THE SIZE EFFECT OF SCHOOL DISTRICT ON NETWORK SECURITY MANAGEMENT:
A COMPARATIVE ANALYSIS OF RURAL VS CITY PUBLIC SCHOOL DISTRICT’S NETWORK SECURITY IN MISSOURI
by
Shawn E. Bentley

An Abstract
of a thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in
School of Technology
University of Central Missouri

December, 2014
ABSTRACT

by

Shawn E. Bentley

Technology is being used in most school districts. Every school has at least one computer in it. Those schools who connect to the internet and any other outside facilities need to make sure they have the proper network security. The purpose of this study was to determine if smaller public school districts in the state of Missouri have the same proper computer and network security as larger school districts. Further, the study ascertained if there was a difference in the network security training between the large and small school districts in the state of Missouri.

A questionnaire was sent out to 390 school districts attempting to gather the data needed to determine answers to questions. Of the 390 questionnaires sent out, 60 school districts participated this is a 15% return rate.

The data collected from the 60 participants was organized, analyzed, and summarized using descriptive statistics. The questions were analyzed with One-Way ANOVA. The null hypotheses were set at an Alpha 0.05 or 95% level of confidence and probability p-value of .05.

The results are being presented using tables, figures, and narrative descriptions. The statistical package for the Social Sciences (SPSS) was used to analyze the data. The findings suggest at this time there is no statistical difference in network security between the larger and smaller school districts within the state of Missouri. Additionally, the study showed there was no difference in the network security training the faculty and students receive between large and small school districts.
THE SIZE EFFECT OF SCHOOL DISTRICT ON NETWORK SECURITY MANAGEMENT: A COMPARATIVE ANALYSIS OF RURAL VS CITY PUBLIC SCHOOL DISTRICT’S NETWORK SECURITY IN MISSOURI

by

Shawn E. Bentley

A Thesis presented in partial fulfillment of the requirements for the degree of Master of Science in School of Technology University of Central Missouri

December, 2014
THE SIZE EFFECT OF SCHOOL DISTRICT ON NETWORK SECURITY MANAGEMENT: A COMPARATIVE ANALYSIS OF RURAL VS CITY PUBLIC SCHOOL DISTRICT’S NETWORK SECURITY IN MISSOURI

by

Shawn E. Bentley

December, 2014

APPROVED:

Thesis Chair: Dr. Ronnie Rollins

Thesis Committee Member: Dr. Suhansa Rodchua

Thesis Committee Member: Dr. Ronald Woolsey

ACCEPTED:

Chair, School of Technology: Dr. Douglas Koch

UNIVERSITY OF CENTRAL MISSOURI

WARRENSBURG, MISSOURI
AKNOWLEDGEMENTS

I would like to express my gratitude to all of those who made it possible for the completion of this thesis. I want to personally thank the members of my thesis committee. Their support over the last few months have been greatly appreciated.

I would like to particularly thank the chair of my committee, Dr. Ronnie Rollins. He has ensured I stayed on track with my research and writing. He ensured I stayed focused on the task at hand. Dr. Rollins was more than just an advisor he was/is a great mentor for me an all students. Further, I would like to thank Dr. Suhansa Rodchua. Her knowledge in the thesis and research process at the University of Central Missouri was impeccable. Dr. Ronald Woolsey I would like to thank you for approval to move forward with my research and providing a good time schedule via the use of the university’s blackboard service.

On a personal standpoint, I have to thank my loving wife Marcia and our three wonderful children Jordyan, Austin, and Tyler. They have supported me in my decision to continue my education and finish my degree. They have allowed me to give full attention to my studies and I greatly thank them for this. I would have never made it without their loving support and understanding.

Finally, I would like to thank my late grandfather Edward “Hawkeye” Bentley. He was a person who may have only had a sixth grade education but he was very educated on life. He was my mentor and my best friend. He instilled a great work ethic in me and always made me better myself. Without his guidance through life I may not be where I am today.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>LIST OF TABLES</th>
<th>ix</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF FIGURES</td>
<td>x</td>
</tr>
<tr>
<td><strong>CHAPTER 1: NATURE AND SCOPE OF THE STUDY</strong></td>
<td>1</td>
</tr>
<tr>
<td>Statement of Problem</td>
<td>2</td>
</tr>
<tr>
<td>Purpose of Study</td>
<td>3</td>
</tr>
<tr>
<td>Research questions</td>
<td>3</td>
</tr>
<tr>
<td>Research Hypothesis</td>
<td>3</td>
</tr>
<tr>
<td>Limitations of Study</td>
<td>4</td>
</tr>
<tr>
<td>Definition of Terms</td>
<td>4</td>
</tr>
<tr>
<td><strong>CHAPTER 2: REVIEW OF LITERATURE</strong></td>
<td>6</td>
</tr>
<tr>
<td>Summary</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>11</td>
</tr>
<tr>
<td><strong>CHAPTER 3: METHODOLOGY</strong></td>
<td>12</td>
</tr>
<tr>
<td>Participants</td>
<td>13</td>
</tr>
<tr>
<td>Instrumentation</td>
<td>13</td>
</tr>
<tr>
<td>Data Collection</td>
<td>15</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>16</td>
</tr>
<tr>
<td><strong>CHAPTER 4: FINDINGS</strong></td>
<td>17</td>
</tr>
<tr>
<td>Local Area Network (LAN)</td>
<td>18</td>
</tr>
<tr>
<td>Wireless Network Security</td>
<td>21</td>
</tr>
<tr>
<td>Network Security Training</td>
<td>25</td>
</tr>
<tr>
<td>School District and District Administrators Demographic</td>
<td>26</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>33</td>
</tr>
<tr>
<td>Summary of Findings</td>
<td>39</td>
</tr>
</tbody>
</table>
CHAPTER 5: SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS ......41

Summary ...........................................................................................................................................41

Conclusion and Recommendations .................................................................................................44

REFERENCES ....................................................................................................................................46

APPENDICES

A. Network Security Diagram ..........................................................................................................50

B. Questionnaire ..............................................................................................................................51

C. Institutional Review Board (IRB) Approval ..................................................................................57
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How Secure is Your LAN</td>
<td>18</td>
</tr>
<tr>
<td>2. LAN Security</td>
<td>20</td>
</tr>
<tr>
<td>3. How Secure is Your Wireless Network</td>
<td>21</td>
</tr>
<tr>
<td>5. Do You Allow Anyone on Your Wireless Network</td>
<td>24</td>
</tr>
<tr>
<td>6. BYOD</td>
<td>24</td>
</tr>
<tr>
<td>7. Training Conducted</td>
<td>25</td>
</tr>
<tr>
<td>8. Number of Schools in School District</td>
<td>26</td>
</tr>
<tr>
<td>9. Annual IT Budget</td>
<td>28</td>
</tr>
<tr>
<td>10. Percent of Budget Dedicated to Network Security</td>
<td>29</td>
</tr>
<tr>
<td>11. Age of Network Administrators</td>
<td>31</td>
</tr>
<tr>
<td>12. Network Administrators Level of Education</td>
<td>32</td>
</tr>
<tr>
<td>13. ANOVA</td>
<td>37</td>
</tr>
<tr>
<td>14. Training ANOVA</td>
<td>39</td>
</tr>
</tbody>
</table>
### LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Number of Students in School Districts</td>
<td>27</td>
</tr>
<tr>
<td>2. School districts’ network administrators’ gender</td>
<td>31</td>
</tr>
<tr>
<td>3. Who do they work for</td>
<td>32</td>
</tr>
</tbody>
</table>
CHAPTER 1  
NATURE AND SCOPE OF THE STUDY

Computer networks are all around us. For example, they are essential for communication, sharing of knowledge, research and deployment, entertainment, e-commerce and, of course education.

The Internet Protocol (IP), the core the TCP/IP protocol suite, is widespread in today’s high speed computer networks. In comparison to now, the Internet was a closed network in the 1980’s. Academic computing systems were isolated as a result of limited interconnectivity so there was no need to consider security standpoints in the infrastructure design (Jolinas, 2009). However, with the advancement in technology, it seems that any information that academic institutions provide can be obtained through the Internet. Course materials are presented and student assignments are submitted. With the proper credentials, parents can even access school lunch accounts and grades via the Internet.

Mobile technology is transforming the way billions of adults and young adults around the world go about their daily lives. Smart phones and tablet computers have made access to the Internet, personal communication, and learning applications so indispensable that mobile devices are an essential part of daily living. With inventories of mobile devices on the rise and prices in decline (Bailey, Henry, McBride, & Puckett, 2011), mobile devices have found their way into the hands, pockets, and backpacks of millions of American teenagers (Lenhart, Ling, Campbell, & Purcell, 2010). Even more than their parents, teenagers use mobile devices to connect with friends, find inspiration and creative outlets, and work on school projects. Educators have found success implementing mobile devices in the classroom (Gulek & Demirtas, 2005; Hloden, 2010; Kozma, 2005; Messinger, Sparks, Goodale, & McManus, 2011; Motiwalla, 2005; Özdemir, 2005; Jolinas, 2009).
2010). Despite tough financial times districts across the country are looking for ways to provide every student some form of portable computing device (Johnstone, 2003). Every day, millions of American teenagers bring exponentially more computing power to school in their smart phones than all of NASA had when it sent Apollo astronauts to the moon (Kaku, 2011; Robertson, 2009).

Statement of Problem

The Internet and the Bring Your Own Device (BYOD) movements are a great way to communicate and to facilitate learning; however, they both introduce security threats that did not threaten walled-off systems of the past. According to the U.S. Department of Homeland Security, a quarter of all network security problems occur within schools (Technologies, 2009). There are several things that schools have to take into consideration when referring to network security. Installing an antivirus program on computers and not considering other precautionary measures is unacceptable. School districts must now take into account equipment and personnel cost. According to the United States Bureau of Labor Statistics website, the expected annual salary of the typical network administrator in the United States is $77,910 (“Network and Computer Systems Administrators,” 2014). For this reason it may be better to hire a private company to come once a month to ensure the school district’s computer network security and computers are properly maintained. During a personal interview with Peter Camuso from Tech-Savvy Services, he stated “the average monthly cost for his company to maintain the computers and network security for schools would be $300-$900 a month which is considerably cheaper than hiring one person for a day to day network monitoring” (Camuso, 2013).
Purpose of the Study

The purpose of this study is to investigate whether small public school districts in the state of Missouri are as secure as the larger school districts in the state.

Research Questions

1. Are large school districts’ network security more secure than small school districts’ network security?
2. Is there a difference between large and small school district training of faculty and student as it relates to network security?

Research Hypotheses

Question 1

H₀₁= There is no significant statistical difference in the network security within larger school districts compared to smaller school districts.

Hₐ₁= There is a significant statistical difference in the network security within larger school districts compared to smaller school districts.

Question 2

H₀₂= There is no significant statistical difference in the network security training of faculty and students within larger school districts compared to smaller school districts.

Hₐ₂= There is a significant statistical difference in the network security training of faculty and students within larger school districts compared to smaller school districts.
Limitations of Study

1. This evaluation utilizes self-reporting data. Findings of the study are based on perception data of network administrators and the assumption that the network administrators will respond thoroughly and interpret the instrument as intended.

2. The evaluation also suggests that each network administrator has the knowledge, experience, practicality, and education to identify security issues in their school district.

3. The population of the study is limited to the viewpoints of school network administrators in the state of Missouri.

Definition of Terms

Access Control: Restricting who you allow on your network and/or equipment (“What is Access Control?” 2014).

Botnets: Are computers that have been infected by malware. These computers are being controlled from a single source to gain user’s information (“Botnet Definition,” 2014).

Hacking: The act of manipulating technology in any way whether it is legal or illegal (Holt & Schell, p. 17, 2013).

K-12 Rural Public School District: The researcher has determined for the purpose of this evaluation that this is a school district that contains kindergarten through twelfth grade with 600 or fewer students (Rios, 1988).

Malware & Spyware: Unwanted software that has been installed without the user’s knowledge or consent (“Malware: What it is and how to help protect your computer,” 2014).

Phishing: A deceitful email that gives the impression to be coming from a authentic business. The emails are sent in hopes that the end user will open the site and give the network attacker vital personal financial information (“FDIC: Phishing scam,” 2014).
Social Networks (Social Media): The gathering of people on websites that allow them to meet and interact with people via the Internet (Nations, 2014).

Viruses – A malicious software that has been installed within or attached to another piece of computer software without user’s knowledge (Brain & Fenion, 2014).
CHAPTER 2
REVIEW OF LITERATURE

With school systems utilizing more and more computer technology each day, a problem arises of finding a way to ensure that the technology is secure for the students, faculty and staff. There are many types of security threats to a public school’s computers and networks. According to the U.S. Department of Homeland Security, a quarter of all network security problems occur within schools (Technologies, 2009). The main threats to schools, according to WatchGuard Technologies (a provider of internet security), are: Malware, Spyware, Viruses, Botnets, Phishing, Hacking, Access Control, and Social Networks/Media. Further they explained each:

Malware is any software that is installed on a computer willingly or unwillingly that performs unwanted tasks. Spyware is software that surreptitiously gathers information and transmits it to the people who were unauthorized to install it. Spyware is usually unknown to the user and it is attached to something that someone downloads. This could very easily be done in a school system with adolescent children by visiting corrupted websites.

Viruses are software programs that can replicate themselves and can spread from one computer to another. Viruses are usually programmed to damage a computer by deleting files from the computer’s memory. In a school system this can be done by faculty, staff, and students via email.

Botnets is a network of computers that are controlled from a single source for attempting malicious activity such as span. This can be accomplished again via email or downloading of unauthorized files from the internet.
Phishing (fishing) is someone trying to steal a person’s personal information. This is done by the phishers posing as a reputable company such as EBay with a message stating they lost your personal information and need your information back for their system.

Hacking is someone trying to gain unauthorized access to a computer. In the schools system, the trouble is with student hackers who try to gain unauthorized access into the school’s computers that house the secure electronic files and website information.

Access Control is controlling the access to a computer system. This can be accomplished by user names and passwords on each computer and having a login prompt on the school website. The problem with this in schools is the students giving their information to other students. Other students may not be very honest and conduct malicious activity using another student’s information.

Social Networks or Social Media is basically a virtual community of people you may know. The most popular right now is Facebook. Social networks/media are an ideal place for people to push viruses, malware, and for phishing. The students may feel they are secure because they know the people they are talking to online. On the flip side, the people they may know might not have any security setup on the computer they are working with and it may have a virus. The virus can then be passed down to the unknowing student just by clicking on a picture on the other person’s profile (Technologies, 2009).

The last threat, not listed above, is the lack of knowledge. Faculty and staff may not be properly trained in all of the malicious activity that occurs with computers and the network. If they are not properly trained, how can they effectively supervise the students in the computer and
network usage? Just as in a business, the managers have to be trained before they can conduct any training. They have to be trained to ensure the subordinates are doing as they should.

*Internet in Education*

In a study conducted by the Federal Communications Commission (FCC), 97 percent of schools were using the internet in 2010 (Education, 2011). With this, there were still that three percent that were not on the internet. Most often the reason for the non-internet usage was due to funding. The FCC created E-Rate for internet. This is a federal program which helps schools purchase internet. With this, it is easier for schools to get up to date with the newer technology coming about every day.

*Securing the network in a k-12 public school environment*

Today a schools system has to be run as a business data network and not just a home network. Some business networks have built in security features. There are now laws regarding student confidentiality. This law is called Family Educational Rights and Privacy Act (FERPA). With this law, student’s records have to be secured and only accessed by school faculty for faculty use or by faculty for parent use. With this there comes more than just the built in security features of the business data network. There has to be physical security on equipment along with security within the network itself. One of the biggest concerns different from a normal business environment is the students themselves hacking into the system to change files.

One of the main security features of k-12 schools is anti-virus software. The software should be installed on each computer and kept up to date. With email comes the danger of opening a virus infected mail that can damage the computer. Some of the things to look for are and to block on the network are .exe, .vbs, .com, pif, cmd, and .bat files. Another way to help
stop the problems is to establish a list and block prohibited websites (Penner, 2003). For basic network security diagram (Appendix A).

BYOD and Security

With the economy the way it is now, some schools do not have the funding to provide each student with their own computer. There is a new push to allow students to bring in their own laptop through a program called Bring Your Own Device (BYOD). This allows the school to save money on the purchase of computers and save money on the purchase of hardback books due to the students being able to have the eBooks on their own laptop. The one drawback is, the devices may not be secure. With this said, the school has to have a better security system in place. The student will have access to the wireless networks so the schools will have to ensure each student has their own log in to the Wi-Fi system (Ullman, 2011).

Summary

With more and more schools using technology there will be the need for security. With grants and federal programs in place, schools have more access to funds to ensure they have better technology within the schools. Even with the grants the schools receive, there are still ways to save money. Schools can have students bring in their own devices to schools. With the students bringing in their own devices, there will be somewhat a lack of security due to the school not being able to monitor what the student has on their own device. With this the students have the opportunity to conduct malicious activity within the network. One of the biggest treats to a school’s network is the students who attempt to hack into the school’s file system. There was as study done in New York City, New York. The study was conducted by Tufin Technologies (a cyber-security company). They took a questionnaire of 1000 students. Half of the students reported their social media and email accounts were hacked. Sixteen percent of those students
stated they tried to hack themselves (Ash, 2010). To prevent this, the schools need to ensure they implement proper security measures within the network. Schools unlike business, have to ensure they secure students personal information and records. Only the faculty may access the information and share it with other faculty, students and student parents only. With this there has to be stronger security in place to prevent unauthorized access to the information. This can be accomplished by using access control techniques. The simplest access control technique is a login to the schools network and computers. Ensure students, faculty, and staff have to use a username and password to gain access.

Sometimes the students themselves are the biggest threats to a school’s computer network. Students attempt to seek unauthorized access to school’s files in order to change them. Other than the basic access control (usernames and passwords) on the network and computers, the easiest thing to do is install anti-virus software on all of the computers. Ensure the students that bring in their own devices have updated anti-virus software installed as well. Another attempt to secure a network in the school is to ensure the students, faculty, and staff avoid opening any emails that have attachments or links in them from unknown senders. Some of the key items to look for in an email are any files that have .exe, .vbs, .com, pif, cmd, and .bat attached to them.

One of the biggest forms of security is proper training and awareness. If the faculty and staff are not properly trained and informed on the malicious activity that may occur on the computer and computer networks, then how can they effectively ensure the students are adhering to the security standards of the school? This process starts at the top and goes down to ensure the ones in charge are aware of all new technology problems that will occur.
There are very simple ways to ensure the computers and computer networks are secured. The literature suggests there is no way of getting around new technology within the schools. Computers are getting easier and easier to use. Students are getting easier access to computers by bringing their own in to the school. There are computer and network security measures for most situations that will occur in the schools. Technology is constantly changing. As a society it may not be hard to adjust to the newer technology. For small public schools with a small budget may not be able to maintain the newer technology needed to sustain.

At this time there are still some unanswered questions about the research. Are the schools really securing their networks like they should be? If not what are the reasons. As in any business, are the managers getting the proper training so they can in turn ensure the subordinates are doing as they should be when it comes to computers and computer networks? There will need to be some more research to answer these questions. A questionnaire may be sent out to several small rural school districts enquiring about the previous questions. The researcher may need to conduct interviews with the school’s network administrators to answer the questions.
CHAPTER 3
METHODOLOGY

The purpose of this study was to analyze to what extent does school district size impact network security management. This chapter describes the methodology, participants, instrumentation, data collection, validity, reliability, and data analysis.

Methodology

This research study utilized a quantitative approach to answer the stated research questions. In quantitative research, the researcher decides what to study, asks specific narrow questions, collects data from participants, and analyses the data using statistics (Creswell, 2003). Further, quantitative research establishes relationships between measured variables and seeks to explain causes to these relationships (McMillan & Schumacher, 1997). The questionnaire for this research study included several structured closed-response questions. The independent variable will be size of school districts.

Research Questions

The following research questions were formulated to examine the perceptions of network administrators’ within the public school system in the state of Missouri:

1. Are large school districts’ network security more secure than small school districts’ network security?

2. Is there a difference between school district training of faculty and student as it relates to network security?
Research Hypotheses

Question 1

$H_0^1$: There is no significant statistical difference in the network security within larger school districts compared to smaller school districts.

$H_a^1$: There is a significant statistical difference in the network security within larger schools compared to smaller schools.

Question 2

$H_0^2$: There is no significant statistical difference in the network security training of faculty and students within larger school districts compared to smaller school districts.

$H_a^2$: There is a significant statistical difference in the network security training of faculty and students within larger school districts compared to smaller school districts.

Participants

The participants in this research involved network administrators within the public school system in the state of Missouri. Names of network administrators were obtained from the Missouri Department of Elementary and Secondary Education (DESE). In order to generalize findings to Missouri, the researcher used 390 listings of public school districts available from DESE. The researcher’s rationale is to increase accuracy by using the largest sample possible.

Instrumentation

The web-based online instrument called the *School District’s Network Security Questionnaire* was developed by the researcher and implemented via Google Docs. Google Docs is a free, web-based office suite web offered by Google within its Google Drive service. It allows users to create and edit documents online while collaborating with other users.
(Appendix B). The instrument was developed, refined, and adapted from available instruments based on research literature in the field.

The *School District’s Network Security Questionnaire* was divided into five sections. Section I contained nine questions relating to school district. Section II contained five questions relating to the districts’ local area network (LAN). Section III had five questions which solicits wireless network information. Section IV contained seven questions relating to the network administrators’ personal demographic information. Section V allowed the participants to provide additional comments.

Likert scales were chosen based on their ability to measure attitudes, their relative ease of completion by respondents, and the relative ease of scoring and analyzing results when compared to other scales (Likert, 1932). Likert originally stated there are a variety of possible response scales (1 to 7, 1 to 9, 0 to 4, etc.) and the use of odd-numbered scales allows a middle value which is often labeled Neutral or Undecided. However, and Kerlinger stated it is possible to use a force-choice response scale with even number of responses and no middle neutral or undecided choice without jeopardizing statistical validity of results. They concur that when a forced-choice response scale is used, respondents are encouraged to think through their decisions and to avoid the tendency to select a middle-of-the-road response as they are forced to decide whether they lean more towards the agree or disagree end of the scale for each item (Kerlinger, 1986).
Data Collection

Network administrators in the State of Missouri were recruited from a list provided by DESE. The network administrators were contacted via an e-mail; the e-mail would explain the study and invite them to participate. In the case where an e-mail address was not provided, the researcher placed telephone calls to obtain e-mail address. They were made aware of all human participants’ rights and the fact that this study received approval of the Institutional Review Board (IRB) at the University of Central Missouri (Appendix C). In order to participate, the network administrator simply clicked on the link provided to them through the e-mail. The survey was administered over the Internet via a secured website through Google Docs.

Upon reading the confidentiality, consent, and debriefing pages that describe the study, participants could choose to participate, not to participate, or to have their questions answered via email before they participate. Continuation of the survey did imply consent. Because there are no sign in parameters other than clicking on the provided link, the data provided would remain anonymous. Participants read the instructions for completing the survey.

Reliability

To ensure reliability of the instrument, a panel of four computer networking experts and one statistical expert were selected to review the instrument. Each panel member completed an official review and evaluation of the reliability of the instrument.

Validity

A pilot study was conducted to test the online format, questionnaire items, and gathering of data. This process was used to identify problems with the possibility of solving the problems with ease rather than when the main study was underway (Gall, Gall, & Borg, 2003). During the Spring 2014 semester, four industry professionals and one industrial management professional
who were not part of the study, were invited via email to review the online instrument. The professionals were asked for feedback regarding the survey, including ease of taking the survey, clarity of questions, and appropriateness of the study.

Of the five respondents choosing to complete the survey, one had substantial training in research survey, four had extended experience within the computer networking field. Results of the review were positive for all items including instrument construction, content validity, construct validity, face validity, item bias, and consequential validity. The instrument was finalized and administered to the sample population.

Data Analysis

The data from the online survey was organized, analyzed, and summarized using descriptive statistics, including frequencies, percent, means, and standard deviations (Gall, Borg, & Gall, 2003). Findings relating to each research question are presented using tables, figures, and narrative descriptions as appropriate to the data collected. The Statistical Package for the Social Sciences (SPSS), version 19 was used to analyze the data. To answer Research Questions 1 and 2, One-Way ANOVA was used to determine if there is significant difference in the network security within larger schools compared to smaller schools. The null hypotheses were set at an alpha confidence of 95% and probability p-value of .05.
CHAPTER 4
FINDINGS

This chapter presents the results from the data analysis of the information gathered from the questionnaires sent out to the school districts within the state of Missouri. The data collection began on July 28, 2014 and ended on August 28, 2014. In total there were 60 responses out of 390 questionnaires sent out resulting in a 15% return on responses.

As described in Chapter One, the purpose of this study was to decipher whether or not smaller rural school’s computer networks were just as secure as the bigger schools within the state of Missouri. For the purpose of this study the designation of the school district’s size was determined by looking at the United States Department of Education. According to the United States Department of Education, rural (small) school districts consist of student population size fewer than 600 (Rios, 1988). The findings were organized into five subsections.

– Information gathered from school districts Local Area Networks (LANs)
– Information gathered from school districts Wireless Network
– Information gathered on network security training.
– School district and district network administrators’ demographics
– Overall Data Analysis
Local Area Networks (LANs) Security

In the local area network security section there were a total of two questions that are being used in the final analysis. The questions asked were: How the participant felt their Local Area Network security was using a Likert scale. The second question asked the participant what specifically they used to secure their LAN.

Using a Likert scale, the first question the participants answered had the choice of 1=Not secure at all, 2= Somewhat secure, 3=Secure, and 4=Very secure. The results indicated of 60 participants, 17 (28.3 %) selected their LAN was somewhat secure, 33 (55%) selected their LAN was secure, 10 (16.7%) selected their LAN was very secure, and 0 (0%) selected their LAN was not secure at all. Table 1 presents this information

Table 1

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Secure</td>
<td>17</td>
<td>28.3</td>
<td>28.3</td>
<td>28.3</td>
</tr>
<tr>
<td>Secure Secure</td>
<td>33</td>
<td>55.0</td>
<td>55.0</td>
<td>83.3</td>
</tr>
<tr>
<td>Very Secure</td>
<td>10</td>
<td>16.7</td>
<td>16.7</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>

The second question in the local area network security section asked what network security features are utilized within their school districts. This question asked the participant to select from a list of 10 items their school district uses for LAN network security. The list included Access-Lists, Virtual Local Area Networks (VLANS), Filters, Usernames/Passwords,
Demilitarized Zones (DMZ), Virtual Private Networks (VPN), Firewalls, Switchport Security, Anti-Virus, and Intrusion Prevention System (IPS).

The results for the second question indicated of the 60 participants, 22 (36.7%) used access lists and 38 (63.3%) did not use access lists, 36 (60%) used virtual LANs and 24 (40%) did not use virtual LANs, 53 (88.3%) used network filters and 7 (11.7%) did not. The results further indicated 59 (98.3%) used usernames/passwords and 1 (1.7%) participant did not use usernames/passwords, 14 (23.3%) used a DMZ (demilitarized zone) and 46 (76.7%) did not use DMZs, 33 (55%) used VPN (Virtual Private Network) and 27 (45%) did not use VPNs. The results finally indicated 57 (95%) used firewalls and 3 (5%) did not use firewalls, 15 (25%) used switchport security and 45 (75%) did not use switchport security, 58 (96.7%) used anti-virus and 2 (3.3%) did not use any type of anti-virus, 22 (36.7%) used IPS (Intrusion Prevention System) and 38 (63.3%) did not use IPS. Table 2 presents this information.
Table 2

LAN Security

<table>
<thead>
<tr>
<th>Security Type</th>
<th>Selection</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Lists</td>
<td>No</td>
<td>38</td>
<td>63.3</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>22</td>
<td>36.7</td>
</tr>
<tr>
<td>VLANN</td>
<td>No</td>
<td>24</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>36</td>
<td>60</td>
</tr>
<tr>
<td>Filters</td>
<td>No</td>
<td>7</td>
<td>11.7</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>53</td>
<td>88.3</td>
</tr>
<tr>
<td>DMZ</td>
<td>No</td>
<td>46</td>
<td>76.7</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>14</td>
<td>23.3</td>
</tr>
<tr>
<td>VPN</td>
<td>No</td>
<td>27</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>33</td>
<td>55</td>
</tr>
<tr>
<td>Firewalls</td>
<td>No</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>57</td>
<td>95</td>
</tr>
<tr>
<td>Switchport</td>
<td>No</td>
<td>45</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>No</td>
<td>2</td>
<td>3.3</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>58</td>
<td>96.7</td>
</tr>
<tr>
<td>IPS</td>
<td>No</td>
<td>38</td>
<td>63.3</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>22</td>
<td>36.7</td>
</tr>
</tbody>
</table>
Wireless Network Security

This section evaluates the wireless network security within the school districts. In the wireless network security section there were a total of four questions that were being used in the final analysis and they were: how the participant felt as to how secure their wireless network security was utilizing a Likert scale. The next question in part two was asking the participant what security features they use in their wireless network. The third question asked the participant if they allow just anyone to login to their wireless network. Finally, the last question asked the participant if their school district participated in the BYOD concept.

The first question was a Likert scale asking the participants to rate how they felt their wireless network security was. They had the choice of 1=Not secure at all, 2=Somewhat secure, 3=Secure, and 4=Very secure. The results indicate of the 60 participants, 16 (26.7%) selected their wireless network was somewhat secure, 28 (46.7%) selected their wireless network was secure, 13 (21.7%) selected their wireless network was very secure, and 3 (5%) selected their wireless network was not secure at all. Table 3 presents this information.

Table 3

<table>
<thead>
<tr>
<th>How Secure is Your Wireless Network</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Secure</td>
<td>3</td>
<td>5.0</td>
<td>5.0</td>
<td>5.0</td>
</tr>
<tr>
<td>Somewhat Secure</td>
<td>16</td>
<td>26.7</td>
<td>26.7</td>
<td>31.7</td>
</tr>
<tr>
<td>Secure</td>
<td>28</td>
<td>46.7</td>
<td>46.7</td>
<td>78.3</td>
</tr>
<tr>
<td>Very Secure</td>
<td>13</td>
<td>21.7</td>
<td>21.7</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
The second question in the wireless network security section asked what wireless network security features are utilized within their school districts. This question asked the participant to select from a list of eight items their school district uses for wireless network security. The list included Usernames/Passwords, Wired Equivalent Privacy (WEP) Encryptions, Non Broadcasting of Service Set Identifier (SSID), Non Default SSID, Disabled Auto-Connect Features, Wireless Firewalls, Media Access Control (MAC) Filtering, and Static IP Addressing.

The results for the second question indicates of the 60 participants, 51 (85%) used usernames/passwords and 9 (15%) did not use usernames/passwords, 35 (58.3%) used WEP and 25 (41.7%) did not use WEP, 19 (31.7%) used the no broadcast SSID feature and 41 (68.3%) did not use the no broadcast SSID. The results further indicates 18 (30%) used the no default SSID feature and 42 (70%) participants did not use the no default SSID, 5 (8.3%) disabled the auto connect option and 55 (91.7%) did not disable the auto connect option, 44 (73.3%) selected they used wireless firewalls and 16 (26.7%) did not use wireless firewalls. Finally, the results indicated 21 (35%) selected they used MAC filtering and 39 (65%) did not use MAC filtering, 15 (25%) used static IP addressing and 45 (75%) did not use static IP addressing. Table 4 presents this information.
<table>
<thead>
<tr>
<th>Security Type</th>
<th>Selection</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username Passwords</td>
<td>No</td>
<td>9</td>
<td>15.0</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>51</td>
<td>85.0</td>
</tr>
<tr>
<td>WEP</td>
<td>No</td>
<td>25</td>
<td>41.7</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>35</td>
<td>58.3</td>
</tr>
<tr>
<td>No Broadcast SSID</td>
<td>No</td>
<td>41</td>
<td>68.3</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>19</td>
<td>31.7</td>
</tr>
<tr>
<td>No Default SSID</td>
<td>No</td>
<td>42</td>
<td>70.0</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>18</td>
<td>30.0</td>
</tr>
<tr>
<td>Disabled Auto Connect</td>
<td>No</td>
<td>55</td>
<td>91.7</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>5</td>
<td>8.3</td>
</tr>
<tr>
<td>Wireless Firewall</td>
<td>No</td>
<td>16</td>
<td>26.7</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>44</td>
<td>73.3</td>
</tr>
<tr>
<td>MAC Filtering</td>
<td>No</td>
<td>39</td>
<td>65.0</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>21</td>
<td>35.0</td>
</tr>
<tr>
<td>Static IP Addressing</td>
<td>No</td>
<td>45</td>
<td>75.0</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>15</td>
<td>25.0</td>
</tr>
</tbody>
</table>
The third question asked the participant if they let anyone log into their wireless network. The results indicates of 60 participants, 23 (38.3%) allow just anyone to log onto their wireless networks, and 37 (61.7%) do not allow just anyone to log onto their wireless network. Table 5 presents this information.

Table 5

*Do You Allow Anyone on Your Wireless Network*

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>No</td>
<td>37</td>
<td>61.7</td>
<td>61.7</td>
</tr>
<tr>
<td>Yes</td>
<td>23</td>
<td>38.3</td>
<td>38.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The fourth question within this section asks the participant if their school participants in the BYOD (bring your own device) concept on their wireless network. The results indicates of the 60 participants, 33 (55%) use the BYOD concept, and 27 (45%) do not participate in the BYOD concept. Table 6 presents this information.

Table 6

*BYOD*

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>No</td>
<td>27</td>
<td>45.0</td>
<td>45.0</td>
</tr>
<tr>
<td>Yes</td>
<td>33</td>
<td>55.0</td>
<td>55.0</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Network Security Training

This section gathered information regarding the school districts’ network security training. There was one question asked in this section for analysis. The question was as follows: Does your school district provide network security training for faculty and students?

The only question in this section asked the participant if their school district provided network security training to the faculty and students of the district. The results indicates of 60 participants, 37 (61.7%) get network security training, 23 (38.3%) do not received network security training. Table 7 presents this information.

Table 7

<table>
<thead>
<tr>
<th>Training</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>23</td>
<td>38.3</td>
<td>38.3</td>
<td>38.3</td>
</tr>
<tr>
<td>Yes</td>
<td>37</td>
<td>61.7</td>
<td>61.7</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
School District and District Administrators’ Demographic

The school district demographic had nine total questions within it. The first question was attempting to ascertain how many schools were within the individual school districts. The question was broken down into five sections: (1) 1 school, (2) 2 schools, (3) 3 schools, (4) 4 schools, and (5) 5 or more schools. The findings indicate that of the 60 participants, 28 (46.7%) had five or more schools within the district, 4 (6.7%) had four schools within the district, 10 (16.7%) had three schools within their districts, 6 (10%) had two districts within their school districts, and 12 (20%) had only one school within their district. Table 8 presents this information.

Table 8

Number of Schools

<table>
<thead>
<tr>
<th># of Schools</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12</td>
<td>20.0</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10.0</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>16.7</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>6.7</td>
</tr>
<tr>
<td>5+</td>
<td>28</td>
<td>46.7</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100.0</td>
</tr>
</tbody>
</table>

The second question in the school district demographic was asking how many students were enrolled within the school district. The results indicate that of the 60 participants, 17 (28.3%) had 600 students or less, 43 (71.7%) had more than 600 students within the districts. Figure 1 presents this information.
Figure 1. Number of students in school districts. This figure shows the total numbers of students in the school districts.

The third question in the school demographic section queried the participants for their school districts yearly information technology budget. The question provided five levels of responses: (1) $0-$5,000, (2) $5,001-$10,000, (3) $10,001-$15,000, (4) $15,001-$20,000, and (5) $>20,000. The results indicates of the 60 participants, 2 (3.3%) had a budget of $0-$5,000, 3 (5%) had a budget of $5,001-$10,000, 3 (5%) had a budget of $15,001-$20,000, 5 (8.3%) had a budget of $10,001-$15,000, and 47 (78.3%) had a budget greater than $20,000. Table 9 presents this information.
Table 9

*Annual IT Budget*

<table>
<thead>
<tr>
<th>Budget</th>
<th>Frequency</th>
<th>Percent %</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0-$5,000</td>
<td>2</td>
<td>3.3</td>
</tr>
<tr>
<td>$5,001-$10,000</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>$10,001-$15,000</td>
<td>5</td>
<td>8.3</td>
</tr>
<tr>
<td>$15,001-$20,000</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Greater than $20,000</td>
<td>47</td>
<td>78.3</td>
</tr>
</tbody>
</table>

Question four in the school district demographic section was asking the participant what percent of their yearly IT budget is dedicated to their network security. The question was broke down into six sections: (1) 0%-10%, (2) 11%-20%, (3) 21%-30%, (4) 31%-40%, (5) 41%-50%, and (6) greater than 50%. Of the 60 participants, 33 (55%) selected 0%-10% of their IT budget was dedicated to network security, 18 (30%) selected 11%-20% of their IT budget was dedicated to their network security, 5 (8.3%) selected 21%-30% of their IT budget was dedicated to their network security, 1 (1.7%) selected 31%-40% of their IT budget was dedicated to their network security, 1 (1.7%) selected 41%-50% of their IT budget was dedicated to their network security, and 2 (3.3%) selected they dedicated more than 50% of their IT budget to their network security. Table 10 presents this information.
Table 10

Percent of IT Budget Dedicated to Network Security

<table>
<thead>
<tr>
<th>Percent of Budget</th>
<th>Frequency</th>
<th>Percent%</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%-10%</td>
<td>33</td>
<td>55</td>
</tr>
<tr>
<td>11%-20%</td>
<td>18</td>
<td>30</td>
</tr>
<tr>
<td>21%-30%</td>
<td>5</td>
<td>8.3</td>
</tr>
<tr>
<td>31%-40%</td>
<td>1</td>
<td>1.7</td>
</tr>
<tr>
<td>41%-50%</td>
<td>1</td>
<td>1.7</td>
</tr>
<tr>
<td>Greater than 50%</td>
<td>2</td>
<td>3.3</td>
</tr>
</tbody>
</table>

The fifth question in the school district demographic was asking the participant how many computers are used within the school districts. This question was broke down into six sections: (1) 0-10, (2) 11-20, (3) 21-30, (4) 31-40, (5) 41-50, and (6) greater than 50. Of the 60 participants, only selected two of the six sections were selected. The results indicated 1 (1.7%) had 21-30 computers within their school district, and 59/98.3% had more than 50 computers within their district.

The sixth question in the school district demographic was asking the participants of they use laptops, desktops or tablets within their school districts. Of the participants, all 60 selected they all use laptops and desktops. There were 54 (90%) that use tablets within their school district. This left 6 (10%) of the participants did not use tablets within their perspective school districts.
The seventh through ninth questions in the school district demographic asked the participants who their primary vendors were for their laptops, desktops and tablets. The question was broken down into the different vendors along with a section for any vendor not listed. The results indicates of the 60 participants, 20 (33.3%) selected their laptop vendor was Dell, 3 (5%) selected Macintosh was their primary vendor of their laptops, 7 (11.7%) used Hewett Packard as their primary vendor for laptops, 9 (15%) used Chromebooks as their primary laptops, 12 (20%) used Lenovo as their primary vendor for their laptops, and 4 (6.7%) use vendors that were not listed. For some reason 5 (8.3%) selected N/A as they did not have Laptops even though all participants selected they all used laptops.

Of the participants that used tablets 44 (73.3%) used Apple Ipads as their tablet devices. Two (3.3%) participants selected Asus as their primary vendor of their tablets. Two (3.3%) selected Samsung as their primary tablet vendor.

The next section of this part was the school district network administrator demographic. In this section there were four major questions: Gender, Age, level of education, and employed with school district or an outside agency. Of the 60 participants 45 (75%) of the network administrators were male while 15 (25%) were female. Figure 2 presents this information. Of the 60 participants, 30% was in the 35-44 age group. This was the highest selection. The second section was the ages of 45-54. Table 11 presents this information. Of the participants, 27 (45%) has some sort of a Master’s Degree as the highest level of education. Table 12 presents this information. Of the participants, 56 (93.3%) work from an outside agency and not for the school district. Figure 3 presents this information.
Figure 2. School districts’ network administrators’ gender. This figure shows the breakdown of the school districts’ network administrators’ genders.

Table 11

*Age of Network Administrators*

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Frequency</th>
<th>Percent%</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>2</td>
<td>1.7</td>
</tr>
<tr>
<td>25-34</td>
<td>13</td>
<td>21.7</td>
</tr>
<tr>
<td>35-44</td>
<td>18</td>
<td>30</td>
</tr>
<tr>
<td>45-54</td>
<td>16</td>
<td>26.7</td>
</tr>
<tr>
<td>55-64</td>
<td>11</td>
<td>18.3</td>
</tr>
<tr>
<td>65 or older</td>
<td>1</td>
<td>1.7</td>
</tr>
</tbody>
</table>
Figure 3. Who do they work for? This figure shows the numbers on whether the school districts’ network administrators work for the school of an outside agency.

Table 12

*Network Administrator Level of Education*

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid High School/GED</td>
<td>6</td>
<td>10.0</td>
<td>10.0</td>
<td>10.0</td>
</tr>
<tr>
<td>Associate's Degree</td>
<td>8</td>
<td>13.3</td>
<td>13.3</td>
<td>23.3</td>
</tr>
<tr>
<td>Bachelor's Degree</td>
<td>17</td>
<td>28.3</td>
<td>28.3</td>
<td>51.7</td>
</tr>
<tr>
<td>Master's Degree</td>
<td>27</td>
<td>45.0</td>
<td>45.0</td>
<td>96.7</td>
</tr>
<tr>
<td>Doctoral Degree</td>
<td>2</td>
<td>3.3</td>
<td>3.3</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td>100.0</td>
<td>100.0</td>
<td></td>
</tr>
</tbody>
</table>
Data Analysis

The first research question for this research: Are large school districts’ network security more secure than small school districts’ network security? The calculation of the one-way Anova was performed to test this hypothesis; the F value was calculated at the level of 0.05 statistical significance.

Table 13 displays the ANOVA results for research question one. The reliability was used in this ANOVA calculation, each part was compared together. There are 21 variables being compared within this section. All the variables are being compared between the large and small school districts.

The first variable being compared was the question of how secure they felt their LAN was, the F statistic is 1.703. The observed significance level is 0.197, so the null hypothesis is not rejected. There is no significant statistical difference in how the participants felt their network security was. The second variable being compared was the question of the use of Access Lists, with the F statistic of 0.524. The observed significance level is 0.472, so the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security. The third variable being compared was the use of virtual local area networks, the F statistic is 10.568. The observed significance level is 0.002, so the null hypothesis is rejected. There is a significant statistical difference in this selection of network security.

The fourth variable being compared was the use of network filters, the F statistic is 3.310. The observed significance level is 0.074, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security. The fifth variable being compared was the use of LAN usernames/passwords, the F statistic is 2.598. The observed
significance level is 0.112, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The sixth variable being compared was the use of a DMZ, the F statistic is 1.768. The observed significance level is 0.189, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security. The seventh variable being compared was the use of VPNs, the F statistic is 3.836. The observed significance level is 0.055, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The eighth variable being compared was the use of LAN Firewalls, the F statistic is 0.038. The observed significance level is 0.847, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security. The ninth variable being compared was the use of switchport security, the F statistic is 0.026. The observed significance level is 0.871, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The tenth variable being compared was the use of anti-virus software, the F statistic is 0.466. The observed significance level is 0.498, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security. The eleventh variable being compared was the use of intrusion prevention system, the F statistic is 0.524. The observed significance level is 0.472, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The twelfth variable being compared was how the participant felt their wireless security was, the F statistic is 1.465. The observed significance level is 0.231, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security. The
thirteenth variable being compared was the use of wireless usernames/passwords, the F statistic is 1.535. The observed significance level is 0.220, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The fourteenth variable being compared is the use of wired equivalent privacy (WEP) encryption, the F statistic is 0.276. The observed significance level is 0.602, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The fifteenth variable being compared is the use of a no broadcast SSID feature, the F statistic is 0.710. The observed significant level is 0.403, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The sixteenth variable being compared is the use of the no default SSID feature, the F statistic is 0.004. The observed significant level is 0.951, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The seventeenth variable being compared is the use of the disabled auto connect feature, the F statistic is 2.162. The observed significant level is 0.147, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The eighteenth variable being compared is the use of a wireless firewall, the F statistic is 2.578. The observed significant level is 0.114, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

The nineteenth variable being compared is the use of MAC filtering, the F statistic is 6.005. The observed significant level is 0.017, the null hypothesis is rejected. There is significant statistical difference in this selection of network security.

The twentieth variable being compared is the use of static IP addressing, the F statistic is 1.326. The observed significant level is 0.254, the null hypothesis is not rejected. There is no
significant statistical difference in this selection of network security. The twenty-first variable being compared is asking the participant if they allow just anyone to log into their wireless network, the F statistic is 0.782. The observed significant level is 0.380, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security. The twenty-second and last variable being compared for the first research question asked the participant if they participate in the BYOD (bring your own device) concept, the F statistic is 3.836. The observed significant level is 0.055, the null hypothesis is not rejected. There is no significant statistical difference in this selection of network security.

Even though two variables (VLAN and MAC Filtering) rejected the null hypothesis, after comparing all the variables together within the one-way ANOVA, it was overall determined the null hypothesis was not rejected. There is no major significant statistical difference in the network security between large and small school districts. Table 13 presents this information.
Table 13

ANOVA

<table>
<thead>
<tr>
<th>Variable</th>
<th>F Statistic</th>
<th>Significant Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>How secure is LAN</td>
<td>1.703</td>
<td>0.197</td>
</tr>
<tr>
<td>Access Lists</td>
<td>0.524</td>
<td>0.472</td>
</tr>
<tr>
<td>VLAN</td>
<td>10.568</td>
<td>0.002</td>
</tr>
<tr>
<td>Filters</td>
<td>3.310</td>
<td>0.074</td>
</tr>
<tr>
<td>LAN Username/Password</td>
<td>2.598</td>
<td>0.112</td>
</tr>
<tr>
<td>DMZ</td>
<td>1.768</td>
<td>0.189</td>
</tr>
<tr>
<td>VPN</td>
<td>3.836</td>
<td>0.055</td>
</tr>
<tr>
<td>LAN Firewall</td>
<td>0.038</td>
<td>0.847</td>
</tr>
<tr>
<td>Switchport Security</td>
<td>0.026</td>
<td>0.871</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>0.466</td>
<td>0.498</td>
</tr>
<tr>
<td>IPS</td>
<td>0.524</td>
<td>0.472</td>
</tr>
<tr>
<td>How Secure is Wireless Network</td>
<td>1.465</td>
<td>0.231</td>
</tr>
<tr>
<td>Wireless Username/Password</td>
<td>1.535</td>
<td>0.220</td>
</tr>
<tr>
<td>WEP</td>
<td>0.276</td>
<td>0.602</td>
</tr>
<tr>
<td>No Broadcast SSID</td>
<td>0.710</td>
<td>0.403</td>
</tr>
<tr>
<td>No Default SSID</td>
<td>0.004</td>
<td>0.951</td>
</tr>
<tr>
<td>Disabled Auto Connect</td>
<td>2.162</td>
<td>0.147</td>
</tr>
</tbody>
</table>
Table 13

ANOVA Continued

<table>
<thead>
<tr>
<th>Variable</th>
<th>F Statistic</th>
<th>Significant Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Firewall</td>
<td>2.578</td>
<td>0.114</td>
</tr>
<tr>
<td>MAC Filtering</td>
<td>6.005</td>
<td>0.017</td>
</tr>
<tr>
<td>Static IP Addressing</td>
<td>1.326</td>
<td>0.254</td>
</tr>
<tr>
<td>Allow Anyone to Log In</td>
<td>0.782</td>
<td>0.380</td>
</tr>
<tr>
<td>BYOD</td>
<td>3.836</td>
<td>0.055</td>
</tr>
</tbody>
</table>

The second research question: Is there a difference between school district training of faculty and student as it relates to network security? The calculation of the one-way ANOVA was performed to test this hypothesis; the F value was calculated at the level of 0.05 statistical significance. Table 9 shows the ANOVA results for research question two. The variable for this question was if the participant’s school district provided network security training to faculty and students, the F statistic is 0.79. The observed significance level is 0.780, the null hypothesis of no difference is not rejected. There is no significant statistical difference in the network security training between large and small school districts. Table 14 presents this information.
Table 14

*Training ANOVA*

<table>
<thead>
<tr>
<th></th>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Between Groups</td>
<td>.019</td>
<td>1</td>
<td>.019</td>
<td>.079</td>
<td>.780</td>
</tr>
<tr>
<td>Within Groups</td>
<td>14.164</td>
<td>58</td>
<td>.244</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>14.183</td>
<td>59</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Summary of Findings**

The results included a total of 60 respondents who completed the questionnaire. The survey results were gathered from the 60 respondents who were from public school districts within the state of Missouri. The *School District’s Network Security Questionnaire* was divided into five sections. Section I contained nine questions relating to school district.

Section II contained five questions relating to the districts’ local area network (LAN). Section III had five questions which solicits wireless network information. Section IV contained seven questions relating to the network administrators’ personal demographic information. Section V allows the participants to provide additional comments. The questionnaire used multiple choice, Likert scales, multiple selection and fill in the blank questions.

The only sections used to query and answer the research questions were sections II & III. There was one question from section I that was used. This question was the number of students the school district had. The reason for this was due to the variable needed to determine large and small school districts. The questions from sections II & III were regarding the LAN (local area network) and the wireless networks.
After compiling the data from these questions, the researcher determined the overall null hypothesis for question one was not rejected. There were two variables within the data that were rejected: The use of VLANs (virtual local area networks) which had a p-value of 0.002 and the use of MAC filtering which had a p-value of 0.017. For question one, the researcher determined the overall null hypothesis was not rejected as well. As a result, it was determined there is no significant difference in network security between larger and smaller school districts within the state of Missouri. Further, for question two, the researcher determined the overall null hypothesis was not rejected. This too was determined there is no significant difference in the network security training the faculty and students receive from their school districts in the state of Missouri.
CHAPTER 5
SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

This chapter consists of three sections: Summary, conclusions, and recommendations. The first section provides a summary of the statement of problem, purpose of the study, significance of the study, research questions, hypothesis, and findings. The second section concludes the results of this study. The third gives recommendation for further study and conclusion.

SUMMARY

The problem of all the new technology is finding a way to ensure that it is secure. There are many types of security threats to a public school’s computers and networks. According to the U.S. Department of Homeland Security, a quarter of all network security problems occur within schools (Technologies, 2009). There are several things that schools have to take into consideration when referring to network security. They can’t just put an antivirus program on their computers and expect this to ward off all types of network security threats. The other thing the schools will have to consider is the cost. The schools will have to purchase equipment that gives the students access to the internet and the security devices that may go along with it. The schools will then have to train or hire a new person to take care of the equipment and the network. According to the United States Bureau of Labor Statistics website, the expected annual salary of the typical network administrator in the United States is $77,910 (“Network and Computer Systems Administrators,” 2014). For this reason it may be better to hire a private company to come once a month to ensure the school district’s computer network security and computers are up and running as they are supposed to be.
According to Peter Camuso from Tech-Savvy Services, Warrensburg, MO, the average monthly cost for his company to go into a school to maintain the computers and network security would be $300-$900 a month which is considerably cheaper than hiring one person for a day to day network monitoring (Camuso, 2013). There are things the schools need to consider when incorporating new technology into schools. Cost and finding a person to maintain the technology seem to be the important two topics for discussion.

Purpose of the Study

To find out if the smaller public school districts in the state of Missouri have the same proper computer and network security as larger school districts.

Research Questions

1. Are large school districts’ network security more secure than small school districts’ network security?

   Question 1

   H₀₁= There is no significant statistical difference in the network security within larger school districts compared to smaller school districts.

   Hₐ₁= There is a significant statistical difference in the network security within larger school districts compared to smaller school districts.

2. Is there a difference between school district training of faculty and student as it relates to network security?

   Question 2

   H₀₂= There is no significant statistical difference in the network security training of faculty and students within larger school districts compared to smaller school districts.

   Hₐ₂= There is a significant statistical difference in the network security training of faculty and students within larger school districts compared to smaller school districts.
H₂: There is a significant statistical difference in the network security training of faculty and students within larger school districts compared to smaller school districts.

The results included a total of 60 respondents who completed the questionnaire. The survey results were gathered from the 60 respondents who were from public school districts within the state of Missouri. The *School District’s Network Security Questionnaire* was divided into five sections. Section I contained nine questions relating to school district. Section II contained five questions relating to the districts’ local area network (LAN). Section III had five questions which solicits wireless network information. Section IV contained seven questions relating to the network administrators’ personal demographic information. Section V allows the participants to provide additional comments. The questionnaire used multiple choice, Likert scales, multiple selection and fill in the blank questions.

The only sections used to query and answer the research questions were sections II & III. There was one question from section I that was used. This question was the number of students the school district had. The reason for this was due to the variable needed to determine large and small school districts. The questions from sections II & III were regarding the LAN (local area network) and the wireless networks.

After compiling the data from these questions, the researcher determined the overall null hypothesis for question one was not rejected. There were however, two variables within the data that were rejected, the use of VLANs (virtual local area networks) which had a p-value of 0.002 and the use of MAC filtering which had a p-value of 0.017. For question two, the researcher determined the overall null hypothesis was not rejected as well. As a result, it was determined there is no significant statistical difference in network security between larger and smaller school districts within the state of Missouri. The results also showed there is no significant statistical
difference in the network security training of faculty and student between larger and smaller school districts in the state of Missouri.

CONCLUSION and RECOMMENDATIONS

With technology being the forefront of the way many schools are teaching now, network security should be a major concern. One would think that the larger school districts with the most money would have a securer network than those school districts with smaller budgets. One would also think with network security there should be adequate training for the students and faculty. One could also think that the larger school districts would have the better training since they have the better network security.

The findings of this research included that there was no significant difference in the network security and network security training between large and smaller school districts within the state of Missouri. Of the 390 questionnaires sent out, only 60 participated in the study. This resulted in a 15% return rate. Out of the 60 participants, 43 (72%) were from school districts with more than 600 students; leaving 17 (28%) from 600 or less students (See Figure 1).

From the additional comment responses some of the participants left show there is quite a lack of user awareness when it comes to computer network security. Some of the major problems that the participants noted were the lack of care for network security. One participant stated, “It is hard, especially in larger schools, to get the users to adhere to network security protocols”.

Some of the additional problems the network administrators are facing stem from users using school computers to look at online pornography, users opening virus infected emails, users selling wireless network passwords, and students and faculty not getting proper training. Some other administrators have a problem with this network security due to having to ensure the network does not interfere with the educational process.
For future research, the researcher could look at the gender makeup of network administrators. The research showed of the 60 participants 45 (75%) were male network administrators with 15 (25%) as female network administrators (See Figure 2). In addition, the study revealed that 20% (12) were between the ages of 55 and older. Further research could be conducted to see if this population is getting up-to-date training and/or pursing retiring. Finally, this researched exposed the outsourcing of school districts IT support to an outside agency; 93% of the network administrators worked for an outside agency instead of the school districts.

REFERENCES
http://www.excitingip.net/27/a-basic-enterprise-lan-network-architecture-block-diagram-and-components/


APPENDIX A

Network Security Diagram

(A Basic Enterprise LAN Network Architecture-Block Diagram and Components, 2010)
APPENDIX B
Questionnaire

School District's Network Security Questionnaire

This questionnaire is being conducted by Shawn Bentley, a graduate student at the University of Central Missouri. The purpose is to obtain information on network and information security for school districts in MO. The submission of your responses will remain anonymous, and will in no way be connected with your school.

This questionnaire is related to your school district’s network security infrastructure. This questionnaire is intended for the computer network professional in charge of your school district’s computer network. Please answer the following questions by selecting the choice or filling in the blank when appropriate; your responses will be held in strict confidence. No questions ask for your school’s name and address.

Thank you for participating in this endeavor. If you have any questions please contact Shawn Bentley at seb21460@ucmo.edu

Respectfully,
Shawn Bentley

* Required

By clicking below you are consenting to participate in this questionnaire. *

I understand and consent to participate

Continue »

16% completed
School District's Network Security Questionnaire

* Required

Part 1: General information about your School District

How many schools are within your school district? *
- 1
- 2
- 3
- 4
- >5

How many students do you have within your district? *
- <100
- 100-200
- 201-400
- 401-600
- >600

What is your school district’s yearly IT budget? *
- $0-$5,000
- $5,001-$10,000
- $10,001-$15,000
- $15,001-$20,000
- $20,000

Of your IT budget, what percentage is dedicated to your network security? *
- 0%-10%
- 11%-20%
- 21%-30%
- 31%-40%
- 41%-50%
- >50%

How many computers are in your school district *
- 0-10
- 11-20
- 21-30
- 31-40
- 41-50
- >50

What types of computers does your school district use? (Select all that apply) *
- Laptops
- Tablets
- Desktops

Who is the primary vendor of your school district’s laptops? (If you do not have any please put n/a in other block) *
- Dell
- Macintosh
- Hewlett-Packard
- Asus
- Chromebook
- Lenovo
- Other

Who is the primary vendor of any tablet devices? (If you do not have any please put n/a in other block) *
- Apple Ipad
- Asus
- Samsung
- RCA
- Hisano
- Nexus
- Microsoft
- Other

What is the primary vendor of your school district’s desktop computers? (If you do not have any please put n/a in other block) *
- Dell
- Hewlett-Packard
- Macintosh
- Compag
- Other
School District's Network Security Questionnaire

Part 2: Information on District's Local Area Network (LAN)

How would you rate your school district's LAN network security? *

<table>
<thead>
<tr>
<th>Not Secure at all</th>
<th>Somewhat Secure</th>
<th>Secure</th>
<th>Very Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How Secure? [ ]  [ ]  [ ]  [ ]  [ ]

What operating system are on your school district's computers? (Choose all that apply) *

- [ ] Windows XP
- [ ] Windows 7
- [ ] Windows Vista
- [ ] Windows 8(8.1)
- [ ] MAC System
- [ ] Linux System

What network security features are utilized within your school district? (Check all that apply) *

- [ ] Access-Lists
- [ ] Virtual Local Area Networks (VLANS)
- [ ] Filters
- [ ] Usernames/Passwords
- [ ] Demilitarized zones (DMZ)
- [ ] Virtual Private Networks (VPN)
- [ ] Firewalls
- [ ] Switchport Security
- [ ] Anti-Virus
- [ ] Intrusion Prevention System (IPS)
- [ ] Other: _______________________

Is your school district's computer network equipment stored secured or unsecured? *

- [ ] Secured
- [ ] Unsecured

Does your school district train faculty and students on proper computer network security measures? If so how? *

______________________________
School District's Network Security Questionnaire

* Required

Part 3: Information on District's Wireless Network

Does your school district have a wireless network? *

- Yes
- No

How would you rate your school district's wireless network security? *

<table>
<thead>
<tr>
<th>Not Secure</th>
<th>Somewhat Secure</th>
<th>Secure</th>
<th>Very Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What wireless network security features are utilized within your school district? (Check all that apply) *

- Usernames/Passwords
- Wired Equivalent Privacy (WEP) Encryptions
- Non Broadcasting of Service Set Identifier (SSID)
- Non Default SSID
- Disabled Auto-Connect Features
- Firewalls
- Media Access Control (MAC) Filtering
- Static IP Address
- Do Not Have a Wireless Network
- Other: ___________________________

Do you allow anyone on your wireless network? *

- Yes
- No
- Do not have a wireless network

Does your school district support the Bring Your Own Device (BYOD) concept? *

- Yes
- No
- Do not have wireless network

[Progress bar: 66% completed]
School District's Network Security Questionnaire

* Required

Part 4: Personal Demographic

What is your gender? *
- Male
- Female

What is your age range? *
- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55-64 years old
- >64 years old

What is your highest level of education? *
- High School/GED
- Associate's Degree
- Bachelor's Degree
- Master's Degree
- Doctoral Degree

What is your highest IT related degree in? *

What is your job title? *

Are you a staff member of the school district or work for an outside agency? *
- School District
- Outside Agency

Please indicate any IT related certificates/certifications you may have. *

[Form fields]

[Progress bar: 83% completed]
School District's Network Security Questionnaire

* Required

**Part 5: Conclusion**

What problems have you had with your school district’s network security? *

[Text box for input]

Please leave any additional comments here, thank you. *

[Text box for input]

Thank you for completing this questionnaire. For further questions please contact Shawn Bentley at seb21460@ucmo.edu

Never submit passwords through Google Forms.

100%: You made it.
APPENDIX C
IRB APPROVAL LETTER

6/19/2014

Shawn Bentley
seb21460@ucmo.edu

Dear Shawn Bentley,

Your research project, 'The Size Effect of School District on Network Security Management: A Comprehensive Analysis of Rural vs City School District's Network Security in Missouri', was approved by the Human Subjects Review Committee on 6/18/2014. This approval is valid through 6/18/2015.

Please note that you are required to notify the committee in writing of any changes in your research project and that you may not implement changes without prior approval of the committee. You must also notify the committee in writing of any change in the nature or the status of the risks of participating in this research project.

Should any adverse events occur in the course of your research (such as harm to a research participant), you must notify the committee in writing immediately. In the case of any adverse event, you are required to stop the research immediately unless stopping the research would cause more harm to the participants than continuing with it.

At the conclusion of your project, you will need to submit a completed Project Status Form to this office. You must also submit the Project Status Form if you wish to continue your research project beyond its initial expiration date.

If you have any questions, please feel free to contact me.

Have a Healthy Day and Fruitful Research!

Dr. Janice Putnam
Professor of Nursing
Research Compliance Officer
ADM 214 University of Central Missouri
Warrensburg, MO 64093
*putnam@ucmo.edu*

Confidentiality Notice & Disclaimer: This email and any attachments may be confidential and may contain privileged information. If you are not the intended recipient, please notify the sender that you received the message in error. Please do not copy, distribute or use this email.