0	1
1	1	1	1
1	1	0.05	1
0	1	1	1
1	0	0	1
0	1	0	1
1	1	0.3	1
1	1	0.01	1
0	0	1	1
1	0	0	1
0	1	0	0
1	1	0.01	1
0	1	0.01	1
0	1	0	1

Security officer	24/7 security personnel	Security personnel maturity level	Separation of duties	Lock out for terminated employees
1	0	0.8	1	0.75
0	0	0.7	1	0.67
0	1	0.4	0	0.90
1	1	0.8	0	0.99
0	1	0.7	1	0.50
0	0	0	1	0.00
1	0	0.7	0	1.00
1	1	0.5	1	0.00
0	0	0.8	0	0.00
1	1	0.7	1	0.50
1	1	0.9	1	0.00
1	1	0.8	1	0.00
1	1	0.9	0	0.67
1	1	0.8	0	0.00
1	1	0.7	0	0.00
0	1	0.5	0	1.00
1	0	0.6	0	0.00
1	1	0.8	0	0.00
1	1	0.9	1	0.67
1	1	0.7	1	0.00
0	1	0.8	0	0.00

Escort terminated employees	Least privilege	Secured physical access	Block ports on web facing firewall	Block ports on backend facing firewall	Up to date virus signatures	Test password policy
0	0.95	1	0	1	0.86	0
0	0	1	0	0	1.00	0
0	0.9	1	0	1	1.00	0
1	0.1	1	0	0	1.00	0
0	0.8	0	0	1	0.00	0
0	0	1	0	0	1.00	0
1	0.5	1	1	1	1.00	0
0	0	1	1	1	0.86	0
0	0.05	1	0	1	0.86	0
1	0.25	1	1	1	0.86	0
1	0	1	0	1	0.86	0
0	0.1	1	0	0	0.86	0
1	0.8	1	0	1	0.86	0
1	0.2	1	0	0	0.86	0
0	0.5	1	0	1	1.00	0
0	0.9	1	1	1	1.00	0
1	0.9	1	1	1	0.86	0.5
1	0.85	1	0	1	0.00	0
1	0	1	1	1	0.86	0
1	0.9	1	0	0	1.00	0
1	0	1	0	0	1.00	0

Test strong password	Password reuse	Directory services	Group policy	Access Control Lists	Encrypted File System Usage	Intrusion Detection System
0	0.00	0	0	1	0	1
1	0.00	1	1	1	0	1
0	0.00	1	1	1	0	1
0	0.00	1	0	1	0	0
1	0.00	1	1	1	0	1
1	0.00	1	1	1	0	0
1	0.00	1	1	1	0	1
0	0.00	1	1	1	0	1
1	0.00	1	1	1	1	1
0	0.00	1	1	1	1	1
1	0.00	1	1	1	0	1
1	0.00	1	1	1	1	1
1	0.00	1	1	1	0	1
1	0.00	1	1	1	0	1
1	0.00	1	1	1	0	1
1	0.00	1	1	1	0	1
1	0.00	1	1	1	0	1
0	0.00	1	1	1	1	1
1	0.00	1	1	1	1	1
0	0.00	1	1	1	0	1
0	0.00	1	1	1	1	1

IP restrictions	DNS restrictions	Multi-token authentication	Encrypted login	Digital Rights Management	Instant Messaging Allowed
1	1	0	1	1	0
0	1	1	1	0	1
1	1	1	1	0	1
0	0	0	0	0	1
1	1	0	0	0	1
0	0	0	0	0	1
1	1	1	0	1	0
0	0	1	0	0	0
1	1	0	0	0	1
1	1	0	1	0	1
1	1	0	1	0	0
1	1	1	1	0	1
1	1	0	1	0	1
0	0	0	1	0	1
1	1	0	1	0	0
1	0	0	1	0	1
1	1	0	0	0	0
1	1	0	0	0	0
1	1	0	1	0.5	1
1	1	1	1	0	1
1	1	1	1	1	0

Email Attachments Blocked	Email Quotas	Digital Certificates	Domain accounts changed when IT Pro terminated	IPSEC
1	1	0	0	0
1	1	1	1	1
1	0	0	0	0
1	1	1	1	0
1	0	0	1	0
1	0	1	0	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
0	1	1	1	0
1	1	1	0	1
1	0	0	0	1
1	1	1	0	1
1	1	0	1	0
1	1	1	0	0
1	1	1	0	1
1	1	0	1	0
1	1	0	0.5	1
1	1	1	1	1
1	0	0	1	1
1	1	1	1	1

Code reviews for in house apps	QA for in house apps	Input validation for in house apps	Error message filtering for in house apps	Threat modeling for in house apps
0	0	0	0	0
1	1	1	1	1
0	0	0	0	0
0	0	0	0	0
0	0	1	1	1
1	1	1	1	1
1	1	0	0	0
1	1	0	0	0
0	0	0	0	0
1	1	1	1	0
0	0	0	0	0
1	0	0	1	0
1	1	1	1	1
0	0	0	0	0
1	1	0	0	0
0	0	0	0	0
1	1	1	1	1
0.5	1	0	0	0
1	1	1	1	1
0	0	0	0	0
0	0	0	1	0

Back up	Pay scale for security personnel	Pay scale for IT Pros	Production Risk	Client Machine Risk
0.00	0.5	0.5	0.05	0.05
0.00	0.5	0.5	0	0.01
0.00	0	0	0	0.01
0.00	0.5	0.5	0	0.001
0.00	1	0	0	0
0.00	1	0.5	0	0
0.00	1	1	0	0
0.00	0.5	0.5	0	0
0.00	0.5	0.5	0	0
0.00	0.5	0.5	0.1	0.1
0.00	1	0.5	0	0.03
0.00	0.5	0.5	0	0
0.00	0	0	0.01	0.01
0.00	0.5	0.5	0	0.07
0.00	0.5	0.5	0	0.01
0.00	0	0.5	0.15	0.8
0.00	1	1	0.05	0.05
0.00	0.5	0.5	0.10	0.8
0.00	0.5	0.5	0.00	0
0.00	0.5	0.5	0.00	0.1
0.00	0.5	0.5	0.00	0

Appendix D

Averaged Weights and Biases Associated the Predictor Model Built using Generated Data

Layers:

Neurons in the Input Layer	Neurons in the Hidden Layer	Neurons in the Output Layer
46	25	2

Biases:

Node ID	Layer #	Neuron #	Activation Function	Bias
N1,1	1	1	purelin	0.493935
N1,2	1	2	purelin	0.861392
N1,3	1	3	purelin	0.663258
N1,4	1	4	purelin	0.867076
N1,5	1	5	purelin	-0.783493
N1,6	1	6	purelin	0.904942
N1,7	1	7	purelin	0.001269
N1,8	1	8	purelin	-0.007588
N1,9	1	9	purelin	-0.810463
N1,10	1	10	purelin	-0.648547
N1,11	1	11	purelin	-0.611344
N1,12	1	12	purelin	-0.056233
N1,13	1	13	purelin	0.219575
N1,14	1	14	purelin	-0.126197
N1,15	1	15	purelin	-0.109497
N1,16	1	16	purelin	-0.950029
N1,17	1	17	purelin	0.467853
N1,18	1	18	purelin	-0.6364
N1,19	1	19	purelin	-0.10791
N1,20	1	20	purelin	0.373653
N1,21	1	21	purelin	0.428677
N1,22	1	22	purelin	-0.301855
N1,23	1	23	purelin	-0.691266
N1,24	1	24	purelin	-0.364558
N1,25	1	25	purelin	0.925404
N1,26	1	26	purelin	-0.404707
N1,27	1	27	purelin	0.23508
N1,28	1	28	purelin	-0.664576
N1,29	1	29	purelin	0.092739
N1,30	1	30	purelin	-0.600047
N1,31	1	31	purelin	0.252599
N1,32	1	32	purelin	0.165617

N1,33	1	33	purelin	0.814111
N1,34	1	34	purelin	0.145972
N1,35	1	35	purelin	-0.885967
N1,36	1	36	purelin	-0.692788
N1,37	1	37	purelin	0.582883
N1,38	1	38	purelin	0.737172
N1,39	1	39	purelin	0.023548
N1,40	1	40	purelin	-0.293668
N1,41	1	41	purelin	0.256132
N1,42	1	42	purelin	-0.408731
N1,43	1	43	purelin	-0.768662
N1,44	1	44	purelin	0.922053
N1,45	1	45	purelin	0.669764
N1,46	1	46	purelin	-0.409569
N2,1	2	1	logsig	0.408118
N2,2	2	2	logsig	0.007267
N2,3	2	3	logsig	-0.823641
N2,4	2	4	logsig	0.828579
N2,5	2	5	logsig	-0.381537
N2,6	2	6	logsig	-0.197377
N2,7	2	7	logsig	0.617874
N2,8	2	8	logsig	0.360576
N2,9	2	9	logsig	-0.902963
N2,10	2	10	logsig	-0.231285
N2,11	2	11	logsig	0.157857
N2,12	2	12	logsig	-0.470795
N2,13	2	13	logsig	-0.89701
N2,14	2	14	logsig	-0.923409
N2,15	2	15	logsig	0.637806
N2,16	2	16	logsig	-0.951283
N2,17	2	17	logsig	-0.947694
N2,18	2	18	logsig	0.809114
N2,19	2	19	logsig	-0.251051
N2,20	2	20	logsig	0.672725
N2,21	2	21	logsig	0.622592
N2,22	2	22	logsig	0.131807
N2,23	2	23	logsig	-0.025849
N2,24	2	24	logsig	-0.097142
N2,25	2	25	logsig	0.235519
N3,1	3	1	logsig	-0.150297
N3,2	3	2	logsig	0.023945

Weights:

Weight ID	Source Layer #	Source Neuron #	Target Layer #	Target Neuron #	Weight
W1,1,2,1	1	1	2	1	-0.160458
W1,1,2,2	1	1	2	2	-0.046777
W1,1,2,3	1	1	2	3	0.11645
W1,1,2,4	1	1	2	4	0.164436
W1,1,2,5	1	1	2	5	0.58847
W1,1,2,6	1	1	2	6	0.306219
W1,1,2,7	1	1	2	7	-0.043741
W1,1,2,8	1	1	2	8	0.888825
W1,1,2,9	1	1	2	9	-0.268881
W1,1,2,10	1	1	2	10	-0.871529
W1,1,2,11	1	1	2	11	-0.544709
W1,1,2,12	1	1	2	12	-0.064104
W1,1,2,13	1	1	2	13	0.280467
W1,1,2,14	1	1	2	14	-0.650036
W1,1,2,15	1	1	2	15	0.390022
W1,1,2,16	1	1	2	16	0.600315
W1,1,2,17	1	1	2	17	0.470086
W1,1,2,18	1	1	2	18	-0.455363
W1,1,2,19	1	1	2	19	0.62123
W1,1,2,20	1	1	2	20	0.709712
W1,1,2,21	1	1	2	21	-0.710408
W1,1,2,22	1	1	2	22	0.60703
W1,1,2,23	1	1	2	23	0.192537
W1,1,2,24	1	1	2	24	-0.874257
W1,1,2,25	1	1	2	25	-0.210343
W1,2,2,1	1	2	2	1	-0.246498
W1,2,2,2	1	2	2	2	-0.014863
W1,2,2,3	1	2	2	3	-0.66686
W1,2,2,4	1	2	2	4	0.09854
W1,2,2,5	1	2	2	5	0.605175
W1,2,2,6	1	2	2	6	-0.973507
W1,2,2,7	1	2	2	7	-0.326147
W1,2,2,8	1	2	2	8	-0.167962
W1,2,2,9	1	2	2	9	0.765416
W1,2,2,10	1	2	2	10	1.019347
W1,2,2,11	1	2	2	11	0.266753
W1,2,2,12	1	2	2	12	-0.875647
W1,2,2,13	1	2	2	13	-0.932659
W1,2,2,14	1	2	2	14	0.122003
W1,2,2,15	1	2	2	15	0.605992
W1,2,2,16	1	2	2	16	-0.889185
W1,2,2,17	1	2	2	17	0.915585
W1,2,2,18	1	2	2	18	0.023536
W1,2,2,19	1	2	2	19	-0.472761

W1,2,2,20	1	2	2	20	-0.357405
W1,2,2,21	1	2	2	21	0.21388
W1,2,2,22	1	2	2	22	0.995062
W1,2,2,23	1	2	2	23	0.562994
W1,2,2,24	1	2	2	24	-0.308461
W1,2,2,25	1	2	2	25	-0.510897
W1,3,2,1	1	3	2	1	0.318601
W1,3,2,2	1	3	2	2	0.177576
W1,3,2,3	1	3	2	3	0.573386
W1,3,2,4	1	3	2	4	0.117209
W1,3,2,5	1	3	2	5	-0.819895
W1,3,2,6	1	3	2	6	0.49021
W1,3,2,7	1	3	2	7	-0.599267
W1,3,2,8	1	3	2	8	0.155369
W1,3,2,9	1	3	2	9	-0.156117
W1,3,2,10	1	3	2	10	-0.352935
W1,3,2,11	1	3	2	11	-0.6531
W1,3,2,12	1	3	2	12	1.064246
W1,3,2,13	1	3	2	13	-0.302432
W1,3,2,14	1	3	2	14	0.695889
W1,3,2,15	1	3	2	15	-0.307017
W1,3,2,16	1	3	2	16	-0.235537
W1,3,2,17	1	3	2	17	0.895149
W1,3,2,18	1	3	2	18	0.011738
W1,3,2,19	1	3	2	19	0.609721
W1,3,2,20	1	3	2	20	-0.139305
W1,3,2,21	1	3	2	21	0.537113
W1,3,2,22	1	3	2	22	0.725148
W1,3,2,23	1	3	2	23	-0.882668
W1,3,2,24	1	3	2	24	-0.770414
W1,3,2,25	1	3	2	25	-0.750546
W1,4,2,1	1	4	2	1	-0.555131
W1,4,2,2	1	4	2	2	-0.601382
W1,4,2,3	1	4	2	3	0.24596
W1,4,2,4	1	4	2	4	0.671279
W1,4,2,5	1	4	2	5	0.33775
W1,4,2,6	1	4	2	6	0.171306
W1,4,2,7	1	4	2	7	-0.51814
W1,4,2,8	1	4	2	8	-0.571614
W1,4,2,9	1	4	2	9	-0.793961
W1,4,2,10	1	4	2	10	0.666084
W1,4,2,11	1	4	2	11	0.082683
W1,4,2,12	1	4	2	12	-0.327864
W1,4,2,13	1	4	2	13	0.850589
W1,4,2,14	1	4	2	14	-0.559673
W1,4,2,15	1	4	2	15	0.18483
W1,4,2,16	1	4	2	16	0.082431

W1,4,2,17	1	4	2	17	-0.303238
W1,4,2,18	1	4	2	18	0.321119
W1,4,2,19	1	4	2	19	0.683187
W1,4,2,20	1	4	2	20	-0.581843
W1,4,2,21	1	4	2	21	-1.044957
W1,4,2,22	1	4	2	22	-0.538104
W1,4,2,23	1	4	2	23	-0.433982
W1,4,2,24	1	4	2	24	-0.45449
W1,4,2,25	1	4	2	25	-0.019083
W1,5,2,1	1	5	2	1	0.431071
W1,5,2,2	1	5	2	2	-0.709853
W1,5,2,3	1	5	2	3	-0.908978
W1,5,2,4	1	5	2	4	-0.257426
W1,5,2,5	1	5	2	5	0.035264
W1,5,2,6	1	5	2	6	-0.326753
W1,5,2,7	1	5	2	7	-0.390912
W1,5,2,8	1	5	2	8	0.693847
W1,5,2,9	1	5	2	9	-0.66854
W1,5,2,10	1	5	2	10	0.617919
W1,5,2,11	1	5	2	11	0.873805
W1,5,2,12	1	5	2	12	-0.841778
W1,5,2,13	1	5	2	13	0.216334
W1,5,2,14	1	5	2	14	-0.704582
W1,5,2,15	1	5	2	15	-0.811761
W1,5,2,16	1	5	2	16	-0.483852
W1,5,2,17	1	5	2	17	-0.817763
W1,5,2,18	1	5	2	18	1.002609
W1,5,2,19	1	5	2	19	0.101816
W1,5,2,20	1	5	2	20	0.846227
W1,5,2,21	1	5	2	21	-0.39399
W1,5,2,22	1	5	2	22	-0.408015
W1,5,2,23	1	5	2	23	0.456716
W1,5,2,24	1	5	2	24	-0.568666
W1,5,2,25	1	5	2	25	-0.249422
W1,6,2,1	1	6	2	1	0.085219
W1,6,2,2	1	6	2	2	0.44249
W1,6,2,3	1	6	2	3	-0.249864
W1,6,2,4	1	6	2	4	0.691674
W1,6,2,5	1	6	2	5	-0.607413
W1,6,2,6	1	6	2	6	0.750896
W1,6,2,7	1	6	2	7	0.477972
W1,6,2,8	1	6	2	8	0.105378
W1,6,2,9	1	6	2	9	0.995307
W1,6,2,10	1	6	2	10	0.702987
W1,6,2,11	1	6	2	11	-0.400461
W1,6,2,12	1	6	2	12	0.711819
W1,6,2,13	1	6	2	13	-0.796158

W1,6,2,14	1	6	2	14	0.720468
W1,6,2,15	1	6	2	15	0.583095
W1,6,2,16	1	6	2	16	-0.131024
W1,6,2,17	1	6	2	17	-0.334032
W1,6,2,18	1	6	2	18	-0.389575
W1,6,2,19	1	6	2	19	0.904169
W1,6,2,20	1	6	2	20	-0.29097
W1,6,2,21	1	6	2	21	0.227275
W1,6,2,22	1	6	2	22	0.881223
W1,6,2,23	1	6	2	23	-0.456806
W1,6,2,24	1	6	2	24	-0.733604
W1,6,2,25	1	6	2	25	-0.846062
W1,7,2,1	1	7	2	1	-0.542631
W1,7,2,2	1	7	2	2	0.902491
W1,7,2,3	1	7	2	3	0.286486
W1,7,2,4	1	7	2	4	-0.369858
W1,7,2,5	1	7	2	5	-0.355646
W1,7,2,6	1	7	2	6	0.073102
W1,7,2,7	1	7	2	7	-0.358108
W1,7,2,8	1	7	2	8	0.088671
W1,7,2,9	1	7	2	9	0.971061
W1,7,2,10	1	7	2	10	0.093981
W1,7,2,11	1	7	2	11	0.105157
W1,7,2,12	1	7	2	12	0.523845
W1,7,2,13	1	7	2	13	0.301585
W1,7,2,14	1	7	2	14	0.82269
W1,7,2,15	1	7	2	15	0.81927
W1,7,2,16	1	7	2	16	-0.847858
W1,7,2,17	1	7	2	17	0.846085
W1,7,2,18	1	7	2	18	-0.066134
W1,7,2,19	1	7	2	19	-0.35616
W1,7,2,20	1	7	2	20	0.26281
W1,7,2,21	1	7	2	21	-0.600349
W1,7,2,22	1	7	2	22	-0.875737
W1,7,2,23	1	7	2	23	-0.233864
W1,7,2,24	1	7	2	24	0.438169
W1,7,2,25	1	7	2	25	-0.64629
W1,8,2,1	1	8	2	1	-0.166452
W1,8,2,2	1	8	2	2	0.560911
W1,8,2,3	1	8	2	3	0.639827
W1,8,2,4	1	8	2	4	-0.192264
W1,8,2,5	1	8	2	5	-0.586223
W1,8,2,6	1	8	2	6	-0.384897
W1,8,2,7	1	8	2	7	0.772779
W1,8,2,8	1	8	2	8	-0.45404
W1,8,2,9	1	8	2	9	0.67305
W1,8,2,10	1	8	2	10	-0.050532

W1,8,2,11	1	8	2	11	0.855184
W1,8,2,12	1	8	2	12	-0.615997
W1,8,2,13	1	8	2	13	-0.180574
W1,8,2,14	1	8	2	14	0.292663
W1,8,2,15	1	8	2	15	-0.427585
W1,8,2,16	1	8	2	16	-0.976456
W1,8,2,17	1	8	2	17	-0.84781
W1,8,2,18	1	8	2	18	-0.305208
W1,8,2,19	1	8	2	19	0.540318
W1,8,2,20	1	8	2	20	0.065189
W1,8,2,21	1	8	2	21	-0.591853
W1,8,2,22	1	8	2	22	-0.624848
W1,8,2,23	1	8	2	23	0.6436
W1,8,2,24	1	8	2	24	-0.833445
W1,8,2,25	1	8	2	25	0.037264
W1,9,2,1	1	9	2	1	0.445491
W1,9,2,2	1	9	2	2	0.532183
W1,9,2,3	1	9	2	3	-0.650794
W1,9,2,4	1	9	2	4	0.286934
W1,9,2,5	1	9	2	5	-0.412392
W1,9,2,6	1	9	2	6	-0.856232
W1,9,2,7	1	9	2	7	-0.715585
W1,9,2,8	1	9	2	8	-0.935846
W1,9,2,9	1	9	2	9	0.006593
W1,9,2,10	1	9	2	10	0.951734
W1,9,2,11	1	9	2	11	-0.645692
W1,9,2,12	1	9	2	12	-0.202275
W1,9,2,13	1	9	2	13	-0.491765
W1,9,2,14	1	9	2	14	0.193676
W1,9,2,15	1	9	2	15	0.100596
W1,9,2,16	1	9	2	16	0.041851
W1,9,2,17	1	9	2	17	-0.191022
W1,9,2,18	1	9	2	18	-0.697715
W1,9,2,19	1	9	2	19	0.223771
W1,9,2,20	1	9	2	20	0.072344
W1,9,2,21	1	9	2	21	-0.588773
W1,9,2,22	1	9	2	22	0.790758
W1,9,2,23	1	9	2	23	0.246548
W1,9,2,24	1	9	2	24	-0.970855
W1,9,2,25	1	9	2	25	0.82289
W1,10,2,1	1	10	2	1	-0.047551
W1,10,2,2	1	10	2	2	-0.300191
W1,10,2,3	1	10	2	3	-0.394627
W1,10,2,4	1	10	2	4	0.162425
W1,10,2,5	1	10	2	5	0.227517
W1,10,2,6	1	10	2	6	-0.282263
W1,10,2,7	1	10	2	7	0.85312

W1,10,2,8	1	10	2	8	0.673104
W1,10,2,9	1	10	2	9	-0.783761
W1,10,2,10	1	10	2	10	-0.529862
W1,10,2,11	1	10	2	11	-0.375309
W1,10,2,12	1	10	2	12	-0.573875
W1,10,2,13	1	10	2	13	0.69555
W1,10,2,14	1	10	2	14	0.862296
W1,10,2,15	1	10	2	15	0.339666
W1,10,2,16	1	10	2	16	-0.973386
W1,10,2,17	1	10	2	17	-0.014794
W1,10,2,18	1	10	2	18	0.872876
W1,10,2,19	1	10	2	19	-0.655136
W1,10,2,20	1	10	2	20	-1.041214
W1,10,2,21	1	10	2	21	-0.646133
W1,10,2,22	1	10	2	22	0.093141
W1,10,2,23	1	10	2	23	0.230927
W1,10,2,24	1	10	2	24	0.658372
W1,10,2,25	1	10	2	25	0.300786
W1,11,2,1	1	11	2	1	0.141696
W1,11,2,2	1	11	2	2	-0.470958
W1,11,2,3	1	11	2	3	0.634648
W1,11,2,4	1	11	2	4	-0.051727
W1,11,2,5	1	11	2	5	0.825625
W1,11,2,6	1	11	2	6	-0.395417
W1,11,2,7	1	11	2	7	-0.003051
W1,11,2,8	1	11	2	8	-0.846127
W1,11,2,9	1	11	2	9	-0.496346
W1,11,2,10	1	11	2	10	0.340828
W1,11,2,11	1	11	2	11	0.135711
W1,11,2,12	1	11	2	12	0.302299
W1,11,2,13	1	11	2	13	-0.122848
W1,11,2,14	1	11	2	14	0.971056
W1,11,2,15	1	11	2	15	-0.500018
W1,11,2,16	1	11	2	16	-0.973114
W1,11,2,17	1	11	2	17	0.881368
W1,11,2,18	1	11	2	18	-0.208503
W1,11,2,19	1	11	2	19	-0.476312
W1,11,2,20	1	11	2	20	0.952967
W1,11,2,21	1	11	2	21	0.287698
W1,11,2,22	1	11	2	22	0.07238
W1,11,2,23	1	11	2	23	0.348501
W1,11,2,24	1	11	2	24	-0.77951
W1,11,2,25	1	11	2	25	-0.183571
W1,12,2,1	1	12	2	1	0.836348
W1,12,2,2	1	12	2	2	0.835934
W1,12,2,3	1	12	2	3	0.21048
W1,12,2,4	1	12	2	4	0.203115

W1,12,2,5	1	12	2	5	0.172957
W1,12,2,6	1	12	2	6	-0.026406
W1,12,2,7	1	12	2	7	0.666619
W1,12,2,8	1	12	2	8	-0.157695
W1,12,2,9	1	12	2	9	-0.305869
W1,12,2,10	1	12	2	10	-0.648123
W1,12,2,11	1	12	2	11	-0.156605
W1,12,2,12	1	12	2	12	-0.131113
W1,12,2,13	1	12	2	13	-0.93351
W1,12,2,14	1	12	2	14	-0.938034
W1,12,2,15	1	12	2	15	-0.284783
W1,12,2,16	1	12	2	16	-0.911963
W1,12,2,17	1	12	2	17	-0.355612
W1,12,2,18	1	12	2	18	-1.009721
W1,12,2,19	1	12	2	19	-0.75199
W1,12,2,20	1	12	2	20	0.572229
W1,12,2,21	1	12	2	21	0.653359
W1,12,2,22	1	12	2	22	-0.394651
W1,12,2,23	1	12	2	23	-0.125676
W1,12,2,24	1	12	2	24	-0.856951
W1,12,2,25	1	12	2	25	0.578742
W1,13,2,1	1	13	2	1	-0.519032
W1,13,2,2	1	13	2	2	0.783912
W1,13,2,3	1	13	2	3	0.282061
W1,13,2,4	1	13	2	4	-0.69874
W1,13,2,5	1	13	2	5	0.022409
W1,13,2,6	1	13	2	6	0.366786
W1,13,2,7	1	13	2	7	-0.438312
W1,13,2,8	1	13	2	8	-0.812644
W1,13,2,9	1	13	2	9	0.98618
W1,13,2,10	1	13	2	10	0.831348
W1,13,2,11	1	13	2	11	0.590574
W1,13,2,12	1	13	2	12	0.474474
W1,13,2,13	1	13	2	13	-0.528823
W1,13,2,14	1	13	2	14	0.770461
W1,13,2,15	1	13	2	15	-0.852036
W1,13,2,16	1	13	2	16	-0.387382
W1,13,2,17	1	13	2	17	-0.928491
W1,13,2,18	1	13	2	18	0.206354
W1,13,2,19	1	13	2	19	0.592012
W1,13,2,20	1	13	2	20	0.32886
W1,13,2,21	1	13	2	21	-0.827488
W1,13,2,22	1	13	2	22	0.500274
W1,13,2,23	1	13	2	23	0.554167
W1,13,2,24	1	13	2	24	0.429961
W1,13,2,25	1	13	2	25	-0.650352
W1,14,2,1	1	14	2	1	-0.476475

W1,14,2,2	1	14	2	2	0.066352
W1,14,2,3	1	14	2	3	-0.120218
W1,14,2,4	1	14	2	4	-0.933713
W1,14,2,5	1	14	2	5	-0.680764
W1,14,2,6	1	14	2	6	-0.198256
W1,14,2,7	1	14	2	7	0.932845
W1,14,2,8	1	14	2	8	-1.029573
W1,14,2,9	1	14	2	9	-0.274226
W1,14,2,10	1	14	2	10	-0.314558
W1,14,2,11	1	14	2	11	-0.272579
W1,14,2,12	1	14	2	12	-0.584137
W1,14,2,13	1	14	2	13	-0.43646
W1,14,2,14	1	14	2	14	-0.320276
W1,14,2,15	1	14	2	15	-0.286287
W1,14,2,16	1	14	2	16	-0.513392
W1,14,2,17	1	14	2	17	0.604433
W1,14,2,18	1	14	2	18	0.951332
W1,14,2,19	1	14	2	19	-0.724079
W1,14,2,20	1	14	2	20	-0.824664
W1,14,2,21	1	14	2	21	0.004465
W1,14,2,22	1	14	2	22	0.914459
W1,14,2,23	1	14	2	23	-0.732633
W1,14,2,24	1	14	2	24	0.391281
W1,14,2,25	1	14	2	25	-0.261647
W1,15,2,1	1	15	2	1	-0.900712
W1,15,2,2	1	15	2	2	0.608548
W1,15,2,3	1	15	2	3	0.818561
W1,15,2,4	1	15	2	4	-0.445928
W1,15,2,5	1	15	2	5	-0.264791
W1,15,2,6	1	15	2	6	0.674987
W1,15,2,7	1	15	2	7	0.367737
W1,15,2,8	1	15	2	8	-0.485818
W1,15,2,9	1	15	2	9	0.685264
W1,15,2,10	1	15	2	10	0.216878
W1,15,2,11	1	15	2	11	0.532866
W1,15,2,12	1	15	2	12	0.081296
W1,15,2,13	1	15	2	13	-0.243675
W1,15,2,14	1	15	2	14	-0.892548
W1,15,2,15	1	15	2	15	-0.58198
W1,15,2,16	1	15	2	16	0.455192
W1,15,2,17	1	15	2	17	0.988984
W1,15,2,18	1	15	2	18	-0.320431
W1,15,2,19	1	15	2	19	0.727662
W1,15,2,20	1	15	2	20	-0.634641
W1,15,2,21	1	15	2	21	-0.372553
W1,15,2,22	1	15	2	22	-0.487128
W1,15,2,23	1	15	2	23	-0.327511

W1,15,2,24	1	15	2	24	-0.394483
W1,15,2,25	1	15	2	25	0.568145
W1,16,2,1	1	16	2	1	0.599447
W1,16,2,2	1	16	2	2	-0.712546
W1,16,2,3	1	16	2	3	-0.429277
W1,16,2,4	1	16	2	4	-0.928634
W1,16,2,5	1	16	2	5	0.001394
W1,16,2,6	1	16	2	6	0.217322
W1,16,2,7	1	16	2	7	-0.067282
W1,16,2,8	1	16	2	8	-0.238995
W1,16,2,9	1	16	2	9	0.828514
W1,16,2,10	1	16	2	10	-0.502551
W1,16,2,11	1	16	2	11	-0.858281
W1,16,2,12	1	16	2	12	0.809893
W1,16,2,13	1	16	2	13	0.221403
W1,16,2,14	1	16	2	14	0.274117
W1,16,2,15	1	16	2	15	0.717178
W1,16,2,16	1	16	2	16	-0.409264
W1,16,2,17	1	16	2	17	0.698564
W1,16,2,18	1	16	2	18	0.926147
W1,16,2,19	1	16	2	19	0.338709
W1,16,2,20	1	16	2	20	0.911045
W1,16,2,21	1	16	2	21	0.247028
W1,16,2,22	1	16	2	22	-0.150242
W1,16,2,23	1	16	2	23	0.485707
W1,16,2,24	1	16	2	24	-0.297714
W1,16,2,25	1	16	2	25	0.286435
W1,17,2,1	1	17	2	1	0.177826
W1,17,2,2	1	17	2	2	0.65745
W1,17,2,3	1	17	2	3	0.971315
W1,17,2,4	1	17	2	4	0.10672
W1,17,2,5	1	17	2	5	-0.507177
W1,17,2,6	1	17	2	6	-0.6814
W1,17,2,7	1	17	2	7	0.030288
W1,17,2,8	1	17	2	8	-0.134284
W1,17,2,9	1	17	2	9	0.240766
W1,17,2,10	1	17	2	10	-0.32256
W1,17,2,11	1	17	2	11	0.505947
W1,17,2,12	1	17	2	12	0.150985
W1,17,2,13	1	17	2	13	-0.916798
W1,17,2,14	1	17	2	14	-0.753261
W1,17,2,15	1	17	2	15	-0.112721
W1,17,2,16	1	17	2	16	-0.807218
W1,17,2,17	1	17	2	17	0.557718
W1,17,2,18	1	17	2	18	-0.131019
W1,17,2,19	1	17	2	19	-0.195959
W1,17,2,20	1	17	2	20	-0.823399

W1,17,2,21	1	17	2	21	-0.236772
W1,17,2,22	1	17	2	22	-0.087557
W1,17,2,23	1	17	2	23	-0.080195
W1,17,2,24	1	17	2	24	0.447898
W1,17,2,25	1	17	2	25	-0.665275
W1,18,2,1	1	18	2	1	-0.163778
W1,18,2,2	1	18	2	2	0.31928
W1,18,2,3	1	18	2	3	0.812448
W1,18,2,4	1	18	2	4	-0.718519
W1,18,2,5	1	18	2	5	0.21773
W1,18,2,6	1	18	2	6	0.899671
W1,18,2,7	1	18	2	7	-0.891532
W1,18,2,8	1	18	2	8	0.657905
W1,18,2,9	1	18	2	9	0.976071
W1,18,2,10	1	18	2	10	-0.918249
W1,18,2,11	1	18	2	11	-0.902537
W1,18,2,12	1	18	2	12	-0.253857
W1,18,2,13	1	18	2	13	-0.748144
W1,18,2,14	1	18	2	14	-0.041647
W1,18,2,15	1	18	2	15	0.522904
W1,18,2,16	1	18	2	16	0.994533
W1,18,2,17	1	18	2	17	0.626322
W1,18,2,18	1	18	2	18	-0.757174
W1,18,2,19	1	18	2	19	0.86861
W1,18,2,20	1	18	2	20	-0.631693
W1,18,2,21	1	18	2	21	-0.985899
W1,18,2,22	1	18	2	22	0.636414
W1,18,2,23	1	18	2	23	-0.603453
W1,18,2,24	1	18	2	24	-0.110894
W1,18,2,25	1	18	2	25	0.933853
W1,19,2,1	1	19	2	1	0.774271
W1,19,2,2	1	19	2	2	-0.5875
W1,19,2,3	1	19	2	3	0.673871
W1,19,2,4	1	19	2	4	0.760569
W1,19,2,5	1	19	2	5	0.274428
W1,19,2,6	1	19	2	6	-0.090246
W1,19,2,7	1	19	2	7	-0.738535
W1,19,2,8	1	19	2	8	-0.572517
W1,19,2,9	1	19	2	9	-0.382043
W1,19,2,10	1	19	2	10	0.381038
W1,19,2,11	1	19	2	11	0.389618
W1,19,2,12	1	19	2	12	0.998724
W1,19,2,13	1	19	2	13	-0.131021
W1,19,2,14	1	19	2	14	0.546557
W1,19,2,15	1	19	2	15	0.87638
W1,19,2,16	1	19	2	16	-0.060157
W1,19,2,17	1	19	2	17	-0.008927

W1,19,2,18	1	19	2	18	0.190863
W1,19,2,19	1	19	2	19	-0.126205
W1,19,2,20	1	19	2	20	0.799099
W1,19,2,21	1	19	2	21	-0.134086
W1,19,2,22	1	19	2	22	-0.77186
W1,19,2,23	1	19	2	23	0.628138
W1,19,2,24	1	19	2	24	-0.781054
W1,19,2,25	1	19	2	25	0.134349
W1,20,2,1	1	20	2	1	-0.769616
W1,20,2,2	1	20	2	2	-0.82366
W1,20,2,3	1	20	2	3	-0.410741
W1,20,2,4	1	20	2	4	0.309656
W1,20,2,5	1	20	2	5	-0.428003
W1,20,2,6	1	20	2	6	-0.780159
W1,20,2,7	1	20	2	7	-0.408506
W1,20,2,8	1	20	2	8	-0.231192
W1,20,2,9	1	20	2	9	-0.326771
W1,20,2,10	1	20	2	10	-0.713976
W1,20,2,11	1	20	2	11	-0.837795
W1,20,2,12	1	20	2	12	0.752464
W1,20,2,13	1	20	2	13	-0.702552
W1,20,2,14	1	20	2	14	0.581997
W1,20,2,15	1	20	2	15	0.006804
W1,20,2,16	1	20	2	16	0.113139
W1,20,2,17	1	20	2	17	-0.135056
W1,20,2,18	1	20	2	18	-0.288816
W1,20,2,19	1	20	2	19	0.909794
W1,20,2,20	1	20	2	20	0.572514
W1,20,2,21	1	20	2	21	-0.523186
W1,20,2,22	1	20	2	22	0.185331
W1,20,2,23	1	20	2	23	-0.232636
W1,20,2,24	1	20	2	24	0.942669
W1,20,2,25	1	20	2	25	-0.573923
W1,21,2,1	1	21	2	1	0.255144
W1,21,2,2	1	21	2	2	-0.470864
W1,21,2,3	1	21	2	3	-0.699788
W1,21,2,4	1	21	2	4	0.569808
W1,21,2,5	1	21	2	5	0.542312
W1,21,2,6	1	21	2	6	0.244392
W1,21,2,7	1	21	2	7	-0.804764
W1,21,2,8	1	21	2	8	0.878638
W1,21,2,9	1	21	2	9	0.078018
W1,21,2,10	1	21	2	10	0.077956
W1,21,2,11	1	21	2	11	-0.535582
W1,21,2,12	1	21	2	12	0.637734
W1,21,2,13	1	21	2	13	-0.652432
W1,21,2,14	1	21	2	14	0.075113

W1,21,2,15	1	21	2	15	-0.781274
W1,21,2,16	1	21	2	16	0.170022
W1,21,2,17	1	21	2	17	0.82647
W1,21,2,18	1	21	2	18	0.919371
W1,21,2,19	1	21	2	19	0.803445
W1,21,2,20	1	21	2	20	0.59745
W1,21,2,21	1	21	2	21	-0.949164
W1,21,2,22	1	21	2	22	0.94613
W1,21,2,23	1	21	2	23	-0.223839
W1,21,2,24	1	21	2	24	0.928551
W1,21,2,25	1	21	2	25	-0.530676
W1,22,2,1	1	22	2	1	-0.779804
W1,22,2,2	1	22	2	2	-0.815407
W1,22,2,3	1	22	2	3	-0.280159
W1,22,2,4	1	22	2	4	-0.308597
W1,22,2,5	1	22	2	5	-0.953762
W1,22,2,6	1	22	2	6	-0.261605
W1,22,2,7	1	22	2	7	0.741665
W1,22,2,8	1	22	2	8	-0.086119
W1,22,2,9	1	22	2	9	0.027336
W1,22,2,10	1	22	2	10	0.967825
W1,22,2,11	1	22	2	11	0.735711
W1,22,2,12	1	22	2	12	0.367617
W1,22,2,13	1	22	2	13	-0.221993
W1,22,2,14	1	22	2	14	-0.254762
W1,22,2,15	1	22	2	15	-0.991544
W1,22,2,16	1	22	2	16	0.112749
W1,22,2,17	1	22	2	17	0.490793
W1,22,2,18	1	22	2	18	-0.71431
W1,22,2,19	1	22	2	19	-0.135082
W1,22,2,20	1	22	2	20	0.428205
W1,22,2,21	1	22	2	21	0.304094
W1,22,2,22	1	22	2	22	0.933445
W1,22,2,23	1	22	2	23	-0.303144
W1,22,2,24	1	22	2	24	-0.740384
W1,22,2,25	1	22	2	25	-0.3375
W1,23,2,1	1	23	2	1	-0.222172
W1,23,2,2	1	23	2	2	0.918035
W1,23,2,3	1	23	2	3	-0.802744
W1,23,2,4	1	23	2	4	-0.286353
W1,23,2,5	1	23	2	5	-0.396354
W1,23,2,6	1	23	2	6	0.767558
W1,23,2,7	1	23	2	7	-0.2345
W1,23,2,8	1	23	2	8	-0.211677
W1,23,2,9	1	23	2	9	0.543501
W1,23,2,10	1	23	2	10	-0.684306
W1,23,2,11	1	23	2	11	-0.360554

W1,23,2,12	1	23	2	12	0.780484
W1,23,2,13	1	23	2	13	0.070782
W1,23,2,14	1	23	2	14	0.421361
W1,23,2,15	1	23	2	15	0.957721
W1,23,2,16	1	23	2	16	0.040311
W1,23,2,17	1	23	2	17	-0.589916
W1,23,2,18	1	23	2	18	-0.42407
W1,23,2,19	1	23	2	19	0.015867
W1,23,2,20	1	23	2	20	-0.730227
W1,23,2,21	1	23	2	21	-0.427753
W1,23,2,22	1	23	2	22	-0.494252
W1,23,2,23	1	23	2	23	0.629293
W1,23,2,24	1	23	2	24	-0.043806
W1,23,2,25	1	23	2	25	-0.605375
W1,24,2,1	1	24	2	1	-0.451427
W1,24,2,2	1	24	2	2	-0.325746
W1,24,2,3	1	24	2	3	-0.838761
W1,24,2,4	1	24	2	4	-0.665771
W1,24,2,5	1	24	2	5	0.931245
W1,24,2,6	1	24	2	6	-0.579682
W1,24,2,7	1	24	2	7	-1.014044
W1,24,2,8	1	24	2	8	0.337859
W1,24,2,9	1	24	2	9	-0.184999
W1,24,2,10	1	24	2	10	-0.341983
W1,24,2,11	1	24	2	11	0.967281
W1,24,2,12	1	24	2	12	-0.279794
W1,24,2,13	1	24	2	13	-0.422206
W1,24,2,14	1	24	2	14	0.384558
W1,24,2,15	1	24	2	15	-0.070742
W1,24,2,16	1	24	2	16	0.395327
W1,24,2,17	1	24	2	17	-0.365038
W1,24,2,18	1	24	2	18	-0.465414
W1,24,2,19	1	24	2	19	0.316677
W1,24,2,20	1	24	2	20	-0.31876
W1,24,2,21	1	24	2	21	0.833939
W1,24,2,22	1	24	2	22	-0.217147
W1,24,2,23	1	24	2	23	0.412247
W1,24,2,24	1	24	2	24	0.579831
W1,24,2,25	1	24	2	25	0.559354
W1,25,2,1	1	25	2	1	-0.246223
W1,25,2,2	1	25	2	2	-0.528952
W1,25,2,3	1	25	2	3	-0.083859
W1,25,2,4	1	25	2	4	-0.222494
W1,25,2,5	1	25	2	5	0.846027
W1,25,2,6	1	25	2	6	0.294589
W1,25,2,7	1	25	2	7	-0.109339
W1,25,2,8	1	25	2	8	0.411671

W1,25,2,9	1	25	2	9	0.006522
W1,25,2,10	1	25	2	10	-0.469769
W1,25,2,11	1	25	2	11	0.598412
W1,25,2,12	1	25	2	12	1.105351
W1,25,2,13	1	25	2	13	0.828719
W1,25,2,14	1	25	2	14	0.456025
W1,25,2,15	1	25	2	15	0.58186
W1,25,2,16	1	25	2	16	-0.014608
W1,25,2,17	1	25	2	17	0.928219
W1,25,2,18	1	25	2	18	0.68789
W1,25,2,19	1	25	2	19	-0.7021
W1,25,2,20	1	25	2	20	0.83087
W1,25,2,21	1	25	2	21	0.925019
W1,25,2,22	1	25	2	22	-0.880707
W1,25,2,23	1	25	2	23	0.536924
W1,25,2,24	1	25	2	24	-0.107607
W1,25,2,25	1	25	2	25	0.236283
W1,26,2,1	1	26	2	1	-0.498656
W1,26,2,2	1	26	2	2	0.156563
W1,26,2,3	1	26	2	3	0.528946
W1,26,2,4	1	26	2	4	-0.084025
W1,26,2,5	1	26	2	5	0.068418
W1,26,2,6	1	26	2	6	-0.085099
W1,26,2,7	1	26	2	7	0.841451
W1,26,2,8	1	26	2	8	0.226782
W1,26,2,9	1	26	2	9	-0.916438
W1,26,2,10	1	26	2	10	0.824359
W1,26,2,11	1	26	2	11	0.266134
W1,26,2,12	1	26	2	12	-0.214937
W1,26,2,13	1	26	2	13	0.315547
W1,26,2,14	1	26	2	14	-0.074451
W1,26,2,15	1	26	2	15	-0.00998
W1,26,2,16	1	26	2	16	-0.855832
W1,26,2,17	1	26	2	17	-0.597288
W1,26,2,18	1	26	2	18	-0.961406
W1,26,2,19	1	26	2	19	0.787499
W1,26,2,20	1	26	2	20	-0.181853
W1,26,2,21	1	26	2	21	-0.642477
W1,26,2,22	1	26	2	22	0.249519
W1,26,2,23	1	26	2	23	-0.088361
W1,26,2,24	1	26	2	24	0.423505
W1,26,2,25	1	26	2	25	0.620047
W1,27,2,1	1	27	2	1	0.431438
W1,27,2,2	1	27	2	2	0.737896
W1,27,2,3	1	27	2	3	0.999819
W1,27,2,4	1	27	2	4	0.201
W1,27,2,5	1	27	2	5	-0.438658

W1,27,2,6	1	27	2	6	0.513575
W1,27,2,7	1	27	2	7	-0.290792
W1,27,2,8	1	27	2	8	0.437226
W1,27,2,9	1	27	2	9	-0.29218
W1,27,2,10	1	27	2	10	0.071449
W1,27,2,11	1	27	2	11	-0.425251
W1,27,2,12	1	27	2	12	-0.007164
W1,27,2,13	1	27	2	13	0.441843
W1,27,2,14	1	27	2	14	-0.719327
W1,27,2,15	1	27	2	15	-0.204025
W1,27,2,16	1	27	2	16	-0.660922
W1,27,2,17	1	27	2	17	-0.484704
W1,27,2,18	1	27	2	18	0.523137
W1,27,2,19	1	27	2	19	0.17549
W1,27,2,20	1	27	2	20	-0.21945
W1,27,2,21	1	27	2	21	0.307203
W1,27,2,22	1	27	2	22	0.261651
W1,27,2,23	1	27	2	23	0.450176
W1,27,2,24	1	27	2	24	0.201693
W1,27,2,25	1	27	2	25	0.962773
W1,28,2,1	1	28	2	1	-0.237228
W1,28,2,2	1	28	2	2	-0.51331
W1,28,2,3	1	28	2	3	-0.930134
W1,28,2,4	1	28	2	4	0.761875
W1,28,2,5	1	28	2	5	-0.260334
W1,28,2,6	1	28	2	6	-0.411046
W1,28,2,7	1	28	2	7	-0.624197
W1,28,2,8	1	28	2	8	0.200785
W1,28,2,9	1	28	2	9	-0.655449
W1,28,2,10	1	28	2	10	-0.499035
W1,28,2,11	1	28	2	11	0.867838
W1,28,2,12	1	28	2	12	0.424519
W1,28,2,13	1	28	2	13	0.417469
W1,28,2,14	1	28	2	14	-0.414627
W1,28,2,15	1	28	2	15	0.029887
W1,28,2,16	1	28	2	16	-0.277655
W1,28,2,17	1	28	2	17	0.645467
W1,28,2,18	1	28	2	18	-0.206259
W1,28,2,19	1	28	2	19	0.611348
W1,28,2,20	1	28	2	20	0.687345
W1,28,2,21	1	28	2	21	0.254576
W1,28,2,22	1	28	2	22	-0.104222
W1,28,2,23	1	28	2	23	-0.521666
W1,28,2,24	1	28	2	24	0.189525
W1,28,2,25	1	28	2	25	-0.546441
W1,29,2,1	1	29	2	1	0.659691
W1,29,2,2	1	29	2	2	-0.730116

W1,29,2,3	1	29	2	3	-0.879633
W1,29,2,4	1	29	2	4	0.003495
W1,29,2,5	1	29	2	5	0.443605
W1,29,2,6	1	29	2	6	0.429756
W1,29,2,7	1	29	2	7	0.578306
W1,29,2,8	1	29	2	8	-0.830934
W1,29,2,9	1	29	2	9	-0.250514
W1,29,2,10	1	29	2	10	0.628884
W1,29,2,11	1	29	2	11	0.848617
W1,29,2,12	1	29	2	12	-0.632145
W1,29,2,13	1	29	2	13	0.080978
W1,29,2,14	1	29	2	14	-0.619965
W1,29,2,15	1	29	2	15	-0.818801
W1,29,2,16	1	29	2	16	-0.670572
W1,29,2,17	1	29	2	17	-0.402589
W1,29,2,18	1	29	2	18	-0.338146
W1,29,2,19	1	29	2	19	0.709802
W1,29,2,20	1	29	2	20	-0.682884
W1,29,2,21	1	29	2	21	0.216931
W1,29,2,22	1	29	2	22	0.996756
W1,29,2,23	1	29	2	23	0.233693
W1,29,2,24	1	29	2	24	0.940097
W1,29,2,25	1	29	2	25	0.312845
W1,30,2,1	1	30	2	1	0.910119
W1,30,2,2	1	30	2	2	0.811901
W1,30,2,3	1	30	2	3	-0.050562
W1,30,2,4	1	30	2	4	-0.189455
W1,30,2,5	1	30	2	5	0.039203
W1,30,2,6	1	30	2	6	0.111101
W1,30,2,7	1	30	2	7	0.839319
W1,30,2,8	1	30	2	8	-0.539442
W1,30,2,9	1	30	2	9	0.016457
W1,30,2,10	1	30	2	10	0.49933
W1,30,2,11	1	30	2	11	0.642918
W1,30,2,12	1	30	2	12	0.88595
W1,30,2,13	1	30	2	13	0.801785
W1,30,2,14	1	30	2	14	0.561048
W1,30,2,15	1	30	2	15	0.962789
W1,30,2,16	1	30	2	16	-0.770536
W1,30,2,17	1	30	2	17	-0.374203
W1,30,2,18	1	30	2	18	0.86378
W1,30,2,19	1	30	2	19	-0.121382
W1,30,2,20	1	30	2	20	-0.162428
W1,30,2,21	1	30	2	21	0.252136
W1,30,2,22	1	30	2	22	0.294651
W1,30,2,23	1	30	2	23	0.655255
W1,30,2,24	1	30	2	24	-0.110912

W1,30,2,25	1	30	2	25	0.088258
W1,31,2,1	1	31	2	1	0.520891
W1,31,2,2	1	31	2	2	-1.149126
W1,31,2,3	1	31	2	3	-0.219389
W1,31,2,4	1	31	2	4	0.861522
W1,31,2,5	1	31	2	5	-0.88903
W1,31,2,6	1	31	2	6	0.217316
W1,31,2,7	1	31	2	7	-0.33041
W1,31,2,8	1	31	2	8	-0.72541
W1,31,2,9	1	31	2	9	0.269975
W1,31,2,10	1	31	2	10	0.042128
W1,31,2,11	1	31	2	11	-0.870681
W1,31,2,12	1	31	2	12	0.958324
W1,31,2,13	1	31	2	13	-0.475
W1,31,2,14	1	31	2	14	-0.139488
W1,31,2,15	1	31	2	15	1.007876
W1,31,2,16	1	31	2	16	0.838044
W1,31,2,17	1	31	2	17	-0.542226
W1,31,2,18	1	31	2	18	0.17223
W1,31,2,19	1	31	2	19	0.828902
W1,31,2,20	1	31	2	20	0.387254
W1,31,2,21	1	31	2	21	0.919265
W1,31,2,22	1	31	2	22	0.499614
W1,31,2,23	1	31	2	23	-0.579105
W1,31,2,24	1	31	2	24	0.62337
W1,31,2,25	1	31	2	25	0.665367
W1,32,2,1	1	32	2	1	0.72026
W1,32,2,2	1	32	2	2	-0.74183
W1,32,2,3	1	32	2	3	-0.785728
W1,32,2,4	1	32	2	4	-0.09407
W1,32,2,5	1	32	2	5	0.657521
W1,32,2,6	1	32	2	6	0.990467
W1,32,2,7	1	32	2	7	0.423479
W1,32,2,8	1	32	2	8	0.606431
W1,32,2,9	1	32	2	9	0.89489
W1,32,2,10	1	32	2	10	-0.492659
W1,32,2,11	1	32	2	11	-0.534068
W1,32,2,12	1	32	2	12	0.25308
W1,32,2,13	1	32	2	13	-0.19463
W1,32,2,14	1	32	2	14	-0.651299
W1,32,2,15	1	32	2	15	0.486311
W1,32,2,16	1	32	2	16	0.287088
W1,32,2,17	1	32	2	17	0.227727
W1,32,2,18	1	32	2	18	-0.221676
W1,32,2,19	1	32	2	19	-0.682267
W1,32,2,20	1	32	2	20	-0.236138
W1,32,2,21	1	32	2	21	0.607041

W1,32,2,22	1	32	2	22	0.887931
W1,32,2,23	1	32	2	23	0.943926
W1,32,2,24	1	32	2	24	-0.710788
W1,32,2,25	1	32	2	25	-0.466643
W1,33,2,1	1	33	2	1	0.665442
W1,33,2,2	1	33	2	2	0.864761
W1,33,2,3	1	33	2	3	0.406437
W1,33,2,4	1	33	2	4	-0.190931
W1,33,2,5	1	33	2	5	0.582333
W1,33,2,6	1	33	2	6	0.684023
W1,33,2,7	1	33	2	7	-0.462019
W1,33,2,8	1	33	2	8	0.427213
W1,33,2,9	1	33	2	9	0.857911
W1,33,2,10	1	33	2	10	0.476362
W1,33,2,11	1	33	2	11	-0.679767
W1,33,2,12	1	33	2	12	-0.382913
W1,33,2,13	1	33	2	13	-0.811674
W1,33,2,14	1	33	2	14	0.177402
W1,33,2,15	1	33	2	15	-0.180771
W1,33,2,16	1	33	2	16	0.256753
W1,33,2,17	1	33	2	17	-0.555932
W1,33,2,18	1	33	2	18	-0.99851
W1,33,2,19	1	33	2	19	-0.370181
W1,33,2,20	1	33	2	20	-0.744443
W1,33,2,21	1	33	2	21	-0.722326
W1,33,2,22	1	33	2	22	0.52295
W1,33,2,23	1	33	2	23	-0.472439
W1,33,2,24	1	33	2	24	-0.732119
W1,33,2,25	1	33	2	25	-0.008591
W1,34,2,1	1	34	2	1	0.072109
W1,34,2,2	1	34	2	2	-0.907657
W1,34,2,3	1	34	2	3	0.640087
W1,34,2,4	1	34	2	4	0.951099
W1,34,2,5	1	34	2	5	0.511664
W1,34,2,6	1	34	2	6	-0.020338
W1,34,2,7	1	34	2	7	-0.16829
W1,34,2,8	1	34	2	8	-0.199673
W1,34,2,9	1	34	2	9	0.094327
W1,34,2,10	1	34	2	10	-0.793532
W1,34,2,11	1	34	2	11	0.937031
W1,34,2,12	1	34	2	12	-0.257107
W1,34,2,13	1	34	2	13	0.664731
W1,34,2,14	1	34	2	14	0.813968
W1,34,2,15	1	34	2	15	-0.094332
W1,34,2,16	1	34	2	16	-0.660949
W1,34,2,17	1	34	2	17	0.554934
W1,34,2,18	1	34	2	18	0.886962

W1,34,2,19	1	34	2	19	0.611356
W1,34,2,20	1	34	2	20	0.540968
W1,34,2,21	1	34	2	21	-0.779468
W1,34,2,22	1	34	2	22	0.049376
W1,34,2,23	1	34	2	23	-0.610495
W1,34,2,24	1	34	2	24	-0.176203
W1,34,2,25	1	34	2	25	0.258812
W1,35,2,1	1	35	2	1	-0.80371
W1,35,2,2	1	35	2	2	-0.127654
W1,35,2,3	1	35	2	3	0.561379
W1,35,2,4	1	35	2	4	-0.111245
W1,35,2,5	1	35	2	5	0.206556
W1,35,2,6	1	35	2	6	0.076178
W1,35,2,7	1	35	2	7	0.236557
W1,35,2,8	1	35	2	8	-0.841777
W1,35,2,9	1	35	2	9	0.819089
W1,35,2,10	1	35	2	10	0.363028
W1,35,2,11	1	35	2	11	0.661401
W1,35,2,12	1	35	2	12	0.689754
W1,35,2,13	1	35	2	13	-0.027929
W1,35,2,14	1	35	2	14	-0.653349
W1,35,2,15	1	35	2	15	-0.203092
W1,35,2,16	1	35	2	16	0.376309
W1,35,2,17	1	35	2	17	0.036477
W1,35,2,18	1	35	2	18	0.092968
W1,35,2,19	1	35	2	19	0.568414
W1,35,2,20	1	35	2	20	-0.871919
W1,35,2,21	1	35	2	21	0.499986
W1,35,2,22	1	35	2	22	0.642407
W1,35,2,23	1	35	2	23	-0.070283
W1,35,2,24	1	35	2	24	0.226499
W1,35,2,25	1	35	2	25	0.085314
W1,36,2,1	1	36	2	1	0.705366
W1,36,2,2	1	36	2	2	0.885067
W1,36,2,3	1	36	2	3	0.910236
W1,36,2,4	1	36	2	4	-0.444543
W1,36,2,5	1	36	2	5	-0.888239
W1,36,2,6	1	36	2	6	-0.382983
W1,36,2,7	1	36	2	7	0.148717
W1,36,2,8	1	36	2	8	1.152201
W1,36,2,9	1	36	2	9	-0.067082
W1,36,2,10	1	36	2	10	0.90415
W1,36,2,11	1	36	2	11	0.765061
W1,36,2,12	1	36	2	12	-0.018249
W1,36,2,13	1	36	2	13	-0.970364
W1,36,2,14	1	36	2	14	-0.894105
W1,36,2,15	1	36	2	15	0.42431

W1,36,2,16	1	36	2	16	-0.506859
W1,36,2,17	1	36	2	17	-0.406003
W1,36,2,18	1	36	2	18	-0.714786
W1,36,2,19	1	36	2	19	-0.360959
W1,36,2,20	1	36	2	20	0.231542
W1,36,2,21	1	36	2	21	0.539913
W1,36,2,22	1	36	2	22	0.26044
W1,36,2,23	1	36	2	23	0.522087
W1,36,2,24	1	36	2	24	-0.654742
W1,36,2,25	1	36	2	25	-0.286264
W1,37,2,1	1	37	2	1	-0.234695
W1,37,2,2	1	37	2	2	-0.961919
W1,37,2,3	1	37	2	3	0.821281
W1,37,2,4	1	37	2	4	0.622651
W1,37,2,5	1	37	2	5	0.026566
W1,37,2,6	1	37	2	6	0.4201
W1,37,2,7	1	37	2	7	-0.907842
W1,37,2,8	1	37	2	8	-0.262295
W1,37,2,9	1	37	2	9	0.145785
W1,37,2,10	1	37	2	10	-0.839103
W1,37,2,11	1	37	2	11	-0.961945
W1,37,2,12	1	37	2	12	1.041495
W1,37,2,13	1	37	2	13	-0.865466
W1,37,2,14	1	37	2	14	0.133008
W1,37,2,15	1	37	2	15	1.01004
W1,37,2,16	1	37	2	16	-0.937091
W1,37,2,17	1	37	2	17	0.449959
W1,37,2,18	1	37	2	18	-0.846478
W1,37,2,19	1	37	2	19	0.240057
W1,37,2,20	1	37	2	20	0.240829
W1,37,2,21	1	37	2	21	-0.203305
W1,37,2,22	1	37	2	22	0.520288
W1,37,2,23	1	37	2	23	0.446933
W1,37,2,24	1	37	2	24	-0.894055
W1,37,2,25	1	37	2	25	-0.162547
W1,38,2,1	1	38	2	1	0.182138
W1,38,2,2	1	38	2	2	0.32622
W1,38,2,3	1	38	2	3	0.8993
W1,38,2,4	1	38	2	4	0.824587
W1,38,2,5	1	38	2	5	-0.331306
W1,38,2,6	1	38	2	6	-0.34874
W1,38,2,7	1	38	2	7	0.131967
W1,38,2,8	1	38	2	8	0.467498
W1,38,2,9	1	38	2	9	-0.929876
W1,38,2,10	1	38	2	10	-0.922784
W1,38,2,11	1	38	2	11	-0.821011
W1,38,2,12	1	38	2	12	-0.596017

W1,38,2,13	1	38	2	13	-0.737083
W1,38,2,14	1	38	2	14	-0.320028
W1,38,2,15	1	38	2	15	0.09021
W1,38,2,16	1	38	2	16	-0.624338
W1,38,2,17	1	38	2	17	0.797829
W1,38,2,18	1	38	2	18	-0.258972
W1,38,2,19	1	38	2	19	-0.88331
W1,38,2,20	1	38	2	20	0.037414
W1,38,2,21	1	38	2	21	0.097791
W1,38,2,22	1	38	2	22	-0.714238
W1,38,2,23	1	38	2	23	-0.57392
W1,38,2,24	1	38	2	24	0.70158
W1,38,2,25	1	38	2	25	-0.709179
W1,39,2,1	1	39	2	1	-0.318526
W1,39,2,2	1	39	2	2	-0.777572
W1,39,2,3	1	39	2	3	-0.332885
W1,39,2,4	1	39	2	4	-0.177726
W1,39,2,5	1	39	2	5	0.119426
W1,39,2,6	1	39	2	6	0.948837
W1,39,2,7	1	39	2	7	-0.894418
W1,39,2,8	1	39	2	8	0.117633
W1,39,2,9	1	39	2	9	0.298576
W1,39,2,10	1	39	2	10	0.125201
W1,39,2,11	1	39	2	11	0.270432
W1,39,2,12	1	39	2	12	-0.467572
W1,39,2,13	1	39	2	13	-0.432847
W1,39,2,14	1	39	2	14	0.337396
W1,39,2,15	1	39	2	15	-0.538708
W1,39,2,16	1	39	2	16	-0.830802
W1,39,2,17	1	39	2	17	0.774783
W1,39,2,18	1	39	2	18	-0.602549
W1,39,2,19	1	39	2	19	-0.344003
W1,39,2,20	1	39	2	20	0.353412
W1,39,2,21	1	39	2	21	-0.056654
W1,39,2,22	1	39	2	22	0.348785
W1,39,2,23	1	39	2	23	-0.060538
W1,39,2,24	1	39	2	24	-0.304325
W1,39,2,25	1	39	2	25	-0.361539
W1,40,2,1	1	40	2	1	0.412248
W1,40,2,2	1	40	2	2	-0.846701
W1,40,2,3	1	40	2	3	0.41011
W1,40,2,4	1	40	2	4	0.006344
W1,40,2,5	1	40	2	5	-0.691511
W1,40,2,6	1	40	2	6	-0.300012
W1,40,2,7	1	40	2	7	0.854338
W1,40,2,8	1	40	2	8	0.436516
W1,40,2,9	1	40	2	9	-0.39447

W1,40,2,10	1	40	2	10	0.03494
W1,40,2,11	1	40	2	11	0.124181
W1,40,2,12	1	40	2	12	0.102207
W1,40,2,13	1	40	2	13	0.29026
W1,40,2,14	1	40	2	14	-0.142186
W1,40,2,15	1	40	2	15	0.528861
W1,40,2,16	1	40	2	16	0.660277
W1,40,2,17	1	40	2	17	-0.389253
W1,40,2,18	1	40	2	18	0.655016
W1,40,2,19	1	40	2	19	-0.309077
W1,40,2,20	1	40	2	20	-0.259635
W1,40,2,21	1	40	2	21	0.868501
W1,40,2,22	1	40	2	22	0.95379
W1,40,2,23	1	40	2	23	-0.02123
W1,40,2,24	1	40	2	24	0.115058
W1,40,2,25	1	40	2	25	-0.033816
W1,41,2,1	1	41	2	1	-0.60216
W1,41,2,2	1	41	2	2	0.524594
W1,41,2,3	1	41	2	3	-0.331553
W1,41,2,4	1	41	2	4	-0.358517
W1,41,2,5	1	41	2	5	0.913155
W1,41,2,6	1	41	2	6	0.605722
W1,41,2,7	1	41	2	7	0.846348
W1,41,2,8	1	41	2	8	0.071343
W1,41,2,9	1	41	2	9	0.673946
W1,41,2,10	1	41	2	10	-0.512313
W1,41,2,11	1	41	2	11	-0.730028
W1,41,2,12	1	41	2	12	-0.808767
W1,41,2,13	1	41	2	13	0.221882
W1,41,2,14	1	41	2	14	-0.181431
W1,41,2,15	1	41	2	15	0.962585
W1,41,2,16	1	41	2	16	0.260513
W1,41,2,17	1	41	2	17	-0.661065
W1,41,2,18	1	41	2	18	0.546055
W1,41,2,19	1	41	2	19	0.677557
W1,41,2,20	1	41	2	20	-0.500133
W1,41,2,21	1	41	2	21	0.25855
W1,41,2,22	1	41	2	22	0.768738
W1,41,2,23	1	41	2	23	0.593482
W1,41,2,24	1	41	2	24	-0.003616
W1,41,2,25	1	41	2	25	-0.700492
W1,42,2,1	1	42	2	1	0.920746
W1,42,2,2	1	42	2	2	0.82166
W1,42,2,3	1	42	2	3	0.85651
W1,42,2,4	1	42	2	4	0.943062
W1,42,2,5	1	42	2	5	-0.233128
W1,42,2,6	1	42	2	6	-0.661893

W1,42,2,7	1	42	2	7	-0.788749
W1,42,2,8	1	42	2	8	-1.234992
W1,42,2,9	1	42	2	9	0.133969
W1,42,2,10	1	42	2	10	-0.927491
W1,42,2,11	1	42	2	11	0.353957
W1,42,2,12	1	42	2	12	1.008331
W1,42,2,13	1	42	2	13	-0.868128
W1,42,2,14	1	42	2	14	0.49887
W1,42,2,15	1	42	2	15	0.946845
W1,42,2,16	1	42	2	16	0.106763
W1,42,2,17	1	42	2	17	0.849268
W1,42,2,18	1	42	2	18	-0.734231
W1,42,2,19	1	42	2	19	-0.629793
W1,42,2,20	1	42	2	20	-0.145307
W1,42,2,21	1	42	2	21	-0.211871
W1,42,2,22	1	42	2	22	0.031935
W1,42,2,23	1	42	2	23	-0.080096
W1,42,2,24	1	42	2	24	-0.79458
W1,42,2,25	1	42	2	25	-0.285695
W1,43,2,1	1	43	2	1	-0.379941
W1,43,2,2	1	43	2	2	-0.027594
W1,43,2,3	1	43	2	3	0.636744
W1,43,2,4	1	43	2	4	-0.47924
W1,43,2,5	1	43	2	5	-0.27513
W1,43,2,6	1	43	2	6	-0.553087
W1,43,2,7	1	43	2	7	0.841374
W1,43,2,8	1	43	2	8	-0.22924
W1,43,2,9	1	43	2	9	-0.727008
W1,43,2,10	1	43	2	10	-0.633399
W1,43,2,11	1	43	2	11	-0.107021
W1,43,2,12	1	43	2	12	0.677782
W1,43,2,13	1	43	2	13	0.095815
W1,43,2,14	1	43	2	14	-0.846591
W1,43,2,15	1	43	2	15	-0.703316
W1,43,2,16	1	43	2	16	-0.936388
W1,43,2,17	1	43	2	17	0.209678
W1,43,2,18	1	43	2	18	0.075306
W1,43,2,19	1	43	2	19	0.687664
W1,43,2,20	1	43	2	20	-0.224205
W1,43,2,21	1	43	2	21	-0.218253
W1,43,2,22	1	43	2	22	-0.836145
W1,43,2,23	1	43	2	23	0.199292
W1,43,2,24	1	43	2	24	-0.391382
W1,43,2,25	1	43	2	25	0.149672
W1,44,2,1	1	44	2	1	0.842345
W1,44,2,2	1	44	2	2	0.896789
W1,44,2,3	1	44	2	3	0.542328

W1,44,2,4	1	44	2	4	0.813166
W1,44,2,5	1	44	2	5	0.887472
W1,44,2,6	1	44	2	6	0.269971
W1,44,2,7	1	44	2	7	-0.601194
W1,44,2,8	1	44	2	8	-0.725747
W1,44,2,9	1	44	2	9	0.383096
W1,44,2,10	1	44	2	10	0.821534
W1,44,2,11	1	44	2	11	0.256856
W1,44,2,12	1	44	2	12	0.386897
W1,44,2,13	1	44	2	13	0.602865
W1,44,2,14	1	44	2	14	-0.914428
W1,44,2,15	1	44	2	15	-0.253251
W1,44,2,16	1	44	2	16	0.110666
W1,44,2,17	1	44	2	17	-0.093002
W1,44,2,18	1	44	2	18	-1.022589
W1,44,2,19	1	44	2	19	0.853072
W1,44,2,20	1	44	2	20	-0.338728
W1,44,2,21	1	44	2	21	-0.579577
W1,44,2,22	1	44	2	22	-0.596177
W1,44,2,23	1	44	2	23	0.413739
W1,44,2,24	1	44	2	24	-0.715368
W1,44,2,25	1	44	2	25	-0.545815
W1,45,2,1	1	45	2	1	0.417816
W1,45,2,2	1	45	2	2	0.024459
W1,45,2,3	1	45	2	3	0.752436
W1,45,2,4	1	45	2	4	0.399396
W1,45,2,5	1	45	2	5	0.976111
W1,45,2,6	1	45	2	6	-0.236711
W1,45,2,7	1	45	2	7	0.060547
W1,45,2,8	1	45	2	8	0.309603
W1,45,2,9	1	45	2	9	0.80394
W1,45,2,10	1	45	2	10	-0.702924
W1,45,2,11	1	45	2	11	-0.291779
W1,45,2,12	1	45	2	12	-0.664523
W1,45,2,13	1	45	2	13	-0.742384
W1,45,2,14	1	45	2	14	-0.580179
W1,45,2,15	1	45	2	15	-0.280769
W1,45,2,16	1	45	2	16	0.502437
W1,45,2,17	1	45	2	17	0.736982
W1,45,2,18	1	45	2	18	-0.632035
W1,45,2,19	1	45	2	19	0.805642
W1,45,2,20	1	45	2	20	0.810394
W1,45,2,21	1	45	2	21	-0.80191
W1,45,2,22	1	45	2	22	0.0531
W1,45,2,23	1	45	2	23	-0.061747
W1,45,2,24	1	45	2	24	-0.356779
W1,45,2,25	1	45	2	25	0.498776

W1,46,2,1	1	46	2	1	0.221134
W1,46,2,2	1	46	2	2	0.293083
W1,46,2,3	1	46	2	3	-0.482988
W1,46,2,4	1	46	2	4	0.600359
W1,46,2,5	1	46	2	5	0.777075
W1,46,2,6	1	46	2	6	-0.006346
W1,46,2,7	1	46	2	7	0.413358
W1,46,2,8	1	46	2	8	0.464709
W1,46,2,9	1	46	2	9	0.240487
W1,46,2,10	1	46	2	10	-0.073306
W1,46,2,11	1	46	2	11	0.757378
W1,46,2,12	1	46	2	12	-0.261371
W1,46,2,13	1	46	2	13	-0.369098
W1,46,2,14	1	46	2	14	-0.42124
W1,46,2,15	1	46	2	15	-0.844129
W1,46,2,16	1	46	2	16	-0.855997
W1,46,2,17	1	46	2	17	0.060895
W1,46,2,18	1	46	2	18	0.725033
W1,46,2,19	1	46	2	19	0.482952
W1,46,2,20	1	46	2	20	-0.880896
W1,46,2,21	1	46	2	21	0.053632
W1,46,2,22	1	46	2	22	-0.935698
W1,46,2,23	1	46	2	23	-0.654404
W1,46,2,24	1	46	2	24	-0.374562
W1,46,2,25	1	46	2	25	0.263039
W2,1,3,1	2	1	3	1	0.957684
W2,1,3,2	2	1	3	2	-0.105117
W2,2,3,1	2	2	3	1	0.259266
W2,2,3,2	2	2	3	2	0.639372
W2,3,3,1	2	3	3	1	-0.122579
W2,3,3,2	2	3	3	2	0.419991
W2,4,3,1	2	4	3	1	-0.703633
W2,4,3,2	2	4	3	2	0.8204
W2,5,3,1	2	5	3	1	-0.684916
W2,5,3,2	2	5	3	2	0.268818
W2,6,3,1	2	6	3	1	0.844471
W2,6,3,2	2	6	3	2	0.195343
W2,7,3,1	2	7	3	1	-0.930856
W2,7,3,2	2	7	3	2	-0.274255
W2,8,3,1	2	8	3	1	-0.022762
W2,8,3,2	2	8	3	2	-0.720451
W2,9,3,1	2	9	3	1	0.270525
W2,9,3,2	2	9	3	2	-0.901504
W2,10,3,1	2	10	3	1	-0.525204
W2,10,3,2	2	10	3	2	-0.065908
W2,11,3,1	2	11	3	1	0.629999
W2,11,3,2	2	11	3	2	0.092015

W2,12,3,1	2	12	3	1	0.815179
W2,12,3,2	2	12	3	2	-0.161705
W2,13,3,1	2	13	3	1	-0.619516
W2,13,3,2	2	13	3	2	0.042798
W2,14,3,1	2	14	3	1	-0.736596
W2,14,3,2	2	14	3	2	-0.298303
W2,15,3,1	2	15	3	1	-0.513741
W2,15,3,2	2	15	3	2	-0.894287
W2,16,3,1	2	16	3	1	0.919805
W2,16,3,2	2	16	3	2	0.987523
W2,17,3,1	2	17	3	1	-0.050492
W2,17,3,2	2	17	3	2	0.446104
W2,18,3,1	2	18	3	1	0.462285
W2,18,3,2	2	18	3	2	0.581587
W2,19,3,1	2	19	3	1	0.002657
W2,19,3,2	2	19	3	2	-0.087886
W2,20,3,1	2	20	3	1	0.247213
W2,20,3,2	2	20	3	2	0.34755
W2,21,3,1	2	21	3	1	-0.904563
W2,21,3,2	2	21	3	2	0.135284
W2,22,3,1	2	22	3	1	-0.450321
W2,22,3,2	2	22	3	2	-0.079552
W2,23,3,1	2	23	3	1	-0.149916
W2,23,3,2	2	23	3	2	0.338573
W2,24,3,1	2	24	3	1	-0.289359
W2,24,3,2	2	24	3	2	0.283723
W2,25,3,1	2	25	3	1	0.884715
W2,25,3,2	2	25	3	2	0.577099

Appendix E

Averaged Weights and Biases Associated the Predictor Model Built using Customer Data

Layers:

Neurons in the Input Layer	Neurons in the Hidden Layer	Neurons in the Output Layer
46	25	2

Biases:

Node ID	Layer #	Neuron #	Activation Function	Bias
N1,1	1	1	purelin	0.493935
N1,2	1	2	purelin	0.861392
N1,3	1	3	purelin	0.663258
N1,4	1	4	purelin	0.867076
N1,5	1	5	purelin	-0.783493
N1,6	1	6	purelin	0.904942
N1,7	1	7	purelin	0.001269
N1,8	1	8	purelin	-0.007588
N1,9	1	9	purelin	-0.810463
N1,10	1	10	purelin	-0.648547
N1,11	1	11	purelin	-0.611344
N1,12	1	12	purelin	-0.056233
N1,13	1	13	purelin	0.219575
N1,14	1	14	purelin	-0.126197
N1,15	1	15	purelin	-0.109497
N1,16	1	16	purelin	-0.950029
N1,17	1	17	purelin	0.467853
N1,18	1	18	purelin	-0.6364
N1,19	1	19	purelin	-0.10791
N1,20	1	20	purelin	0.373653
N1,21	1	21	purelin	0.428677
N1,22	1	22	purelin	-0.301855
N1,23	1	23	purelin	-0.691266
N1,24	1	24	purelin	-0.364558
N1,25	1	25	purelin	0.925404
N1,26	1	26	purelin	-0.404707
N1,27	1	27	purelin	0.23508
N1,28	1	28	purelin	-0.664576
N1,29	1	29	purelin	0.092739
N1,30	1	30	purelin	-0.600047
N1,31	1	31	purelin	0.252599
N1,32	1	32	purelin	0.165617
N1,33	1	33	purelin	0.814111
N1,34	1	34	purelin	0.145972
N1,35	1	35	purelin	-0.885967
N1,36	1	36	purelin	-0.692788

N1,37	1	37	purelin	0.582883
N1,38	1	38	purelin	0.737172
N1,39	1	39	purelin	0.023548
N1,40	1	40	purelin	-0.293668
N1,41	1	41	purelin	0.256132
N1,42	1	42	purelin	-0.408731
N1,43	1	43	purelin	-0.768662
N1,44	1	44	purelin	0.922053
N1,45	1	45	purelin	0.669764
N1,46	1	46	purelin	-0.409569
N2,1	2	1	logsig	0.533299
N2,2	2	2	logsig	-0.150121
N2,3	2	3	logsig	-0.840072
N2,4	2	4	logsig	0.82858
N2,5	2	5	logsig	-0.381137
N2,6	2	6	logsig	-0.20225
N2,7	2	7	logsig	0.619169
N2,8	2	8	logsig	0.436895
N2,9	2	9	logsig	-0.934217
N2,10	2	10	logsig	-0.255252
N2,11	2	11	logsig	0.134687
N2,12	2	12	logsig	-0.456377
N2,13	2	13	logsig	-0.897059
N2,14	2	14	logsig	-0.94876
N2,15	2	15	logsig	0.650146
N2,16	2	16	logsig	-0.953119
N2,17	2	17	logsig	-0.952215
N2,18	2	18	logsig	1.027608
N2,19	2	19	logsig	-0.251048
N2,20	2	20	logsig	0.6941
N2,21	2	21	logsig	0.627379
N2,22	2	22	logsig	0.130851
N2,23	2	23	logsig	-0.068426
N2,24	2	24	logsig	-0.062526
N2,25	2	25	logsig	0.23281
N3,1	3	1	logsig	-0.913552
N3,2	3	2	logsig	-0.608155

Weights:

Weight ID	Source Layer #	Source Neuron #	Target Layer #	Target Neuron #	Weight
W1,1,2,1	1	1	2	1	0.001999
W1,1,2,2	1	1	2	2	-0.131543
W1,1,2,3	1	1	2	3	0.080198
W1,1,2,4	1	1	2	4	0.164436
W1,1,2,5	1	1	2	5	0.587768

W1,1,2,6	1	1	2	6	0.299484
W1,1,2,7	1	1	2	7	-0.043526
W1,1,2,8	1	1	2	8	0.982469
W1,1,2,9	1	1	2	9	-0.322297
W1,1,2,10	1	1	2	10	-0.9229
W1,1,2,11	1	1	2	11	-0.572683
W1,1,2,12	1	1	2	12	-0.052427
W1,1,2,13	1	1	2	13	0.280438
W1,1,2,14	1	1	2	14	-0.715666
W1,1,2,15	1	1	2	15	0.40332
W1,1,2,16	1	1	2	16	0.597752
W1,1,2,17	1	1	2	17	0.469713
W1,1,2,18	1	1	2	18	-0.181208
W1,1,2,19	1	1	2	19	0.621238
W1,1,2,20	1	1	2	20	0.750841
W1,1,2,21	1	1	2	21	-0.707923
W1,1,2,22	1	1	2	22	0.605744
W1,1,2,23	1	1	2	23	0.149817
W1,1,2,24	1	1	2	24	-0.78522
W1,1,2,25	1	1	2	25	-0.212832
W1,2,2,1	1	2	2	1	-0.029419
W1,2,2,2	1	2	2	2	-0.164196
W1,2,2,3	1	2	2	3	-0.712634
W1,2,2,4	1	2	2	4	0.09854
W1,2,2,5	1	2	2	5	0.604229
W1,2,2,6	1	2	2	6	-0.982569
W1,2,2,7	1	2	2	7	-0.325767
W1,2,2,8	1	2	2	8	-0.018141
W1,2,2,9	1	2	2	9	0.709156
W1,2,2,10	1	2	2	10	0.993775
W1,2,2,11	1	2	2	11	0.226241
W1,2,2,12	1	2	2	12	-0.847636
W1,2,2,13	1	2	2	13	-0.932764
W1,2,2,14	1	2	2	14	0.075839
W1,2,2,15	1	2	2	15	0.628481
W1,2,2,16	1	2	2	16	-0.892642
W1,2,2,17	1	2	2	17	0.914857
W1,2,2,18	1	2	2	18	0.429864
W1,2,2,19	1	2	2	19	-0.472747
W1,2,2,20	1	2	2	20	-0.316849
W1,2,2,21	1	2	2	21	0.216743
W1,2,2,22	1	2	2	22	0.994072
W1,2,2,23	1	2	2	23	0.487819
W1,2,2,24	1	2	2	24	-0.243644

W1,2,2,25	1	2	2	25	-0.515557
W1,3,2,1	1	3	2	1	0.512081
W1,3,2,2	1	3	2	2	-0.062926
W1,3,2,3	1	3	2	3	0.534993
W1,3,2,4	1	3	2	4	0.117209
W1,3,2,5	1	3	2	5	-0.820685
W1,3,2,6	1	3	2	6	0.482651
W1,3,2,7	1	3	2	7	-0.598935
W1,3,2,8	1	3	2	8	0.270692
W1,3,2,9	1	3	2	9	-0.206068
W1,3,2,10	1	3	2	10	-0.402606
W1,3,2,11	1	3	2	11	-0.669912
W1,3,2,12	1	3	2	12	1.073162
W1,3,2,13	1	3	2	13	-0.302525
W1,3,2,14	1	3	2	14	0.63209
W1,3,2,15	1	3	2	15	-0.298612
W1,3,2,16	1	3	2	16	-0.238569
W1,3,2,17	1	3	2	17	0.894503
W1,3,2,18	1	3	2	18	0.36668
W1,3,2,19	1	3	2	19	0.609735
W1,3,2,20	1	3	2	20	-0.098389
W1,3,2,21	1	3	2	21	0.539345
W1,3,2,22	1	3	2	22	0.723829
W1,3,2,23	1	3	2	23	-0.94789
W1,3,2,24	1	3	2	24	-0.708178
W1,3,2,25	1	3	2	25	-0.754556
W1,4,2,1	1	4	2	1	-0.342023
W1,4,2,2	1	4	2	2	-0.870607
W1,4,2,3	1	4	2	3	0.200328
W1,4,2,4	1	4	2	4	0.671279
W1,4,2,5	1	4	2	5	0.336861
W1,4,2,6	1	4	2	6	0.162547
W1,4,2,7	1	4	2	7	-0.517407
W1,4,2,8	1	4	2	8	-0.420881
W1,4,2,9	1	4	2	9	-0.849307
W1,4,2,10	1	4	2	10	0.63345
W1,4,2,11	1	4	2	11	0.042138
W1,4,2,12	1	4	2	12	-0.300548
W1,4,2,13	1	4	2	13	0.850485
W1,4,2,14	1	4	2	14	-0.609827
W1,4,2,15	1	4	2	15	0.210404
W1,4,2,16	1	4	2	16	0.078981
W1,4,2,17	1	4	2	17	-0.304549
W1,4,2,18	1	4	2	18	0.716941

W1,4,2,19	1	4	2	19	0.683202
W1,4,2,20	1	4	2	20	-0.547565
W1,4,2,21	1	4	2	21	-1.04172
W1,4,2,22	1	4	2	22	-0.538992
W1,4,2,23	1	4	2	23	-0.507845
W1,4,2,24	1	4	2	24	-0.386469
W1,4,2,25	1	4	2	25	-0.023737
W1,5,2,1	1	5	2	1	0.458246
W1,5,2,2	1	5	2	2	-0.595277
W1,5,2,3	1	5	2	3	-0.914123
W1,5,2,4	1	5	2	4	-0.257426
W1,5,2,5	1	5	2	5	0.035581
W1,5,2,6	1	5	2	6	-0.323872
W1,5,2,7	1	5	2	7	-0.390964
W1,5,2,8	1	5	2	8	0.666473
W1,5,2,9	1	5	2	9	-0.595251
W1,5,2,10	1	5	2	10	0.613739
W1,5,2,11	1	5	2	11	0.870154
W1,5,2,12	1	5	2	12	-0.85226
W1,5,2,13	1	5	2	13	0.21638
W1,5,2,14	1	5	2	14	-0.673602
W1,5,2,15	1	5	2	15	-0.81518
W1,5,2,16	1	5	2	16	-0.485487
W1,5,2,17	1	5	2	17	-0.817776
W1,5,2,18	1	5	2	18	1.055076
W1,5,2,19	1	5	2	19	0.101814
W1,5,2,20	1	5	2	20	0.852823
W1,5,2,21	1	5	2	21	-0.395078
W1,5,2,22	1	5	2	22	-0.406891
W1,5,2,23	1	5	2	23	0.477748
W1,5,2,24	1	5	2	24	-0.595451
W1,5,2,25	1	5	2	25	-0.24943
W1,6,2,1	1	6	2	1	0.186467
W1,6,2,2	1	6	2	2	0.284901
W1,6,2,3	1	6	2	3	-0.296785
W1,6,2,4	1	6	2	4	0.691674
W1,6,2,5	1	6	2	5	-0.6084
W1,6,2,6	1	6	2	6	0.742572
W1,6,2,7	1	6	2	7	0.478544
W1,6,2,8	1	6	2	8	0.197184
W1,6,2,9	1	6	2	9	0.889059
W1,6,2,10	1	6	2	10	0.646245
W1,6,2,11	1	6	2	11	-0.440273
W1,6,2,12	1	6	2	12	0.719336

W1,6,2,13	1	6	2	13	-0.79621
W1,6,2,14	1	6	2	14	0.69445
W1,6,2,15	1	6	2	15	0.601507
W1,6,2,16	1	6	2	16	-0.132846
W1,6,2,17	1	6	2	17	-0.335121
W1,6,2,18	1	6	2	18	0.026933
W1,6,2,19	1	6	2	19	0.904176
W1,6,2,20	1	6	2	20	-0.243208
W1,6,2,21	1	6	2	21	0.230729
W1,6,2,22	1	6	2	22	0.880752
W1,6,2,23	1	6	2	23	-0.507219
W1,6,2,24	1	6	2	24	-0.678836
W1,6,2,25	1	6	2	25	-0.848622
W1,7,2,1	1	7	2	1	-0.545515
W1,7,2,2	1	7	2	2	0.903079
W1,7,2,3	1	7	2	3	0.285768
W1,7,2,4	1	7	2	4	-0.369858
W1,7,2,5	1	7	2	5	-0.356164
W1,7,2,6	1	7	2	6	0.06888
W1,7,2,7	1	7	2	7	-0.357931
W1,7,2,8	1	7	2	8	0.110423
W1,7,2,9	1	7	2	9	0.971417
W1,7,2,10	1	7	2	10	0.076556
W1,7,2,11	1	7	2	11	0.103785
W1,7,2,12	1	7	2	12	0.523737
W1,7,2,13	1	7	2	13	0.301583
W1,7,2,14	1	7	2	14	0.759759
W1,7,2,15	1	7	2	15	0.81898
W1,7,2,16	1	7	2	16	-0.846444
W1,7,2,17	1	7	2	17	0.846043
W1,7,2,18	1	7	2	18	-0.063974
W1,7,2,19	1	7	2	19	-0.35616
W1,7,2,20	1	7	2	20	0.275876
W1,7,2,21	1	7	2	21	-0.60002
W1,7,2,22	1	7	2	22	-0.877456
W1,7,2,23	1	7	2	23	-0.2328
W1,7,2,24	1	7	2	24	0.456099
W1,7,2,25	1	7	2	25	-0.646709
W1,8,2,1	1	8	2	1	-0.050943
W1,8,2,2	1	8	2	2	0.414924
W1,8,2,3	1	8	2	3	0.614461
W1,8,2,4	1	8	2	4	-0.192264
W1,8,2,5	1	8	2	5	-0.58682
W1,8,2,6	1	8	2	6	-0.389923

W1,8,2,7	1	8	2	7	0.773231
W1,8,2,8	1	8	2	8	-0.360577
W1,8,2,9	1	8	2	9	0.725409
W1,8,2,10	1	8	2	10	-0.103995
W1,8,2,11	1	8	2	11	0.833434
W1,8,2,12	1	8	2	12	-0.594259
W1,8,2,13	1	8	2	13	-0.180574
W1,8,2,14	1	8	2	14	0.227825
W1,8,2,15	1	8	2	15	-0.412334
W1,8,2,16	1	8	2	16	-0.975025
W1,8,2,17	1	8	2	17	-0.848385
W1,8,2,18	1	8	2	18	-0.090036
W1,8,2,19	1	8	2	19	0.540325
W1,8,2,20	1	8	2	20	0.077827
W1,8,2,21	1	8	2	21	-0.592575
W1,8,2,22	1	8	2	22	-0.62557
W1,8,2,23	1	8	2	23	0.604232
W1,8,2,24	1	8	2	24	-0.832999
W1,8,2,25	1	8	2	25	0.034849
W1,9,2,1	1	9	2	1	0.468635
W1,9,2,2	1	9	2	2	0.503707
W1,9,2,3	1	9	2	3	-0.654844
W1,9,2,4	1	9	2	4	0.286934
W1,9,2,5	1	9	2	5	-0.412542
W1,9,2,6	1	9	2	6	-0.856654
W1,9,2,7	1	9	2	7	-0.715862
W1,9,2,8	1	9	2	8	-0.95111
W1,9,2,9	1	9	2	9	-0.001676
W1,9,2,10	1	9	2	10	0.914489
W1,9,2,11	1	9	2	11	-0.647215
W1,9,2,12	1	9	2	12	-0.215225
W1,9,2,13	1	9	2	13	-0.491718
W1,9,2,14	1	9	2	14	0.205081
W1,9,2,15	1	9	2	15	0.097525
W1,9,2,16	1	9	2	16	0.043228
W1,9,2,17	1	9	2	17	-0.190557
W1,9,2,18	1	9	2	18	-0.656484
W1,9,2,19	1	9	2	19	0.223771
W1,9,2,20	1	9	2	20	0.089953
W1,9,2,21	1	9	2	21	-0.590933
W1,9,2,22	1	9	2	22	0.791608
W1,9,2,23	1	9	2	23	0.260695
W1,9,2,24	1	9	2	24	-0.958557
W1,9,2,25	1	9	2	25	0.822697

W1,10,2,1	1	10	2	1	-0.12462
W1,10,2,2	1	10	2	2	-0.33958
W1,10,2,3	1	10	2	3	-0.402255
W1,10,2,4	1	10	2	4	0.162425
W1,10,2,5	1	10	2	5	0.227303
W1,10,2,6	1	10	2	6	-0.283289
W1,10,2,7	1	10	2	7	0.853116
W1,10,2,8	1	10	2	8	0.65915
W1,10,2,9	1	10	2	9	-0.794539
W1,10,2,10	1	10	2	10	-0.540413
W1,10,2,11	1	10	2	11	-0.362634
W1,10,2,12	1	10	2	12	-0.563973
W1,10,2,13	1	10	2	13	0.695532
W1,10,2,14	1	10	2	14	0.820484
W1,10,2,15	1	10	2	15	0.334672
W1,10,2,16	1	10	2	16	-0.970736
W1,10,2,17	1	10	2	17	-0.014967
W1,10,2,18	1	10	2	18	0.950256
W1,10,2,19	1	10	2	19	-0.655133
W1,10,2,20	1	10	2	20	-1.027249
W1,10,2,21	1	10	2	21	-0.64785
W1,10,2,22	1	10	2	22	0.092782
W1,10,2,23	1	10	2	23	0.19856
W1,10,2,24	1	10	2	24	0.670854
W1,10,2,25	1	10	2	25	0.300297
W1,11,2,1	1	11	2	1	0.139137
W1,11,2,2	1	11	2	2	-0.498097
W1,11,2,3	1	11	2	3	0.632272
W1,11,2,4	1	11	2	4	-0.051727
W1,11,2,5	1	11	2	5	0.825457
W1,11,2,6	1	11	2	6	-0.396464
W1,11,2,7	1	11	2	7	-0.003179
W1,11,2,8	1	11	2	8	-0.83727
W1,11,2,9	1	11	2	9	-0.502062
W1,11,2,10	1	11	2	10	0.328712
W1,11,2,11	1	11	2	11	0.133936
W1,11,2,12	1	11	2	12	0.305517
W1,11,2,13	1	11	2	13	-0.122837
W1,11,2,14	1	11	2	14	0.977961
W1,11,2,15	1	11	2	15	-0.497491
W1,11,2,16	1	11	2	16	-0.971384
W1,11,2,17	1	11	2	17	0.881661
W1,11,2,18	1	11	2	18	-0.233885
W1,11,2,19	1	11	2	19	-0.47631

W1,11,2,20	1	11	2	20	0.9557
W1,11,2,21	1	11	2	21	0.287871
W1,11,2,22	1	11	2	22	0.072477
W1,11,2,23	1	11	2	23	0.35162
W1,11,2,24	1	11	2	24	-0.776155
W1,11,2,25	1	11	2	25	-0.183931
W1,12,2,1	1	12	2	1	0.829642
W1,12,2,2	1	12	2	2	0.820281
W1,12,2,3	1	12	2	3	0.211246
W1,12,2,4	1	12	2	4	0.203115
W1,12,2,5	1	12	2	5	0.172316
W1,12,2,6	1	12	2	6	-0.031161
W1,12,2,7	1	12	2	7	0.667004
W1,12,2,8	1	12	2	8	-0.103275
W1,12,2,9	1	12	2	9	-0.253447
W1,12,2,10	1	12	2	10	-0.690959
W1,12,2,11	1	12	2	11	-0.157113
W1,12,2,12	1	12	2	12	-0.10969
W1,12,2,13	1	12	2	13	-0.933509
W1,12,2,14	1	12	2	14	-0.907953
W1,12,2,15	1	12	2	15	-0.278667
W1,12,2,16	1	12	2	16	-0.915148
W1,12,2,17	1	12	2	17	-0.356155
W1,12,2,18	1	12	2	18	-0.800587
W1,12,2,19	1	12	2	19	-0.751984
W1,12,2,20	1	12	2	20	0.581731
W1,12,2,21	1	12	2	21	0.654604
W1,12,2,22	1	12	2	22	-0.393409
W1,12,2,23	1	12	2	23	-0.175848
W1,12,2,24	1	12	2	24	-0.901132
W1,12,2,25	1	12	2	25	0.57644
W1,13,2,1	1	13	2	1	-0.496341
W1,13,2,2	1	13	2	2	0.611316
W1,13,2,3	1	13	2	3	0.276363
W1,13,2,4	1	13	2	4	-0.69874
W1,13,2,5	1	13	2	5	0.022337
W1,13,2,6	1	13	2	6	0.365571
W1,13,2,7	1	13	2	7	-0.438124
W1,13,2,8	1	13	2	8	-0.748667
W1,13,2,9	1	13	2	9	0.980977
W1,13,2,10	1	13	2	10	0.824118
W1,13,2,11	1	13	2	11	0.56672
W1,13,2,12	1	13	2	12	0.483966
W1,13,2,13	1	13	2	13	-0.528886

W1,13,2,14	1	13	2	14	0.760002
W1,13,2,15	1	13	2	15	-0.841275
W1,13,2,16	1	13	2	16	-0.386505
W1,13,2,17	1	13	2	17	-0.928763
W1,13,2,18	1	13	2	18	0.247389
W1,13,2,19	1	13	2	19	0.592017
W1,13,2,20	1	13	2	20	0.346779
W1,13,2,21	1	13	2	21	-0.825976
W1,13,2,22	1	13	2	22	0.498728
W1,13,2,23	1	13	2	23	0.546643
W1,13,2,24	1	13	2	24	0.454385
W1,13,2,25	1	13	2	25	-0.651414
W1,14,2,1	1	14	2	1	-0.374354
W1,14,2,2	1	14	2	2	-0.051676
W1,14,2,3	1	14	2	3	-0.116857
W1,14,2,4	1	14	2	4	-0.933713
W1,14,2,5	1	14	2	5	-0.681241
W1,14,2,6	1	14	2	6	-0.201931
W1,14,2,7	1	14	2	7	0.932998
W1,14,2,8	1	14	2	8	-1.01545
W1,14,2,9	1	14	2	9	-0.349262
W1,14,2,10	1	14	2	10	-0.34302
W1,14,2,11	1	14	2	11	-0.289226
W1,14,2,12	1	14	2	12	-0.593442
W1,14,2,13	1	14	2	13	-0.43645
W1,14,2,14	1	14	2	14	-0.331142
W1,14,2,15	1	14	2	15	-0.27918
W1,14,2,16	1	14	2	16	-0.513137
W1,14,2,17	1	14	2	17	0.604281
W1,14,2,18	1	14	2	18	0.917976
W1,14,2,19	1	14	2	19	-0.724077
W1,14,2,20	1	14	2	20	-0.799057
W1,14,2,21	1	14	2	21	0.004659
W1,14,2,22	1	14	2	22	0.914569
W1,14,2,23	1	14	2	23	-0.711973
W1,14,2,24	1	14	2	24	0.4103
W1,14,2,25	1	14	2	25	-0.261253
W1,15,2,1	1	15	2	1	-0.806735
W1,15,2,2	1	15	2	2	0.605007
W1,15,2,3	1	15	2	3	0.80956
W1,15,2,4	1	15	2	4	-0.445928
W1,15,2,5	1	15	2	5	-0.264596
W1,15,2,6	1	15	2	6	0.675546
W1,15,2,7	1	15	2	7	0.367937

W1,15,2,8	1	15	2	8	-0.444345
W1,15,2,9	1	15	2	9	0.623666
W1,15,2,10	1	15	2	10	0.228096
W1,15,2,11	1	15	2	11	0.524368
W1,15,2,12	1	15	2	12	0.089046
W1,15,2,13	1	15	2	13	-0.243721
W1,15,2,14	1	15	2	14	-0.959679
W1,15,2,15	1	15	2	15	-0.575541
W1,15,2,16	1	15	2	16	0.456521
W1,15,2,17	1	15	2	17	0.988534
W1,15,2,18	1	15	2	18	-0.345618
W1,15,2,19	1	15	2	19	0.727662
W1,15,2,20	1	15	2	20	-0.622679
W1,15,2,21	1	15	2	21	-0.373392
W1,15,2,22	1	15	2	22	-0.488082
W1,15,2,23	1	15	2	23	-0.335822
W1,15,2,24	1	15	2	24	-0.318885
W1,15,2,25	1	15	2	25	0.567729
W1,16,2,1	1	16	2	1	0.603476
W1,16,2,2	1	16	2	2	-0.715857
W1,16,2,3	1	16	2	3	-0.430744
W1,16,2,4	1	16	2	4	-0.928634
W1,16,2,5	1	16	2	5	0.001346
W1,16,2,6	1	16	2	6	0.217221
W1,16,2,7	1	16	2	7	-0.067383
W1,16,2,8	1	16	2	8	-0.25408
W1,16,2,9	1	16	2	9	0.826457
W1,16,2,10	1	16	2	10	-0.501531
W1,16,2,11	1	16	2	11	-0.858369
W1,16,2,12	1	16	2	12	0.792765
W1,16,2,13	1	16	2	13	0.2214
W1,16,2,14	1	16	2	14	0.272365
W1,16,2,15	1	16	2	15	0.713331
W1,16,2,16	1	16	2	16	-0.409363
W1,16,2,17	1	16	2	17	0.698705
W1,16,2,18	1	16	2	18	0.937024
W1,16,2,19	1	16	2	19	0.338709
W1,16,2,20	1	16	2	20	0.922916
W1,16,2,21	1	16	2	21	0.247076
W1,16,2,22	1	16	2	22	-0.150703
W1,16,2,23	1	16	2	23	0.50713
W1,16,2,24	1	16	2	24	-0.294829
W1,16,2,25	1	16	2	25	0.286332
W1,17,2,1	1	17	2	1	0.352914

W1,17,2,2	1	17	2	2	0.571602
W1,17,2,3	1	17	2	3	0.960041
W1,17,2,4	1	17	2	4	0.10672
W1,17,2,5	1	17	2	5	-0.507948
W1,17,2,6	1	17	2	6	-0.688571
W1,17,2,7	1	17	2	7	0.030695
W1,17,2,8	1	17	2	8	-0.032148
W1,17,2,9	1	17	2	9	0.196663
W1,17,2,10	1	17	2	10	-0.327846
W1,17,2,11	1	17	2	11	0.4935
W1,17,2,12	1	17	2	12	0.174883
W1,17,2,13	1	17	2	13	-0.916879
W1,17,2,14	1	17	2	14	-0.762512
W1,17,2,15	1	17	2	15	-0.100253
W1,17,2,16	1	17	2	16	-0.81137
W1,17,2,17	1	17	2	17	0.55694
W1,17,2,18	1	17	2	18	0.189292
W1,17,2,19	1	17	2	19	-0.195949
W1,17,2,20	1	17	2	20	-0.801048
W1,17,2,21	1	17	2	21	-0.236376
W1,17,2,22	1	17	2	22	-0.086585
W1,17,2,23	1	17	2	23	-0.155958
W1,17,2,24	1	17	2	24	0.440071
W1,17,2,25	1	17	2	25	-0.668592
W1,18,2,1	1	18	2	1	-0.120539
W1,18,2,2	1	18	2	2	0.401974
W1,18,2,3	1	18	2	3	0.828306
W1,18,2,4	1	18	2	4	-0.718519
W1,18,2,5	1	18	2	5	0.217526
W1,18,2,6	1	18	2	6	0.898061
W1,18,2,7	1	18	2	7	-0.8916
W1,18,2,8	1	18	2	8	0.668728
W1,18,2,9	1	18	2	9	0.964744
W1,18,2,10	1	18	2	10	-0.915977
W1,18,2,11	1	18	2	11	-0.889754
W1,18,2,12	1	18	2	12	-0.264049
W1,18,2,13	1	18	2	13	-0.748164
W1,18,2,14	1	18	2	14	-0.041528
W1,18,2,15	1	18	2	15	0.515779
W1,18,2,16	1	18	2	16	0.993851
W1,18,2,17	1	18	2	17	0.626413
W1,18,2,18	1	18	2	18	-0.672775
W1,18,2,19	1	18	2	19	0.868611
W1,18,2,20	1	18	2	20	-0.612597

W1,18,2,21	1	18	2	21	-0.985798
W1,18,2,22	1	18	2	22	0.6358
W1,18,2,23	1	18	2	23	-0.611631
W1,18,2,24	1	18	2	24	-0.097723
W1,18,2,25	1	18	2	25	0.932969
W1,19,2,1	1	19	2	1	0.863947
W1,19,2,2	1	19	2	2	-0.694431
W1,19,2,3	1	19	2	3	0.67555
W1,19,2,4	1	19	2	4	0.760569
W1,19,2,5	1	19	2	5	0.27446
W1,19,2,6	1	19	2	6	-0.090556
W1,19,2,7	1	19	2	7	-0.738325
W1,19,2,8	1	19	2	8	-0.52684
W1,19,2,9	1	19	2	9	-0.341648
W1,19,2,10	1	19	2	10	0.389325
W1,19,2,11	1	19	2	11	0.373938
W1,19,2,12	1	19	2	12	0.997103
W1,19,2,13	1	19	2	13	-0.131069
W1,19,2,14	1	19	2	14	0.551481
W1,19,2,15	1	19	2	15	0.882239
W1,19,2,16	1	19	2	16	-0.062831
W1,19,2,17	1	19	2	17	-0.009258
W1,19,2,18	1	19	2	18	0.351019
W1,19,2,19	1	19	2	19	-0.1262
W1,19,2,20	1	19	2	20	0.805064
W1,19,2,21	1	19	2	21	-0.133997
W1,19,2,22	1	19	2	22	-0.771253
W1,19,2,23	1	19	2	23	0.616966
W1,19,2,24	1	19	2	24	-0.844739
W1,19,2,25	1	19	2	25	0.132953
W1,20,2,1	1	20	2	1	-0.610567
W1,20,2,2	1	20	2	2	-0.875099
W1,20,2,3	1	20	2	3	-0.44392
W1,20,2,4	1	20	2	4	0.309656
W1,20,2,5	1	20	2	5	-0.428731
W1,20,2,6	1	20	2	6	-0.786497
W1,20,2,7	1	20	2	7	-0.408145
W1,20,2,8	1	20	2	8	-0.188363
W1,20,2,9	1	20	2	9	-0.417044
W1,20,2,10	1	20	2	10	-0.747832
W1,20,2,11	1	20	2	11	-0.866483
W1,20,2,12	1	20	2	12	0.748602
W1,20,2,13	1	20	2	13	-0.702572
W1,20,2,14	1	20	2	14	0.510001

W1,20,2,15	1	20	2	15	0.017411
W1,20,2,16	1	20	2	16	0.110945
W1,20,2,17	1	20	2	17	-0.135602
W1,20,2,18	1	20	2	18	0.013914
W1,20,2,19	1	20	2	19	0.909797
W1,20,2,20	1	20	2	20	0.618194
W1,20,2,21	1	20	2	21	-0.519935
W1,20,2,22	1	20	2	22	0.183718
W1,20,2,23	1	20	2	23	-0.25977
W1,20,2,24	1	20	2	24	1.037748
W1,20,2,25	1	20	2	25	-0.574783
W1,21,2,1	1	21	2	1	0.42341
W1,21,2,2	1	21	2	2	-0.674788
W1,21,2,3	1	21	2	3	-0.734962
W1,21,2,4	1	21	2	4	0.569808
W1,21,2,5	1	21	2	5	0.542096
W1,21,2,6	1	21	2	6	0.241385
W1,21,2,7	1	21	2	7	-0.80428
W1,21,2,8	1	21	2	8	0.980888
W1,21,2,9	1	21	2	9	0.068738
W1,21,2,10	1	21	2	10	0.025226
W1,21,2,11	1	21	2	11	-0.566396
W1,21,2,12	1	21	2	12	0.65699
W1,21,2,13	1	21	2	13	-0.652455
W1,21,2,14	1	21	2	14	0.008842
W1,21,2,15	1	21	2	15	-0.763084
W1,21,2,16	1	21	2	16	0.167702
W1,21,2,17	1	21	2	17	0.825804
W1,21,2,18	1	21	2	18	1.228638
W1,21,2,19	1	21	2	19	0.803452
W1,21,2,20	1	21	2	20	0.620512
W1,21,2,21	1	21	2	21	-0.945551
W1,21,2,22	1	21	2	22	0.944919
W1,21,2,23	1	21	2	23	-0.280143
W1,21,2,24	1	21	2	24	0.984367
W1,21,2,25	1	21	2	25	-0.531793
W1,22,2,1	1	22	2	1	-0.814393
W1,22,2,2	1	22	2	2	-0.769031
W1,22,2,3	1	22	2	3	-0.272088
W1,22,2,4	1	22	2	4	-0.308597
W1,22,2,5	1	22	2	5	-0.953687
W1,22,2,6	1	22	2	6	-0.260118
W1,22,2,7	1	22	2	7	0.741631
W1,22,2,8	1	22	2	8	-0.100345

W1,22,2,9	1	22	2	9	0.036417
W1,22,2,10	1	22	2	10	0.943332
W1,22,2,11	1	22	2	11	0.742297
W1,22,2,12	1	22	2	12	0.362246
W1,22,2,13	1	22	2	13	-0.221978
W1,22,2,14	1	22	2	14	-0.250142
W1,22,2,15	1	22	2	15	-0.997357
W1,22,2,16	1	22	2	16	0.112816
W1,22,2,17	1	22	2	17	0.490925
W1,22,2,18	1	22	2	18	-0.779128
W1,22,2,19	1	22	2	19	-0.135085
W1,22,2,20	1	22	2	20	0.453031
W1,22,2,21	1	22	2	21	0.303549
W1,22,2,22	1	22	2	22	0.933637
W1,22,2,23	1	22	2	23	-0.290557
W1,22,2,24	1	22	2	24	-0.752751
W1,22,2,25	1	22	2	25	-0.336757
W1,23,2,1	1	23	2	1	-0.186848
W1,23,2,2	1	23	2	2	0.882676
W1,23,2,3	1	23	2	3	-0.810523
W1,23,2,4	1	23	2	4	-0.286353
W1,23,2,5	1	23	2	5	-0.396534
W1,23,2,6	1	23	2	6	0.766045
W1,23,2,7	1	23	2	7	-0.23461
W1,23,2,8	1	23	2	8	-0.20186
W1,23,2,9	1	23	2	9	0.534149
W1,23,2,10	1	23	2	10	-0.673649
W1,23,2,11	1	23	2	11	-0.367018
W1,23,2,12	1	23	2	12	0.785501
W1,23,2,13	1	23	2	13	0.070766
W1,23,2,14	1	23	2	14	0.4132
W1,23,2,15	1	23	2	15	0.962241
W1,23,2,16	1	23	2	16	0.039894
W1,23,2,17	1	23	2	17	-0.589761
W1,23,2,18	1	23	2	18	-0.357524
W1,23,2,19	1	23	2	19	0.01587
W1,23,2,20	1	23	2	20	-0.722267
W1,23,2,21	1	23	2	21	-0.426427
W1,23,2,22	1	23	2	22	-0.494474
W1,23,2,23	1	23	2	23	0.617775
W1,23,2,24	1	23	2	24	-0.033038
W1,23,2,25	1	23	2	25	-0.605755
W1,24,2,1	1	24	2	1	-0.377296
W1,24,2,2	1	24	2	2	-0.278637

W1,24,2,3	1	24	2	3	-0.854305
W1,24,2,4	1	24	2	4	-0.665771
W1,24,2,5	1	24	2	5	0.930896
W1,24,2,6	1	24	2	6	-0.58278
W1,24,2,7	1	24	2	7	-1.013915
W1,24,2,8	1	24	2	8	0.367859
W1,24,2,9	1	24	2	9	-0.204143
W1,24,2,10	1	24	2	10	-0.324756
W1,24,2,11	1	24	2	11	0.953409
W1,24,2,12	1	24	2	12	-0.269971
W1,24,2,13	1	24	2	13	-0.42224
W1,24,2,14	1	24	2	14	0.370381
W1,24,2,15	1	24	2	15	-0.063813
W1,24,2,16	1	24	2	16	0.394316
W1,24,2,17	1	24	2	17	-0.365373
W1,24,2,18	1	24	2	18	-0.323006
W1,24,2,19	1	24	2	19	0.31668
W1,24,2,20	1	24	2	20	-0.304505
W1,24,2,21	1	24	2	21	0.835635
W1,24,2,22	1	24	2	22	-0.21746
W1,24,2,23	1	24	2	23	0.389143
W1,24,2,24	1	24	2	24	0.601971
W1,24,2,25	1	24	2	25	0.558134
W1,25,2,1	1	25	2	1	-0.022141
W1,25,2,2	1	25	2	2	-0.822743
W1,25,2,3	1	25	2	3	-0.131421
W1,25,2,4	1	25	2	4	-0.222494
W1,25,2,5	1	25	2	5	0.84507
W1,25,2,6	1	25	2	6	0.285213
W1,25,2,7	1	25	2	7	-0.108675
W1,25,2,8	1	25	2	8	0.571433
W1,25,2,9	1	25	2	9	-0.051694
W1,25,2,10	1	25	2	10	-0.511017
W1,25,2,11	1	25	2	11	0.556167
W1,25,2,12	1	25	2	12	1.133938
W1,25,2,13	1	25	2	13	0.82861
W1,25,2,14	1	25	2	14	0.405459
W1,25,2,15	1	25	2	15	0.606746
W1,25,2,16	1	25	2	16	-0.018194
W1,25,2,17	1	25	2	17	0.927074
W1,25,2,18	1	25	2	18	1.102336
W1,25,2,19	1	25	2	19	-0.702084
W1,25,2,20	1	25	2	20	0.870299
W1,25,2,21	1	25	2	21	0.928316

W1,25,2,22	1	25	2	22	-0.881673
W1,25,2,23	1	25	2	23	0.457839
W1,25,2,24	1	25	2	24	-0.04054
W1,25,2,25	1	25	2	25	0.231438
W1,26,2,1	1	26	2	1	-0.546004
W1,26,2,2	1	26	2	2	0.213235
W1,26,2,3	1	26	2	3	0.539664
W1,26,2,4	1	26	2	4	-0.084025
W1,26,2,5	1	26	2	5	0.068608
W1,26,2,6	1	26	2	6	-0.082943
W1,26,2,7	1	26	2	7	0.841501
W1,26,2,8	1	26	2	8	0.192621
W1,26,2,9	1	26	2	9	-0.935454
W1,26,2,10	1	26	2	10	0.799957
W1,26,2,11	1	26	2	11	0.273081
W1,26,2,12	1	26	2	12	-0.220015
W1,26,2,13	1	26	2	13	0.315568
W1,26,2,14	1	26	2	14	-0.060547
W1,26,2,15	1	26	2	15	-0.016707
W1,26,2,16	1	26	2	16	-0.855046
W1,26,2,17	1	26	2	17	-0.597506
W1,26,2,18	1	26	2	18	-1.048213
W1,26,2,19	1	26	2	19	0.787501
W1,26,2,20	1	26	2	20	-0.159683
W1,26,2,21	1	26	2	21	-0.643045
W1,26,2,22	1	26	2	22	0.250239
W1,26,2,23	1	26	2	23	-0.073762
W1,26,2,24	1	26	2	24	0.472935
W1,26,2,25	1	26	2	25	0.61924
W1,27,2,1	1	27	2	1	0.574829
W1,27,2,2	1	27	2	2	0.686824
W1,27,2,3	1	27	2	3	0.969239
W1,27,2,4	1	27	2	4	0.201
W1,27,2,5	1	27	2	5	-0.439281
W1,27,2,6	1	27	2	6	0.507886
W1,27,2,7	1	27	2	7	-0.290436
W1,27,2,8	1	27	2	8	0.53673
W1,27,2,9	1	27	2	9	-0.329624
W1,27,2,10	1	27	2	10	0.063167
W1,27,2,11	1	27	2	11	-0.452233
W1,27,2,12	1	27	2	12	0.013345
W1,27,2,13	1	27	2	13	0.441773
W1,27,2,14	1	27	2	14	-0.749759
W1,27,2,15	1	27	2	15	-0.188257

W1,27,2,16	1	27	2	16	-0.660109
W1,27,2,17	1	27	2	17	-0.485259
W1,27,2,18	1	27	2	18	0.794597
W1,27,2,19	1	27	2	19	0.175497
W1,27,2,20	1	27	2	20	-0.191545
W1,27,2,21	1	27	2	21	0.309258
W1,27,2,22	1	27	2	22	0.260791
W1,27,2,23	1	27	2	23	0.402208
W1,27,2,24	1	27	2	24	0.24472
W1,27,2,25	1	27	2	25	0.959674
W1,28,2,1	1	28	2	1	-0.198443
W1,28,2,2	1	28	2	2	-0.423274
W1,28,2,3	1	28	2	3	-0.938567
W1,28,2,4	1	28	2	4	0.761875
W1,28,2,5	1	28	2	5	-0.260526
W1,28,2,6	1	28	2	6	-0.412375
W1,28,2,7	1	28	2	7	-0.624168
W1,28,2,8	1	28	2	8	0.226456
W1,28,2,9	1	28	2	9	-0.665679
W1,28,2,10	1	28	2	10	-0.488024
W1,28,2,11	1	28	2	11	0.860628
W1,28,2,12	1	28	2	12	0.432132
W1,28,2,13	1	28	2	13	0.41745
W1,28,2,14	1	28	2	14	-0.450262
W1,28,2,15	1	28	2	15	0.034164
W1,28,2,16	1	28	2	16	-0.275167
W1,28,2,17	1	28	2	17	0.645429
W1,28,2,18	1	28	2	18	-0.350962
W1,28,2,19	1	28	2	19	0.611348
W1,28,2,20	1	28	2	20	0.697284
W1,28,2,21	1	28	2	21	0.252609
W1,28,2,22	1	28	2	22	-0.104627
W1,28,2,23	1	28	2	23	-0.502157
W1,28,2,24	1	28	2	24	0.201661
W1,28,2,25	1	28	2	25	-0.547294
W1,29,2,1	1	29	2	1	0.788113
W1,29,2,2	1	29	2	2	-0.773977
W1,29,2,3	1	29	2	3	-0.906791
W1,29,2,4	1	29	2	4	0.003495
W1,29,2,5	1	29	2	5	0.443028
W1,29,2,6	1	29	2	6	0.424694
W1,29,2,7	1	29	2	7	0.578724
W1,29,2,8	1	29	2	8	-0.74159
W1,29,2,9	1	29	2	9	-0.283587

W1,29,2,10	1	29	2	10	0.627628
W1,29,2,11	1	29	2	11	0.824565
W1,29,2,12	1	29	2	12	-0.614213
W1,29,2,13	1	29	2	13	0.080918
W1,29,2,14	1	29	2	14	-0.579286
W1,29,2,15	1	29	2	15	-0.803536
W1,29,2,16	1	29	2	16	-0.671095
W1,29,2,17	1	29	2	17	-0.40315
W1,29,2,18	1	29	2	18	-0.321786
W1,29,2,19	1	29	2	19	0.70981
W1,29,2,20	1	29	2	20	-0.675531
W1,29,2,21	1	29	2	21	0.218796
W1,29,2,22	1	29	2	22	0.997675
W1,29,2,23	1	29	2	23	0.221178
W1,29,2,24	1	29	2	24	0.919374
W1,29,2,25	1	29	2	25	0.310067
W1,30,2,1	1	30	2	1	0.83793
W1,30,2,2	1	30	2	2	0.895433
W1,30,2,3	1	30	2	3	-0.036612
W1,30,2,4	1	30	2	4	-0.189455
W1,30,2,5	1	30	2	5	0.039546
W1,30,2,6	1	30	2	6	0.113756
W1,30,2,7	1	30	2	7	0.839414
W1,30,2,8	1	30	2	8	-0.574207
W1,30,2,9	1	30	2	9	0.084267
W1,30,2,10	1	30	2	10	0.565167
W1,30,2,11	1	30	2	11	0.63682
W1,30,2,12	1	30	2	12	0.880189
W1,30,2,13	1	30	2	13	0.801767
W1,30,2,14	1	30	2	14	0.645874
W1,30,2,15	1	30	2	15	0.960545
W1,30,2,16	1	30	2	16	-0.769626
W1,30,2,17	1	30	2	17	-0.374162
W1,30,2,18	1	30	2	18	0.953561
W1,30,2,19	1	30	2	19	-0.121382
W1,30,2,20	1	30	2	20	-0.191444
W1,30,2,21	1	30	2	21	0.253996
W1,30,2,22	1	30	2	22	0.295464
W1,30,2,23	1	30	2	23	0.666764
W1,30,2,24	1	30	2	24	-0.194804
W1,30,2,25	1	30	2	25	0.087527
W1,31,2,1	1	31	2	1	0.54754
W1,31,2,2	1	31	2	2	-1.195976
W1,31,2,3	1	31	2	3	-0.250449

W1,31,2,4	1	31	2	4	0.861522
W1,31,2,5	1	31	2	5	-0.889746
W1,31,2,6	1	31	2	6	0.211526
W1,31,2,7	1	31	2	7	-0.330119
W1,31,2,8	1	31	2	8	-0.646105
W1,31,2,9	1	31	2	9	0.313866
W1,31,2,10	1	31	2	10	0.018819
W1,31,2,11	1	31	2	11	-0.876739
W1,31,2,12	1	31	2	12	0.96806
W1,31,2,13	1	31	2	13	-0.47507
W1,31,2,14	1	31	2	14	-0.147218
W1,31,2,15	1	31	2	15	1.010046
W1,31,2,16	1	31	2	16	0.838806
W1,31,2,17	1	31	2	17	-0.542637
W1,31,2,18	1	31	2	18	0.227461
W1,31,2,19	1	31	2	19	0.828909
W1,31,2,20	1	31	2	20	0.418608
W1,31,2,21	1	31	2	21	0.920836
W1,31,2,22	1	31	2	22	0.498328
W1,31,2,23	1	31	2	23	-0.591611
W1,31,2,24	1	31	2	24	0.587335
W1,31,2,25	1	31	2	25	0.662088
W1,32,2,1	1	32	2	1	0.738003
W1,32,2,2	1	32	2	2	-0.779848
W1,32,2,3	1	32	2	3	-0.790065
W1,32,2,4	1	32	2	4	-0.09407
W1,32,2,5	1	32	2	5	0.657448
W1,32,2,6	1	32	2	6	0.989501
W1,32,2,7	1	32	2	7	0.423888
W1,32,2,8	1	32	2	8	0.633146
W1,32,2,9	1	32	2	9	0.892399
W1,32,2,10	1	32	2	10	-0.498765
W1,32,2,11	1	32	2	11	-0.556601
W1,32,2,12	1	32	2	12	0.252951
W1,32,2,13	1	32	2	13	-0.194638
W1,32,2,14	1	32	2	14	-0.623345
W1,32,2,15	1	32	2	15	0.493179
W1,32,2,16	1	32	2	16	0.286619
W1,32,2,17	1	32	2	17	0.227163
W1,32,2,18	1	32	2	18	-0.186984
W1,32,2,19	1	32	2	19	-0.682265
W1,32,2,20	1	32	2	20	-0.244694
W1,32,2,21	1	32	2	21	0.606859
W1,32,2,22	1	32	2	22	0.887946

W1,32,2,23	1	32	2	23	0.953644
W1,32,2,24	1	32	2	24	-0.721569
W1,32,2,25	1	32	2	25	-0.467471
W1,33,2,1	1	33	2	1	0.759787
W1,33,2,2	1	33	2	2	0.598158
W1,33,2,3	1	33	2	3	0.38592
W1,33,2,4	1	33	2	4	-0.190931
W1,33,2,5	1	33	2	5	0.581951
W1,33,2,6	1	33	2	6	0.679333
W1,33,2,7	1	33	2	7	-0.461512
W1,33,2,8	1	33	2	8	0.560321
W1,33,2,9	1	33	2	9	0.883596
W1,33,2,10	1	33	2	10	0.442637
W1,33,2,11	1	33	2	11	-0.70041
W1,33,2,12	1	33	2	12	-0.349315
W1,33,2,13	1	33	2	13	-0.811778
W1,33,2,14	1	33	2	14	0.112995
W1,33,2,15	1	33	2	15	-0.165262
W1,33,2,16	1	33	2	16	0.253515
W1,33,2,17	1	33	2	17	-0.556826
W1,33,2,18	1	33	2	18	-0.828629
W1,33,2,19	1	33	2	19	-0.370166
W1,33,2,20	1	33	2	20	-0.705911
W1,33,2,21	1	33	2	21	-0.718518
W1,33,2,22	1	33	2	22	0.521994
W1,33,2,23	1	33	2	23	-0.533096
W1,33,2,24	1	33	2	24	-0.692774
W1,33,2,25	1	33	2	25	-0.012877
W1,34,2,1	1	34	2	1	0.205027
W1,34,2,2	1	34	2	2	-1.082775
W1,34,2,3	1	34	2	3	0.61138
W1,34,2,4	1	34	2	4	0.951099
W1,34,2,5	1	34	2	5	0.511176
W1,34,2,6	1	34	2	6	-0.025976
W1,34,2,7	1	34	2	7	-0.168134
W1,34,2,8	1	34	2	8	-0.111428
W1,34,2,9	1	34	2	9	0.059724
W1,34,2,10	1	34	2	10	-0.78634
W1,34,2,11	1	34	2	11	0.912132
W1,34,2,12	1	34	2	12	-0.23935
W1,34,2,13	1	34	2	13	0.664667
W1,34,2,14	1	34	2	14	0.783386
W1,34,2,15	1	34	2	15	-0.078281
W1,34,2,16	1	34	2	16	-0.663092

W1,34,2,17	1	34	2	17	0.554551
W1,34,2,18	1	34	2	18	1.133743
W1,34,2,19	1	34	2	19	0.611366
W1,34,2,20	1	34	2	20	0.535058
W1,34,2,21	1	34	2	21	-0.777396
W1,34,2,22	1	34	2	22	0.04874
W1,34,2,23	1	34	2	23	-0.658382
W1,34,2,24	1	34	2	24	-0.13629
W1,34,2,25	1	34	2	25	0.255944
W1,35,2,1	1	35	2	1	-0.792265
W1,35,2,2	1	35	2	2	-0.12885
W1,35,2,3	1	35	2	3	0.558709
W1,35,2,4	1	35	2	4	-0.111245
W1,35,2,5	1	35	2	5	0.206444
W1,35,2,6	1	35	2	6	0.076308
W1,35,2,7	1	35	2	7	0.236224
W1,35,2,8	1	35	2	8	-0.867355
W1,35,2,9	1	35	2	9	0.766891
W1,35,2,10	1	35	2	10	0.325784
W1,35,2,11	1	35	2	11	0.660667
W1,35,2,12	1	35	2	12	0.670066
W1,35,2,13	1	35	2	13	-0.02788
W1,35,2,14	1	35	2	14	-0.664482
W1,35,2,15	1	35	2	15	-0.205643
W1,35,2,16	1	35	2	16	0.379397
W1,35,2,17	1	35	2	17	0.036991
W1,35,2,18	1	35	2	18	0.120144
W1,35,2,19	1	35	2	19	0.568408
W1,35,2,20	1	35	2	20	-0.847209
W1,35,2,21	1	35	2	21	0.500332
W1,35,2,22	1	35	2	22	0.641124
W1,35,2,23	1	35	2	23	-0.049291
W1,35,2,24	1	35	2	24	0.277638
W1,35,2,25	1	35	2	25	0.087297
W1,36,2,1	1	36	2	1	0.622384
W1,36,2,2	1	36	2	2	0.858668
W1,36,2,3	1	36	2	3	0.90304
W1,36,2,4	1	36	2	4	-0.444543
W1,36,2,5	1	36	2	5	-0.888509
W1,36,2,6	1	36	2	6	-0.384297
W1,36,2,7	1	36	2	7	0.148826
W1,36,2,8	1	36	2	8	1.12029
W1,36,2,9	1	36	2	9	-0.042541
W1,36,2,10	1	36	2	10	0.860057

W1,36,2,11	1	36	2	11	0.778784
W1,36,2,12	1	36	2	12	-0.031159
W1,36,2,13	1	36	2	13	-0.970327
W1,36,2,14	1	36	2	14	-0.903933
W1,36,2,15	1	36	2	15	0.414274
W1,36,2,16	1	36	2	16	-0.507087
W1,36,2,17	1	36	2	17	-0.405999
W1,36,2,18	1	36	2	18	-0.867647
W1,36,2,19	1	36	2	19	-0.360962
W1,36,2,20	1	36	2	20	0.243088
W1,36,2,21	1	36	2	21	0.540813
W1,36,2,22	1	36	2	22	0.259374
W1,36,2,23	1	36	2	23	0.548725
W1,36,2,24	1	36	2	24	-0.677765
W1,36,2,25	1	36	2	25	-0.284581
W1,37,2,1	1	37	2	1	-0.044033
W1,37,2,2	1	37	2	2	-1.194333
W1,37,2,3	1	37	2	3	0.807667
W1,37,2,4	1	37	2	4	0.622651
W1,37,2,5	1	37	2	5	0.026237
W1,37,2,6	1	37	2	6	0.416912
W1,37,2,7	1	37	2	7	-0.907401
W1,37,2,8	1	37	2	8	-0.168853
W1,37,2,9	1	37	2	9	0.090803
W1,37,2,10	1	37	2	10	-0.904271
W1,37,2,11	1	37	2	11	-0.976444
W1,37,2,12	1	37	2	12	1.065319
W1,37,2,13	1	37	2	13	-0.865499
W1,37,2,14	1	37	2	14	0.120946
W1,37,2,15	1	37	2	15	1.024241
W1,37,2,16	1	37	2	16	-0.938161
W1,37,2,17	1	37	2	17	0.449098
W1,37,2,18	1	37	2	18	-0.504815
W1,37,2,19	1	37	2	19	0.240064
W1,37,2,20	1	37	2	20	0.263321
W1,37,2,21	1	37	2	21	-0.199815
W1,37,2,22	1	37	2	22	0.520527
W1,37,2,23	1	37	2	23	0.363302
W1,37,2,24	1	37	2	24	-0.851915
W1,37,2,25	1	37	2	25	-0.163984
W1,38,2,1	1	38	2	1	0.264427
W1,38,2,2	1	38	2	2	0.216212
W1,38,2,3	1	38	2	3	0.881785
W1,38,2,4	1	38	2	4	0.824587

W1,38,2,5	1	38	2	5	-0.332085
W1,38,2,6	1	38	2	6	-0.35646
W1,38,2,7	1	38	2	7	0.132293
W1,38,2,8	1	38	2	8	0.533472
W1,38,2,9	1	38	2	9	-0.983052
W1,38,2,10	1	38	2	10	-0.938982
W1,38,2,11	1	38	2	11	-0.837587
W1,38,2,12	1	38	2	12	-0.583611
W1,38,2,13	1	38	2	13	-0.737125
W1,38,2,14	1	38	2	14	-0.361588
W1,38,2,15	1	38	2	15	0.0984
W1,38,2,16	1	38	2	16	-0.624106
W1,38,2,17	1	38	2	17	0.797189
W1,38,2,18	1	38	2	18	-0.098403
W1,38,2,19	1	38	2	19	-0.883299
W1,38,2,20	1	38	2	20	0.0633
W1,38,2,21	1	38	2	21	0.101625
W1,38,2,22	1	38	2	22	-0.715801
W1,38,2,23	1	38	2	23	-0.605931
W1,38,2,24	1	38	2	24	0.808595
W1,38,2,25	1	38	2	25	-0.712902
W1,39,2,1	1	39	2	1	-0.198154
W1,39,2,2	1	39	2	2	-0.792242
W1,39,2,3	1	39	2	3	-0.357989
W1,39,2,4	1	39	2	4	-0.177726
W1,39,2,5	1	39	2	5	0.119431
W1,39,2,6	1	39	2	6	0.948036
W1,39,2,7	1	39	2	7	-0.894199
W1,39,2,8	1	39	2	8	0.165992
W1,39,2,9	1	39	2	9	0.305993
W1,39,2,10	1	39	2	10	0.108023
W1,39,2,11	1	39	2	11	0.250316
W1,39,2,12	1	39	2	12	-0.468746
W1,39,2,13	1	39	2	13	-0.432845
W1,39,2,14	1	39	2	14	0.40848
W1,39,2,15	1	39	2	15	-0.530293
W1,39,2,16	1	39	2	16	-0.83396
W1,39,2,17	1	39	2	17	0.774627
W1,39,2,18	1	39	2	18	-0.377368
W1,39,2,19	1	39	2	19	-0.343997
W1,39,2,20	1	39	2	20	0.3796
W1,39,2,21	1	39	2	21	-0.053386
W1,39,2,22	1	39	2	22	0.349463
W1,39,2,23	1	39	2	23	-0.073093

W1,39,2,24	1	39	2	24	-0.263137
W1,39,2,25	1	39	2	25	-0.363494
W1,40,2,1	1	40	2	1	0.495252
W1,40,2,2	1	40	2	2	-0.807881
W1,40,2,3	1	40	2	3	0.393367
W1,40,2,4	1	40	2	4	0.006344
W1,40,2,5	1	40	2	5	-0.691327
W1,40,2,6	1	40	2	6	-0.298823
W1,40,2,7	1	40	2	7	0.854377
W1,40,2,8	1	40	2	8	0.439731
W1,40,2,9	1	40	2	9	-0.466694
W1,40,2,10	1	40	2	10	0.023151
W1,40,2,11	1	40	2	11	0.111486
W1,40,2,12	1	40	2	12	0.088067
W1,40,2,13	1	40	2	13	0.290278
W1,40,2,14	1	40	2	14	-0.094429
W1,40,2,15	1	40	2	15	0.53325
W1,40,2,16	1	40	2	16	0.657723
W1,40,2,17	1	40	2	17	-0.389115
W1,40,2,18	1	40	2	18	0.81227
W1,40,2,19	1	40	2	19	-0.309079
W1,40,2,20	1	40	2	20	-0.229436
W1,40,2,21	1	40	2	21	0.871288
W1,40,2,22	1	40	2	22	0.954166
W1,40,2,23	1	40	2	23	-0.019684
W1,40,2,24	1	40	2	24	0.185552
W1,40,2,25	1	40	2	25	-0.032927
W1,41,2,1	1	41	2	1	-0.45026
W1,41,2,2	1	41	2	2	0.475799
W1,41,2,3	1	41	2	3	-0.337925
W1,41,2,4	1	41	2	4	-0.358517
W1,41,2,5	1	41	2	5	0.912984
W1,41,2,6	1	41	2	6	0.603581
W1,41,2,7	1	41	2	7	0.8466
W1,41,2,8	1	41	2	8	0.164461
W1,41,2,9	1	41	2	9	0.668521
W1,41,2,10	1	41	2	10	-0.547778
W1,41,2,11	1	41	2	11	-0.737159
W1,41,2,12	1	41	2	12	-0.789346
W1,41,2,13	1	41	2	13	0.221869
W1,41,2,14	1	41	2	14	-0.147065
W1,41,2,15	1	41	2	15	0.973443
W1,41,2,16	1	41	2	16	0.256907
W1,41,2,17	1	41	2	17	-0.661339

W1,41,2,18	1	41	2	18	0.600088
W1,41,2,19	1	41	2	19	0.67756
W1,41,2,20	1	41	2	20	-0.481874
W1,41,2,21	1	41	2	21	0.261731
W1,41,2,22	1	41	2	22	0.769277
W1,41,2,23	1	41	2	23	0.56011
W1,41,2,24	1	41	2	24	0.003611
W1,41,2,25	1	41	2	25	-0.70117
W1,42,2,1	1	42	2	1	0.994959
W1,42,2,2	1	42	2	2	0.869881
W1,42,2,3	1	42	2	3	0.866298
W1,42,2,4	1	42	2	4	0.943062
W1,42,2,5	1	42	2	5	-0.23298
W1,42,2,6	1	42	2	6	-0.661046
W1,42,2,7	1	42	2	7	-0.788757
W1,42,2,8	1	42	2	8	-1.185201
W1,42,2,9	1	42	2	9	0.198345
W1,42,2,10	1	42	2	10	-0.946441
W1,42,2,11	1	42	2	11	0.361122
W1,42,2,12	1	42	2	12	1.024132
W1,42,2,13	1	42	2	13	-0.868105
W1,42,2,14	1	42	2	14	0.589639
W1,42,2,15	1	42	2	15	0.949498
W1,42,2,16	1	42	2	16	0.10439
W1,42,2,17	1	42	2	17	0.849446
W1,42,2,18	1	42	2	18	-0.823341
W1,42,2,19	1	42	2	19	-0.62979
W1,42,2,20	1	42	2	20	-0.15163
W1,42,2,21	1	42	2	21	-0.209852
W1,42,2,22	1	42	2	22	0.033238
W1,42,2,23	1	42	2	23	-0.088307
W1,42,2,24	1	42	2	24	-0.827435
W1,42,2,25	1	42	2	25	-0.286656
W1,43,2,1	1	43	2	1	-0.347721
W1,43,2,2	1	43	2	2	0.079498
W1,43,2,3	1	43	2	3	0.655576
W1,43,2,4	1	43	2	4	-0.47924
W1,43,2,5	1	43	2	5	-0.274689
W1,43,2,6	1	43	2	6	-0.550305
W1,43,2,7	1	43	2	7	0.841224
W1,43,2,8	1	43	2	8	-0.23278
W1,43,2,9	1	43	2	9	-0.701428
W1,43,2,10	1	43	2	10	-0.61462
W1,43,2,11	1	43	2	11	-0.091674

W1,43,2,12	1	43	2	12	0.682058
W1,43,2,13	1	43	2	13	0.095861
W1,43,2,14	1	43	2	14	-0.783983
W1,43,2,15	1	43	2	15	-0.705364
W1,43,2,16	1	43	2	16	-0.938086
W1,43,2,17	1	43	2	17	0.21008
W1,43,2,18	1	43	2	18	-0.091343
W1,43,2,19	1	43	2	19	0.687658
W1,43,2,20	1	43	2	20	-0.258904
W1,43,2,21	1	43	2	21	-0.216742
W1,43,2,22	1	43	2	22	-0.835108
W1,43,2,23	1	43	2	23	0.208498
W1,43,2,24	1	43	2	24	-0.419839
W1,43,2,25	1	43	2	25	0.151577
W1,44,2,1	1	44	2	1	1.053512
W1,44,2,2	1	44	2	2	0.625365
W1,44,2,3	1	44	2	3	0.498865
W1,44,2,4	1	44	2	4	0.813166
W1,44,2,5	1	44	2	5	0.887083
W1,44,2,6	1	44	2	6	0.264879
W1,44,2,7	1	44	2	7	-0.600619
W1,44,2,8	1	44	2	8	-0.566712
W1,44,2,9	1	44	2	9	0.352219
W1,44,2,10	1	44	2	10	0.767512
W1,44,2,11	1	44	2	11	0.233741
W1,44,2,12	1	44	2	12	0.416263
W1,44,2,13	1	44	2	13	0.602762
W1,44,2,14	1	44	2	14	-0.967415
W1,44,2,15	1	44	2	15	-0.236234
W1,44,2,16	1	44	2	16	0.107347
W1,44,2,17	1	44	2	17	-0.094023
W1,44,2,18	1	44	2	18	-0.829215
W1,44,2,19	1	44	2	19	0.853087
W1,44,2,20	1	44	2	20	-0.30245
W1,44,2,21	1	44	2	21	-0.57645
W1,44,2,22	1	44	2	22	-0.597077
W1,44,2,23	1	44	2	23	0.349554
W1,44,2,24	1	44	2	24	-0.639545
W1,44,2,25	1	44	2	25	-0.550304
W1,45,2,1	1	45	2	1	0.614464
W1,45,2,2	1	45	2	2	-0.158714
W1,45,2,3	1	45	2	3	0.723334
W1,45,2,4	1	45	2	4	0.399396
W1,45,2,5	1	45	2	5	0.975205

W1,45,2,6	1	45	2	6	-0.244973
W1,45,2,7	1	45	2	7	0.061059
W1,45,2,8	1	45	2	8	0.417364
W1,45,2,9	1	45	2	9	0.769142
W1,45,2,10	1	45	2	10	-0.736677
W1,45,2,11	1	45	2	11	-0.327387
W1,45,2,12	1	45	2	12	-0.640291
W1,45,2,13	1	45	2	13	-0.742421
W1,45,2,14	1	45	2	14	-0.581596
W1,45,2,15	1	45	2	15	-0.258214
W1,45,2,16	1	45	2	16	0.497999
W1,45,2,17	1	45	2	17	0.736226
W1,45,2,18	1	45	2	18	-0.380912
W1,45,2,19	1	45	2	19	0.805652
W1,45,2,20	1	45	2	20	0.824376
W1,45,2,21	1	45	2	21	-0.799794
W1,45,2,22	1	45	2	22	0.053684
W1,45,2,23	1	45	2	23	-0.1119
W1,45,2,24	1	45	2	24	-0.343113
W1,45,2,25	1	45	2	25	0.495907
W1,46,2,1	1	46	2	1	0.291231
W1,46,2,2	1	46	2	2	0.284651
W1,46,2,3	1	46	2	3	-0.485133
W1,46,2,4	1	46	2	4	0.600359
W1,46,2,5	1	46	2	5	0.777017
W1,46,2,6	1	46	2	6	-0.006874
W1,46,2,7	1	46	2	7	0.413494
W1,46,2,8	1	46	2	8	0.459566
W1,46,2,9	1	46	2	9	0.23744
W1,46,2,10	1	46	2	10	-0.087528
W1,46,2,11	1	46	2	11	0.746233
W1,46,2,12	1	46	2	12	-0.270267
W1,46,2,13	1	46	2	13	-0.369075
W1,46,2,14	1	46	2	14	-0.423516
W1,46,2,15	1	46	2	15	-0.84264
W1,46,2,16	1	46	2	16	-0.856061
W1,46,2,17	1	46	2	17	0.060739
W1,46,2,18	1	46	2	18	0.744936
W1,46,2,19	1	46	2	19	0.482952
W1,46,2,20	1	46	2	20	-0.873339
W1,46,2,21	1	46	2	21	0.053983
W1,46,2,22	1	46	2	22	-0.935936
W1,46,2,23	1	46	2	23	-0.638101
W1,46,2,24	1	46	2	24	-0.347667

W1,46,2,25	1	46	2	25	0.262927
W2,1,3,1	2	1	3	1	0.875622
W2,1,3,2	2	1	3	2	-0.171594
W2,2,3,1	2	2	3	1	0.235204
W2,2,3,2	2	2	3	2	0.57559
W2,3,3,1	2	3	3	1	-0.124866
W2,3,3,2	2	3	3	2	0.400988
W2,4,3,1	2	4	3	1	-0.775218
W2,4,3,2	2	4	3	2	0.821545
W2,5,3,1	2	5	3	1	-0.756448
W2,5,3,2	2	5	3	2	0.271043
W2,6,3,1	2	6	3	1	0.773724
W2,6,3,2	2	6	3	2	0.205293
W2,7,3,1	2	7	3	1	-0.924577
W2,7,3,2	2	7	3	2	-0.274343
W2,8,3,1	2	8	3	1	-0.087627
W2,8,3,2	2	8	3	2	-0.499472
W2,9,3,1	2	9	3	1	0.182859
W2,9,3,2	2	9	3	2	-0.928836
W2,10,3,1	2	10	3	1	-0.486225
W2,10,3,2	2	10	3	2	-0.235479
W2,11,3,1	2	11	3	1	0.593734
W2,11,3,2	2	11	3	2	0.06804
W2,12,3,1	2	12	3	1	0.741467
W2,12,3,2	2	12	3	2	-0.094208
W2,13,3,1	2	13	3	1	-0.612982
W2,13,3,2	2	13	3	2	0.04242
W2,14,3,1	2	14	3	1	-0.673322
W2,14,3,2	2	14	3	2	-0.322056
W2,15,3,1	2	15	3	1	-0.581873
W2,15,3,2	2	15	3	2	-0.888271
W2,16,3,1	2	16	3	1	0.925555
W2,16,3,2	2	16	3	2	0.987182
W2,17,3,1	2	17	3	1	-0.122236
W2,17,3,2	2	17	3	2	0.44806
W2,18,3,1	2	18	3	1	0.448772
W2,18,3,2	2	18	3	2	0.603805
W2,19,3,1	2	19	3	1	-0.068927
W2,19,3,2	2	19	3	2	-0.086702
W2,20,3,1	2	20	3	1	0.054317
W2,20,3,2	2	20	3	2	0.096412
W2,21,3,1	2	21	3	1	-0.900105
W2,21,3,2	2	21	3	2	0.127248
W2,22,3,1	2	22	3	1	-0.522192

W2,22,3,2	2	22	3	2	-0.07903
W2,23,3,1	2	23	3	1	-0.21261
W2,23,3,2	2	23	3	2	0.248325
W2,24,3,1	2	24	3	1	-0.072561
W2,24,3,2	2	24	3	2	0.798046
W2,25,3,1	2	25	3	1	0.89125
W2,25,3,2	2	25	3	2	0.574762

VITA

MONICA DEZULUETA

1985	Founding president of the Delta Mu Omega Engineering Honor Society
1986	Engineer of the Year Award Association of Cuban Engineers (AIC Society)
1986	B.S., Electrical Engineering Florida International University
1987	Electronics Engineer NASA, Kennedy Space Center
1991	NASA Superior Performance Award NASA, Kennedy Space Center, FL
1992	Project Lead for Communications System NASA, Kennedy Space Center, FL
1993	Senior Software Development Engineer Coulter Corporation, Miami, FL
1994	M.S., Computer Engineering Florida International University
1994	M.S., Engineering Management University of Central Florida
1996	Senior Software Development Engineer II Coulter Corporation, Miami FL
1999	Consultant Microsoft Corporation, Fort Lauderdale, FL
2001	Microsoft US Vice Presidential Award Microsoft Corporation, Fort Lauderdale, FL
2002	E-Business Systems Engineer Microsoft Corporation, Fort Lauderdale, FL

PRESENTATIONS AND PUBLICATIONS

DeZulueta, M., Adjouadi, M., "Using Threat Modeling When Architecting a Healthcare System", Proceedings of the 8th World Multi-Conference on Systematics, Cybernetics and Informatics (Orlando, Florida, July 18-21, 2004).

DeZulueta, M., HIPAA Accelerator for BizTalk Server 2004 Overview Webcast, May 2004

DeZulueta, M., Developing Solutions for BizTalk Server 2004
FL and AL, April – July 2004

DeZulueta, M., Managing and Deploying BizTalk Server Solutions, July 2004

DeZulueta, M., Building a Custom Pipeline for BizTalk Server 2004
Microsoft Global Briefing, Atlanta, GA, July 2004

DeZulueta, M., Technical Webcasts on Commerce Server 2002 and Content Management Server 2002

DeZulueta, M., Orchestrating Web Services, Lockheed Mission Critical Enterprise Symposium Conference, Orlando, FL, October 2003

DeZulueta, M., Information Worker Infrastructure, Windows Server 2003 Launch, FL and AL, May 2003

CONTRIBUTIONS

Meier, J. D. and etal, "Building Secure Microsoft ASP.NET Applications". Redmond, Washington: MS Press, 2003.

"XML Data Islands, Updategrams, Stored Procedures, and More", MSDN Magazine, May 2002

CERTIFICATIONS

Certified Information Systems Security Professional

DISCLOSURE

DeZulueta, M., Adjouadi, M., and Ayala M., Methodology and Tool for Assessing Risks in Information Systems, Oct 2004.