Global Information Assurance Certification Paper

Dennis Bliss
GIAC Security Essentials Certification (GSEC)
Practical v.1.4b Option 1

Security for the Small Business - At What Cost?

ABSTRACT

While it is widely accepted that all networks and computers connected to the Internet should be adequately secured, many times this is not the case. In particular, very small businesses (which shall be defined as less than 10 users for the purpose of this paper) make up a large percentage of enterprises and are especially vulnerable to attacks and compromise due to their limited, if not nonexistent, network security. This is due to the very nature of the very small business with regards to limitations on resources. While large and mid-sized companies can usually afford the time and money required to adequately secure their systems, either by internally managing the issue or outsourcing their security solution, the small business owner normally does not have such luxuries.

Further, the ramifications of a compromised network at the very small business level can be dire indeed, to the point of potential failure of the firm itself. Loss of customer information, theft of proprietary or financial data, or potential liability if the system is hijacked and used maliciously could all spell disaster for the struggling start-up.

It is the intent of this paper to offer a low-cost and minimal-maintenance security plan which can be implemented by the very small business owner and provide a reasonably adequate level of security for the company network. Since the primary concern of the small business owner is the bottom-line cost of implementing any proposed security solution, the main thrust of this paper will be to illustrate these costs and how they can be minimized. Specific detailed costs (in both time and money) will be addressed for securing such a network.

> Disclaimer: While this paper describes several manufacturers' products which may be used to secure a small business network, it is not intended to be an endorsement of those products. Similar products by other vendors may be available which offer comparable value.

BACKGROUND

According to the 1999 U.S. Census Bureau[1] there were 3,713,000 establishments within the United States that were comprised of less than 10 employees.

It is a fair assumption that:

- Using a conservative estimate of 40%, we can assume that 1,485,200 of these small businesses have networks which are connected to the Internet. Of these, we can further estimate that each of these networks has at least 2 devices (computers, printers, etc.). Upon mathematical projection, this establishes that there are nearly 3 million devices connected to the Internet by very small businesses which are potential targets of attacks.
- Many of the computer systems used by these businesses are quickly thrown together in rudimentary networks and connected to broadband Internet connections, with little to no thought given to securing them.
- Due to the relative newness of computer and networking technologies, most small business owners and their employees have a very limited knowledge of securing these networks.
- Funding for computer and network security usually receives a low priority when ranked against other technical and non-technical small business needs.

While most small business owners agree that their networks should be secure, many of these managers feel the task may be beyond their reach. Caught up with the daily tasks of trying to make their business successful, some simply cross their fingers and hope for the best. It doesn't have to be this way. By using a basic Defense in Depth[2] strategy, these systems can be given an acceptable level of protection with a minimal expenditure of time and money.

For discussion purposes in this paper, a hypothetical business with the attributes shown below will be used. Attributes were chosen to simulate a small, family-owned, service company which provides limited services over a relatively small geographic area.

- Type of Business: Small service company
- Business location: Leased storefront
- Number of Employees: 4, plus 1 manager
- Type of network: Peer to Peer network, connected via a small hub, running a mixture of Microsoft Windows 95 and 98 machines which are sharing the network using the Internet Connection Sharing feature.
- Internet Connectivity: Via leased Digital Subscriber Line (DSL) connection
- E-mail: Provided by the Internet Service Provider (ISP)
- Web presence: Small site of several pages, with static content (no e-commerce). Hosting is provided by the ISP

RISK ANALYSIS

The first step in determining what security measures to implement is to understand the most likely risks to the small business network. Unless you know what you are trying to protect, any methodology used will most likely be a haphazard attempt which may do more harm then good.

To determine the dangers to our small business, a simple checklist can be used to determine the risks:

	Susceptible?	
Type of Risk	**Yes**	**No**
Physical Security		
Theft of Equipment	•	
Damage to Equipment (flood, fire, power surges)	•	
Unauthorized Access		
By insiders		•
By outsiders	•	
Malicious Software		
Virus Infection	•	
Trojans/Hijacking of Systems	•	
Data Security		
Loss of company data	•	
Loss of customer data	•	
Web page security		
e-commerce risks		•
Static content (loss or change)	•	

After completing the checklist, we have discovered that our hypothetical business is not particularly susceptible to two particular risks:

- Insider unauthorized access – Because our business is so small, there are probably no clearly delineated departments within the company. Employees on the network may be called upon to do any number of tasks, meaning that they need access to all data on the network. For the very small firm, it is not unusual to find family and friends in positions throughout the company. Because each of these people has a vested interest in helping the business succeed (and is not likely to do anything malicious), risk in this area is minimal at this time.

- E-commerce risks – Since our hypothetical company is not involved in e-commerce, there are no risks in this area. Because no proprietary company information is available via the web site, and no personal customer information is stored on e-commerce database servers, there is no reason to expend resources protecting against these types of risks.

After a quick analysis of the remaining potential threats, it is determined that the small business network is susceptible in a number of areas. By clearly identifying what the potential losses are for each of these weaknesses, we can then choose appropriate protection mechanisms to minimize the risks.

Theft

In the event that any (or all) of the company's equipment is stolen, the result could be catastrophic. Almost all firms today rely heavily on technology and count on it to conduct virtually all aspects of their business, from ordering supplies, to providing the service or product, to employee payroll, to management of overhead costs. This is especially true for the very small business just starting out. While insurance coverage will likely cover the cost of new equipment, the data cannot be easily replaced. Nor could the man hours required to attempt restoration. In the time it could take to replace the data (which could be just as long as the business has been in existence), the small business could go under.

Damage to Equipment (flood, fire, etc.)

Most of the same principles that apply for equipment theft also apply to the damage of network equipment. Again, while insurance may cover the cost of the equipment itself, some data is irreplaceable.

Outsider Unauthorized Access

Unauthorized outsider access to company systems could result in a number of unwanted actions, affecting the confidentiality, integrity, or availability[3] of system resources or data. If attackers with malicious intent manage to break into the small company's network, the results could be disastrous. Operating systems could be rendered useless. Changes (even subtle ones) to data files could cause long term financial loss. Company vendor information or proprietary business processes could be stolen. Worst yet, the entire system could be hijacked (as described in the *Trojans/Hijacking of Systems* description below) and used to perform illegal or unethical attacks against other companies, government agencies, or individuals. Liability for such an attack could break the back of our small business.

This type of risk is especially high, given the company's always-on DSL Internet connection. Attackers would find the unprotected network's resources lucrative indeed.

Virus Infection

According to the McAfee Security Corporation, which specializes in antivirus software, at the time of this writing there were "more than 62,000 virus threats in

existence"[4] with new viruses or variants created by hackers each month. While some of these viruses can be spread by specific services and applications running on a computer system, the vast majority are distributed via e-mail. In today's e-mail dependent business environment, this creates a tremendous potential risk to which the small business is no exception.

While most viruses can be relatively benign, many of these malicious programs carry what is known as a payload[5], much the same as military ordnance. Damage can range from silly messages which appear on the computer screen, to total formatting of hard drives, causing complete deletion of all data.

Trojans/Hijacking of Systems

According to SOPHOS Antivirus, Trojans are "programs that hide their true purpose", [6] much the same as the famed Trojan Horse used by the Greeks to gain access to the city of Troy. Similar to a virus, this type of malicious software is designed to perform activities unwanted by the system's owner. Often, the intent is to commandeer the system for use by the attacker at a later date to perform illegal activities. These malicious software devices can be placed on a system directly by the perpetrator, or may also be distributed by e-mail messages. As with viruses, the ability to stop their use on the small business system is imperative.

Loss of Company Data

Loss of company data could be extremely detrimental to the success of the business. In the event that files containing business processes or management information were lost or corrupted, it could severely cripple the company. Although loss of this type of data might be transparent to the customer at first, the long term effects would be apparent. Reconstruction of these files could be a long and arduous process, resulting in inefficiencies throughout the business.

Loss of Customer Data

The loss or corruption of customer data, especially financial information, could immediately destroy the small business. Not only would the company's reputation be forever tarnished, but liability could become a huge issue. If customer billing information such as credit cards or bank accounts should fall into the wrong hands, the small business could face numerous lawsuits, a situation the small firm could ill afford.

Changes to web page content

Since our hypothetical small business uses a web page with strictly static content, the risk in this area is minimal. This is especially true since the site is hosted by the company's ISP. All files for the site are off the network and on the

provider's system. Although the page could be defaced, causing embarrassment to the company, the ISP would retain most of the liability.

Risk analysis summary:

After conducting a quick analysis of the identified risks, we find that the company does indeed require some form of security program to protect its network assets. Now we can begin to construct our defense system, keeping in mind the limited resources available.

It should be pointed out that this type of risk analysis should be conducted at least once a year by the business owner. As the business grows (i.e. additional employees added, e-commerce capability added, etc.), additional risks may become identified. Although initially several hours may be needed to perform a network's risk analysis, subsequent analyses should be much quicker.

Risk Analysis			
Initial Cost		*Recurring annual cost*	
Description of activity	Cost	Description of activity	Cost
Financial - none	$ 0.00	Financial - none	$ 0.00
Labor - Conducting initial risk analysis of the network	8 hours	Labor - Conducting annual re-analysis of risk(s)	4 hours*

***Note:** Because labor prices may vary according to the salary of the individual performing the work, costs in this area are computed in man hours throughout this paper.

EMPLOYEE AWARENESS TRAINING

The properly trained user can provide a very strong first line of defense for any network and usually provides the small business owner with the biggest bang for the buck as far as defense methodologies go. Since they are working with the network resources on a daily basis, they are in the best position to recognize a potential attack and stop it in its tracks.

By the same token, an uneducated or inexperienced worker can cause great damage to a workstation or network, sometimes unwittingly. Opening unsolicited e-mail attachments, installing unapproved applications, using the network resources for unintended purposes, or giving away passwords to unauthorized people can all spell trouble for the small business network. To avoid these hazards, our business owner should consider a two pronged approach to employee security training; orientation training and recurring training. When properly developed, implemented, and maintained, the small business owner can avoid a multitude of headaches down the road.

As a minimum, security training should encompass the following topics[7]:

Physical Security

- Restriction of access to network components
- Locking of doors when leaving for the day
- Safe office practices to avoid:
  - Fire
  - Drinks spilled on computers
  - Using network resources for other than intended purposes

Passwords and Authentication

- Strength of passwords (length at least 8 characters long, avoiding the use of common names, adding numbers and special characters, mixing upper and lower case, etc.)
- Avoiding the urge to write passwords down
- Social engineering. This can be defined, as John Palumbo did in his recent SANS submission as: "An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) he needs to gain access to the system."[8] Users must be made to understand that there is no reason to EVER give anyone their password.

Permissible behavior

- Limited personal use of company assets (i.e. printing)
- Limited personal use of Internet access to lunch hours.

E-mail safety

- Caution opening attachments – confirm with sender if not anticipated
- Multiple e-mails with same subject line – notify manager
- Antivirus software configuration – “hands off”

Configuration Management

- Installation of hardware (modems, etc.) - prohibited
- Installation of software (chat programs, games, etc.) - prohibited

Backup procedures

- What should be backed up? How often?
- Where to back it up.

Since this may be a lot of information for employees to grasp, the small business owner might consider creating a desktop reference[9] for the employee to keep. Not only will it provide a quick source document for the employee to consult, but it will serve as a constant reminder of the importance of network security to the business, and ultimately to the employee's job. In conjunction with refresher training (given annually to all employees) this could serve to strongly mitigate mistakes which uneducated workers sometimes make.

Finally, once training is completed, the business owner should have each employee sign a short statement indicating their acceptance of the company policy. Since people tend to take signed documents seriously, it will strengthen their resolve to avoid security risks. Additionally, it provides the business owner with recourse should employees cause undo harm to the network through misuse or negligence.

Employee Awareness Training			
Initial Cost		*Recurring annual cost*	
Description of activity	Cost	Description of activity	Cost
Financial - none	$ 0.00	Financial - none	$ 0.00
Labor - Developing and performing employee security training	8 hours	Labor - Performing annual employee security training	2 hours

OPERATING SYSTEM UPGRADE

In order to have a fighting chance of securing this small business network, it is absolutely essential that the owner strongly consider upgrading the existing operating systems of Windows 95 and 98. While these systems are user friendly, they offer little to no security capabilities besides turning off file sharing. Implementing user authentication, securing the file systems, or restriction of software installations will not be possible with these wide-open systems. Additionally, because of their limited security, these versions of Windows offer hackers a very attractive target that is easy to exploit from anywhere on the Internet.

Since the users of the network have most likely become used to the Windows environment, perhaps the best solution would be to upgrade. By upgrading to another Microsoft system, the learning curve of users could be reduced while at the same time providing a much more secure environment. Specifically, the Windows XP Professional (XP Pro) edition, if properly configured, would probably be a more secure alternative to the operating systems, while at the same time allowing for future growth of the network. The cost to upgrade to XP Pro,

including the software and license, would be approximately $180.00 per computer[10] and would offer much stronger controls over the network and its data, such as[11]:

- Access Control Groups & Group Policies - Through these security applets, managers can apply restricted access and appropriate rights to users by placing them in pre-defined security groups. This allows more control over what users can do and what they can access. For our small business, this means that new users can be restricted to only the files which they need to perform their jobs, greatly enhancing the security of the network as a whole. Additionally, it will allow the manager the possibility of redefining roles of existing employees within the company, perhaps lending itself to better organization and use of network resources.

- Password Controls & Managed Network Authentication - By implementing hardened password requirements, password guessing by an attacker becomes much more difficult. Our business owner should consider restricting passwords to those with a specified number of characters, upper and lower case letters, numbers, and special characters, those not based on personal information, and not based on any language or jargon (i.e. not found in any dictionary).[12] To complement this, XP Pro controls network access by limiting anyone trying to gain access to the computer from an outside network to a special guest level account with extremely limited privileges.

- Encrypting File System (EFS) - EFS is based on public-key encryption and takes advantage of the New Technology File System (NTFS), a more secure file system derived from XP Pro's big brother operating systems; Windows NT and 2000 which are widely used in corporate network environments. In essence, when using EFS, only the user who encrypts a protected file (or the public key issuer - i.e. the administrator) can open the file and work with it. The benefits of such a technology are apparent. The small business owner can ensure that all high-value or sensitive files on the network are strictly controlled and accessible only by authorized individuals.

- Software Restriction Policies - These policies, if properly administered, can confine execution of software to a predefined set of trusted applications. This can greatly aid in protecting the network against script-based viruses, Trojan horses, or even unauthorized software which users try to install that may contain these malicious devices. Should antivirus software fail to stop one of these applications from making it into the network, the XP Pro system will prohibit its operation anyway.

- Internet Connection Firewall (ICF) - ICF functions as a stateful packet filter that can be used on a shared Internet connection. The filter blocks all unsolicited connections originating from the Internet by validating incoming flow against the outgoing flow of packets. Incoming packets are only allowed if there is a corresponding outgoing packet that originated within the network. In other words, if the network communication did not originate within the protected network, the incoming data will be dropped. This system, although not foolproof, will provide another layer of firewall defense, in addition to the hardware discussed later.

As we can see, upgrading to the XP Pro operating system could greatly enhance the security of our small business network. While Windows 95 and 98 have very limited ability to protect network resources and are more suited to a stand-alone or home computer, XP Pro is clearly an upgrade. As with any operating system, keeping it updated is essential. Updating will be covered under the Applying Patches section, later in this paper. Estimated cost of initially upgrading this small network is as follows:

Operating System Upgrade			
Initial Cost		*Recurring annual cost*	
Description of activity	Cost	Description of activity	Cost
Financial - Purchase of XP Pro upgrades for 5 workstations @ $ 180.00 per workstation	$ 900.00	Financial - none	$ 0.00
Labor - Installation and configuration of the new operating system (3 hours per workstation)	15 hours	Labor - Performing re-configuration of 5 workstations (dependent on changes in risk analysis)	5 hours

COMBINATION DSL ROUTER/FIREWALL

Although the software firewall which is integrated into XP Pro offers some protection against unwanted intrusions, additional protection in the form of a hardware device is always a good idea. This is where a network appliance with firewall capabilities helps enhance the security of the system.

Traditional hardware firewalls can come in many shapes and sizes, albeit with prices that usually match. It is not uncommon to find firewall appliances used on large corporate networks which cost many thousands of dollars. This is the type of expenditure many small business owners envision when someone mentions the term firewall as it relates to network security. Because of this, many small

companies do without; they assume they cannot afford such an expensive addition to their network and take their chances. Luckily, there are a few manufacturers which have realized the need for low cost firewall devices and have developed alternatives which fit the bill nicely. With an expenditure of about $100.00, small businesses can now afford a reasonable combination router and hardware firewall that provides the protection they need without breaking the bank.

> Caution: When choosing a device that includes a hardware firewall, the small business owner should ensure that the technical support literature provided with the device is easy to understand. Step-by-step configuration instructions with plain-language explanations can do wonders to ensure even the most technically challenged individual can quickly and easily configure the device.

One of these devices, the Etherfast Cable/DSL Router model BEFSR81, manufactured by Linksys[13], offers many features that will enhance the security model of our hypothetical network.

With that said, let's take a look at some of the features of the BEFSR81:[14]

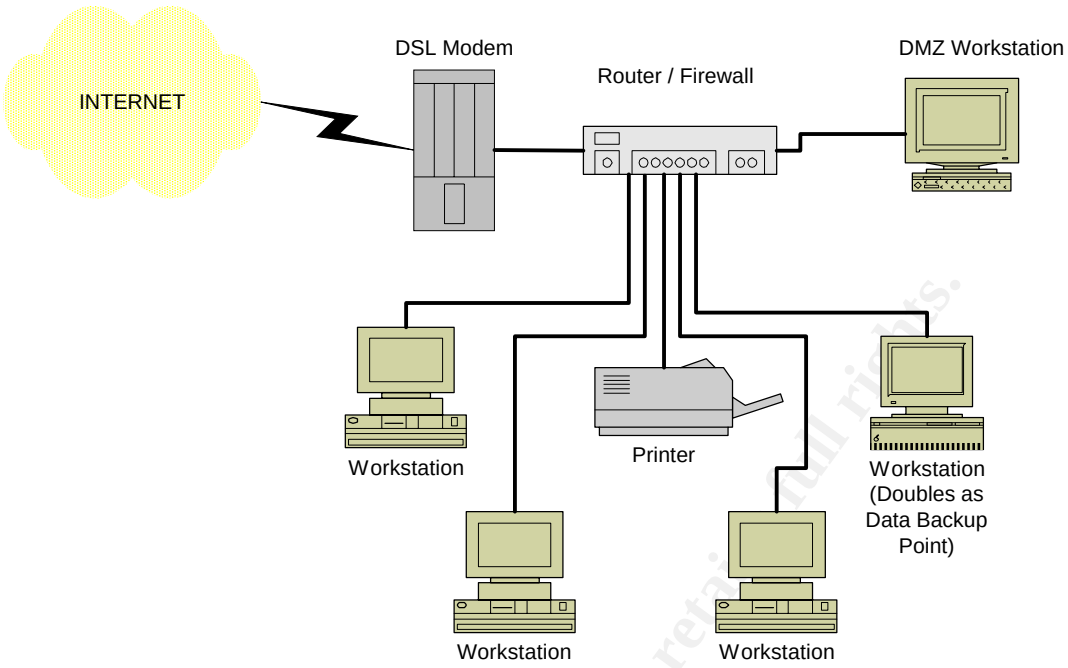
- The ability to share an Internet connection among multiple workstations and devices on a network while only displaying a single IP address to the outside world.

- The capability to close unnecessary ports and services. The amount of open ports and services should be reduced to the bare minimum necessary for the network to efficiently operate.

- The ability to internally assign local IP addresses to each network device, making troubleshooting and maintenance of the network easier. This is accomplished through the use of a Dynamic Host Configuration Protocol (DHCP) server, a nice option. As an added bonus, if a machine is somehow compromised, this configuration allows the owner to quickly isolate and remove it from the network.

- The capability to create a Demilitarized Zone (DMZ). Only the IP address of computers in this zone can be seen from outside of the network, enabling them to become a download point for patches, upgrades, and antivirus signature file updates. Later, machines on the internal (invisible) network can download patches and updates from this machine, as described later in this paper.
- Easy to understand setup procedures.

The illustration on the following page shows a sample network architecture, using the DMZ option.



Configuration of the BEFSR81 is achieved remotely through the use of a web browser, allowing the small business owner to quickly configure and adjust settings from his desktop computer. Additionally, this device easily handles add-on software firewall applications such as Zone Labs, Inc.'s[15] *Zone Alarm Pro* or Trend Micro's *PC-Cillin*[16] should the business owner wish to further enhance security of the network at a later date.

As we can see, adding a hardware firewall clearly enhances both the organization and the security of our small business network. The estimated cost of implementing this firewall appliance solution is shown below[17]:

Combination DSL Router / Firewall			
Initial Cost		*Recurring annual cost*	
Description of activity	Cost	Description of activity	Cost
Financial - Purchase of Linksys BEFSR81 device	$ 99.00	Financial - none	$ 0.00
Labor - Installation and configuration of the new device	4 hours	Labor - Performing re-configuration Router / Firewall Device (dependent on changes in risk analysis)	1 hour

PATCHES AND SERVICE PACKS

Many of the biggest vulnerabilities to today's network systems can be directly attributed to systems that have never been updated since they were installed. Security holes are found nearly every day and manufacturers are usually quite good in creating security patches for vulnerable systems in a timely manner. However, most small business owners (and many corporate network administrators as well) do not think to update systems on a regular basis. Often, they are too busy, or fool themselves into believing that they are not a potential target. They may be concerned that applying patches to an operational system may cause malfunctions. The term "If it isn't broke, don't fix it" does not and should not apply. In fact, it is these types of networks and systems that hackers specifically look for. They rely on the fact that updating applications and operating systems can be a time consuming process with seemingly little payoff.

By putting a centralized machine in the DMZ, all patches and service packs for the operating system and applications can be downloaded using a single address visible to the Internet. This ensures that other machines on the network remain obscured from public view, but because they can see the computer in the DMZ, they can download updates from it.

It is usually a good idea to check for new patches and service packs at least once a month[18], or whenever a new vulnerability is discovered. Then, once patches and service packs have been downloaded and virus scanned by the DMZ computer, the other machines on the internal network can download updates from the DMZ with relative safety. This portion of the update process can also be automated in our selected operating system of XP Pro, thanks to the Automatic Updates feature available through the System application in Control Panel. If automated updating is not desired, it can also be performed manually.

Based on the initial setup required and monthly searches for updates, the resources expended to implement the above patching methodology are shown below.

Updating Patches and Service Packs			
Initial Cost		*Recurring annual cost*	
Description of activity	Cost	Description of activity	Cost
Financial - None	$ 0.00	Financial - none	$ 0.00
Labor - Configuring the DMZ computer for patch and service pack handling	4 hours	Labor - Performing patch downloads and installations (5 per month X 12 months X 30 minutes per workstation)	30 hours

ANTIVIRUS

Perhaps the single most recognized part of computer and network security is the existence of antivirus protection. There is no doubt that viruses are the most widely publicized threat, and with good reason. Small businesses must institute an effective countermeasure in the form of antivirus software.

The first step in determining which antivirus application to employ is to find out what, if any, type of solution the ISP is using on the e-mail server itself. Since our small business is dependent on their leased DSL connection, it is only appropriate that they insist on some sort of protection from the provider. Normally, this is part of the lease agreement, but the business owner should definitely check. Knowing that protection is being used at the server is not enough, however. It is important to know which product is being used.

Once it has been determined which product is being used at the ISP, the small business owner can determine which product to purchase for the desktop environment. To ensure several layers of defensive measures[19], one solution is to use an application created and supported by a different vendor. This will increase the odds that when a new virus is discovered, at least one of the vendors will have an appropriate signature update available right away, in effect doubling the chances of quick and responsive defenses against new threats.

Fortunately, many of the latest desktop antivirus software packages are very affordable and are relatively easy to use. Vendors have recognized the need for small enterprise solutions within the small business community and have created multi-pack licenses for these situations. One such application, Norton Antivirus 8.0 Small Business Edition[20], offers what they call a "license in a box" solution encompassing coverage for up to 5 computers, a perfect fit for our small business. Cost of the software and a one year subscription is relatively inexpensive at approximately $329.00[21], before tax or shipping. In addition to the base pack, the company offers per-seat add-on licenses, which enable the number of applications to grow with the network.

As with patches and upgrades, it is important to develop an antivirus signature strategy to keep the software current. Again, the value of our workstation in the DMZ is realized. Updates can be downloaded to the single DMZ machine and automatically pulled down as scheduled to the individual network computers, saving the business owner countless hours. Updates should be done as often as possible, most effectively on a daily basis. This can be accomplished by configuring the software to download updates in off-peak hours, such as at night, to avoid interrupting workflow during normal business hours.

The estimated cost of implementing our antivirus solution follows.

Antivirus Software Deployment			
Initial Cost		*Recurring annual cost*	
Description of activity	Cost	Description of activity	Cost
Financial - Purchase of Norton Antivirus Small Business Edition, 8.0 for a 5 computer network	$ 265.00	Financial - Annual antivirus subscription renewal	$ 199.00
Labor - Configuring the DMZ computer for antivirus signature update handling. Installing and configuring the antivirus software on 4 other workstations. (30 minutes for each)	2.5 hours	Labor - Installing subscription renewals for 5 workstations (30 minutes per workstation)	2.5 hours

BACKUPS

Having backups to important data is crucial to the small business in the event of a disaster. Loss could happen in a number of ways, including equipment failure, exposure to a virus, fire, flood, or even tampering. No matter what the cause, it is absolutely crucial that the business owner develop a strategy to back up the most important files to the firm.

Perhaps the most important step in developing a backup methodology is to determine which pieces of data need to be backed up. This requires a careful analysis by the owner to determine which data are critical, important, or simply mundane[22]. Not all files have the same level of importance to the company. Primarily, the business owner should consider only those files which fall into the critical or important categories. Those data files considered being mundane, while probably nice to have, would not be vital to restoration of the business should disaster happen. Factors to consider should include those files which contain proprietary business processes, financial information (of both the company and the customer base), databases of potential customers, marketing information, web page information, and personnel files.

Once it has been determined what should be backed up, the next step is to decide on what media to use. Since our small business may not have the resources necessary to implement an extensive data storage methodology, the best bet is to create a simple but effective technique that does not require an extensive amount of time or money. Thanks to the advance of technology, one such method might be to employ the CD-ROM Readable-Writable drive. These come standard on most new systems, or an external CD-RW can be added for an expenditure of less than $100.00[23]. CD-RW media holds approximately 650

Megabytes of information per disk and is also very affordable, running anywhere from 50 cents to $1.00 per disk.

Where to deploy the drive or drives is the next question we must answer. Instead of having to purchase numerous CD-RWs and spend an inordinate amount of time to back up numerous workstations and files, it might be better to pick a single workstation with a rather large hard drive and designate it as the critical storage area. This is illustrated in the sample architecture drawing, shown earlier in this paper. To be effective as a storage area, it is important to instruct employees of the location and designate which files they should save to that location during the course of normal business. Then, when it comes time to back up those critical files, it is a simple matter of copying them to the CD-RW media.

The next step in establishing procedures is to determine how often backups should be performed. While many large corporations find it necessary to perform backups on a nightly basis, primarily due to the massive amounts of information being utilized, an aggressive strategy such as this might not be necessary for our small business. While the comfort level and time constraints of the business owner are the primary factors which will dictate the frequency, the owner must be careful not to let too much time lapse between saves. A fairly conservative frequency of once each week should satisfy most business needs while not overtaxing resources to ensure a timely recovery is possible. Therefore, a good method is to copy the critical files to a CD-RW once each week, perhaps on Fridays before close of business.

Finally, we must answer the question of where to keep the backup media. Storing it on-site in the business space is generally not a good idea, especially in the event of a physical disaster such as fire or flood which causes loss of the original files. If this were to happen, not only would the original data be lost, but the emergency data as well. Maintaining a separate facility is generally not an option given the limited resources of the firm. A good low cost alternative, which provides a great deal of physical security, is the use of a safety deposit box in a bank. This is especially efficient if backups are made weekly, on Fridays as suggested. Banks are normally open later on this day of the week. Normal rental of these boxes can be as little as $50.00 a year and the costs can, in most cases, be used as a tax write-off.

The cost of our backup methodology follows.

Backup methodology			
Initial Cost		*Recurring annual cost*	
Description of activity	Cost	Description of activity	Cost
Financial - Purchase of CD-RW drive ($100.00), Purchase of media (52 disks @ $1.00 per disk = $52.00), Rental of safety deposit box ($50.00)	$ 202.00	Financial - Purchase of media (52 disks @ $1.00 per disk = $52.00), Rental of safety deposit box ($50.00)	$ 102.00
Labor - Defining critical and important data, installation and setup of the CD-RW drive, Employee instruction	4 hours	Labor - Conducting backups of data on the critical data computer (15 minutes per week X 52 weeks)	13 hours

SUMMARY

Now that a basic security system for our small business network has been created, we can review what we have accomplished. While on the surface it appears as though we have developed a fairly sound system, it is always important to weigh the proposed solution against the original risk picture. By establishing a clear traceability from the different mitigation methods back to the risk analysis, it can be established whether or not the system should be effective. This will also help the business owner clearly see what the defensive scheme is and how it relates to the data and resources he or she is trying to protect. By revisiting the risks which were identified during the analysis, we can quickly determine if we have covered all of the bases:

Theft of Equipment - Although we cannot completely eliminate the risk of having equipment stolen, we can reduce the possibility of occurrence and lessen the affect on the company, should a theft occur. Employee education (instructing workers to limit access to network components and ensuring facilities are locked) will reduce the possibility of loss due to theft. In the event hardware is stolen, recovery via the use of our data backups would limit the loss.

Damage to Equipment - Loss due to flood, fire, power outages, or other physical means has also been reduced by the employment of employee education (general office safety practices and policies), and data backup abilities.

Outsider Unauthorized Access - Through the use of the new software and hardware firewall devices, unauthorized access from the outside world has been significantly decreased. Only Internet traffic which originates from inside the network is allowed and for the most part, computers on the inside of the network are fairly transparent to the outside world. Additionally, our new user

authentication requirements (namely the strong password authentication) will slow down even the most determined hacker.

Virus Infection - Again, a comprehensive training program will pay off. Employees, when informed of the dangers of opening e-mail attachments, will limit exposure to this risk. Restricting the installation of unauthorized software (via profile management features in the new operating system) will further limit the possibility of infection. A two-tiered approach to antivirus (using different vendors) should make the risk smaller still.

Trojans / Hijacking of Systems - The new virus fighting techniques discussed above will also assist with the reduction of risk in this area. Additionally, regular patching and application of service packs will diminish the ability of attackers to poke holes in the operating system and workstation applications.

Loss of Company or Customer Data - By educating employees on proper data handling techniques and employing a regular data backup strategy, the permanent loss of critical and important information will be averted. Preventing unauthorized access to network components (as previously discussed) will help ensure it doesn't happen in the first place.

Changes to Web Page Content - Although most of the liability in this area falls on the shoulders of the ISP, loss of web content due to defacement or sabotage can be easily rectified. By considering this data to be important, the backup strategy will ensure a quick remedy.

CONCLUSION

Now that it has been established that all identified risks can be lowered, we can determine if the proposed solution is affordable to the business owner. As the table on the next page illustrates, the initial cost to set up such a system can be accomplished by the business owner for less than $ 1500.00 and 50 hours worth of work. Subsequent annual costs are estimated at around $ 300.00 and less than 60 man-hours per year.

The ultimate question the small business owner now must ask is whether they are willing to make the investment necessary to secure the firm's network. Perhaps a better question to ask is whether they are willing to accept the consequences for not making the investment.

Overall Costs				
	Initial		*Recurring*	
Methodology	**Financial**	**Labor**	**Financial**	**Labor**
Risk Analysis	$ 0.00	8 Hours	$ 0.00	4 Hours
Employee Training	$ 0.00	8 Hours	$ 0.00	2 Hours
Operating System Upgrade	$ 900.00	15 Hours	$ 0.00	5 Hours
Employment of Firewall appliance	$ 99.00	4 Hours	$ 0.00	1 Hours
Patch and Service Pack Updates	$ 0.00	4 Hours	$ 0.00	30 Hours
Antivirus deployment	$ 265.00	2.5 Hours	$ 199.00	2.5 Hours
Backup methodology	$ 202.00	4 Hours	$ 102.00	13 Hours
Totals:	$ 1466.00	45.5 Hours	$ 301.00	57.5 Hours

REFERENCES

1. Statistics about Business Size (including Small Business) from the U.S. Census Bureau, http://www.census.gov/epcd/www/smallbus.html

2. "SANS Security Essentials II: Network Security Overview", 2002, page 1-3

3. "SANS Security Essentials II: Network Security Overview", 2002, page 1-6

4. Virus Information Library, McAfee Security Corporation, http://vil.nai.com/vil/default.asp

5. Virus Glossary, MacAfee Security Corporation, http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/virus-glossary.asp

6. Glossary of Terms, Sophos Antivirus for Business, 19 November 2001 http://www.sophos.com/virusinfo/articles/glossary.html#trojan

7. "Security Awareness - Implementing an Effective Strategy", Chelsa Russell, October 25, 2002, http://www.sans.org/rr/aware/sec_aware.php

8. "Social Engineering: What is it, why is so little said about it, and what can be done?" John Palumbo, July 26, 2000, http://www.sans.org/rr/social/social.php

9. "Security Awareness - Implementing an Effective Strategy", Chelsa Russell, October 25, 2002, http://www.sans.org/rr/aware/sec_aware.php

10. Microsoft Windows XP Professional Upgrade, Available at Computer Discount Warehouse, http://www.cdw.com/shop/products/default.asp?ProductID=323092

11. "What's New in Security for Windows XP Professional and Windows XP Home Edition", Microsoft Corporation, July 2001, Available at: http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/default.asp

12. "Password Protection Policy", The SANS Security Policy Project, Available for download at: http://www.sans.org/resources/policies/

13. Linksys Corporation Home Page, http://www.linksys.com

14. Etherfast Cable/DSL Router model BEFSR81 specifications and User Guide, available at: http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=155

15. Zone Labs Incorporated, http://www.zonelabs.com/store/content/home.jsp

16. Trend Micro, PC-cillin software description, http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm

17. Linksys BEFSR81 Etherfast Cable/DSL Router, Available at Best Buy, http://www.bestbuy.com/Detail.asp?m=488&cat=540&scat=1574&e=11043240

18. "Why small businesses need to secure their computers (and How to Do it!)", Bruce Diamond, August 16, 2001, http://www.sans.org/rr/securitybasics/need_sec.php

19. "SANS Security Essentials II: Network Security Overview", 2002, page 2-31

20. Symantec Corporation, Antivirus Vendor, http://www.symantec.com/product/index_smallbiz.html

21. Norton Antivirus Small Business Edition, Version 8.0, Available at Symantec, http://www.symantecstore.com/dr/sat/ec_MAIN.Entry17c?CID=0&SID=&SP=10007&PN=5&PID=426882&DSP=&CUR=840&PGRP=0&CACHE_ID=39910

22. "CISSP All-In-One Certification Exam Guide", Shon Harris, Copyright 2002, pg. 294

23. Digital Research 52x24x52 Internal CD-RW Drive available at Best Buy, http://www.bestbuy.com/Detail.asp?m=488&cat=511&scat=514&e=11181430

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event