Computer Networking and Information Security for the Small Business

Dennis D. Hill and Suhansa Rodchua

Abstract— Computer networking, and networking devices together, has become an interregnal part of today's business operations. If a business does not have a secure infrastructure within its computer networking system, it can greatly impact a business daily operations and cause many problems within a business such as information loss, identity theft, stolen information, and other threats that can impede an organization. This study investigates the threats to businesses' networking systems, level of annual incomes, and safety precautions.

The target population are businesses in the states of Missouri and Kansas. The online questionnaire was created in Google Doc. and it was also split into various sections, such as computer information, networking information, demographics, and open-ended question about computer networking security. The SPSS version 19.0 with computation of ANOVA one-way was performed to test the hypotheses; the F ratios were considered at the 95% level of confidence.

The survey results from 49 enterprises showed that there was no significant difference between the company's annual income and levels of providing training to employees and basic network security systems. In addition, most small businesses have standard safety procedures put into place with antivirus software and firewalls and the most common threat that businesses worry about is malware and viruses. Any small business can implement some basic procedures to make them less venerable and to make a hacker look elsewhere for a potential victim. Setting up a secure network with employee training is paramount to the success of a business having a secure network

Index Terms—Computer Networking Security, External Threats, Internal Threats, Networking Systems, Secure Network, Small Business, Survey Research

1 Introduction

Computer networking, and the ability to network devices, is an import element of a small enterprise today. The need for organizations to keep their computer networks, and information, secure has become an important factor in business performing day-to-day transactions. Nowadays, security on the Internet and on Local Area Networks (LAN) is an integral part of computer networking-related issues [1]. Businesses need to utilize electronic transactions on some level to keep their organization running smoothly and efficiently, especially small businesses. Vail points out that "[s]mall businesses account for over fifty percent of the Gross National Product of the U.S. economy; and the security of their information systems is critical for them to operate, compete, and remain profitable" [2].

As electronic transactions become highly popular, more and more threats show up on a daily basis. Some of these threats are designed to cause loss of revenue, some can be caused by disgruntled employees, and some are just designed to cause malice for no particular reason other than a hacker wanting to see if they can infiltrate someone's system. Sometimes threats come from teenagers who are just trying to have fun, and do not realize the consequences of their actions. Computer network also have issues that can be corrected when the employees are properly trained to recognize threats to the company's network. There are many times when a threat can be simply received such as when a virus is sent through spamming where someone gets an email that seems safe and appropriate in nature but contains malicious content (virus, worm, etc.). Even though there is much literature about computer network security available, the fact that training could be a factor in preventing threats does not seem to be emphasized enough. Much of the literature written about computer network security the does not place a lot of the accountability on the employees to help maintain a safe computer network.

Proper electronic security tends to correlate directly to a business's growth. There are many types of threats a business can face, and businesses should be aware of the dangers of not protecting its data. Computer security can also be an issue when a company is implementing new technology into their business system. "New security challenges arise when new—or old—technologies are put to new use" [3]. Organizations that do not have its information secure can have its business greatly compromised by security intrusions that can damage its network infrastructure and cause loss and/or theft of information. According to the Federal Communications Commission (FCC), Cyber space and the Internet are a critical infrastructure for commerce and communications. Disruptions in the networks and lapses in security now place at risk lives, jobs, our economy and well-being [4].

If a business does not take the appropriate measures to keep its information secure then the whole business can be compromised. The business then might face many repercussions, such as loss of revenue, loss of clients, and more. There are even further precautions that need to be taken for businesses that conduct sales over the internet. According to the Federal Bureau of Investigation (FBI), "As business and financial institutions continue to adopt Internet-based commerce systems, the opportunities for [internet] crime increase at retail and consumer levels" [5]. The repercussions of poor internet security can affect the consumer, as well.

2 PURPOSE OF STUDY AND QUESTIONS

This study intends to investigate the threats to businesses' networking systems, level of annual incomes, and safety precautions. This paper also determines types of safety measures presently lacking in computer network systems for small businesses; the survey research was conducted to find the answers for the following questions:

1. What are the internal and external threats to the small business' network security system?
2. Has the level of business' annual income affected the providing Information Technology training to employees?
3. Has the level of business' annual income affected the company's basic network and information security system?
4. What safety precautions do small businesses have in place to protect its data and computers?
5. Is there a more efficient need for small businesses to protect their data?

To assist in answering research questions 2 and 3, null hypotheses 1 and 2 were set up:

H_{01}: There is no statistically significant difference of level of business' annual income on providing Information Technology training to employees.

H_{o2}=: There is no significant relationship between the business' annual income and taking more measures to keep their data secure.

The next section is a part of literature reviews from various sources. Major points discussed in this paper included internal and external threats to networking systems, together with the plan for data protection.

3 THREATS TO NETWORKING SYSTEMS

Computers get used daily in our lives for personal use, business, networking and more. Almost every business such as banks, schools, government organizations, etc., utilizes computers to improve efficiency for their operations. Computers have become an integral part to running, and maintaining, a small business in today's market economy. Computers perform tasks on many levels of a business infrastructure, such as communication between different departments via computing devices. Computer processing and information technology have become increasingly more important to any type of business whether larger or small. The threat of hackers and cyber-criminals is very real, for large companies and small businesses alike [6]. Computers are valuable for the various tasks they perform, but many times this investment is not protected properly which causes inefficiency in a business. Keeping computers and information secure should be a primary part of operating any business, and keeping smaller businesses protected is just as important as keeping computer networks in large corporations protected.

Businesses that have computer systems that become compromised can cause damage to a company's reputation and loss of trust with its customer base. "As network security concerns escalate, new Internet threats appear on a daily basis, and enterprises that are classified as small businesses are put at risk" [7]. Computer network security for small businesses is central, according to the Small Business Administration (SBA) over 50% of the American population work for small businesses. Even though there are many major corporations in the United States, almost every corporation started out as a small business at one time. More than half of small businesses survive for five or more years, and about a third of them survive for more than 10 years meaning that two-thirds of small businesses fail within ten years of startup [8].

Internal Threats: Internal threats to a computer network are threats that are made internally within a system. For example, an employee bringing in a flash drive and plugging it into a work computer and then finding out that there was a virus transferred to the computer network, which can be intentional on unintentional. These types of threats can include social engineering wherein someone might convince a friend to use a flash drive that is corrupted for the purpose of doing damage a company's computer network. There are several types of internal threats including:

- Social engineering
- Bringing in a threat via another device (i.e. USB drive, cell phone, etc.)
- Peer-to-peer file sharing
- Media Files

Internal threats can be intentional or unintentional. Rhodes states that there are many things that can be done about internal threats such as limiting internet capabilities, scanning internal files, and closing unused ports [9].

External Threats: External threats include such attacks as viruses, worms, Trojan horses, and denial of service (DOS) attacks. External viruses can also come via email from spam attacks or another type of email that looks like it might be something harmless. External types of threats are more common than internal threats, but they are much easier to safeguard against. However, external threats can usually get past simple internet security because they are often disguised as something that is going to be beneficial to an individual and/or their computer. Many types of external threats include: computer hackers, Trojan horses, denial of service (DOS), viruses, and phishing.

4 NETWORK SECURITY AND DATA PROTECTION

Even though there is much literature available about computer network security there is not a lot of awareness about keeping networks safe for small businesses. While many aspects of network security are applied to large corporations due to the fact that they deal with much larger sums of money, the security of computers at a small business should not be overlooked because small businesses makeup a large portion of the American economy. According to the Small Business and Entrepreneurship Council, "In 2011, according to U.S. Census Bureau data, there were 5.68 million employer firms in the United States. Firms with fewer than 500 workers accounted for 99.7 percent of those businesses, and businesses with less than 20 workers made up 89.8 percent" [10]. Large corporations seem to get most of the attention when it comes to being infiltrated (i.e. lots of news coverage, trending topics on the internet, etc.) but there is little mentioned about it when a small business faces an attack.

There are many layers of network security that can be looked at. It can be taken from an ethical standpoint to simple training methods. Unethical behavior is something that can always cause business harm, but can do monetary damage in a company, especially if an employee is disgruntled and feel like they want to get revenge on the company by causing damage. This is just one reason why a company should keep rules and regulations about computer usage in place. If a company sets up rules it sets a standard, and it could reduce the people who introduce future threats. Putting a system of rules regarding security in place can not only clearly instruct all employees of what is expected, it can help a company's future on many levels including placing blame where it should be placed.

Computer network also have issues that can be corrected when the employees are properly trained to recognize threats to the company's network. There are many times when a threat can be simply resolved such as when a virus is sent through spamming where someone gets an email that seems safe and appropriate in nature but contain malicious content (virus, worm, etc.). Even though there is much literature about computer network security available, the fact that training could be a factor in preventing threats does not seem to be emphasized enough. Much of the literature that concentrates on computer networking for the small business tends to focus on keeping anti-viruses updated, and does not place a lot of the accountability on the employees to help maintain a safe computer network.

There are also many other aspects to network security which should seem commonplace, but are not. The implement of a firewall and/or an antivirus program should be a top priority in keeping a network secure, but this alone will not be enough to keep it running smoothly. It should not, however, be taken lightly, or be overlooked. With the rate that technology grows computers become more vulnerable, but they also become more valuable since they are relied upon for so many task. The scope of a network also does not simply rely on computers in this day and age either. There are many other devices that can become a part of a network including tablets, cell phones, and many other electronic devices.

5 METHOD OF STUDY

This study population targeted on businesses in the states of Missouri and Kansas through various local offices of the Chamber of Commerce. The participants in the survey were managers, proprietors, or information technology (IT) specialists. Small businesses were contacted via email, and asked if a manager, owner, or other qualifying person, would be able to fill out a survey regarding computer networking security. The online questionnaire was created in Google Doc. and it was approved by the Human Subject Committee at the university on February 23, 2016. The data was also split into various sections, such as computer information, networking information, demographics, and open-ended question about computer networking security. The survey that was utilized is shown in Appendix A. The SPSS version 19.0 with computation of ANOVA one-way was performed to test the hypotheses; the F ratios were considered at the 95% level of confidence.

6 FINDINGS AND DATA ANALYSIS

The online questionnaire was posted for 12 weeks and 49 survey respondents were collected. This section is divided into 3 parts: 1) the demographic data of respondents, 2) The hypothesis testing, and 3) answers the five research questions.

6.1 Demographics

A total of 49 businesses completed the survey with an aggregate of 517 computers and a mean of 12 computers per business. A total of 83 computers had been sent to a shop annually for repair not counting the ones that were repaired by the small businesses that employees in-house IT technicians that maintained and repaired their own computers. An average of 1.7 computers had been sent to a computer maintenance shop to be repaired annually. Many businesses have indicated that their Point-Of-Sale (POS) computers have much higher security requirements than computers used by office personnel and managers, and in many cases POS systems security was contracted outside of the business. Businesses that have security requirements such as requiring employees to change passwords on a regular basis had less computers (none in most cases) taken to a shop for repairs, or that were required to be repaired by an IT technician. Many of the businesses that chose the option that they did not have any threats to their computer security were among the highest to have their computer required to be repaired. For example, one business that claimed that they did not see a need for any security, or view any threats to their computer network, were required to have 14 computers repaired annually. Smaller business, in general, did not see the need to obtain as much security as larger business because they did not view lack of security as a threat although they generally had more issues with computers not running efficiently due to improper security maintenance. In addition, two people experienced cases of identity theft via their computers at work.

Most of the businesses that completed the survey 46.94% required to change password 1-4 times per month, 73% had 1-20 full-time employees, 44.90% had 1-10 part-time employees, 30.61% updated operating systems 1-4 times a month, 61.22% were business owners, and 28.57% had annual income of less than US$250,000 and between $250K - $500K as shown in Table 1.

TABLE 1
DEMOGRAPHICS DATA OF RESPONDENTS

Survey Questions	Freq.	Percent
1. Password Changes Required		
1-4 Times per week	0	0%
1-4 Times per month	4	8.16%
1-4 Times per year	23	46.94%
Never	22	44.90%
2. Number of Full Time Employees		
1-10	36	73.47%
11-100	10	20.40%
100-500	3	6.12%
3. Number of Part Time Employees		
None	19	38.78%
1-10	22	44.90%
11-40	3	4.12%
40 or more	5	10.20%
4. How often operating systems are updated?		
Daily	7	14.29%
Once per week	8	16.33%
1-4 times a month	15	30.61%
1-4 times a year	10	20.41%
Never	9	18.37%
5. Job title of person competing survey.		
Business Owner	30	61.22%
Manager	12	24.49%
IT Technician	2	4.08%
Other	5	10.20%
6. Annual income of company in US dollar amount.		
less than 250,000	14	28.57%
250,001 – 500,000	14	28.57%
500,001 – 750,000	3	6.12%
750,001 – 1 million	5	10.20%
1 million – 2 million	3	6.12%
More than 2 million	10	20.41%

6.2 Hypotheses Testing

The computation of ANOVA one-way was performed to test two hypotheses; the F ratios were considered at the 0.05 alpha or 95% level of confidence. Table 2 presents the results of computation, and detailed outputs of ANOVA statistical testing.

TABLE 2
ANOVA ONE-WAY

Hypothesis Testing		df	Mean Square	F	Sig.
Password Change	Between Gr	5	0.399	0.988	0.436
	Within Gr	43	0.404		
	Total	48			
Windows Updated	Between Gr	5	3.569	2.42	0.051
	Within Gr	43	1.475		
	Total	48			
Antivirus	Between Gr	5	0.354	1.851	0.123
	Within Gr	43	0.191		
	Total	48			
Firewall	Between Gr	5	0.385	0.981	0.44
	Within Gr	43	0.392		
	Total	48			
Security Training	Between Gr	5	0.034	0.101	0.991
	Within Gr	43	0.34		
	Total	48			

Hypothesis one tests whether level of business' annual income has a main effect on providing Information Technology training to employees. In Table 2, the F statistic for security training is 0.101. The observed significance level is 0.991, so the null hypothesis is not *rejected* at the .05 alpha. The mean of providing employee training is *the same* for any level of business's annual income. Therefore, we can conclude, based on the sample results, that there is no statistical difference of business' annual income on providing training to employees.

Hypothesis two tests whether level of business' annual income has a main effect on company's basic network and information security. In this study, five main variables are used in representing the basic network and information security of the company:

- Frequency of employees' password change
- Frequency of updating Window
- Utilizing an antivirus protection program
- Utilizing a firewall
- Providing IT training to employees

In Table 2, the F statistic for password change is 0.988. The observed significance level is 0.436; the F statistic for updating window is 2.42. The observed significance level is 0.051; the F statistic for utilizing an antivirus protection program is 1.851. The observed significance level is 0.123; the F statistic for utilizing a firewall is 0.981. The observed significance level is 0.440; and the F statistic for employee training is 0.101. The observed significance level is 0.991. The null hypothesis is not *rejected* at the 95% level of confidence. The mean of basic network security system is *the same* for any level of business's annual income. Therefore, we can conclude, based on the sample results, that there is no statistical difference of business' annual income on basic network security system.

6.3 Research Questions Answered

According to the literature reviews and survey questionnaire with 49 small and medium enterprise, the answers to these 5 research questions are:

Q1: What are the internal and external threats to the small business' network security system?

A1: Many of the businesses were able to identify some of the internal threats that they might face, such as personnel not having strong enough passwords. Others have stated that although they allow workers free access to the internet that they may feel that they might face external threats, such as viruses, if their usage was not monitored. Other situations that pose a threat include a lack of employee knowledge from not getting the proper training in simple security measures. External threats can also include former employees who have not had their passwords terminated, and still have access to the network. While some businesses do not worry about any type of threats whatsoever one of the threats that businesses worry about is the loss or theft of customer information. However, the most common threat that businesses worry about is malware and viruses.

Q2: Has the level of business' annual income affected the providing Information Technology training to employees?

A2: As we can see from the data collected most employees of small businesses do not receive any type of security training. Only 36% of employees receive training in security methods, such as keeping computer operating systems updated, keeping passwords updated, using passwords that are secure, making sure computers are locked when they leave their station, keeping software updated, etc. The level of a company's income did not seem to reflect the amount of training that an employee received. Even though many larger companies employ an IT technician to keep software and operating systems updated, most companies that employ smaller amounts of employees can often not afford to also keep an IT technician on their staff; therefore, must rely on its employees to practice proper safety techniques when it comes to keeping computers secure. However, as we can see the level of income did not affect the amount of training that employees received.

Q3: Has the level of business' annual income affected the company's basic network and information security system?

A3: According to the survey results most business did also not face any type of security breaches with their computer network, although 4% said that they did that did not know whether or not their computer network had faced any security breaches. While there were more security breaches than there were cases of identity theft there were two people who had experienced cases of identity theft through the computer network at the business they worked for. However, as we can see in out testing of hypothesis one there was no effect on a business's security level and its amount of annual income.

Q4: What safety precautions do small businesses have in place to protect its data and computers?

A4: Most small businesses have standard safety procedures put into place. While the amount of annual income did not affect the level of security that small businesses maintained there were 14% of businesses faced some type of security breach while another 14% of businesses listed that they did not know if they had experienced some type of security breach meaning it is possible that they had. According to this information, there is a more efficient need to protect data for small businesses. However, most small businesses already have methods to protect data put into place such as protection for their computer networks with antivirus software and firewalls. However, we cannot assume that all firewalls are set up properly with the appropriate password protection put into place. This biggest factor that small businesses utilize for protection is antivirus with a larger percentage having antivirus than firewalls or utilizing training.

Q5: Is there a more efficient need for small businesses to protect their data?

A5: According to the data collected approximately 14% of businesses have experienced computer breaches while another 14% did not know if they have experience any breaches. While there was only two cases of identity theft due to lack of security there were also 36 computers out of the 517, which is 6%, had to be repaired due to viruses which shows some level of need to protect computers and data more efficiently.

7 CONCLUSION AND DISCUSSION

The overriding purpose of this study was to determine if computer network security was a growing concern to small businesses, whether the amount of revenue a small business generated made a difference in the amount of security an organization maintained, and to see if vast improvements could be made regarding computer network security for small businesses. Even though small businesses do not generate the amount of revenue that larger businesses do "small businesses must cope with the same Internet security threats as larger companies do, but usually without the same budget and manpower" [11]. Most security breaches that have happened to small businesses surveyed can potentially be resolved by offering employees more training in security techniques such as using passwords that are more secure, not leaving computers logged onto accounts while away from their computers, etc. Even though many smaller companies may not view computer and information security as important as larger companies might, Caramela argues that "Cybersecurity is important for companies of all sizes. Small businesses are just as at risk for cyber attacks as larger companies, and should be prepared for a breach at all times [12].

While many of the respondents to the survey listed that they had faced computer security threats in the past or they did not know whether their computer network had been infiltrated, 65% of the respondents to the survey claimed that there was not any threats to their current network security. Furthermore, even though it was determined that annual income of a small business did not reflect the amount of security training the employees received, and we can also see that annual income did not affect the amount security breaches small businesses faced, although more businesses in the less than US$ 250,000 to 750,000 range stated that they did not know if they had experienced any security breaches within their small business.

Even though many businesses did not face any security threats in the past they also stated that they did not foresee any threats happening to their organization in the future, and some even stated that there was zero risk for a security breach in the future.

8 RECOMMENDATION

Cyber threats are growing and businesses of all sizes are at risk. As the dangers increase, smaller firms that are proactive in securing their networks will benefit as much as their larger counterparts [13]. Keeping networks secure can largely depend on employees taking some simple steps other than a business implementing standard security practices such as implementing antivirus and firewalls. Since close to 60% of businesses do not offer any type of security training and a large quantity of small businesses do not employ an IT technician organizations can make their networks more secure by offering network security training to new, and existing employees. Even though most small businesses have standard security procedures in place less than five of the businesses surveyed do not utilize an antivirus program and less than ten businesses do not utilize a firewall, see Figures 1 and 2. Some of the businesses surveyed even stated that there was no need to put security measures, or further security measures, such as training employees in security techniques in place. However, many would argue that setting up a secure network with employee training is paramount to the success of a business having a secure network.

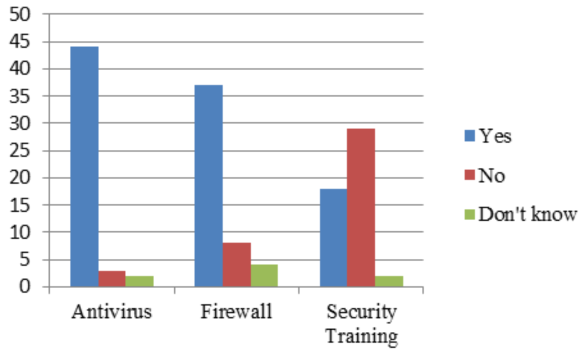

Fig 1: Antivirus, firewall and security training of 49 companies

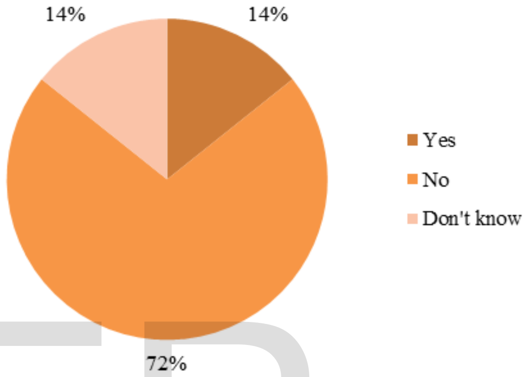

Figure 1: Amount of security breaches that 49 small businesses experienced on a yearly basis.

Even though technology is constantly changing and developing it is possible many trends in computer and information security will remain constant. Even though we have seen a shift in developing technology such as the implementation of tablets, smart phones, and other smart devices into the way business is being done the way that computer networks are set up and protected essentially remains a relative constant. Small businesses can vastly improve their network security by implementing some simple procedures such as:

1) Create mandatory training for all employees to take concerning network and information security.
2) Hiring a part time IT technician or find affordable outside help to assess the company's network security needs and use the assistance to help in setting up guidelines for network security.
3) Making sure that all endpoints are secure such as all devices on the network, and one the wireless network, such as smart phones, tablets, USB drives, etc.
4) Making sure to follow simple security procedures such as making sure employees use passwords that are secure, keeping computer software such as operating systems and antivirus software up-to-date, etc.
5) Building a secure wireless network through, encryption, authentication, not broadcasting the network name, and MAC address filtering.

In the end it is ultimately up to the business to make sure its own network is secure. A potential hacker is most likely going to look for the easiest target that they can find. There is a plethora of reasons that a hacker might want to attack a company's network from monetary reasons, to network vandalism and more. Any small business can implement some basic procedures to make them less venerable and to make a hacker look elsewhere for a potential victim.

REFERENCES

[1] Akin, T. (2002). Hardening Cisco routers. Sebastopol, CA: O'Reilly & Associates.

[2] Vail, J. E. III. (2012). Small business information security Carolina University. Retrieved from ProQuest Dissertations and Theses, 124.

[3] Gollmann, D. (2010). Computer security. *Wiley Interdisci plinary Reviews: Computational Statistics,2*(5), 544-554. doi:10.1002/wics.106

[4] Cyber Security and Network Reliability. (2012). Retrieved July 25, 2016, from https://www.fcc.gov/general/cyber-security-and- network-reliability

[5] Federal Bureau of Investigation (2011, September 14). Retrieved April 30, 2015, from http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

[6] Strauss, K. (2015, August 6). How Small Businesses Can Improve Their Cyber Security. Retrieved December 4, 2015, from http://www.forbes.com/sites/smallbusinessworkshop

[7] Cisco Press (2012). CCNA security booklet version 1.1 (2nd edition). Indianapolis.

[8] Advocacy: The Voice of Small Business in Government. (2012, September). Retrieved June 13, 2016, from https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf

[9] Rhodes, Charles (2003). The internal threat to security of users can really mess things up. Retrieved from http://www.sans.org/reading-room/whitepapers/bestprac/internal-threat- security-users-mess-things-856

[10] U.S. Small Business Administration. (n.d.). [document] Retrieved from http://www.sba.gov/content/summary-size-standards-industry

[11] Arar, Y. (2009, July 1). Small-Business Network Security 101. Retrieved July 13, 2016, from http://www.pcworld.com/article

[12] Caramela, S. (2016, July 11). Cybersecurity: A Small Business Guide. Retrieved August 04, 2016, from http://www.businessnewsdaily.com

[13] TechRadar: Network security: Your best practice guide. (2013, August 5). Retrieved June 08, 2016, from http://www.techradar.com/us/news/networking

APPENDIX: QUESTIONNAIRE

Section One: Information on Computers at your Organization		
1)	Number of computers that the company has:	Fill in the blank
2)	Number of times computers have been taken to a shop for repairs (annually):	Fill in the blank
3)	How often does the company require employees to change passwords?	□ 1-4 times a week □ 1-4 times a month □ 1-4 times a year □ Never
4)	Number of full-time employees:	□ 1-10 □ 11-20 □ 21-30 □ 31-40 □ 41-50 □51-60 □61-70 □71-80 □81-90 □91-100 □100 or more □500 or less (manufacturing industry)
5)	Number of part-time employees:	□ 1-10 □ 11-20 □ 21-30 □ 31-40 □ 40 or more
6)	How often are computer operating systems (such as Windows, for example) updated:	□ Daily □ Once per week □ 1-4 times a month □ 1-4 times a year □ Never
Section Two: Information on Computer Networking at your Organization		
7)	Does the company utilize an antivirus protection program?	o Yes o No o Don't Know
8)	Does the company utilize a firewall?	o Yes o No o Don't Know
9)	Does your company allow its employees to use company Wi-Fi?	o Yes o No o Don't Know
10)	Does your company provide training to all of its employees regarding maintaining network security?	o Yes o No o Don't Know
11)	Does your company provide training to some of its employees regarding main-	o Yes o No

taining network security?	o Don't Know
12) Employees should be able to surf the internet at any time at your business.	o Yes o No o Don't Know
13) Employees use of the Internet at your business is limited.	o Yes o No o Don't Know
14) Computer users at the business share accounts.	o Yes o No o Don't Know
15) Have there been any known breaches to the network security at your company?	o Yes o No o Don't Know
16) Is there a single employee solely responsible for maintaining network security at your business?	o Yes o No o Don't Know
17) If so, what is his/her job title?	
Section Three: Demographics	
18) Job title of person competing this survey.	Business Owner Manager IT Technician Other
Section Four: Company Income	
19) What is the annual income for your company in US dollar amount?	☐ less than 250,000 ☐ 250,001– 500,000 ☐ 500,001– 750,000 ☐ 750,001– 1 million ☐ 1– 2 million ☐ more than 2 million
Section Five: Essay (Open-Ended Questions)	
20) Identify any potential internal and external threats to your computer network.	Fill in the blank
21) What safety measures are in place to prevent it?	Fill in the blank
22) What might be some successful measures to be added to enhance the protection of your computer network?	Fill in the blank
23) In areas identified as being lacking or susceptible to internal and external threats, what are some reasons why they have yet to be corrected?	Fill in the blank
24) Has anyone in your organizations had their identity, or money such as from debit cards, stolen via a computer at your business?	Fill in the blank