Regis University

ePublications at Regis University

Regis University Student Publications (comprehensive collection)

Regis University Student Publications

Spring 2010

Information Security Among Small Organizations: a Survey

Jason Carter
Regis University

Follow this and additional works at: https://epublications.regis.edu/theses

 Part of the Computer Sciences Commons

Recommended Citation

Carter, Jason, "Information Security Among Small Organizations: a Survey" (2010). *Regis University Student Publications (comprehensive collection)*. 432.
https://epublications.regis.edu/theses/432

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

INFORMATION SECURITY AMONG SMALL ORGANIZATIONS: A SURVEY

A THESIS

SUBMITTED ON 14 OF APRIL, 2010

TO THE DEPARTMENT OF INFORMATION SYSTEMS

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

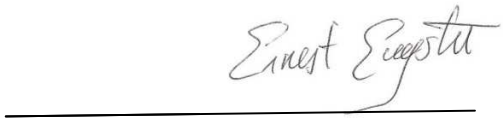
COMPUTER INFORMATION TECHNOLOGY

by

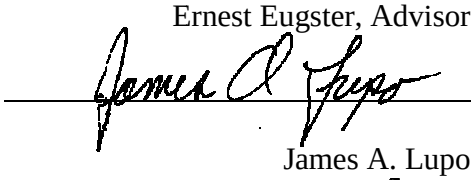


Jason Carter

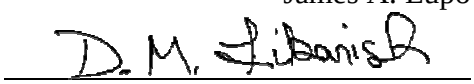
APPROVALS



Ernest Eugster, Advisor



James A. Lupo



Daniel M. Likarish

Abstract

Small businesses are at extreme risk from network based attacks. A lack of security budget for hardware such as firewalls, intrusion detection systems, proxy servers, and web 2.0 gateway filters, plus a lack of technical expertise in network security, put small businesses at higher risk than larger companies. This paper researches the current state of small business network security and the types of threats they are seeing. It also looks at the factors that determine when and why security is implemented or modified.

Keywords: Small Business, Network Security, Threats, Risks, Firewalls, Intrusion Detection Systems, Network Authentication, Small Business Security Survey

Acknowledgements

I would like to thank all of my instructors and advisors at Regis for helping me complete all of the steps needed to get to this final research paper. I could never have gotten this far without their dedication to their jobs and the students.

And more than anyone else, I would like to thank my beautiful wife Jill. She has stood by me for over 19 years and supported my education the entire time. I love you very much.

Table of Contents

Abstract ii
Acknowledgements iii
List of Figures vi
List of Tables vii
Chapter 1 – Introduction 1
Information Technology, Threats, and Small Business 1
Summary 6
Chapter 2 – Review of Literature and Research 7
What is Network Security? 7
Firewalls 9
Anti-virus and Anti-malware 9
Anti-spam 10
Intrusion Detection Systems 11
Security Policies 11
Summary 13
Chapter 3 - Methodology 14
Research Phases and Design 14
Summary 15
Chapter 4 – Data Analysis and Findings 17
Results 17
Staffing Conditions 17
Network Considerations 21
Threats 23
Safeguards 25
Policy Implementation 32
Summary 36
Chapter 5 – Discussion and Conclusion 37
Limitations 37
Implications for Practice and Research 38
References 43
Appendix A 48

List of Figures

Figure 4-1 Employee Number Percentages.....18
Figure 4-2 Employee Number Breakdown……...18
Figure 4-3 Overall IT Staff Levels……....19
Figure 4-4 Percentage of Companies Using Outsourced IT…….20
Figure 4-5 Percentages of Companies with Dedicated Connections……...…….21
Figure 4-6 Dedicated Connection Count Breakdown …….……..…...22
Figure 4-7 Internet Facing Services…….……..……22
Figure 4-8 Threats Seen in the Last 12 Months …….…..…….23
Figure 4-9 Threat Rankings…….……..…..……...24
Figure 4-10 Firewall Deployment…….....…..…….25
Figure 4-11 Intrusion Detection System Deployment …….……...…….26
Figure 4-12 Network Authentication Methods……...…..…….……27
Figure 4-13 Percentages of Small Businesses Enforcing Security Policies…….....…….28
Figure 4-14 Common Enforced Security Policies ……..…..…….29
Figure 4-15 Antivirus Implementations …….…..…….…….30
Figure 4-16 Types of Security Training Provided by Small Businesses ……..…….……...31
Figure 4-17 Penetration Testing……...…..…….32
Figure 4-18 Security Policy Implementation Factors …….…..……..…..…….33
Figure 4-19 New Security Implementations …….…..……..…..……34

List of Tables

Table 4-1 Full Time IT Staff Company Size Breakdown…….....19
Table 4-2 Outsourced IT Breakdown……20
Table 4-3 IDS Deployment Breakdown by Company Size ……..26
Table 4-4 Security Policy Breakdown……...……29
Table 4-5 Breakdown by Company Size of Training Provided……..…31

Chapter 1 – Introduction

One of the most significant challenges faced by small business owners today is securing their computer networks to protect the data that provides a competitive business advantage. Just like large businesses, small businesses are faced with threats including hackers, disgruntled employees, malware, and even contractors stealing trade secrets. But small businesses are especially vulnerable due to a lack of resources, both financial and in qualified, experienced personnel. This paper is an examination of network security at typical small businesses in the United States including a look at software, hardware, and security policies implemented. Random small businesses were asked a variety of network security questions anonymously. Surveyed businesses have provided information not only on the types of defenses implemented but also on the motivating factors behind security implementation or policy changes as well as the types of threats that small businesses have seen. As will been seen, these small businesses may be at greater risk to network based attacks then they realize.

Information Technology, Threats, and Small Business

Small businesses are a major engine in the American economy. The National Institute of Standards and Technology (NIST) estimates that small and medium businesses represent over 95 percent of all businesses in the United States (National Institute of Standards and Technology, 2009). In the U.S., over 29.6 million small businesses were registered in 2008 (Score.org, 2009). This represents just over half of the nation's private workforce and 40 percent of all high tech workers including computer workers, scientists, and engineers (Score, 2009).

What is the size of a small business? The U.S. Small Business Administration (SBA) defines a small business as having less than 500 employees, with a maximum annual revenue of

$7.0 million for most businesses (Small Business Administration, 2009). And the growth in the number of small businesses remains strong. Over 670,000 new small businesses will be opened this year alone although only half will survive the next five years (Score, 2009).

One of the ways small businesses can survive long term is through strategic utilization of information technology. Mobility and advanced networks can add new productivity capabilities to small businesses. For example, companies can take advantage of devices like smart phones to conduct business virtually anywhere. A 2010 survey by AT&T showed that nearly two-thirds (65 percent) of small businesses surveyed said that they could not survive – or it would be a major challenge to survive – without wireless technology. This is up dramatically from a similar 2007 survey in which only about four in ten (42 percent) of small businesses said they would have difficulty surviving with wireless technologies (AT&T, 2010). According to a market researcher, the small- and medium-sized businesses are projected to spend $18 billion globally on IT in 2010 (IDC.com, 2010).

Despite the business benefits to technology, technology can put businesses at risk to network based attacks. A 2009 security survey conducted by the Computer Security Institute (CSI) estimated the average loss due to a security incident in 2009 was over $234,000 (Computer Security Institute, 2009). The survey also found that one quarter of all responders felt that over 60 percent of their financial losses were due to non-malicious actions by insiders. And the consequences can be far reaching. A study by Computer Associates found that, “79 percent of consumers cite loss of trust and confidence, damage to reputation, and reduced customer satisfaction as consequences of major security and privacy breaches suffered,” by the businesses they work with (Computer Associates, 2008). A single security breach can mean the difference between a growing business and being out of business.

Businesses in the United States seem especially vulnerable to attack. In 2009, 57 percent of all attacks worldwide were against sites and businesses based in the United States with Europe a distant second at 23 percent (Breach, 2009). The number one reported attack in 2009 was website defacement, but that category included not only visually altering the appearance of a website, but also the introduction of malicious code.

There has also been a shift in the motives for attacks away from simply hacking websites and messaging systems to hacking for profit. One example involves the sophisticated ACH (automated clearinghouse) attack, which according to the FBI has already moved more than $100 million out of U.S. bank accounts (McMillan, 2009). This type of attack usually involves sending an email with embedded malicious code to a company's bookkeeper or financial officer designed to look like a software patch from Microsoft. Once the victim executes the code, a key logger is installed that tracks all of the keystrokes the user is making which usually include usernames and passwords for financial applications and websites. Once obtained, the hacker simply creates new payee accounts in the company's financial records and moves large sums of money overnight.

In addition to growing threats, increased network security is being prompted by expanded regulatory compliance. The Sarbanes-Oxley Act (also known as SOX) was implemented in 2002 as a control framework to prevent corporate scandals. Of the various provisions, Section 404 requires public companies to provide an effective system of internal control to protect the integrity of financial reporting data and the safeguarding of assets (Institute of Internal Auditors, 2008). But Section 404 is also the most expensive to implement. The cost of this compliance averaged $78,474 in 2008 per company (Evans-Correia, 2008). Companies that are required to comply with SOX need to expect higher operating costs associated with compliance in addition to the hardware, software, and manpower costs required keeping their data safe.

Clearly, large businesses are more likely to have the resources to meet the challenges of threats and compliance. Large companies spend millions of dollars annually to provide security and keep up with the latest network defense systems including firewalls, intrusion detection systems (IDS), and the manpower to maintain these network defenses. Indeed, studies have shown that large businesses generally did not cut back on security even during slow economic times. According to market researcher IDC, many organizations will defer discretionary projects, freeze hiring, and actively look for savings from virtualization, hosted services, and automated security management (Burke, Hudson, Kolodgy, Crotty, & Christiansen, 2009).

But, small businesses have a poor track record when it comes to security. One 2010 survey reported that 23 percent of small- and medium-sized businesses surveyed received either a flunking or "D" grade when it comes to IT effectiveness (Johnson, 2009). The same survey found that two-thirds of companies with 100 or few employees were falling behind when it comes to implementing accepted best practices for IT operations and management. Only 37 percent managed to maintain their IT operations and best practices. At the same time, the survey found that 43.5 percent were postponing, downsizing, or canceling IT projects.

The reasons are varied. Many smaller businesses do not see themselves as being a target for hackers. More than 30 percent of those polled by a National Cyber Security Alliance (NCSA) survey believed that the risk of being hit by lightning was greater than having computers being violated in an Internet attack (Brenner, 2004). But the SANS/Internet Storm Center found that the average time a "clean" unpatched and undefended system can be connected directly to the Internet before being attacked or scanned averaged 4 minutes (Internet Storm Center, 2010).

In addition to a false sense of security, small businesses do not have the money or manpower to invest in security, especially during hard economic times. According to a Yankee Group study, 40 percent of small businesses ranked computer security breaches as an important issue, but nearly half deferred security upgrades due to cost concerns. Many others waved off network security concerns claiming that the size of the company and its insignificance in the market would deter hackers from targeting their networks. Similarly, market researcher IDC found that the extent to which small and medium-sized businesses were adversely affected b y the current economic recession was greater than anticipated, projecting that SMB IT spending levels would not return to 2008 levels until 2011 (IDC, 2010).

The potential damage caused by a hack can be more serious to a small business than a large one because few computer systems often control most of the running the business. A single computer may be used to track inventory, handle all accounting, and also serve as a personal computer. Thus, a single infection such as a denial of service attack could bring down important parts of the business. A single threat affecting many small businesses can represent a threat to the Nation's economic stability.

The rising challenges of threats, budgets, and compliance that small businesses face has not escaped the United States government. The Federal government has provided many resources to small businesses in an attempt to counter the effects of network based threats. The U.S. Computer Emergency Readiness Team, for example, has regularly provided lists of threats and their associated transmission methods, the systems affected, and instructions for cleaning up and reporting a security breach. Another agency, the Small Business Administration, has organized workshops designed to help small businesses secure their networks at little or no cost (National Institute of Standards and Technology, 2009).

Summary

In this chapter, we have seen that security should provide for business enablement. But small businesses do not have the resources that large businesses devote to security. The key challenge will be to balance both cost and security concerns to an equal degree.

The next chapter explores IT security literature. Its purpose is to further examine the relationship between security and small business performance.

Chapter 2 – Review of Literature and Research

As the use of computers and networks has expanded, researchers and practitioners have shown increasing interest in the role of network security in protecting the confidentiality, integrity, and availability of information and its impact on organizations. Although both large and small organizations potentially face the same rising threats and regulations (Mathur, 2008), small businesses generally lack the technical expertise and the budget that larger companies have available for their defenses.

What is Network Security?

Stallings (2007) defined network security as "the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks" (Stallings, 2007). The strategic impact of network security is vast; a survey conducted by PricewaterhouseCoopers (PwC) of 4900 IT professionals across 30 countries found that poor network security resulted in a loss of 39,363 human years of productivity in 2008; costing an estimated $1.6 trillion worldwide (Final IT Solutions, Inc, 2008). Denial of Service (DoS) attacks cost Amazon.com over $600,000 during the ten hours the site was down in February, 2000 (Kessler, 2000). The U.S. government alone is expected to spend $30 billion on securing their network infrastructure between 2008 and 2015 (Gold, 2008). Large companies like Wal-Mart and Target use sophisticated network security technologies to limit Internet access to their internal networks, including their e-Commerce sites, to specific ports.

Is security a business enabler? The IT literature seemed to confirm that it is, focusing largely on different threats and safeguards. Identity management is increasingly required to

enable interactions and transactions on the Internet among people, enterprises, service providers, and government institutions (Ahn & Lam, 2005). Security architectures which are business-driven and which describes a structured inter-relationship between the technical and procedural solutions to support the long-term needs of the business of the organization are needed (Coviello, 2008). Coviello (2008) stated the businesses need to work security into their business models instead of creating models in spite of security. In any business, the long term goal is the success and growth of the business. Security has its place protecting data and minimizing risk but should not interfere with business initiatives when possible.

Security researchers have identified four concepts that are central to network security: threat, vulnerabilities, risk, and countermeasures. Risk is "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization" (Stoneburner, Goguen, & Feringa, 2002). Put simply, a threat is any action that can cause damage or allow unauthorized access. A vulnerability is a known bug or opening that can be used to cause damage or gain unauthorized access. A risk is the potential for someone to exploit that vulnerability. Countermeasures are designed to minimize risk by securing vulnerabilities and reducing the overall threat to the systems and data.

A number of researchers have examined the countermeasures to safeguard data. Cannata (2009), for example, focused on six components small businesses should focus on when deploying their defenses: firewalls, anti-virus software, anti-spam utilities or hardware, anti-malware software, intrusion detection systems (IDS), and security policies (Cannata, 2009). When properly deployed, these components provide "defense in depth" by layering several defenses each independent of the others.

Firewalls

One of the most common network defenses for both small and large companies is the firewall. Firewalls can be physical devices setup to control access between network segments (such as the internal business network and the Internet) or software applications running on individual systems. A hybrid approach of using both the physical device at the network perimeter(s) and software firewalls on the individual systems is generally the best approach. According to VeriSign, “65 percent of the interviewed companies reported attacks from inside their own company, and the remaining companies did not know the source” (Raggo, 2007). Traditional hardware firewalls only protected the network at the perimeter and could not block traffic already inside the network. Software or application firewalls installed on the local systems can help block unauthorized access coming from within the network. An example of where this type of firewall can be useful could be seen in 2003 when the SQL Slammer worm was released (Computer Emergency Readiness Team, 2003). This particular worm replicated itself using a well known SQL port (1434/UDP) to any unpatched SQL server and caused performance issues (including Denial of Service attacks) and could allow a hacker to take administrative permissions on any infected server. A software firewall configured to block SQL traffic from all but a select few systems that need to interact with it would have drastically reduced the number of infections.

Anti-virus and Anti-malware

Generally grouped together since the functionality is similar, these two can run on the local systems or run though an appliance known as a web filter or web gateway. When running on the local systems, anti-virus (AV) and anti-malware software will detect malicious code and delete or quarantine the files before they have a chance to infect the local systems and replicate. When running on an appliance, the gateway will intercept and inspect each file before allowing

them to continue to the end node. Any malicious code will be deleted at the appliance. AV and anti-malware software is common at the local system but gaining popularity at the gateway layer. The most common method for identifying malicious code is by definitions updated regularly by the AV software. As new threats emerge, AV software manufacturers identify the threats and create definitions that are downloaded by the local systems. Once the definitions are known, the local system can identify any file matching that description and remove it. Some AV versions can also identify malicious code by tracking what the files are doing or attempting to execute on the local system. Best practice for AV or anti-malware is to use a centralized server instance to update the definitions and create alerts when threats are found on the local systems. This allows for centralized management and reporting. In general, the AV definitions should be updated a couple of times a week (MarketersProtection.com, 2010) or whenever a particularly destructive or virulent virus is reported. Administrators can receive regular updates on new threats by subscribing to the alerts list through the U.S. Computer Emergency Readiness Team.

Anti-spam

One of the most common threats is unrequested emails that could contain links to harmful sites. These unsolicited emails are referred to as spam and while most do not cause as much destruction as malware, the sheer numbers can create a real threat. Spam is often the method of transport of viruses, spyware, Trojans, and phishing schemes aimed at gaining unauthorized access to computer accounts (Yeung, 2009). Anti-spam software installed on local systems and linked to an email application like Microsoft's Outlook can be effective in reducing the amount of spam received but this can be cumbersome to maintain for a large number of systems. Other options include installing a spam filter that intercepts all inbound and outbound messages if the small business hosts their own mail server, contracting with the local Internet service provider to

filter mail servers, or using a third party tool to filter all messages before they are uploaded to the mail server.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) pick up where the firewalls leave off. They are designed to inspect packets either at the host or traveling between networks for well known patterns (Rodriguez, 2004) and report and/or prevent the connection. An IDS can prevent attacks that may be allowed through a firewall because they operate a level that firewalls do not protect against. IDS systems can be host based or appliances that protect the network perimeter. IDS systems are still not as popular as firewalls for small businesses but are being bundled with other hardware and software applications and becoming more common (Kizza, 2005).

Security Policies

Security policies are one of the best ways to increase security with little or no incremental cost. A security policy is a general statement of the business rules that define the goals and purposes of security within an organization (HP, 2010). Security policies are designed to force users to work more securely without added software or hardware. Security policies can be assigned to every system in the network or applied to individual systems.

One common small business security tool is Microsoft's Active Directory. Active Directory (AD) is available with all Windows Server editions including Small Business Edition. AD allows businesses to enforce common security policy aspects such as password length and complexity, account lockout time, password reset frequency, Internet proxy settings, login times, executable permissions, and access logging. While this can be set locally, centralized management and automatic configuration ensures that all systems will be configured to follow the same policy.

One of the most important policies that can be set is the security updates. For example, whenever vulnerabilities are discovered in the Windows operating system or other Microsoft applications, Microsoft develops patches to prevent exploits of the newly discovered vulnerability. For these patches to be effective, they need to be installed in a timely fashion. Many times a patch will exist for months before hackers have developed exploits that can be used to attack unpatched systems. Keeping systems up to date can prevent problems before they happen.

Another important aspect of a security policy should be user training. All of the network defenses in the world will not help if users ignore updates, visit questionable sites, and click on unsolicited links. Users must be made aware of the dangers that exist and how hackers and malicious code get into the systems. Small businesses have good reason to train their employees. In 2008, the Identity Theft Resource Center (ITRC) reported that data breaches had increased 47 percent compared to 2007. Of those, 35.2 percent were due to human error (Haber, 2009). This averaged to about $6.6 million per incident per company compared to $6.43 million in 2007 and $4.7 million in 2006 (Haber, 2009).

No security policy, network defenses, or security software will make a network 100 percent secure. Short of disconnecting the systems from any outside access, powering the system down, and sending it to a watery grave at the bottom of the ocean, systems will remain vulnerable to some form of attack. Implementing network defenses and security policies can only reduce the risk exposure a company faces. In many cases, simple security policies and hardware can be enough to discourage an attack before it ever starts.

Summary

This chapter took a look at computer network security and best practices for implementing defenses. The differences between threats, vulnerabilities, risks, and countermeasures were explained and a business case was made for protecting a company's data. Small businesses have proven to be especially vulnerable to network attacks due in part to a lack of user training, low security budgets, and a lack of technical expertise among small business staff when in it comes to network security. Small businesses can reduce their risk by implementing security devices such as firewalls and intrusion detection systems, security software such as anti-virus, anti-spam, and anti-spyware, and security policies that limit Internet access, force strong passwords, and track user activity within the network.

In the next chapter, we will describe a methodology to determine what small businesses are doing to protect themselves.

Chapter 3 - Methodology

The purpose of this research is to examine the current state of small business network security and compare those findings to industry best practices. As we saw in Chapter 2, small businesses often lack the technical expertise and budgets to protect their networks and data to the same degree as large companies. As a result, small businesses are often at a higher risk from unauthorized access (hackers) and malicious code such as viruses, worms, Trojans, and spyware.

Research Phases and Design

To get an understanding of the current state of small business network security, research proceeded in three phases. In the first phase, a survey questionnaire was prepared. Six basic questions were examined. First, what challenges are facing small businesses in network security? Next, what is the current state of the network security in small businesses? What specific solutions are typically used? Is outsourcing used? What costs are involved? And finally, what expertise is required for these solutions to be successful?

These questions were posted in a survey placed on the Survey Monkey website. The survey had three purposes. First, to determine the current level of network security a typical small business had deployed. Second, the survey was used to get an idea of what threats small businesses are protecting themselves against or which threats have already been realized. Finally, the survey was used to get an understanding of what factors drive small business decisions when it comes to deploying network security

In the second phase, a list of small business owners was assembled using email addresses provided by the United States Department of Veteran Affairs. The businesses were chosen at random from the small businesses registered with the Veteran's Affairs list. Emails containing a link to the Survey Monkey questionnaire were emailed to approximately 4,000 businesses of all

sizes. Potential responders were asked to respond only if their businesses had less than 500 employees. In an effort to prevent any single business from responding more than one time, the survey would only accept a single response from any one IP address. Any attempt to submit a second survey would result in an error message and any results from subsequent attempts discarded. Due to the sensitive nature of the questions being asked, responses were kept completely anonymous and, aside from the logged source IP address, responses could not be tracked back to the source companies for verification. While checking the companies responding for size and revenue qualifications would help ensure that only small businesses were responding, keeping the responses anonymous help ensure that answers were honest and security was not artificially inflated.

The businesses were diverse in industry, size, and location but based entirely in the United States.

In the third phase, using an abridged version of the original questionnaire, an onsite interview was conducted with the Director of IT operations for an IT outsourcing company working with many small businesses in the Denver metro area. Questions posed included topics such as the trends seen in small business security implementation, the threats seen at the various offices, what was missing in small business security systems, the factors in determining which defenses or policies are implemented, and the priority small businesses placed on securing their networks. The purpose of this survey was to compare the perspectives of a service provider to those of business owners relative to network security and business challenges.

Summary

After a review of existing literature, survey questions were prepared to determine the current level of network security for a typical small business. The survey also included sections

on the threats that small businesses have faced and the factors that influence how and when security initiatives are implemented. These questions were then placed on the Survey Monkey website. Emails were sent to small business owners in diverse industries and geographic locations at random. An onsite interview was also conducted with a security service provider to provide insight on how security providers and business owners approach security and business objectives.

The next chapter will provide the results of the survey including pie and bar charts showing the actual number of responses from the small businesses as well as the overall percentages.

Chapter 4 – Data Analysis and Findings

This chapter presents the results of a survey of small business managers who are concerned with network security and business performance and costs. The relationship between staffing, networking considerations, threats, and safeguards as well as policy implementation are examined. The results indicate that small businesses know that their networks are at risk and have a good understanding the types of threats that are circulating the Internet and their own networks at the moment. Most of the businesses have been attacked at some point recently despite having some kind of defense or defenses in place. Many have security policies in place but few actually conduct testing to see if the policies and other defenses are protecting their networks as designed. Few provide any structured or organized security training for their employees relying only on casual security conversations that may vary from employee to employee. New security measures are generally implemented based on budget concerns and perceived threats.

Results

Of the 4,010 emails send using the Veterans Affairs Small Business Resource email list, 54 responses were gathered. Responses were not required on all the questions and some questions have multiple answers. The emails were sent between February 12-22, 2010 and responses gathered until February 28, 2010.

Staffing Conditions

As can be seen in Figures 4-1 and 4-2, most of the responding businesses had ten or fewer employees. These “ultra” small businesses did not have any full time IT staff employed and instead relied on self taught employees functioning as the onsite IT technician or outsourced

help. Smaller businesses like these did not have large security budgets, but were also less likely to house any public facing services like web pages or Email servers.

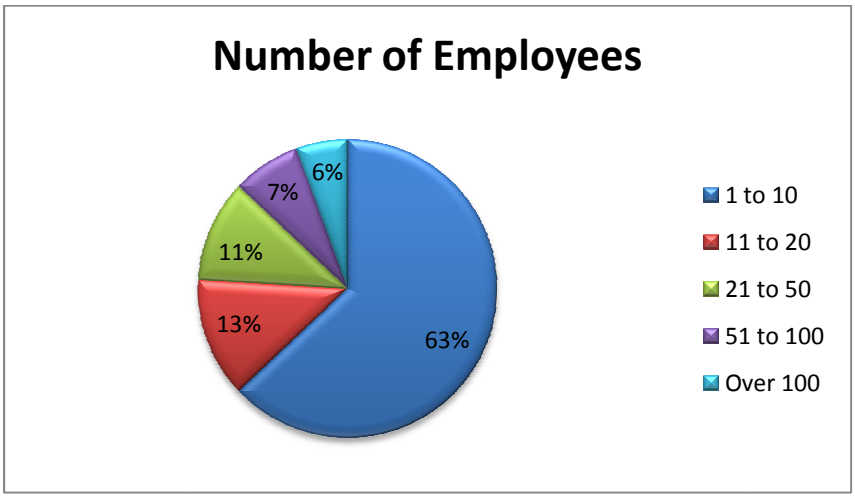


Figure 4-1 Employee Number Percentages

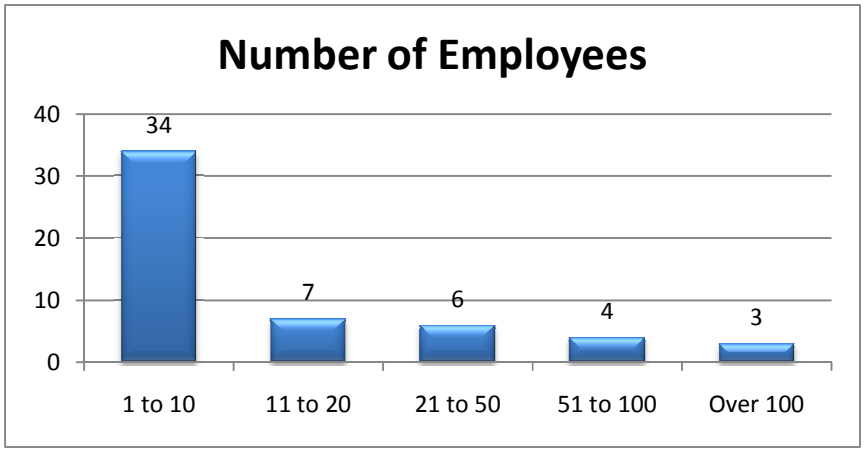


Figure 4-2 Employee Number Breakdown

Figure 4-3 confirms that the majority of responding companies do not employ a single full time IT professional in their offices. Businesses without full time staff have to rely on either outsourced IT staffing, which can be expensive when used for ten or more hours per week, or employees with multiple responsibilities to handle any security incident or monitor the network.

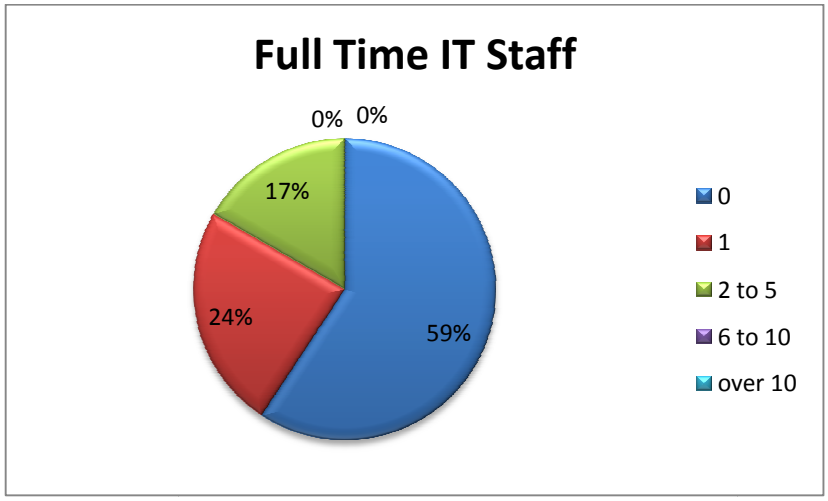


Figure 4-3 Overall IT Staff Levels

Table 4-1 shows the breakdown of full time IT employees by overall company size for the surveyed small businesses.

Table 4-1 Full Time IT Staff Company Size Breakdown

Company Size	**0**	**1**	**2 to 5**	**6 to 10**	**over 10**
1 to 10	23	5	6	0	0
11 to 20	3	3	1	0	0
21 to 50	3	2	1	0	0
51 to 100	2	2	0	0	0
over 100	1	1	1	0	0
Totals	**32**	**13**	**9**	**0**	**0**

As seen in Figure 4-4, only 9 percent of responding small businesses outsourced all of their IT and security needs. Most respondents handled some or all of their security and other IT needs themselves. Table 4-2 shows the breakdown of outsourced IT utilization by overall company size. It appears that the smaller the overall size of the company, the more likely that IT and security needs will be handled exclusively by outsourced IT companies. Of the businesses with ten or less employees, 11.7 percent outsourced all of their IT needs versus only 4.3 percent of the larger companies.

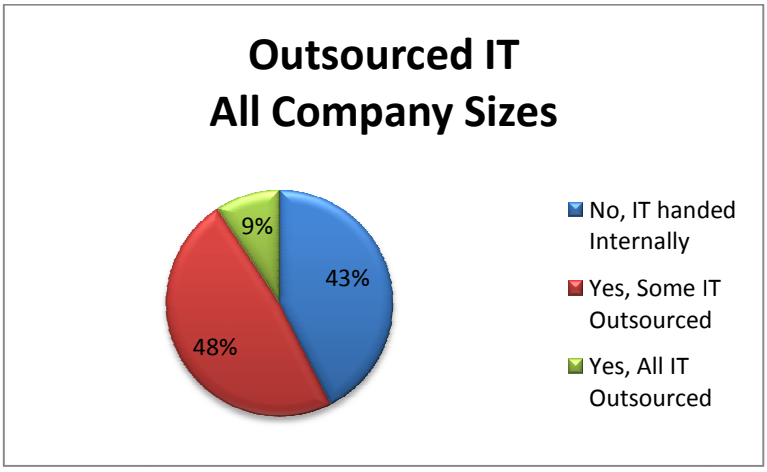


Figure 4-4 Percentage of Companies Using Outsourced IT

Table 4-2 Outsourced IT Breakdown

Company Size	No, IT handed Internally	Yes, Some IT Outsourced	Yes, All IT Outsourced
1 to 10	19	11	4
11 to 20	1	5	1
21 to 50	2	4	0
51 to 100	0	4	0
over 100	1	2	0
Totals	23	26	5

Looking at the percentage of IT handled in house versus the amount outsourced is important when determining the current level of security in these small businesses because employees that handle network security part time will often lack technical expertise on network setup and security best practices. This can result in a network that is business friendly but unsecure. Basic setup procedures can often be found after a few minutes browsing the Internet, but a lack of understanding of the underlying principles of network security can put a business at risk from threats resulting from a poorly configured firewall or website. Many of these unsecured sites may become vessels for malicious code placed inside the html code unknowingly. With

little or no monitoring, hackers can use poorly secured sites to transmit malicious code for years without the host ever knowing they have been hacked.

Network Considerations

Special consideration must be given whenever a company maintains dedicated connections to other locations or companies. Security must be implemented at all access points into the network. Dedicated connections have traditionally been associated with larger companies due to the cost and complexity of maintaining these dedicated circuits. Recently though, VPNs and dedicated circuits have been offered by ISPs as leased services making dedicated lines available to any size business. As Figure 4-5 shows, roughly one quarter of the businesses surveyed utilize dedicated circuits to other businesses or locations.

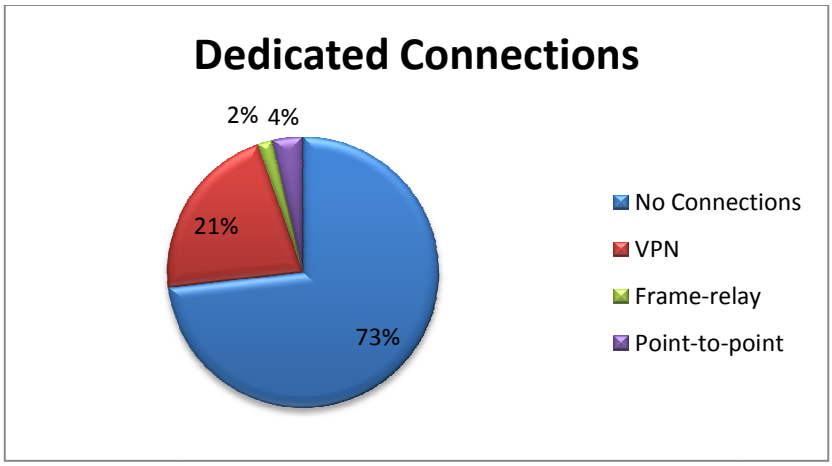


Figure 4-5 Percentages of Companies with Dedicated Connections

This represents risk to the small business. If these dedicated circuits are not protected by properly configured firewalls, any infection or attack in any of the connected networks can affect the local network as well. As such, companies with dedicated circuits must not only audit their own security, but must also ensure that remote offices and companies have adequate defenses deployed as well. Figure 4-6 shows the actual breakdown of reported dedicated connections.

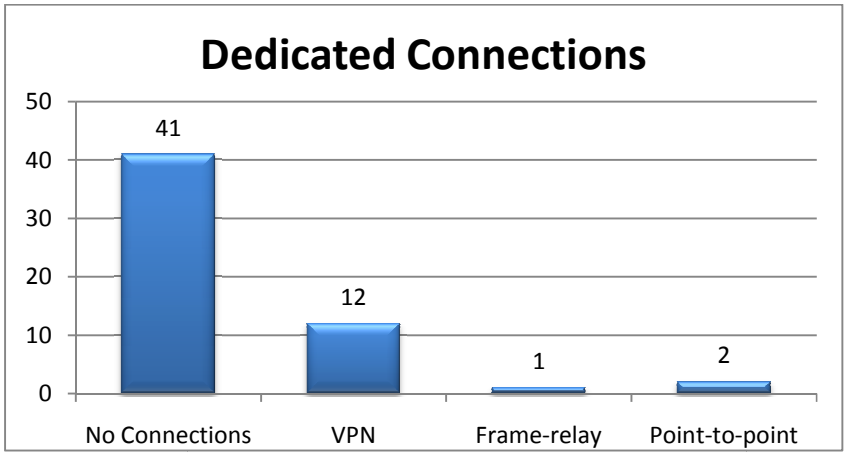


Figure 4-6 Dedicated Connection Count Breakdown

In addition to dedicated connections, many small businesses host Internet facing services such as Email servers, employee VPNs, and websites. These services require access from the Internet over specific ports and need to be carefully configured to prevent hackers from using these servers to conduct attacks (or to attack the services directly.) Figure 4-7 shows the types of Internet facing services that the surveyed small businesses are hosting within their networks.

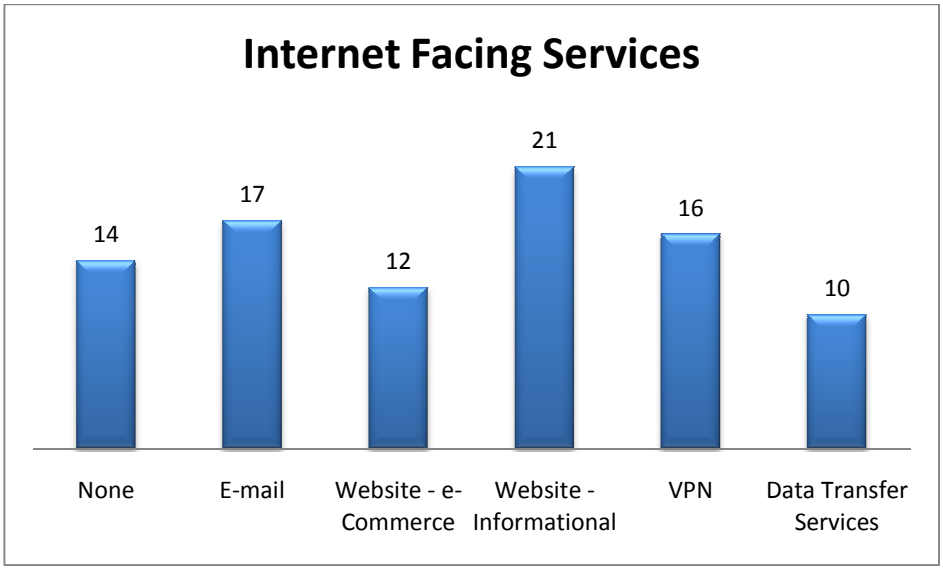


Figure 4-7 Internet Facing Services

Slight configuration errors in application setup or missing operating system patches can put each server hosting public facing services at risk. Exposed servers can not only be altered or damaged; they can also be used as launching points for attacks against other internal systems.

Threats

Small businesses are likely at greater risk than large businesses when it comes to network due to budget and manpower limitations, but also in part to the fact that so many critical business functions may be handled on one or relatively few machines. A single infection can render several business critical functions useless. Figure 4-8 shows the threats that have been seen by the small businesses surveyed in the last 12 months.

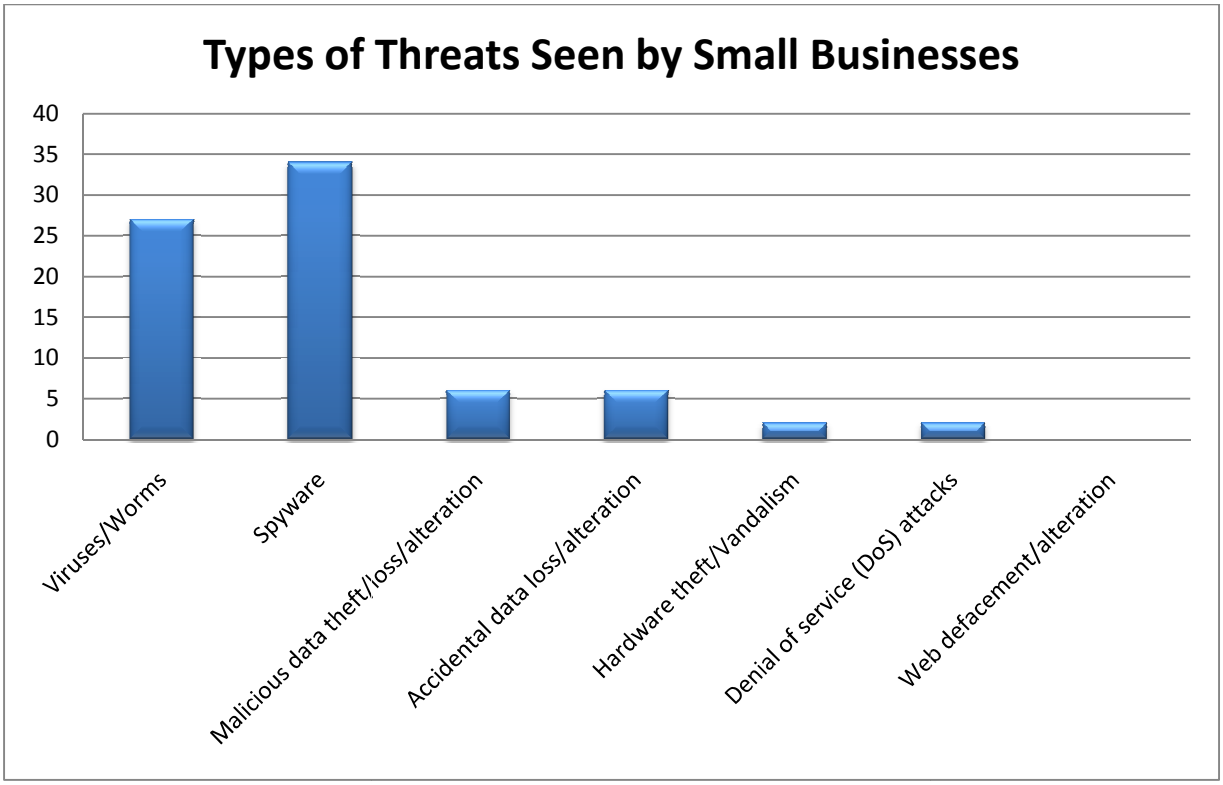


Figure 4-8 Threats Seen in the Last 12 Months

Of the threats shown in Figure 4-8, spyware and virus represent the majority of attacks, but malicious data loss or theft and Denial of Service (DoS) attacks are also seen even in the

relatively small sample. These results do not take into account the possible number of small businesses that have been attacked without realizing it.

Figure 4-9 shows the types of threats that small businesses are trying to protect against.

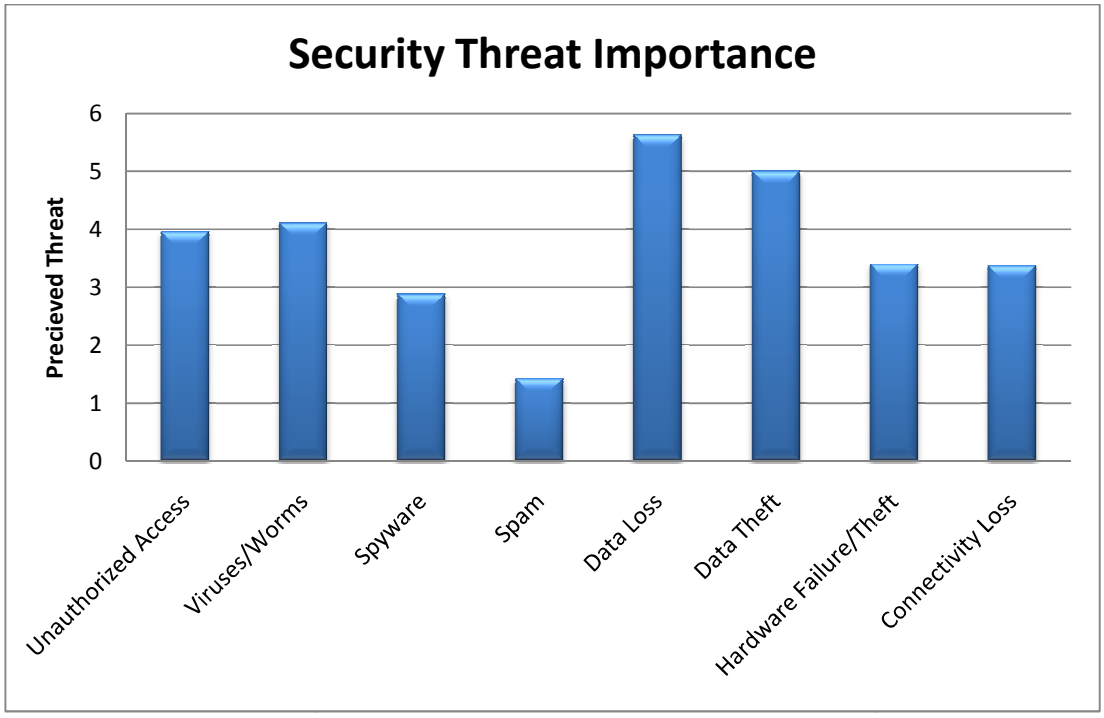


Figure 4-9 Threat Rankings

Ranking from one to eight (with one being the least important and eight being the most important), businesses ranked data loss and data theft as the worst possible outcome from an attack. This would be expected as data loss can put a company out of business quickly. Viruses and worms came in next based probably on the sheer likelihood of becoming infected. Spyware and spam rounded out the bottom as bothersome but apparently deemed relatively harmless in the eyes of the surveyed small business owners.

During the research, the researcher had the opportunity to interview the Directory of IT Operations for Spatial Business, a IT consulting firm working with Denver area small and medium business specializing in network configuration and security. When asked which threats

his business had seen when working with other small businesses, he said, “I have seen a lot of viruses and spyware. Most of the small businesses do not use proxy servers so their outbound connections are pretty wide open. It is not uncommon to get hit with the latest versions of ‘Antivirus’ malware since there are no controls to prevent this. Even the companies with fairly good controls get hit with this one when laptop users use their systems outside the protected network perimeter. Accidental deletion of data is pretty common as well. As a consultant, one of the first things I recommend implemented is a good backup scheme. Malware can be a real pain, but data loss can bring down an entire company.” His experience with network threats seems to echo those of the surveyed small businesses.

Safeguards

Safeguards are countermeasures deployed to prevent attacks from occurring. These are deployed in businesses of all sizes and should be carefully configured and monitored. As shown in Figure 4-10, most small businesses recognize the need to protect their network perimeters with some kind of dedicated firewall.

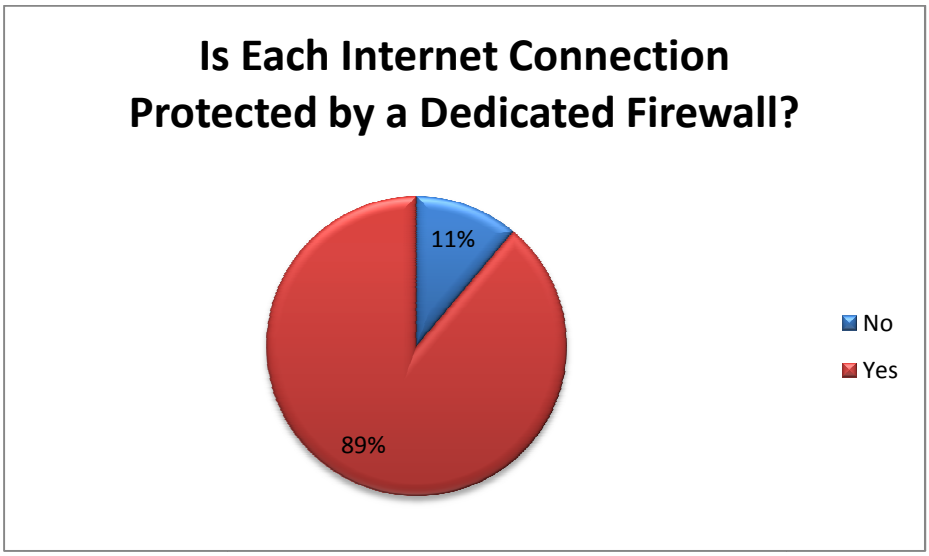


Figure 4-10 Firewall Deployment

Figure 4-11 shows the deployment of Intrusion Detection Systems appears to be growing. While not as common as a firewall, IDS systems are deployed at the majority of the small businesses surveyed (59 percent have some form of IDS deployed.) Table 4-3 shows the breakdown of IDS deployments based on overall company size.

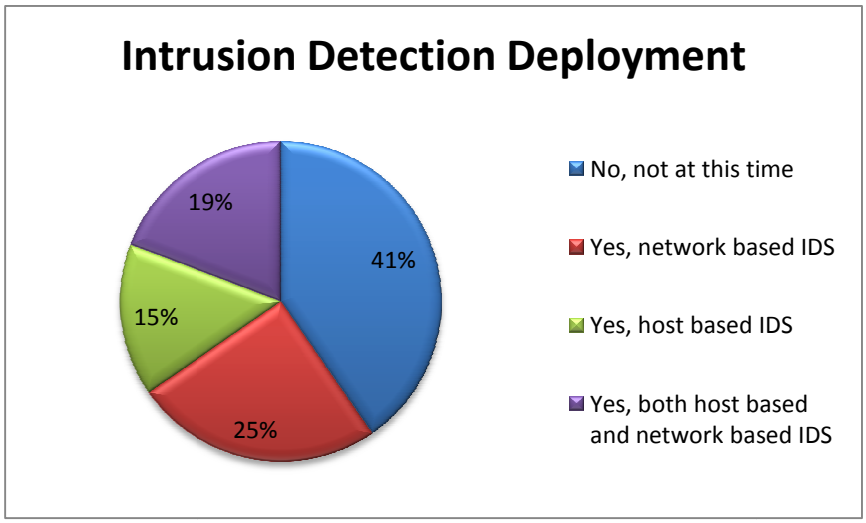


Figure 4-11 Intrusion Detection System Deployment

Table 4-3 IDS Deployment Breakdown by Company Size

Company Size	No, not at this time	Yes, network based IDS	Yes, host based IDS	Yes, both host based and network based IDS
1 to 10	13	8	4	7
11 to 20	2	1	2	2
21 to 50	3	1	1	1
51 to 100	2	1	1	0
over 100	1	2	0	0
Totals	**21**	**13**	**8**	**10**

As can be seen in Table 4-3, company size does not appear to be a factor in determining the likelihood of IDS deployment among these small businesses. For companies sized one to ten employees, 59 percent of the companies deployed some kind of IDS (network based, host based, or a hybrid of the two) which is directly in line with the overall deployment rate of 59 percent.

Figure 4-12 shows the percentage of companies using centralized network authentication. Centralized authentication allows companies to control access to resources in a single location and is much more secure than peer-to-peer authentication. Peer-to-peer authentication requires user credentials to be setup on each resource identically (and changed manually if required) and is not considered very secure.

The interview with the Directory of IT Operations for Spatial Business may reveal part of why IDS and other safeguard implementations were so high. When asked about trends seen in small business security implementation, he responded, “The biggest trend I have seen is the ISP (Internet Service Provider) offering several security aspects either built into the equipment or offered as a purchased service. Small business DSL or cable modems are coming with more advanced features such as stateful firewalls, IDS, and wireless access points with enterprise level encryption. Most ISPs also offer static IP addresses allowing the small business to host more services on site rather than paying the ISP to host the services. ISPs are also offering spam filtering and malware detection as a purchased service.” With services offered as part of a business package with little to no user setup or monitoring needed, businesses seem to be taking advantage of these services.

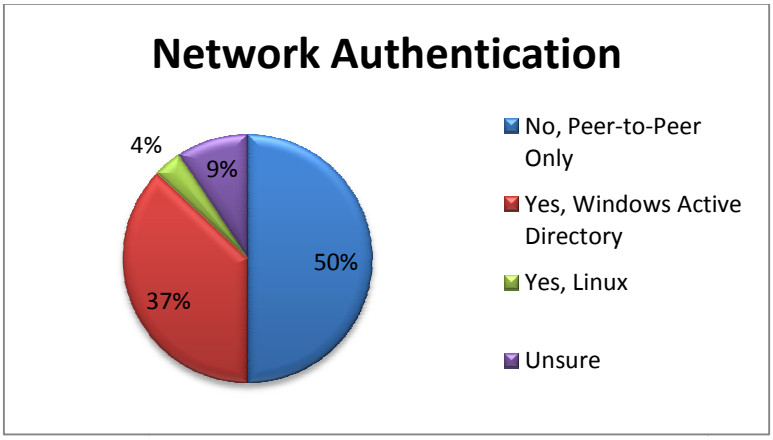


Figure 4-12 Network Authentication Methods

For businesses of all sizes, network authentication using usernames and passwords remains the most common form of security implemented and in many cases, the only form of security. Of the companies surveyed, only 37 percent use Windows Active Directory to centrally manage the user accounts. The remaining 63 percent are using peer-to-peer authentication.

When accounts are managed centrally, security can be enforced using security policies pushed for every user and/or computer in the network. Figure 4-13 shows the percentage of small businesses surveyed that enforce some kind of security policy.

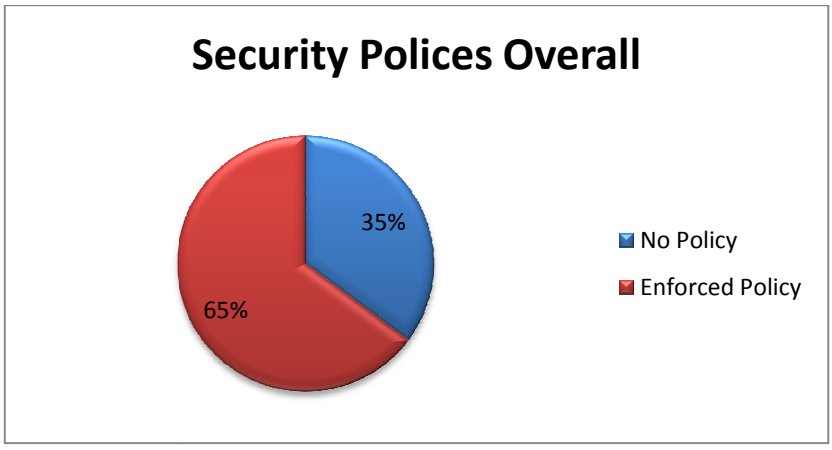


Figure 4-13 Percentages of Small Businesses Enforcing Security Policies

Approximately two-thirds of all the companies surveyed enforce some kind of security policy. The most common method when using an AD domain structure is to push this through Group Policy. Since only 37 percent of those surveyed indicated that AD was in use, the remaining 28 percent would either use the local security policy or may be referring to verbal policies where companies simply forbid certain activities or request password compliance but have no method to audit or enforce those policies. Table 4-4 provides a breakdown the types of policies enforced by company size. Figure 4-14 shows the overall most common policies enforced by the surveyed businesses.

Table 4-4 Security Policy Breakdown

Company Size	No enforced security policy	Complex passwords	Account lockout after 3 attempts	Access auditing	Password expiration	Internet Acceptable Use policies
1 to 10	15	16	8	5	5	6
11 to 20	1	5	4	3	3	4
21 to 50	1	3	3	2	1	4
51 to 100	1	1	1	1	1	2
over 100	1	1	1	0	1	1
Totals	**19**	**26**	**17**	**11**	**11**	**17**

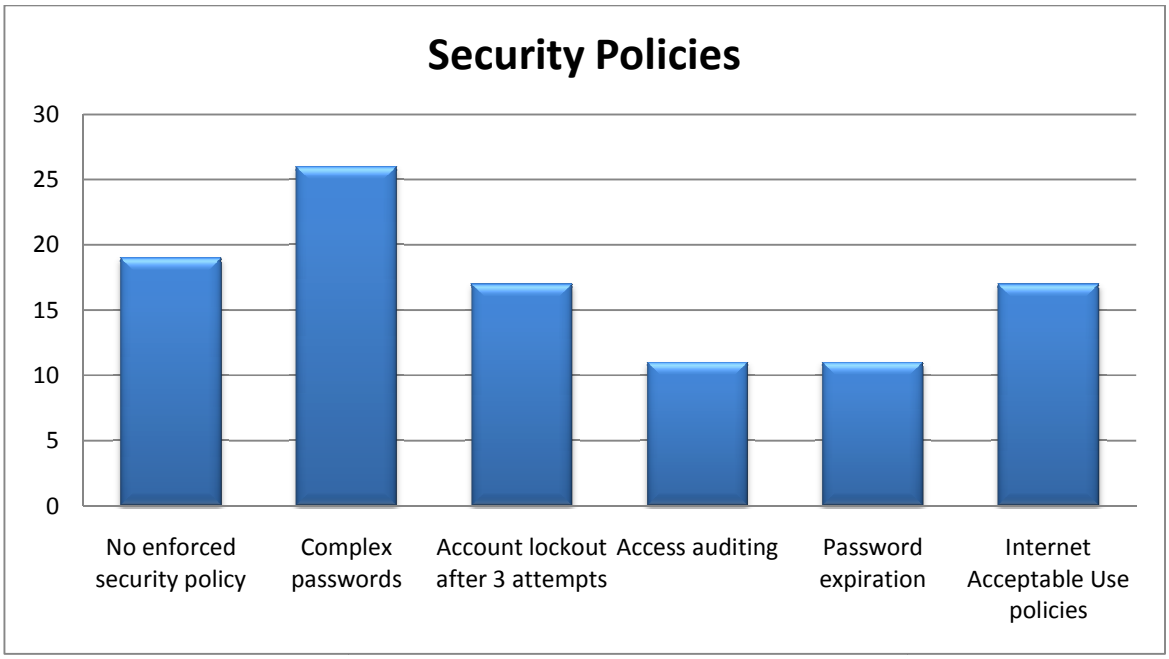


Figure 4-14 Common Enforced Security Policies

One of the most common and most important safeguard implemented today is antivirus protection. Antivirus protection can be installed in managed and unmanaged configurations. Managed protection uses a centralized server to push out updated definitions and provide centralized reporting on any malware found on the managed systems. Managed systems can also be programmed to run a scheduled system scan automatically. Unmanaged systems contact the

antivirus manufacturer websites directly and upload the latest definitions either manually or on a set schedule. If any malware is found, only the local system user would receive notification. Figure 4-15 shows the percentage of companies with antivirus protection and the type implemented.

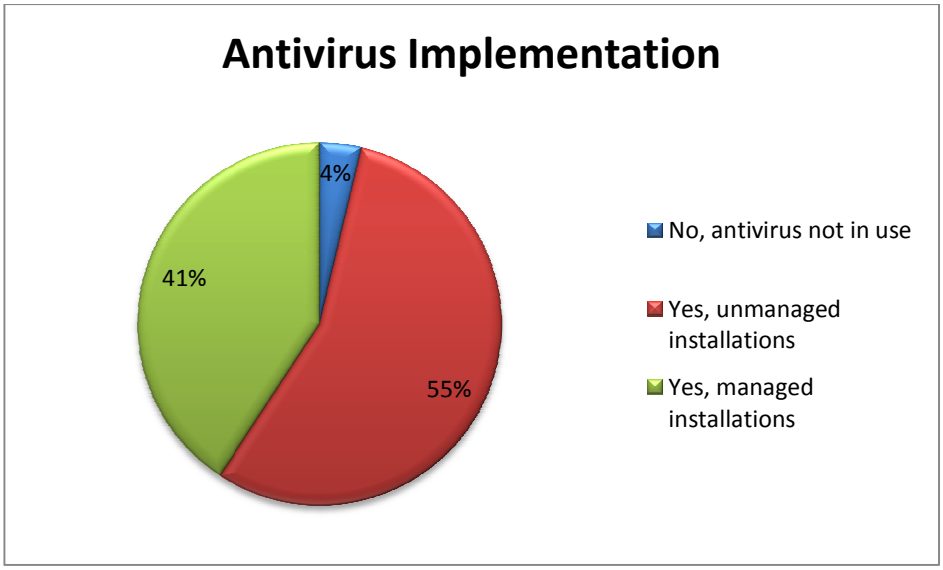


Figure 4-15 Antivirus Implementations

Companies that implement policies and safeguards but fail to train their employees on common security threats and mistakes are only partially protecting themselves. Firewalls and IDS can prevent threats from penetrating the perimeter of the network, but users that access infected sites or execute viruses sent through Email or shared program effectively allow hackers to bypass the strongest perimeter defenses. Formal training on the types of threats that are common and how hackers will attempt to gain access is essential. The Small Business Administration website provided by the government provides workstations and podcast training at no cost to help small businesses train their employees on the best ways to keep the networks safe. This includes the steps to take if a virus is suspected or how to deal with suspect email

attachments. Figure 4-16 shows the overall training provided to employees of the surveyed companies. Table 4-5 provides a breakdown of the training by company size.

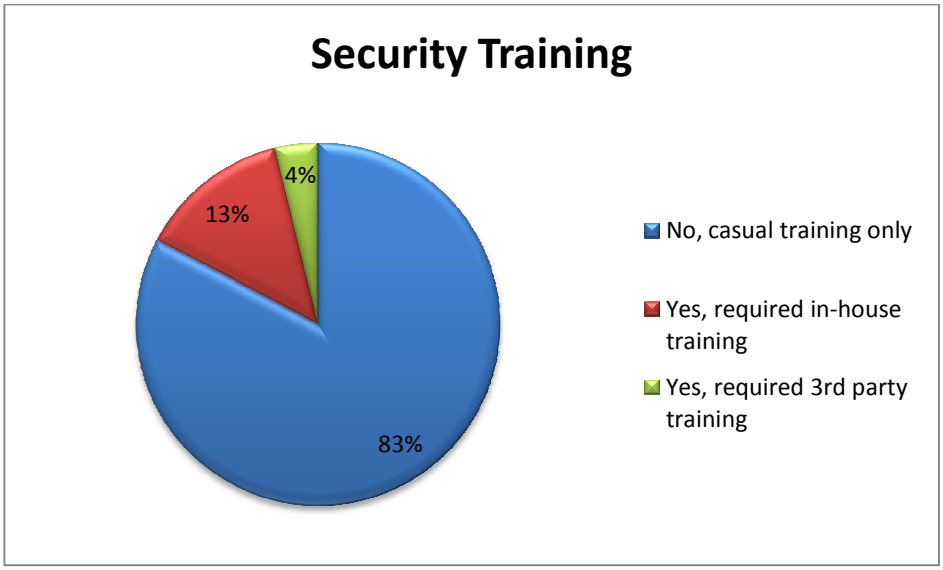


Figure 4-16 Types of Security Training Provided by Small Businesses

Table 4-5 Breakdown by Company Size of Training Provided

Company Size	No, casual training only	Yes, required in-house training	Yes, required 3rd party training
1 to 10	27	3	2
11 to 20	4	3	0
21 to 50	6	0	0
51 to 100	4	0	0
over 100	2	1	0
Totals	43	7	2

Most of the surveyed companies provided little or no formal training to the employees on how to keep their computers and the company network as safe as possible when working on the Internet. Failing to train employees on the best ways to work with Internet based applications or email will surely limit the effectiveness of any software or hardware defenses.

Along with training the employees, companies should take the time to test the defenses they have implemented. This can be done using simple methods such as port scanning or using third party security companies to attempt to penetrate the networks. Figure 4-17 provides a look at the penetration testing being conducted by the surveyed small businesses.

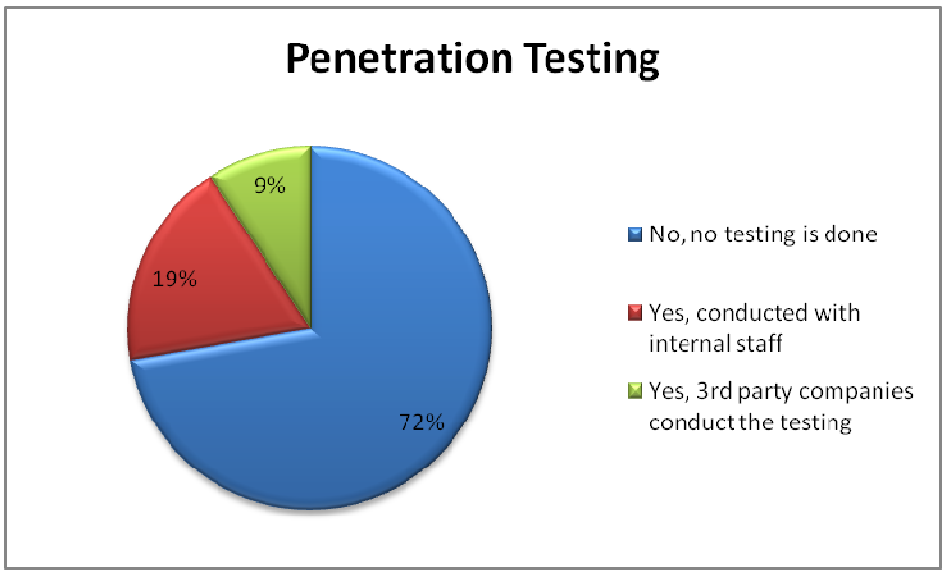


Figure 4-17 Penetration Testing

Policy Implementation

There are many factors that help determine when new policies are implemented. Figure 4-18 lists some of the common reasons for determining when policies (meaning security policies, hardware, or software) changes are made.

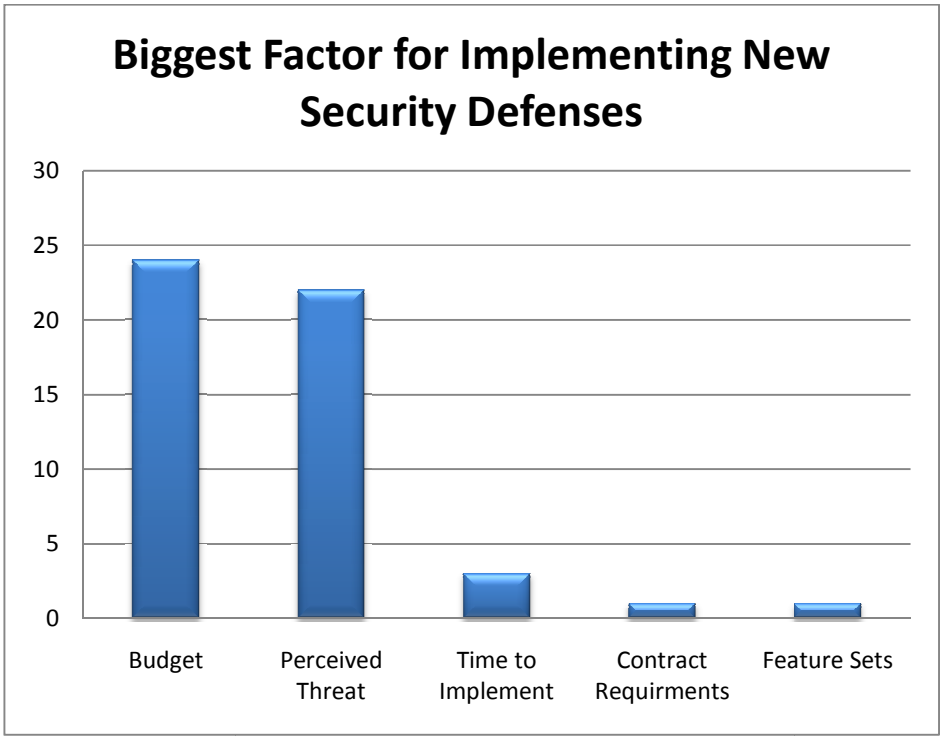


Figure 4-18 Security Policy Implementation Factors

This researcher found a strong correlation between budget and network security. This suggests that during hard business times, network security spending will decrease. The small businesses surveyed did however list perceived threats as another major factor in determining if and when new security is implemented. This means that if a business feels threatened enough, new security may be implemented in spite of a shrinking IT budget.

Even with the rising challenges of threats, most of the surveyed small businesses have no plans to change their current level of protection. Figure 4-19 shows the implementation plans for the surveyed small businesses for new security equipment and policies.

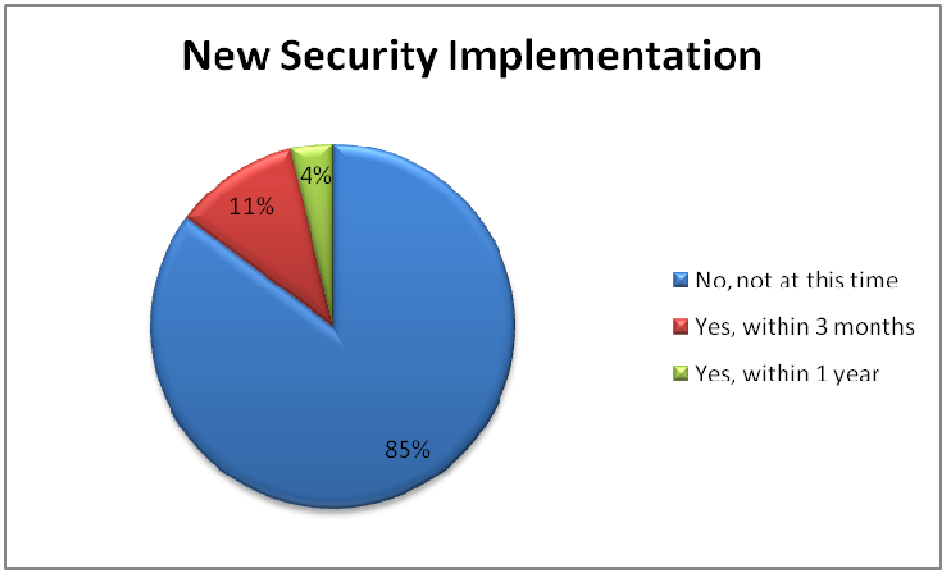


Figure 4-19 New Security Implementations

In the interview with the IT Operations Directory for Spatial Business, this researcher had the opportunity to ask several questions on current trends in small business network security. When asked what he thought was the biggest factor in determining which factors were seen most often when determining which security initiatives where implemented, his response was, "Budget is the biggest concern. All of the companies would like to be as secure as possible but cannot always afford the best equipment or software. Most do not even know what is available. For example, one office recently needed to upgrade their antivirus software and was given a choice between one suite that would protect from spyware as well as viruses but opted to go with just the antivirus software to save about 33 percent. They would have liked to get the extra protection but simply could not afford it right now. Other factors definitely come into play though. I can recommend certain procedures or new software but many of the users do not want to take the time to learn a new way of doing something even if it means better security." When asked if the small businesses he had worked with place a large emphasis on network security, he responded, "Yes and no. They all agree that their security is very important and never want to get

hit with malware or hacked in anyway but I still think most feel like it will not happen to them so minimal security is usually the norm. That mostly comes down to budget issues." This seems to confirm that many businesses still believe that they are not at risk for attack. Finally, when asked about what he felt was missing from small business network security on the whole, he responded, "It would be good to see more companies push security policies across the entire company rather than just to certain users. I see way too many companies put IDS or proxy servers in that create policies for the regular staff while leaving key vulnerabilities open for the executive level staff. If anything, you would hope the executive level staff would need the most protection since many keep confidential information on their local systems. They have the policies adjusted to allow their computers to do the exact things that they try to prevent the other staff from doing. This includes access to sites that are considered unsafe by proxy servers or turning off the proactive scanning because it may slow down Internet access. I would also really like to see companies focus a bit more on centralizing their data for backup and security reasons. Many have data spread across desktops, laptops, servers, flash drives, and external disks. It is very difficult to create a backup scheme when data is spread across so many locations. When user systems become infected or crash completely, often times that data is lost. It would be best to get it on some kind of file server, but the smaller companies could even use a network accessible external disk kept in a secure location. You can get a one TB disk for around $150 these days that would allow any user in the network to use the external disk as their primary storage or at least a location to backup their data (personal communication, March 26, 2010)."

Summary

The survey results show that small businesses are aware of the types of threats that exist and are at least trying to secure their systems as much as possible given the budgets they have to work with. Many have taken advantage of built-in functionalities and services that their ISPs offer to improve their security with little or no extra cost. But the results also show that while most of companies have implemented hardware and software to protect the perimeters of their networks, most have neglected to test their defenses or train their employees on the best ways to keep their networks safe. A lack of testing and training can translate into higher risks of being attacked. In addition, small changes in configurations or errors in setups can allow hackers to penetrate the network and steal valuable information such as account numbers and customer contact lists. Business owners that assume their network is protected may miss the warning signs that something is wrong or may misinterpret evidence indicating a breach. Lastly, a strong correlation exists between budgets and IT security spending.

Chapter 5 – Discussion and Conclusion

A bird swoops down over two gazelles being chased by a cheetah and asks, "Why are you bothering to run at all? You cannot outrun a cheetah!" One of the gazelles replies, "I do not have to outrun the cheetah…..I have to out run the other gazelle!" – Author unknown

This chapter recaps key elements of the research: discussing limitations of the study, implications for small business network security, and discusses areas for future research.

Limitations

Before discussing the survey results, it is important to look at the limitations of this survey and the method of deployment. This researcher must stress that the findings are exploratory, and not comprehensive. There were important limitations. Obtaining accurate information on small business network security was difficult. Since many small businesses do not have a full time IT administrator, many of the responses come from individuals who lack any real IT experience or training. In many cases, responses received were often accompanied by requests for clarification on exactly what each question was asking. For example, one response asked for clarification on the dedicated firewall question as to whether a cable modem qualified as a firewall. Some of the companies indicated that outsourced IT companies were utilized for at least some of their security and network setup needs. Many times the outsourced companies may be implementing security measures or policies without the responder's knowledge. Responders could assume that certain security defenses are in place when they are not and vice versa.

Another limitation may be the honesty of the responses. This survey asked questions about network security that could be interpreted by the respondents as an attempt to hack into a network. Hackers would love to have information on network authentication, firewalls, and other

network defenses before attempting to hack into a network. If the responders assumed that this study was an attempt to find holes that could be exploited, their responses may lean more towards an ideal security model rather than the reality of their networks. While perfectly understandable, this may skew the results towards a more secure model than is really in place at many of these businesses.

The results are also limited by what is referred to in statistics as the, "Self Selected Sample" (Jackson, 1985). A self-selected sample is created when surveys are distributed and only those that want to respond will actually respond. Several may not want to respond because they do not want to admit the current state of their networks is less than the ideal. Many may be embarrassed by the security that is implemented. This can skew the results further making the general state of small business networks appear more secure than they really are.

Another unexpected result of the survey was the lack of responses. In all, only 54 responses were received from over 4000 sent. This represents a return rate of only 1.35 percent. In some cases, responses were received indicating that the recipient had employed an antispam application either at their Email server or using a service through their ISP. Other responses included questions as to the legitimacy of my request and even refusals to answer based on the fact that the questions may reveal sensitive information about their networks. This in itself indicates that businesses are becoming more security savvy and distrustful of unsolicited emails.

Implications for Practice and Research

So what do the survey results tell us about small business network security? The results paint a picture of businesses trying to balance security with cost. These businesses are aware that having their networks connected to the Internet can be very advantageous but also recognize the risks involved. There were little surprises in the results. Businesses and individuals today are part

of an information age where data on security is freely available. New attacks are vulnerabilities are discovered everyday and usually there is no shortage of information to be found on how to protect systems from the latest threats. Operating systems and modern applications are in constant communication with manufacturers through the Internet for automatic updates and patches making keeping the systems up to date easier than ever. These small businesses recognize the need for antivirus (with 96 percent of the businesses surveyed reporting antivirus installations) and firewalls (with 89 percent of the businesses reporting dedicated firewalls at each Internet connection point.) It would be expected the budget would be a limiting factor for small businesses.

There were a few surprises though. It was unexpected that the small businesses would implement IDS at a constant rate independent of the size of the company. IDS is not a new technology, but traditionally has required a complex setup and constant monitoring to get any value. The implementation rate (59 percent) across all the company sizes surveyed would indicate that these small businesses are becoming much more aware of the severity of malware and hacking. The relatively high implementation rate could be a result of ISPs taking a more active stance against malware and hackers though. As reported by the Spatial Business IT director, ISPs are offering IDS as a built-in service on routers or cable modems or as an extra service filtering all traffic before it ever comes to the small business. This could account for the unexpected high rate of implementation.

The most important result from the survey was the confirmation that while security is considered important and steps have been taken at the ISP and business network levels to implement perimeter defenses and security software, these defenses are rarely being tested. Network based attacks are constantly changing. Brute attacks on user passwords, once a fairly

common way to hack into a remote system, are being replaced by social engineering, viruses and worms, and spyware uploaded into computers from malware infected websites. Protection schemes that may have prevented brute attacks will no longer protect against modern threats such as these. Assuming that protection schemes implemented in years past will continue to protect against these newer threats is unrealistic. These small businesses would be well served by performing audits on firewall rules and IDS policies at least once per quarter. Port scanners are freely available and many offer detailed explanations of the potential dangers when open ports are.

Since modern attacks attempt to circumvent the perimeter defenses, employee training is also very important. Many attacks come in the form of email spam. Users may receive unsolicited emails warning (ironically) of other attacks and requesting confirmation of account numbers, user IDs, and passwords. This may appear to be legitimate in every way. Attacks like this have cost businesses billions of dollars in lost funds and productivity. Taking the time to train employees to recognize that legitimate companies will never request sensitive information using email takes little time and can save not only money but keep the company's reputation in good standing as well.

Cyber attackers are not much different than the cheetah in short story at the start of this chapter. All things being equal, they generally will go after networks and systems that have the weakest defenses. Many of these attacks are completely anonymous. Viruses, worms, or other malware may originate in one particular network, but will spread indiscriminately. Many directed attacks, such as unauthorized access attempts or denial of service attacks, are also directed almost at random. In some cases, hackers may direct their attacks at particular

companies, but many times victims are chosen after port scanners, scanning random blocks of IP addresses, detect openings or vulnerabilities that can easily be exploited.

Even companies with large security budgets and the technical expertise required to secure a large network cannot create a network that is 100 percent secure. Networks that may be considered as close to 100 percent as possible today may find that as attacks change, employees come and go, and policies change, their networks can quickly be exposed. Vulnerabilities can be exposed as new applications are introduced or partnerships with other companies are formed. In some cases, security must be relaxed in order to meet the business needs if the risk is acceptable. The constantly changing environments of businesses make keeping security at adequate levels very challenging. Looking at the survey results, it does appear that most small businesses are at least aware of the dangers that exist even if they are not entirely sure of the best way to protect against them. They must keep securing their data and networks a priority at all times. This is often a fine balance of security, usability, and budget.

Small businesses can be especially vulnerable to the cyber attacks. With generally smaller budgets for security equipment and software and a lack of trained IT staff, security can quickly become outdated or ignored for long stretches at time. Since malware incidents can go undiscovered for long periods (or may never be discovered), security exposure is high in many small business networks. Add to that a lack of central authentication in many of the businesses (50 percent use peer-to-peer authentication only as the survey showed) and any hacker with a foothold on any one system may be able to access all of the data inside a network. Malware, such as viruses and worms, may also run rampant in any network where application, software, and operating system vulnerabilities are not patched regularly and antivirus definitions are out of date. Unfortunately the nature of what make a small business “small” can also be its undoing

when defending against the global threats found on the Internet. Budget concerns are the biggest factor but not the only factor. It takes time to implement a new system and training for the users; an idea unpopular with companies that may be operating on razor thin margins already.

There appears to be hope for many small businesses though. Internet Service Providers are providing more and more security services integrated into their small business packages taking some of the burden off of the small business owner. ISPs can provide the expertise needed to monitor malicious activity before it can spread to the small businesses if the small businesses take advantage of these services and protect their internal networks. Small businesses that make themselves difficult targets are much less likely to be affected by the malware circling the globe on the Internet right now.

Future research may be conducted on small business backup strategies and how they relate to an overall security structure. The number one fear from the small businesses surveyed was data loss. Data loss is data loss whether it is caused by a hacker, virus, data corruption, or accidental deletion. How the data would be lost is usually of little solace to business owners struggling to recover. Since disasters can take many forms, backup strategies and their effectiveness relative to their costs would make an excellent area for further research.

Another area for further research would involve researching the types of centralized resources being used in small businesses. Any shared resource, including storage area networks (SAN) devices, printers, and databases, could be at risk from network based attacks. A look at the types of devices being employed and how they are managed, configured, and audited, would make an excellent addition to any security paper on small businesses.

References

Ahn, G.-J., & Lam, J. (2005). Managing privacy preferences for federated identity management. Proceedings from the 2005 workshop on Digital identity management. AMC, USA, 28-36. DOI 10.1145/1102486.1102492

AT&T (2010, March 6). AT&T survey finds wireless technologies crucial to survival for nearly two-thirds of small business owners . Retrieved from http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=30636

Breach (2009, August). The web hacking incidents database 2009. Retrieved from http://www.breach.com/resources/whitepapers/downloads/WP_TheWebHackingIncidents-2009.pdf

Brenner, B. (2004, October 1). Poll: Lightning strike more likely than breach. Retrieved from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1011092,00.html

Burke, B., Hudson, S., Kolodgy, C., Crotty, J., & Christiansen, C. (2009, December). Worldwide IT security products 2009-2013 forecast adn 2008 vendor shares. Retrieved from http://www.idc.com/getdoc.jsp?sessionId=&containerId=221351&sessionId=16002E579F11F503113A9A9D09C18537

Cannata, M. (2009). Best practices for network security in small and medium-size businesses . Retrieved from http://www.helium.com/items/1245325-effective-network-security

Computer Associates (2008, July 18). Windows 7 bitlocker executive overview. Retrieved from http://technet.microsoft.com/en-us/library/dd548341(WS.10).aspx

Computer Emergency Readiness Team (2003, January 27). CERT advisory ca-2003-04 ms-sql server worm. Retrieved from http://www.cert.org/advisories/CA-2003-04.html

Computer Security Institute (2009, December 1). CSI computer crime and security survey 2009. Retrieved from http://gocsi.com/survey

Coviello, A. (2008, June 3). Security becomes a business enabler. Retrieved from http://www.eweek.com/c/a/Security/Security-as-an-Enabler-of-Business/

Edwards, J. (2008, January 18). DoS attacks take aim at small business. Retrieved from http://www.networksecurityjournal.com/features/DoS-attacks-011708/

Evans-Correia, K. (2008, January 15). SOX 404 compliance costs are lower than expected after first year. Retrieved from http://searchcio-midmarket.techtarget.com/news/article/0,289142,sid183_gci1293739,00.html

Final IT Solutions, Inc. (2008, January 16). Hackers and viruses to cost business $1.6 trillion. Retrieved from http://www.facebook.com/topic.php?uid=7918512285&topic=3812

Global Digial Forensics (2005). Penetration testing. Retrieved from http://www.evestigate.com/Penetrationpercent20testing.htm

Gold, T. (2008, 02 01). $30 billion to be spent on US network security. Retrieved from http://www.terrygold.com/t/2008/02/30-billion-to-b.html

Haber, L. (2009, April 27). Security training 101 . Retrieved from http://www.networkworld.com/news/2009/042709-user-security-training.html

Hight, S. D. (2005, November). The importance of a security, education, training and awareness program. Retrieved from http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf

HP (2010). Define a network security policy - understand it. Retrieved from http://www.hp.com/sbso/productivity/howto/security/understand_it.html

IDC (2010, March 23). Worldwide SMB spending will return to growth in 2010, but full recovery not expected until 2011. Retrieved from http://www.idc.com/getdoc.jsp?sessionId=&containerId=prUS22260610&sessionId=C539BC78DD30EBE4B4F11648575494AA

IDC.com (2010, January). Worldwide SMB 2010 top 10 predictions. Retrieved from http://www.idc.com/getdoc.jsp?sessionId=&containerId=221674&sessionId=16002E579F11F503113A9A9D09C18537

Innella, P. (2002, April 4). Managing intrusion detection systems in large organizations, part one. Retrieved from http://www.securityfocus.com/infocus/1564

Institute of Internal Auditors (2008, January). Sarbanes-Oxley section 404. Retrieved from http://www.theiia.org/guidance/technology/it-resources/sarbanes-oxley-resources/

Internet Storm Center (2010). Survival time. Retrieved from http://isc.sans.org/survivaltime.html

Jackson, E. E. (1985, April). ED263158 - How biased is a self-selected sample? Retrieved from http://www.eric.ed.gov/ERICWebPortal/custom/portlets/recordDetails/detailmini.jsp?_nfpb=true&_&ERICExtSearch_SearchValue_0=ED263158&ERICExtSearch_SearchType_0=no&accno=ED263158

Johnson, S. (2009, July 22). SMBs hurt by lack of it budget. Retrieved from http://itmanagement.earthweb.com/cnews/article.php/3831121/SMBs-Hurt-by-Lack-of-IT-Budget.htm

Kessler, G. (2000, Novemeber). Defenses against distributed denial of service attacks. Retrieved from http://www.garykessler.net/library/ddos.html

Kizza, J. (2005). Computer Network Security. In J. Kizza, Computer Network Security. Springer Sciense Business Media, Inc., MA

Kolodgy, J., & Crotty, J. (2009, December). Worldwide network security 2009 forecast. Retrieved from http://www.idc.com/getdoc.jsp?sessionId=&containerId=220936&sessionId=BYHXZBWAOX2VYCQJAFDCFEYKBEAVAIWD

MarketersProtection.com (2010). How often should you update anti-virus definitions? Retrieved from http://www.marketersprotection.com/wp/how-often-should-you-update-anti-virus-definitions/

Mathur, S. (2008, July 25). Networking solution for small and large business. Retrieved from http://www.articlesbase.com/networks-articles/networking-solution-for-small-and-large-business-496470.html

McDowell, M. (2009). Avoiding social engineering and phishing attacks. Retrieved from http://www.us-cert.gov/cas/tips/ST04-014.html

McMillan, R. (2009, Novemeber 3). FBI warns of 100m cyber-threat to small business . Retrieved from http://www.networkworld.com/news/2009/110309-fbi-warns-of-100m-cyber-threat.html

Mogul, R. (2007). Disgruntled employee alert. Retrieved from http://www.realtimenorthamerica.com/download/disgruntled_employee_alert.pdf

National Institute of Standards and Technology (2009, Novemeber 17). Small business corner (SBC). Retrieved from http://csrc.nist.gov/groups/SMA/sbc/index.html

Nijnik, I. (2007, March). Small business network security 101. Retrieved from http://www.safeatoffice.com/landing/SMB_Security_101.pdf

Pirc, J. (2009, May 6). Common network security misconceptions: Firewalls exposed. Retrieved from http://www.sans.edu/resources/securitylab/pirc_john_firewalls.php

Posey, B. (2000, August 17). Security on a peer-to-peer network. Retrieved from http://articles.techrepublic.com.com/5100-10878_11-5033516.html

Raggo, M. T. (2007). Hacking and network defense. Retrieved from http://www.spy-hunter.com/Hacking_Brief.pdf

Rodriguez, E. (2004, July 16). IDS - intrusion detection system. Retrieved from http://www.skullbox.net/ids.php

Score (2009, September). Small biz stats & trends. Retrieved from http://www.score.org/small_biz_stats.html

Stallings, W. (2007). *Network security essentials.* Trenton, NJ: Pearson Education, Inc.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

U.S. Department of State (2010). Small business in the United States. Retrieved from http://economics.about.com/od/smallbigbusiness/a/us_business.htm

University of Nevada, Las Vegas (2010). Definition of information security. Retrieved from http://oit.unlv.edu/network-and-security/definition-information-security

US Small Business Administration (2009). Size standards. Retrieved from http://www.sba.gov/contractingopportunities/officials/size/index.html

Whitney, L. (2010, February 17). Malware and social network attacks surge in '09. Retrieved from http://news.cnet.com/8301-1009_3-10454870-83.html

Yeung, B. (2009). The convergence of virus & spam threats. Retrieved from Systems http://www.tns.com/virus_spam.asp

Appendix A

Survey Questions

1. How many people are employed at your company?
    a. 1 to 10
    b. 11 to 20
    c. 21 to 50
    d. 51 to 100
    e. Over 100
2. Does your company have any permanent links to other sites or businesses? If so, what kind(s) of connections are used?
    a. No dedicated connections
    b. Virtual Private Network
    c. Point to Point link
    d. Frame-Relay
    e. Other (please specify)
3. How many full time Information Technology does your company have on staff?
    a. 0
    b. 1
    c. 2 to 5
    d. 6 to 10
    e. Over 10
4. Does your company outsource any or all of your IT needs?
    a. No, all IT is handled internally

b. Yes, some IT is outsourced

c. Yes, all IT is outsourced

5. Does your company use a Network Operating System for user authentication?

    a. No, peer-to-peer authentication only

    b. Yes, Windows Active Directory

    c. Yes, Novell Netware

    d. Yes, Other (please specify)

6. Is your Internet connection (or connections if you have more than one site) protected by a dedicated firewall?

    a. Yes

    b. No

7. Is there any kind of Intrusion Detection System deployed?

    a. No, not at this time

    b. Yes, network based IDS

    c. Yes, host based IDS

    d. Yes, both host based and network based IDS

8. Does your company enforce any security policy? If so, please check all that apply.

    a. No enforced policy

    b. Complex passwords

    c. Account lockout after 3 attempts

    d. Password expiration

    e. Access auditing

    f. Other (please specify)

9. Does your company use any kind of anti-virus software?
    a. No, none implemented at this time
    b. Yes, centralized AV server (managed)
    c. Yes, individual AV on each system (unmanaged)
10. Does your company conduct regular penetration testing?
    a. No, no testing is conducted at this time
    b. Yes, internal staff test the external defenses
    c. Yes, 3rd party companies are contracted to conduct the testing
11. What kinds of threats have affected your company in the last 12 months?
    a. Viruses/worms
    b. Malicious data theft/loss/alteration
    c. Accidental data loss/alteration
    d. Hardware theft/vandalism
    e. Denial of Service (DoS) attacks
    f. None reported
    g. Other (please specify)
12. Does your company provide any kind of network security training for the employees?
    a. No, only casual training provided user by user
    b. Yes, employees are required to attend in house training
    c. Yes, employees are required to attend 3rd party training
13. Does your company host any of the following Internet facing services?
    a. Email (Exchange/Lotus Notes)
    b. Website – e-Commerce

c. Website – Informational

d. Virtual Private Network

e. Data transmission services (FTP/HTTPS….)

f. Other (please specify)

14. Please rank the following network based threats in order of importance to your business (rank #1 as the most dangerous; #8 as the least dangerous)

a. Unauthorized Access

b. Viruses/Worms

c. Spyware

d. SPAM

e. Data loss

f. Data theft

g. Hardware failure/theft

h. Connectivity loss

15. Are there any new security measures being implemented?

a. Not at this time

b. Yes, within the next 3 months

c. Yes, within the next year

16. What is the biggest factor for determining which security defenses are deployed in your network?

a. Budget

b. Perceived threat

c. Contract requirements

d. Time to implement

e. Other (please specify)