Phoenix Corporation

Interoffice Memo **Proposal**

To: Dr. Janet Stiers, Director
CC: Chad Lyles, Facilitator
From: Jarrod Sawyer, College Intern
RE: Proposal for Securing Small Business Computer Networks and Data
Date: January 21, 2011

The purpose of this proposal is to obtain approval to research and identify the best way to secure a small business's computer systems and data from cyber attack.

Introduction

In recent years, cybercrime[1] has increased and it is becoming more important for people to protect their computers and data just as they do their homes. The increased need for protection also applies to small businesses. Small businesses keep track of costumer financial information, their own financial information, their product information, and company specific data. With this wealth of information and the increase in cybercrime, small businesses need an effective solution to protect their computer systems and data from cyber attackers.

Small business computer and data security is an important issue that needs solving. Research is necessary to identify what small business owners need to do in order to protect themselves and their customers from the risk associated with data compromise. Small businesses handle a lot of financial transactions and need to protect their data. If the data were to be compromised, hundreds of people would be at risk of identity theft and the small business would be at risk of going out of business. Another reason this project is important is most security recommendations are made to large corporations and government. The security level that large corporations and government need, a lot of times, is much more than a small business needs. Therefore, I think that it is important to provide security solutions that apply specifically to small businesses.

I am a senior at Louisiana Tech University in Ruston, Louisiana, pursuing my Bachelors of Science degree in Computer Science with a minor in Business Administration and have held two internships prior to my internship at Phoenix Corporation. My school and work experience has provided me with a good understanding of the computer science and cyber security industries and qualifies me to work on this research project. Studying computer science for over three years has allowed me to complete all of the computer science classes

[1] "The crimes or harms that result from opportunities created by networked technologies" (Wall 46).

required for graduation, take two cyber security courses, and participate in a cyber security competition. Two previous internships have given me real world cyber security experience by requiring me to attended cyber attack and information security training.

Current Situation

The problem's current situation is described by the causes and effects of the problem, the possible solutions to the problem, the project's scope, and the context of research. The causal analysis describes the problem's causes and effects. The possible solutions section identifies two solutions to the problem already in practice and an innovative solution to the problem. The scope explains the topics that the project will not address, and the context of research describes the project's research plan.

Causal Analysis

Multiple factors contribute to small businesses' need for a computer and data security plan. One issue that contributes to the problem is that employees are ignoring company security protocols (Siponen, Mahmood, and Pahnila 145). According to "Are Employees Putting Your Company at Risk by Not Following Information Security Policies?," "91% of organizations' own employees frequently fail to adhere to information security policies" (Siponen, Mahmood, and Pahnila 145). The effects of employee ignorance are far reaching. Of the forty-seven percent of small businesses that have experienced some sort of data loss, sixteen percent of the loss came from inside of the company (Mamidi 3). Data loss is a serious matter and can result in many different consequences for the business ranging from lost profits to legal action (Siponen, Mahmood, and Pahnila 145).

Another cause of the problem is many small businesses only have a small information technology department or no information technology department at all (Hoffman 1; Mamidi 2). Not having enough people to go around causes the businesses to "often have a huge gap in their security policies regarding behavior and best practices" (Hoffman 1; Mamidi 3). Therefore, even if the company's employees did follow security policies the gaps in the policy still may make the company vulnerable.

An issue that also contributes to the problem is that "SMBs [small-and-medium-sized businesses] are more focused on keeping the business operating rather than strategically planning for future threats" ("80% of Small-to Medium-sized Firms" 3). Small business information technology employees have to worry more about keeping the business's computer systems and network up-and-running ("80% of Small-to Medium-sized Firms" 3). The focus's effect is that small businesses are "less able to take a proactive approach to security threats" ("80% of Small-to Medium-sized Firms" 3). They do not have time to worry about what may happen in the future ("80% of Small-to Medium-sized Firms" 3).

A fourth cause of the computer and data security problems small businesses are having is how easy it is for almost anyone to create harmful software (Giles 1). It is easier now, more than ever, for almost anyone to create harmful software and deploy it to “steal a fortune in cash or get a hold of government documents” (Giles 1). The “low barrier to entry” (Giles 1) results in attacks being more prevalent because more people can launch them (Giles 1).

Another factor that contributes to the problem is the low amount of funding that small businesses have to dedicate to security (Hoffman 1; Mamidi 2). Due to the low funding of small businesses and the high spending of larger corporations on security, small businesses are a prime target for cybercrime (Wilson 1). In fact, “85 percent of the fraud we see in business occurs in small and medium-sized businesses” (Wilson 1). Also due, in part, to low funding, many small businesses do not even implement basic security techniques (Hoffman 1; Mamidi 2). According to both Tim Wilson in “Small Business: The New Black in Cybercrime Targets” and Ashesh Mamidi in “Small Businesses Hammered by Cybercrime,” “Nearly one-fifth of small businesses don’t even use antivirus software. Sixty percent don’t use any encryption on their wireless links, and two-thirds of small businesses don’t have a security plan in place” (Wilson 1; Mamidi 3). The lack of basic security measures leaves small businesses wide open for cyber attack and data compromise.

Possible Solutions

The problem small businesses are facing with securing their computer systems and data from cyber attack is very serious. If nothing is done about the problem, small businesses everywhere could be in danger of going out of business or, at the very least, suffering from reduced productivity due to cyber attacks (Mamidi 3). Unchecked, the problem could result in “dramatic loss of revenue for these entrepreneurial enterprises in the years ahead” (Mamidi 1). Doing nothing about this problem is certain to be harmful to small businesses everywhere.

Based on preliminary research, two solutions that are currently being implemented to solve the problem have been identified as well as an innovative solution to the problem. The solutions that are already being implemented are a basic and an advanced plan for securing a small business’s computer systems. The innovative solution focuses on enhancing the basic plan with a feature similar to the advanced plan’s added feature as well as some new improvements.

The first solution already in practice involves “securing core vulnerabilities” (Kaven 103) of the small business’s network and computer systems (Kaven 103). The plan involves securing four vulnerable areas which are “[the company’s] gateway, wireless networks, desktops and servers, and backup systems” (Kaven 103):

- ***Gateway:*** Concerned with securing the entry and exit point of the business’s internet traffic (Kaven 104).
- ***Wireless Networks:*** Deals with securing the business’s wireless network(s) so that wireless traffic cannot be monitored by people unauthorized to access the network (Kaven 105).
- ***Desktops and Servers:*** Concerned with making sure software is up-to-date, that the systems have antivirus programs installed, users have limited system control (Kaven 106),

and “content filtering” (“Internet Security Issues and Solutions” 7) is in place.

- ***Backup Systems:*** Pertains to making sure that critical data is backed up and stored in a safe place in case something happens (Kaven 106-107).

The second solution already in practice involves all of the elements from the basic security plan with the addition of a “security monitoring system”[2] (Priescu and Nicolăescu 53). A“security monitoring system”[2] (Priescu and Nicolăescu 53) can be implemented in four ways which are Compliance Monitoring, Vulnerability Monitoring, Systems Security Monitoring, and Network Security Monitoring (Priescu and Nicolăescu 53-56):

- ***Compliance Monitoring:*** Events in the business’s systems and network are compared to a defined security policy (Priescu and Nicolăescu 53). If an event breaks the security policy, it could be an attack and is flagged for further analysis and addition to the security policy (Priescu and Nicolăescu 54).
- ***Vulnerability Monitoring:*** Constantly scans the business’s computer systems for software and configuration vulnerabilities (Priescu and Nicolăescu 54). If a system is found to have vulnerabilities, it can be updated and the vulnerabilities fixed (Priescu and Nicolăescu 54).
- ***Systems Security Monitoring:*** Compares a “known good [system] state or policy” (Priescu and Nicolăescu 55) to the current system state or policy (Priescu and Nicolăescu 55). If there is a difference between the two, it could signify an intrusion or attack and is flagged for further analysis (Priescu and Nicolăescu 55).
- ***Network Security Monitoring:*** Monitors network traffic for violations of a defined security policy (Priescu and Nicolăescu 56). If a violation is detected it could indicate an intrusion (Priescu and Nicolăescu 56).

The innovative solution to the problem takes the basic plan and enhances it with additional features which are an intrusion detection system, data encryption, and a policy that dictates what employees are allowed to do on the internet (Klein 3):

- ***Intrusion Detection System:*** Concerned with trying to identify if an attack is imminent and with identifying if there is an attack (Maiwald 278).
- ***Data Encryption:*** Concerned with allowing “the organization to protect the confidentiality of sensitive or critical information” (Calder 276).
- ***Internet Policy:*** Concerned with limiting what employees can do on the internet, educating them on safe internet practices, and monitoring what they do to ensure they are not violating policy (Klein 3).

Scope

Due to the expansiveness of the cyber security industry and the project’s time constraints, the project will not address a few topics regarding the problem. The first topic that will not be discussed is securing the computer systems and data of small businesses that do government contracting. The government requires businesses to implement special security measures

[2] “The Primary goal of a security monitoring system is to help identify suspicious events on a network that may indicate malicious activity or procedural errors” (Priescu and Nicolăescu 53).

when they are dealing with government data, especially, classified data. The project is more concerned with finding a security solution for generic small businesses not with finding ways to implement government level security.

The project will also be unable to recommend specific products that implement security measures outlined in the problem's best solution. Hundreds of security products exist such as antivirus programs, firewall programs, and specialized hardware. The product that the business needs to use will depend on the business's specific situation and will be different for most businesses. Neither the time nor the funds will be available to research and test each product nor will each small business's specific situation be known in order to make an accurate recommendation.

The third topic that will not be covered is the physical security of a small business's computer systems and data. Data can also be compromised through unauthorized physical access to the business's computers. The project is only concerned with securing a small business's computer systems and data from attacks launched without physical access to the computer systems or data and attacks that are inadvertently let in by those with physical access.

The last topic that will not be addressed is the specific instructions on how to implement the security measures recommended by the solution identified to be the best. Setting up security measures such as wireless network encryption is a hardware and software specific task. Listing the steps required to implement each security measure for each hardware and software configuration that a small business may have would be infeasible if not impossible.

Context of Research

All project research will be gathered from the Louisiana Tech University Library and the Internet. The research efforts will be focused on the causes and effects of the problem, solutions to the problem that are currently being implemented, and an innovative solution to the problem. All of the research will be secondary research in the form of two books, five journal articles, and five Internet websites. If two books or five Internet websites are unable to be found, they will be supplemented with journal articles. The purpose of the research is to gain a full understanding of the problem, identify possible solutions to the problem, and help determine the problem's best solution. The research will not only be used in the writing of this proposal but also as the starting place for the extended definition and technical report that will follow the proposal.

The remainder of the proposal will be focused on presenting the project plan, my qualifications, the project's costs and benefits, and the references used.

Project Plan

The project plan's purpose is to present a plan for determining the best way to secure a small business's computer systems and data from cyber attack. The eight step project plan is directed at cyber security professionals with a degree or high end secondary education in computer science or a comparable field. Each step of the project plan addresses applicable preliminary concerns such as costs, benefits, qualifications, and research concerns so that error in carrying out the plan can be avoided. During the project plan's execution, notice will be taken to avoid any biased, incorrect, unqualified, or old research. The project plan shows how I, ideally, intend to find a solution to the problem, and its execution guarantees that a solution will be found. The project plan also includes the project's Gantt chart. The Gantt chart represents all of the minor projects that must be completed in order to complete the project. The project plan's steps correspond to the minor projects listed in the Gantt chart. Step two of the project plan corresponds to the internal proposal. Step three corresponds to the extended definition. Steps four through eight correspond to the technical report.

Projects	Dates of Completion							
	JAN 7	JAN 14	JAN 21	JAN 28	FEB 4	FEB 7	FEB 11	FEB 14
1. Gather Research	🟫	🟫						
2. Write Internal Proposal			🟫					
3. Write Extended Definition				▨				
4. Write Progress Report					▨			
5. Write Technical Report						▨	▨	▨

Table 1: Gantt Chart Timeline for the Project

1. *Gather additional research.*

- Obtain two books from the Louisiana Tech University Library or the Internet (e-books).
- Obtain five journal articles from the Louisiana Tech University Library.
- Obtain five online sources.
- Supplement journal articles from the Louisiana Tech University Library if books or online sources cannot be found.

2. *Identify two solutions to the problem that are already in practice.*

- Use research to identify two solutions to the problem already in practice.
- Gain a complete understanding of the two solutions to the problem.

3. *Define an innovation.*

- Use research to define an innovative solution to the problem.
- Present the solution's definition in the extended definition.

4. *Compare and contrast all three of the solutions.*

- Determine each solution's pros and cons.
- Compare the three solutions based on their pros and cons.

5. Perform a criteria analysis.

- On a scale from one to five where one is the weakest and five is the strongest, rank the strength of each solution per criteria defined in step four.
- Add up each solution's rankings.
- Eliminate the solution with the lowest ranking.
- If a tie occurs, further analyze the solutions involved in the tie and determine the best solution.
- Prepare a graphic for the technical report that presents the results of the analysis.

6. Perform a feasibility test.

- Determine through research at least three criteria that the problem's best solution should possess.
- Take the two solutions resulting from step five and rate them as pass or fail for each of the criteria.
- Choose the most feasible solution to the problem based on the ratings.
- If a tie occurs, further analyze the two solutions and determine the best solution.
- Prepare a graphic for the technical report that presents the test's results.

7. Recommend the best solution.

- Recommend the best solution to the problem based on the feasibility test's results.
- Present the recommendation in the technical report.

8. Present results in a technical report.

- Upon the proposal's acceptance, design and draft a technical report detailing the project's results.
- Deliver the technical report to Dr. Stiers and Mr. Lyles on February 14, 2011.

Qualifications

I believe my extensive education, work, research, writing, problem solving, and industry experience qualifies me to work on this project. I am a senior with a 4.0 G.P.A. at Louisiana Tech University in Ruston, Louisiana, pursuing my Bachelors of Science degree in Computer Science with a minor in Business Administration and will be graduating in May of 2011. Prior to becoming an intern at Phoenix Corporation, I have held software engineering internships at ExxonMobil in Houston, Texas, and L-3 Communications in Greenville, Texas. Both internships taught me a lot and resulted in a fill-time job offer.

- **Researching:** During my college career, I have completed research for English, computer science, and physics classes. My introductory English classes required me to perform research on literary works in order to write papers analyzing them and on authors to gain an understanding of their styles. In my digital forensics and computer programming languages classes, I had to research and present information on course-related computer science topics. My physics classes required me to research proposal writing and physics principles in order to propose and complete term projects. I have also gained research experience through my internships. ExxonMobil tasked me to design and implement a user interface. The task required me to research interface usability as well as interview users about what they would like the interface to include. L-3 Communications tasked me to perform research and present information on how to use certain software packages. Both my school and work related research experience gives me the knowledge needed to perform any research required by this project.

- **Writing:** Writing has been a large part of my college and work career. In my introductory English classes, I had to write essays and research papers on literary works and authors. Technical writing provided me with experience in memo writing. Some of my upper-level computer science classes required written research reports on computer programming languages and digital forensics. At both ExxonMobil and L-3 Communications, I had to write technical documentation and design presentations on the work I performed. The writing experience that I have received through college and work will allow me to efficiently and effectively report my findings after completing the project.
- **Problem Solving:** During my college career, I have participated in three problem solving competitions. The first competition I participated in was a robotics competition. The robotics competition required my team and me to build and program a robot to complete a maze. The team that completed the maze in the fastest time won the competition. My team not only won the robotics competition but also had the fastest time in the competition's history. In addition to the robotics competition, I competed in a cyber security competition. The competition required me to solve multiple problems and puzzles designed to test my cyber security skills. The third competition I competed in was a computer programming competition. During the competition, my team and I were presented with computer programming problems. The team that completed the most problems in the fastest time won the competition. Although my team did not win the competition, we did complete all of the problems. All three competitions have taught me important problem solving skills and give me the experience needed to effectively solve the problem presented by the project.
- **Industry Knowledge:** I have taken two cyber security courses: cyber security and digital forensics. I learned how to penetrate and defend computer systems and networks in cyber security class. My cyber security knowledge learned through the class will be instrumental in working on the project because I already have some idea of what works and what does not work when it comes to securing computers and computer networks. Digital forensics taught me how to recover data after it has been deleted or become corrupted and the techniques people use to hide and protect data. My digital forensics' knowledge will be important to the project because information security is an important part of protecting a business's important data from outsiders. I also have some work experience in the cyber security industry. Both ExxonMobil and L-3 Communications required me to attended information security and cyber attack training. The knowledge gained from the training will help me complete the project because I already have some idea of the threats that businesses are facing.

Costs and Benefits

In conclusion, I am going to summarize the project's costs and benefits. The costs section is going to present and explain the project's required expenses, operating expenses, and total cost. The benefits section is going to explain the benefits that Phoenix Corporation and the cyber security industry will receive from the project's completion.

Costs

Expenses	Quantity	Cost	Total
Required			
American Airlines Flight #720 Round-trip Ticket	1	$520.80	$520.80
Nightly Rate for One Adult at the Hilton in New York City	2	$150.00	$300.00
Dell Precision M4500 Mobile Workstation with Microsoft Office Professional 2010	1	$1678.00	$1678.00
Operating			
Dell Precision M4500 Mobile Workstation Shipping Charge	1	$0.00	$0.00
Wenger Black Legacy 15.6 In. Double Gusset Top Load Computer Case	1	$49.99	$49.99
Wenger Black Legacy Top Load Computer Case Shipping Charge	1	$4.99	$4.99
Estimated Taxi Fair per Day	3	$100.00	$300.00
Estimated Food Cost per Day	3	$150.00	$450.00
American Airlines Checked Baggage Fee	2	$25.00	$50.00
Total Expense			$3353.78

Table 2: Budget Table for the Project

The project's total cost is $3353.78. The project's costs are split into two categories: required and operating expenses. The first required expense is an American Airlines round-trip plane ticket from Shreveport, Louisiana, to New York City, New York. Along with the plane ticket, there will be an operating expense for a piece of checked luggage on both the flight to New York City and the return flight. Once in New York City, I will have to stay for three days and two nights. The second required expense is two nights at the Hilton in New York City. Due to the research and writing that the project will require, a laptop computer is the third required expense. The computer will be purchased directly from Dell and will not require a shipping fee. The laptop computer that I chose comes with Microsoft Office Professional 2010 and is current with the latest technology. It will not become outdated as quickly as a cheaper model would and will be perfect for passing on to someone else once the project is complete. A carrying case to protect the laptop computer and use on the trip to New York City as well as the case's shipping fee will also be an operating expense. The carrying case will be purchased from Newegg.com. The last operating expenses are estimated taxi and food costs during the New York City trip. I will need to take a taxi to and from the meeting with Phoenix's Board of Directors, any other required meetings, and to purchase food. I will also need to purchase food three times a day during the trip.

Benefits

The project will benefit both Phoenix Corporation and the cyber security industry. Phoenix Corporation will receive both research on an important problem in the cyber security industry and an innovative solution to the problem. After the project's completion, Phoenix Corporation will have research on the causes and effects of the problem that small businesses are having with securing their computer systems and data, on two solutions to the problem that are already in place, and on an innovative solution to the problem. Phoenix Corporation will also receive an innovative solution to the problem. The project will produce a solution to the problem that is not already in place as well as detailed information on how that solution was derived and what the solution involves. The cyber security industry will also benefit from the project. The project will show cyber security professionals how to solve their small business customer's problems and allow them to dedicate more work to other industry problems. The industry will also receive a sound project plan. The project plan will help industry professionals solve other pressing industry problems because they can see how I went about finding a solution to this problem and tweak the method to help them solve other problems.

Thank you, Dr. Stiers and Mr. Lyles, for the research opportunity. Once the proposal has been approved, I will produce and provide you with a technical report. If you have any further questions, please feel free to call or e-mail me. My phone number is 318-123-4567 and my e-mail address is jarrod.sawyer@phoenixcorp.com.

References

"80% of Small-to Medium-sized Firms Fear a Security Threat." *Computer Security Update* 8.4 (2007): 3-6. *Academic Search Complete*. EBSCO. Web. 10 Jan. 2011.

Calder, Alan. *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002*. 4th ed. London: Kogan Page Limited, 2008. Web. 13 Jan. 2011.

Giles, Jim. "Cyber Crime Made Easy." *New Scientist* 205.2752 (2010): 20-21. *Academic Search Complete*. EBSCO. Web. 3 Jan. 2011.

Hoffman, Stefanie. "Small Business a Big Target for Cyber Attacks." *CRN.com.* Everything Channel, 11 Jul. 2008. Web. 5 Jan. 2011.

"Internet Security Issues and Solutions for Small and Medium Business." SonicWALL, Inc., n.d. Web. 5 Jan. 2011.

Kaven, Oliver. "Protect Your Business." *PC Magazine* 25.3 (2006): 103-107. *Academic Search Complete*. EBSCO. Web. 10 Jan. 2011.

Klein, Karen E. "Putting a Fair Internet Use Policy in Place." *BusinessWeek.com* (2009): 23. *Academic Search Complete*. EBSCO. Web. 13 Jan. 2011.

Maiwald, Eric. *Network Security: A Beginner's Guide*. 2nd ed. New York: McGraw-Hill/Osborne, 2003. Web. 13 Jan. 2011.

Mamidi, Ashesh. "Small Businesses Hammered by Cybercrime." *Infosec Island*. Infosec Island, LLC., 14 Aug. 2010. Web. 5 Jan. 2011.

Priescu, Iustin, and Sebastian Nicolăescu. "Managing Security Monitoring in Enterprise Networks." *Petroleum - Gas University of Ploiesti Bulletin, Mathematics - Informatics - Physics Series* 60.2 (2008): 53-58. *Academic Search Complete*. EBSCO. Web. 12 Jan. 2011.

Siponen, Mikko, M. Adam Mahmood, and Seppo Pahnila. "Are Employees Putting Your Company at Risk by Not Following Information Security Policies?." *Communications of the ACM* 52.12 (2009): 145-147. *Academic Search Complete*. EBSCO. Web. 10 Jan. 2011.

Wall, David S. "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime." *International Review of Law, Computers & Technology* 22.1/2 (2008): 45-63. *Academic Search Complete*. EBSCO. Web. 15 Jan. 2011.

Wilson, Tim. "Small Business: The New Black in Cybercrime Targets." *darkREADING*. UBM TechWeb, 19 Mar. 2009. Web. 5 Jan. 2011.