Case Study #1: CompanyX

Network Security in the Real World

by Rich Bright

Profile of Company X

CompanyX is locate in a rural community of fewer than 8,000 people. It employs approximately 20 people in two locations. Site1 and Site2 are about 15 miles apart and serve the needs of two communities in the service sector under heavy Federal and State regulation. Site1 and Site2 were connected by a private T1. All network traffic from Site2, including Internet access, was funneled through Site1. CompanyX had approximately 12 Windows PCs at Site1 and 6 Windows PCs at Site2. PCs were generally purchased in blocks of 3 to five units. Typically, high end PCs were replaced for critical users the replaced computers were rotated "down the chain" annually. No domain was in place. The "server" was primarily a higher end workstation with file sharing services. All web and email services were outsourced. ISP and phone services were provided by a well established phone company using separate circuits. No IT staff was present. Most IT needs were handled by a management staff which lacked any formal IT training. Management was able to handle most day to day IT issues with contacted support and IT services were contracted as needed.

Business operations depended access to a mainframe located at Site1. A proprietary PC based "SoftwarePackage2" was also critical to daily operations and shared data via "the server." Heavy use of document imaging among and between locations also played an important role in company operations. Company operations include both walk-in retail and backoffice support.

While CompanyX showed good practice, it had little formal policy or documented practice related to information security at the beginning of this engagement. A cultural understanding trumped written policy in dictating conduct and practice Employee turnover was very low for the majority of company positions. Three positions in the company had turnover about every 6 months with average tenure in those spots of less than 18 months. Interstaff relations were excellent among and between departments with a very flat management hierarchy. A high degree of trust existed within the organization and among the employees.

CompanyX sought outside consulting services to provide and independent, third party review of technology and practices related to the ongoing information security needs of CompanyX in order to develop a comprehensive long term strategy an practice. A baseline assessment was made and followed by quarterly assessments and improvements.

The following reports were submitted to achieve these goals and provide a real world view of the challenges in building and maintaining a secure network over the course of a year.

Baseline Security Audit for CompanyX
April 2006
Executive Summary

Personal computers used by CompanyX were inspected as part of a baseline security audit performed by Bright Ideas. Additional information was gathered through interviews with CompanyX officers, and informal discussions with staff. A significant amount of raw data related to the security baseline has been provided to CompanyX as documentation of the results related to individual computers.

The goal of the information security audit was to:

Assess existing and needed security measures to protect the business information of the CompanyX and privacy of existing and potential customers regarding daily operation and disaster recovery.

In short, I found your security and disaster planning to be adequate with room for some improvement.

Your data security is critical to maintaining business information and protecting the privacy of current and potential customers. While there is no such thing as total data security, many steps can be taken to manage the risk. Your information security is only as strong as the weakest link in a security chain. Mitigation of risk is accomplished by applying best industry practices, correcting configuration errors, and upgrading components as needed. The goal in managing data security and mitigating risk is to provide multiple layers of defense. The layers should offer protection, recognition of breaches in defense and an audit trail for analyzing successful attacks. Because the threats to your data are ever evolving, network security must be seen as a process and not a destination.

You must provide physical security of data systems, security at the network level and security of the individual desktop computer. I observed generally good physical security, CompanyX patrons do not have access to data systems. Data tapes and reports were stored securely.

Your stateful packet inspection firewall should be recognized as a strength of your existing network security. Firewall logs and alerts are routinely emailed to CompanyX personnel and reviewed for unusual activity. Unsecured PC's or high value targets on your LAN are now blocked from Internet access at this level.

Using a firewall to appropriately limit access to the network from the outside is only the first step in securing your network. No modems were found to answer on any phone line. No wireless network, laptop use or VPN access was found. A diagram of physical connectivity should be developed and audited on a routine basis.

You currently depend on the Norton Internet Security program suite to alert you of malicious traffic on your network. The addition of IPS, Antivirus and Anti-spyware services to your SonicWall would be a valuable addition to your network defense. Because malicious traffic or programs can still enter your network, Norton Internet Security will remain an important element of your security plan.

A SYSLOG server should be implemented to provide additional logging of network traffic. This syslog provides a source of forensic data following any successful attacks against your data systems. You may also wish to consider the implementation of a passive internal Intrusion Detection System (IDS) at the network level. I suggest setting the internal IDS to monitor network activities which pose only the highest risk.

There is an ongoing need to maintain good separation between the administrative password of your PC's and of your network devices. You must assess risks and change passwords as needed. Changing administrative passwords should be considered with the departure of any employee. Secured envelopes containing all needed administrative passwords and logins for all systems, both internal and external, should be kept at secured offsite locations.

A baseline of network devices, IP addresses, network shares and service presentation was established. No unexpected devices were found. All expected shares were found. One old share was removed and the files were deleted. All PC's and the firewall now establish a common time base with the time servers maintained by nist.gov. Appropriate backups of network device configuration were made.

It is critical to secure the operating system against known threats by applying appropriate patches provided by the manufacturer. All systems were brought to current standards using the Microsoft Update service. With very few exceptions, PC's were properly configured to download and apply critical patches as soon as they are made available by Microsoft. Any machine not properly configured was changed. Many computers required a great many "noncritical" updates. These "noncritical" updates are not automatically downloaded and installed. All operating systems used at your facilities are currently supported by Microsoft. Extended support for Windows 2000 is scheduled to end on July 13, 2010.

Proper configuration of antivirus, desktop firewall and anti-spyware software is essential to securing the PC from malware. The configuration of Norton Internet Security was reviewed and in some cases changes were made. A full system scan is now being be performed. Your NIS 2006 provides much better anti-spyware protection than the 2005 edition previously used. NIS 2006 lags significantly when compared to Webroot's SpySweeper in terms of real time prevention. You may want to consider purchasing SpySweeper for those computers which use the Internet a great deal involving untrusted sites. Mozilla FireFox 1.5.1 was installed as an alternative to Microsoft's Internet Explorer. The

use of FireFox greatly mitigates the threat of spyware infection from simple browsing. The combination of IDS/IPS at the firewall and FireFox greatly reduces your probability of system compromise due to spyware. All systems were scanned for rootkit infestation. No rootkits were found. All computers were scanned for viruses and spyware infection. Minor adware infections were found and removed on some computers. A large number of adware programs were found on the Site2 Worker23 computer. The hard drive was reformatted and the entire system was reloaded. The Worker23 system is now secured.

User logins were audited on each computer. With few exceptions, no problems were found and those problems were corrected. The most significant problem related to user logins is the widespread use of the administrator account in Site1. This presents a great security risk to the individual PC and also to the network.

The disaster recovery plans of the CompanyX are comprehensive and constantly evolving. The goal of disaster recovery planning is to provide virtually seamless, continuous operations by instituting recovery plans which account for the loss of data due to inaccessibility resulting from physical loss or damage, equipment failure, data corruption or loss of key personnel. Using the Site2 and Site1 CompanyXs as secure offsite storage is a strength of your plan.

Your IBM mainframe was not included in this security baseline. Please consult with your software vendor and IBM Business Partner regarding the security of this system. A peering agreement for hardware and data restoration is in place for your mainframe system. This system is your principle business computer, holding customer balance and transaction data. This plan is tested annually. The disaster recovery plan for this system is excellent.

Your organization is taking basic data backup processes for your PC systems seriously. However, some elements to ensure a quick, successful recovery are missing. Baseline backups of key PC systems must be performed on a routine basis. Data stored at an insecure site should be encrypted. Two generations of monthly backups should be maintained, providing multiple restore points. A formal new tape rotation should be instituted. A compatible or duplicate tape drive should be available in both Site1 and Site2. A test of the backup/data recovery should be performed at least once per year at each site.

A dialup access alternative should be considered to temporarily replace an unavailable T1 between Site1 and Site2. This backup dialup circuit should require manual activation at each end. The will allow you to meet your regulatory requirement to provide Site2 with constant service from Site1.

Data security, privacy security and disaster recovery should be regarded as a process and not a destination. This baseline security audit was designed to identify and correct major issues. Maintaining quarterly reviews of your security and disaster recovery plans must entail adjusting to business changes, adjusting to known threats, and implementing best practices to safeguard your data. Monitoring your network, your endpoint devices and practices is essential to

maintaining data security and mitigating developing risks. Through a process of continual review and enhancement, your systems security and ability to respond to disaster will continue to increase.

Baseline Security Audit for CompanyX
April 2006

Full Report

Conducted by Rich Bright

On April 11, 2006 the Windows computers located the CompanyX were inspected as part of a baseline security audit. On April 26, 2006 the computers at CompanyX - Site2 were inspected as part of a baseline security audit. In both cases, steps to correct immediate a significant security threats were taken. Your IBM mainframe was not included in this security baseline. Please consult with your software vendor and IBM Business Partner regarding the security of this system. Additional information was gathered through interviews with CompanyX officers, and informal discussions with staff. The goal of the information security audit was to:

Assess existing and needed security measures to protect the business information of the CompanyX and privacy of existing and potential customers regarding daily operation and disaster recovery.

Specifically, the general goals of the baseline security audit were to :

1. Identify and correct common security flaws at the network level

2. Identify and correct common security flaws at the desktop level

3. Identify strengths of existing security processes

4. Identify areas for security improvements

5. Assess weakness in the current disaster recovery plan

A significant amount of raw data related to the security baseline has been provided to CompanyX as documentation of the results related to individual computers. This document will provide a written overview of the results with specific recommendations.

Additional verbal reviews and alternative courses of action have be discussed. At the CompanyX's request, this document will not cover detailed testing processes and specific detailed remediation if such remediation is common in the IT industry. According to the privacy policy provided by Bright Ideas to the CompanyX, Bright Ideas will not retain any copies of the detailed data regarding each computer as a measure to decrease the possibility of theft of detailed information related to your network and networking devices. Therefore, the CompanyX is expected to provide off site duplicate storage of this information which may be required for future reference and regulatory compliance. Throughout this document *underlined italics* will be used to denote suggested improvements and **bold type** will be used to indicate needed changes.

Your data security is critical to maintaining business information and protecting the privacy of current and potential customers. While there is no such thing as total data security, many steps can be taken to manage the risk. Your information security is only as strong as the weakest link in a security chain. Security weakness and process weakness will be noted and corrected as quickly as possible. Mitigation of risk is accomplished by applying best industry practices, correcting configuration errors, and upgrading components as needed. The goal in managing data security and mitigating risk is to provide multiple layers of defense, commonly called Defense in Depth. The layers should offer protection, recognition of breaches in defense and an audit trail to determine how and from where successful attacks were launched. Because the threats to your data are ever evolving, network security must be seen as a process and not a destination.

You must provide physical security of data systems, security at the network level and security of the individual desktop computer. In simple terms, you must keep bad data traffic away from your computers and monitor you computers and network for bad traffic. I observed generally good physical security, CompanyX patrons do not have access to data systems. Data tapes and reports were stored securely. As an improvement to physical security, **password protected screen savers** might be employed to restrict access when CompanyX employees momentarily leave the office possibly granting unattended patrons with physical access to the data systems

As discussed, the CompanyX's network security plan provides layers of defense. The first layer of defense is provided by your SonicWall TZ-170 firewall appliance. SonicWall is recognized as an excellent firewall providing stateful packet inspection, network defense and logging of network attacks. This firewall should be recognized as a strength of your existing network security. Firewall logs and alerts are routinely emailed to CompanyX personnel and reviewed for unusual activity. CompanyX personnel can request additional help in determining the nature and/or threat from unexplained firewall logs. These logs are emailed in clear text across the public Internet and could potentially provide hackers with additional knowledge of your network design. While this risk is low, a *private email server*, accessible only from within the CompanyX, could be added to your network for the sole purpose of emailing network alerts. This would eliminate the risk of interception across the public Internet. The estimated cost to implement such a server is less than $100.

The firewall layer sets rules which allow or disallow Internet and LAN network connections. Your firewall is configured to automatically ignore most malicious connections. **Unsecured PC's or high value targets on your LAN can be blocked from Internet access** at this level. Some rules in your firewall already do this. As additional high value targets or relatively unsecured PC's are identified, additional rules should be added. **Your document image servers should be restricted from internet access.** *Your mainframe should be blocked from Internet access.* Firewalls restrict traffic based on rules which define appropriate sources, destinations and type of connection (protocol and port). Your SonicWall firewall can also restrict Internet access by time of day. It is possible to *deny all access to and from the Internet outside normal business hours.* Some time window for software and antivirus updates must be taken into account.

Your SonicWall provides stateful packet inspection as an added feature. In simple terms, stateful packet inspection performs a "context check" to make sure the requested network connection "makes sense" based on the recent flow of traffic. For example, a standard firewall might allow all web connections (on TCP port 80). A stateful firewall might drop an incoming web connection if the LAN PC had not initiated a request for a web document from the

sending server. That is, the connection from outside did not "make sense" without a LAN side request to set a web connection state.

While your firewall is a strength of your current network security, it does nothing to examine the content of traffic allowed to pass from the Internet to your LAN. You currently depend on the Norton Internet Security program suite to alert you of malicious traffic on your network. SonicWall recently introduced additional Intrusion Prevention, Gateway Antivirus and Anti-spyware recognition/preventive services which are available as an add-on to your existing firewall. These services would be useful in determining if "bad traffic" was being sent to your LAN from "good places". These services can automatically stop such traffic or provide alerts. **The addition of IPS, Antivirus and Anti-spyware services to your SonicWall would be a valuable addition to your network defense.** Estimated cost to implement these additions to your SonicWall is about $350. Annual renewal of approximately $200 would be required. Because malicious traffic or programs can be brought into your network through removable storage, Norton Internet Security will remain an important element of your network and more specifically your desktop security plan. Without an IDS you are unaware of the specific types of attacks being launched against your facility. Recognizing attack patterns may lead to improved defenses.

Currently, Norton Internet Security is your only means of logging suspicious or malicious network activity. Currently, your ability to determine how a successful attack was launched is extremely limited. **A SYSLOG server should be implemented to provide additional logging of network traffic.** Your firewall (and other devices) can send message to the SYSLOG server. This syslog provides a source of forensic data following any successful attacks against your data systems. We have discussed the various implementation options, backup options and related costs.

Currently, Norton Internet Security (NIS) is your only means of detecting and preventing network intrusion. NIS protects only the local computer it is installed on and does little to protect other network devices. You will find the addition of Intrusion Detection/Prevention at the firewall level a significant improvement. You may also wish to consider the implementation of a *passive Intrusion Detection System* (IDS) at the network level, inside your existing firewall. Such a system could be used to detect a full array of

network attacks. However, given the high occurrence of false positives with such a system and your lack of full time IT staff, I suggest setting the internal IDS to monitor network activities which pose only the highest risk. Such activities might be any network attempted administrative or root login to your PC's, mainframe, servers, firewall and routers. **A paper log of normal maintenance activity should be kept in order to facilitate the quick explanation of some alerts.**

There is an ongoing need to maintain good separation between the administrative password of your PC's and of your network devices. You must continue to use different passwords on the LAN and on the network devices. In small organizations such as yours, the tendency is to consolidate those passwords to simplify management. To do so would be a mistake. The LAN administrative passwords currently in use have not been changed in a long time. This increases the likelihood that unauthorized persons may have acquired administrative passwords. I understand the small size of your organization makes the widespread sharing of such information likely. *You must assess the risks and change passwords as needed.* Some organizations routinely change administrative passwords every 180 days or more often. **Sealed envelopes containing administrative passwords** should be kept securely onsite and offsite. These files should be reviewed and updated quarterly, or more often as changes dictate. *Changing administrative passwords should be considered with the departure of any employee.* Employees showed appropriate respect for safeguarding passwords. When I asked one employee if she knew the password for a computer, she smiled and wrote it down and then took the paper saying "I'd better shred that."

Using a firewall to appropriately limit access to the network from the outside is only the first step in securing your network. No modems were found to answer on any phone line. No wireless network, laptop use or VPN access was found. Fundamentally, security on the LAN requires securing the desktop PC's, controlling access to the network, identifying all authorized network devices, monitoring for unauthorized devices, identifying and controlling services and devices shared to network users.

There is currently no IDS at the network level. Only Norton Internet Security performs this function at the desktop level. The

addition of IDS/IPS to your firewall and the establishment of network IDS have been discussed in previous paragraphs.

While the current wiring structure is understood, it is not documented. Therefore, it is not possible to say with certainty that no new devices have been physically connected to the network. **A diagram of physical connectivity should be developed and audited on a routine basis**. Unused network ports should be taped off or plugged so they can be easily identified as unused.

I understand the T1 connection between Site1 and Site2 is a private circuit. *A letter from NetworkProvider stating that the circuit is private should be on file.* If the circuit is not private, then you must begin to encrypt traffic between the sites.

A general assessment of the network was made and a detailed checklist has been provided. A baseline of network devices, IP addresses, network shares and service presentation was established. No unexpected devices were found. All expected shares were found. The "old public" share on the "Old Sharon" computer was removed and the files were deleted from the repurposed computer. A Network Time Protocol client was installed as needed and all PC's and the firewall now establish a common time base with the time servers maintained by nist.gov. Network Address Translation is provided by the firewall to isolate the PC's from the public Internet. **Internet access to the VNC service should be blocked at the firewall.** VNC is sometimes used between Site2 and Site1 as a troubleshooting tool.

Appropriate backups of network device configuration were made to facilitate network disaster recovery. This should be done at least quarterly. A copy should be stored securely offsite.

Once basic security of the network has been established, securing the desktop PC must be accomplished. Fundamentally, desktop security requires appropriate updating of the operating system and standard applications software, preventing and detecting malware, control of user logins and control of network shares.

It is critical to secure the operating system against known threats by applying appropriate patches provided by the manufacturer. The updating of applications software is also important in closing known vulnerabilities. **All systems were**

brought to current standards using the Microsoft Update service. With very few exceptions, PC's were properly configured to download and apply critical patches as soon as they are made available by Microsoft. Any machine not properly configured was changed. The exception to this rule is the document imaging computers according to the vendors recommendation. These imaging computers have been blocked from Internet access at the firewall. Many computers required a great many "noncritical" updates. Certainly this process required significantly more time than we estimated due to the number of machines requiring many, many updates. These "noncritical" updates are not automatically downloaded and installed. In some cases, these updates play a significant role in maintaining a secure desktop, despite the fact that Microsoft did not award the "Critical" rating to the patches. These updates will continue to be reviewed in our quarterly audits. We have discussed additional options for dealing with noncritical updates.

All operating systems used at your facilities are currently supported by Microsoft. A majority of your computers use the Windows 2000 operating system. This operating system moved from "Mainstream Support" to "Extended Support" June 30, 2005. In the extended support phase, Microsoft provides only security related fixes and will not add any additional functionality. Extended support is scheduled to end for Windows 2000 on July 13, 2010. There is no expectation Microsoft will extend support of any type beyond that date.

Proper configuration of antivirus, desktop firewall and anti-spyware software is essential to securing the PC from malware. The configuration of Norton Internet Security was reviewed and in some cases changes were made. In most cases, only a quick scan was being performed. **A full system scan is now being be performed.**

Your NIS 2006 provides much better anti-spyware protection than the 2005 edition previously used. According to Symantec, NIS 2006 can be used to detect and prevent spyware infections. Independent testing indicates NIS 2006 is much better at post infection spyware detection than active prevention. NIS 2006 lags significantly when compared to Webroot's SpySweeper in terms of real time prevention. You may want to *consider purchasing SpySweeper* for those computers which use the Internet a great deal involving

untrusted sites. Each computer was inspected to determine if viruses or spyware was installed. Internet Explorer Browser Helper Objects (BHO's) were assessed to determine if the IE browser had been compromised. Mozilla FireFox 1.5.1 was installed as an alternative to Microsoft's Internet Explorer. **The use of FireFox greatly mitigates the threat of spyware infection from simple browsing**. The combination of IDS/IPS at the firewall and FireFox greatly reduces your probability of system compromise due to spyware.

All systems were scanned for rootkit infestation. No rootkits were found. All computers were scanned for viruses and spyware infection. Minor adware infections were found and removed on the following computers: BigBoss, User2, User3, Site2 User4. The adware on these computers altered the normal ads on a page and/or caused popup ads. The adware found on these computers did not pose a significant threat to the overall security of the system. Details of the infections are provided for each computer. These computers should be rescanned for possible reinfection which might indicate a more significant problem. The introduction of the FireFox browser is a significant step in limiting the spyware problem.

A large number of adware programs were found on the Site2 Worker23 computer. Reinfection occurred following removal. Therefore the hard drive was reformatted and the entire system was reloaded. The system is now secured. The Winfixer virus was also found. The Winfixer virus must be manually downloaded and installed. It raises popups exaggerating security problems to entice the user to buy security programs online in order to fix the (alleged) security problems. No trojans or other keylogging types of programs were found. This infection probably started when a former employee downloaded the Grokster file sharing program. Filesharing sites pose a risk to your network because the source of the file is unknown. *Filesharing probably has no legitimate business use and should be banned by your acceptable use policy.* Grokster and the MySearch adware appear to have been installed 8/12/2005. Additional adware was installed on 10/26/2005 and 11/25/2005. There were 118 different adware items found with over 14000 traces (cookies etc) found. The hard drive was reformatted and the entire system was reloaded.

User logins were audited on each computer. With few exceptions, no problems were found and those problems were corrected. The most significant problem related to user logins is the

widespread use of the administrator account in Site1. This presents a great security risk to the individual PC and also to the network. Non administrative logins complicate system modification by users, but also protect the system from unauthorized software installation and system modifications. **Non-administrator logins must be implemented by staff at Site1.** CompanyX officers may still use a common login to avoid file ownership issues, but the common login should not have administrator privileges.

The disaster recovery plan of he CompanyX are comprehensive and constantly evolving. The goal of disaster recovery planning is to provide virtually seamless, continuous operations by instituting recovery plans which account for the loss of data due to inaccessibility resulting from physical loss or damage, equipment failure, data corruption or loss of key personnel. Using Site2 and Site1 as CompanyX's secure offsite storage of reports, data backup and other operational plans is a strength of your plans.

A peering agreement for hardware and data restoration is in place for your mainframe system. This system is your principle business computer, holding customer balance and transaction data. Your service agreements for this hardware and software provide qualified technical support as needed to implement the recovery plan. No assessment was made regarding hardening or auditing of this data system. *A security audit of this system is best performed by the vendors providing hardware and software support for the mainframe or vendors recommended by your support contacts.* The data is backed up to tape and optical storage providing baseline backups, multiple generations of data backup and multiple recovery points. Rotation and replacement of data tapes is adequate. Old data tapes are rendered inoperable and burned when removed from service. This plan is tested annually. The disaster recovery plan for this system is excellent.

Your organization is taking basic data backup processes for your PC systems seriously. However, some elements to ensure a quick, successful recovery are missing. Key data is routinely backed up to tape or CDR and data is stored offsite. Old data tapes are rendered inoperable and burned when removed from service. *The destruction of retired optical media should be clarified.* Qualified technical support is available as needed.

Currently no baseline backups or multi-generational backups are consistently performed on the SoftwarePackage2 or SiteDirector software systems. **Baseline backups of key PC systems must be performed on a routine basis.** I suggest a quarterly baseline backup, maintaining at least two generations. **Data stored at an insecure site should be encrypted.** *Two generations of monthly backups should be maintained to provide multiple restore points.* Tapes have been replaced on an as needed basis. **A formal new tape rotation should be instituted.** The manufactures MTBF data should be consulted in planning the tape rotation plan. Tapes should be marked with a retirement date when inserted into rotation. Suitable options have been discussed. While data is currently backed up consistently, there is no guarantee the data could be read if the original tape drive was unavailable. **A compatible or duplicate tape drive should be available in both Site1 and Site2** to speed recovery of archived data. Complete hardware mirrors available at each site speed and simplify data restoration. **A test of the backup/data recovery should be performed at least once per year at each site.** This test should be performed on a temporary scratch drive and the working drive should be disabled during the test.

The Site2 facility depends on the private T1 line for access to live account balances and other data via the mainframe. This need is currently met using voice communication via telephone in emergency situations. *A dialup access alternative should be considered to temporarily replace an unavailable T1.* **This backup dialup circuit should require manual activation at each end.**

Key passwords are shared among multiple users but are not archived. A significant loss of personnel could leave some systems unavailable in a timely fashion. **Secured envelopes containing all needed administrative passwords and logins for all systems, both internal and external, should be kept at secured offsite locations.** This password CompanyX should be updated and its existence verified monthly. Processes to implement this system have been discussed.

Data security, privacy security and disaster recovery should be regarded as a process and not a destination. This baseline security audit was designed to identify and correct major issues. Maintaining quarterly reviews of your security and disaster recovery plans must entail adjusting to business changes, known threats, and best

practices to safeguard your data. Monitoring your network, your endpoint devices and practices is essential to maintaining data security and mitigating developing risks. Through a process of continual review and enhancement, your systems security will continue to increase with time. F*uture audits should include a complete evaluation of system processes and services started at boot for each computer.* Unneeded process and services can then be stopped to harden the desktop PC.

In short, I found your security and disaster planning to be adequate with room for some improvement as noted in the preceding paragraphs.

Bright Ideas *Complete Computer Solutions*
PO Box 103
Macon MO 63552
(660) 385-5894 voice

Mr. Bigshot, President
CompanyX
PO Box 10
Site1 MO 66666

June 7, 2006

Mr. Bigshot,

Below is a summary of changes and/or plans made to increase your data security and disaster recovery following the recent baseline security audit of CompanyXs information systems. These changes, along with the modifications made during the actual audit substantially increase your security.

The SonicWall TZ-170 firewall was updated to the most recent firmware.

SonicWall Intrusion Prevention Service, SonicWall Gateway Antivirus and SonicWall Gateway Anti Spyware services were added to your firewall. These services are currently operating in notification mode, rather than prevention mode. You will see the additional notification/alert emails along with the current firewall alert emails. Prevention mode offers greater security, but has the potential to create greater disruption of work flow. In time, prevention mode should be tested to achieve an acceptable balance between security and functionality.

Unsecured and high value targets on your network were blocked from internet access at the firewall.

A SYSLOG server was installed to provide forensic data in case of successful attack.

Preparations for comprehensive, secured password storage have begun.

A diagram of physical connectivity will be developed.

The the defective hard disk has been replaced in the computer for the Site2 Worker12 and this machine has passed the same security baseline as your other PCs.

I understand that stronger administrative passwords are now in use at the Site1 facility.

Preparations for compatible/duplicate tape drives at Site1 and Site2 are being made.

Thank you for the opportunity to assist your organization in its plans to protect privacy, secure data and plan for continued operation in difficult circumstances. I look forward to working with you and CompanyX as we continue to improve your efforts in these difficult and rapidly changing areas.

Sincerely

Rich Bright

Quarterly Information Security Audit
CompanyX

July 2006

Personal computers used by CompanyX were inspected as part of a quarterly security audit performed by Bright Ideas. Your IBM mainframe was not included in this security baseline. Please consult with your software vendor and IBM Business Partner regarding the security of this system. Additional information was gathered through interviews with CompanyX officers, and informal discussions with staff. A significant amount of raw data related to the security baseline has been provided to CompanyX as documentation of the results related to individual computers.

The goal of the information security audit was to:

Assess existing and needed security measures to protect the business information of the CompanyX and privacy of existing and potential customers regarding daily operation and disaster recovery.

In short, I found your security and disaster planning to be adequate. Suggested changes are noted below. This security audit is part of an ongoing effort to verify and maintain information security. Changes made during previous security audit were assessed for effectiveness and consistency of application. No significant new threats were discovered.

Your data security is critical to maintaining business information and protecting the privacy of current and potential customers. While there is no such thing as total data security, many steps can be taken to manage the risk. Your information security is only as strong as the weakest link in a security chain. Mitigation of risk is accomplished by applying best industry practices, correcting configuration errors, and upgrading components as needed. The goal in managing data security and mitigating risk is to provide multiple layers of defense. The layers should offer protection, recognition of breaches in defense and an audit trail for analyzing successful attacks. Because the threats to your data are ever evolving, network security must be seen as a process and not a destination.

Your stateful packet inspection firewall should be recognized as a strength of your existing network security. Firewall logs and alerts are routinely emailed to CompanyX personnel and reviewed for unusual activity. Unsecured PC's or high value targets on your LAN are blocked from Internet access at this level. The implementation of SonicWall's Intrusion Prevention Service, Gateway Antivirus and Anti-spyware service is a valuable addition to your network defense. These services were renewed for a period of one year. <u>This service must be annually renewed July 1st.</u>

Using a firewall to appropriately limit access to the network from the outside is only the first step in securing your network. No wireless network, laptop use or VPN access was found. A diagram of physical connectivity should be developed and audited on a routine basis.

You currently depend on the Norton Internet Security (NIS) program suite to alert you of malicious traffic on your local network. Because malicious traffic or programs can still enter your network, Norton Internet Security will remain an important element of your security plan. NIS is updating and scanning the computers on your network appropriately.

A SYSLOG server was recently implemented to provide additional logging of network traffic. This syslog provides a source of forensic data following any successful attacks against your data systems. This server was working properly.

The implementation of stronger administrative passwords at the Site1 facility is a significant improvement. Secured envelopes containing all needed administrative passwords and logins for all systems, both internal and external, should be kept at secured offsite locations.

A baseline of network devices, IP addresses, network shares and service presentation was established. No unexpected devices were found. All expected shares were found. Appropriate backups of network device configuration were made.

It is critical to secure the operating system against known threats by applying appropriate patches provided by the manufacturer. All systems are normally brought to current standards using the Microsoft Update service. Many machines experienced problems installing several patches. Frequently, these types of problems are related to a single computer and/or a single patch. They are often the result of conflicts among, software installed on the individual computer, the Microsoft Update Service and the software patch itself. The needed patches were downloaded from Microsoft and installed manually. Occasional failures of this type are not uncommon. but a pattern of problems should be a concern.. The timeliness and effectiveness of Microsoft Update should be monitored. Relatively inexpensive alternatives to this service are available should problems persist. All operating systems used at your facilities are currently supported by Microsoft.

Mozilla FireFox 1.5 was updated to the current version and Firefox was configured to automatically update itself in the future. The use of FireFox greatly mitigates the threat of spyware infection from simple browsing. The combination of IDS/IPS at the firewall and FireFox greatly reduces your probability of system compromise due to spyware. The addition of Webroot's Spysweeper, especially on high internet usage workstations, would also improve your spyware defences. All systems were scanned for rootkit infestation. No rootkits were found. All computers were scanned for viruses and spyware

infection. Minor adware infections were found and removed on some computers.

User logins were audited on each computer. No problems were found. The implementation of stronger administrative passwords at the Site1 facility is a significant improvement.

Your organization is taking basic data backup processes for your PC systems seriously. However, some elements to ensure a quick, successful recovery are missing. Baseline backups of key PC systems must be performed on a routine basis. Data stored at an insecure site should be encrypted. Two generations of monthly backups should be maintained, providing multiple restore points. A formal new tape rotation should be instituted. A compatible or duplicate tape drive should be available in both Site1 and Site2. A test of the backup/data recovery should be performed at least once per year at each site.

Data security, privacy security and disaster recovery should be regarded as a process and not a destination. This security audit was designed to identify and correct both recent changes and major issues. Maintaining quarterly reviews of your security and disaster recovery plans must entail adjusting to business changes, adjusting to known threats, and implementing best practices to safeguard your data. Monitoring your network, your endpoint devices and practices is essential to maintaining data security and mitigating developing risks. Through a process of continual review and enhancement, your systems security and ability to respond to disaster will continue to increase.

Quarterly Information Security Audit
CompanyX

October 2006

Personal computers used by CompanyX were inspected as part of a quarterly security audit performed by Bright Ideas. Your IBM mainframe was not included in this security baseline. Please consult with your software vendor and IBM Business Partner regarding the security of this system. Additional information was gathered through interviews with CompanyX officers, and informal discussions with staff. A significant amount of raw data related to the security baseline has been provided to CompanyX as documentation of the results related to individual computers.

The goal of the information security audit was to:

Assess existing and needed security measures to protect the business information of the CompanyX and privacy of existing and potential customers regarding daily operation and disaster recovery.

In short, I found your security and disaster planning to be adequate. Suggested changes are noted below. This security audit is part of an ongoing effort to verify and maintain information security. Changes made during previous security audit were assessed for effectiveness and consistency of application. No significant new threats were discovered.

Your data security is critical to maintaining business information and protecting the privacy of current and potential customers. While there is no such thing as total data security, many steps can be taken to manage the risk. Your information security is only as strong as the weakest link in a security chain. Mitigation of risk is accomplished by applying best industry practices, correcting configuration errors, and upgrading components as needed. The goal in managing data security and mitigating risk is to provide multiple layers of defense. The layers should offer protection, recognition of breaches in defense and an audit trail for analyzing successful attacks. Because the threats to your data are ever evolving, network security must be seen as a process and not a destination.

Your stateful packet inspection firewall should be recognized as a strength of your existing network security. Firewall logs and alerts are routinely emailed to CompanyX personnel and reviewed for unusual activity. Unsecured PC's or high value targets on your LAN are blocked from Internet access at this level. The implementation of SonicWall's Intrusion Prevention Service, Gateway Antivirus and Anti-spyware service is a valuable addition to your network defense.

Using a firewall to appropriately limit access to the network from the outside is only the first step in securing your network. No wireless network,

laptop use or VPN access was found. A diagram of physical connectivity should be developed and audited on a routine basis.

You currently depend on the Norton Internet Security (NIS) program suite to alert you of malicious traffic on your local network. Because malicious traffic or programs can still enter your network, Norton Internet Security will remain an important element of your security plan. NIS is updating and scanning the computers on your network appropriately. All computers were configured to perform a full scan on a daily basis, rather than a weekly basis.

A SYSLOG server provides a source of forensic data following any successful attacks against your data systems. This server was working properly. It did experience an undetected failure for a period of several days. A process to routinely test its function should be implemented.

Secured envelopes containing all needed administrative passwords and logins for all systems, both internal and external, should be kept at secured off site locations.

A baseline of network devices, IP addresses, network shares and service presentation was established. No unexpected devices or shares were found. All expected shares were found. Appropriate backups of network device configuration were made. Obsolete file shares were also deleted from the Worker3 computer.

It is critical to secure the operating system against known threats by applying appropriate patches provided by the manufacturer. All systems are normally brought to current standards using the Microsoft Update service. Some machines experienced problems installing several patches. Frequently, these types of problems are related to a single computer and/or a single patch. They are often the result of conflicts among, software installed on the individual computer, the Microsoft Update Service and the software patch itself. The needed patches were downloaded from Microsoft and installed manually. Occasional failures of this type are not uncommon. but a pattern of problems should be a concern.. The timeliness and effectiveness of Microsoft Update should be monitored. Relatively inexpensive alternatives to this service are available should problems persist. Should similar problems acquiring Microsoft Automatic Updates become evident during the next quarterly audit, active investigation into alternatives should begin. All operating systems used at your facilities are currently supported by Microsoft.

A new shutdown process will be implemented for all computers at Site2. Some computers were turned of at night and others were left logged in on low privilege user accounts. This prevented antivirus scans and operating system updates from completing properly. From this point forward, all computers will be left turned on and logged out from all user accounts. Secondary administrative accounts should be created on some computers during the next audit.

Mozilla FireFox 1.5 was updated automatically. The use of FireFox greatly mitigates the threat of spyware infection from simple browsing. The combination of IDS/IPS at the firewall and FireFox greatly reduces your probability of system compromise due to spyware. The addition of Webroot's Spysweeper, especially on high internet usage workstations, such as CompanyX officers, would also improve your spyware defenses. All systems were scanned for rootkit infestation. No rootkits were found. All computers were scanned for viruses and spyware infection. Minor adware infections were found and removed on some computers.

User logins were audited on each computer. Generally, no problems were found. Previously disabled user accounts on the Worker3 computer (which was previously used as a file server) were deleted.

Some unexpected software was found to be installed. Your organization should determine if this software should remain on the computers. The Google Desktop Search and Google Toolbar were installed on the Bookkeeping machine. Yahoo Messenger was installed on Manager4 and MS Messenger was installed on Worker2. The Broadcast PC adware software was found and removed from Worker5.

Several minor changes were found which do not significantly impact your network security, but they do impede the efficiency of your network operations. These items can be addressed during your next audit to improve efficiency. There has been some divergence from the standard hosts file used to resolve names on your local network. A revised, standard hosts file should be placed on each computer during the next audit. A different issue is caused by the lack of a domain controller on your LAN. Normally, the domain controller serves as the master browser on a network. When a domain controller is not on a network, the various computers engage in a process known as a Master Browser War to determine which computer should be in charge of the network. Since the implementation of SoftwarePackage2 in Site2, the number of Master Browser Wars has increased dramatically. This produces large amounts of unnecessary network traffic and causes large numbers of events to be written into the event logs on the hard disk. Registry changes can be made to reduce this unnecessary logging and network traffic.

Your organization is taking basic data backup processes for your PC systems seriously. However, some elements to ensure a quick, successful recovery are missing. Baseline backups of key PC systems must be performed on a routine basis. Data stored at an insecure site should be encrypted. Two generations of monthly backups should be maintained, providing multiple restore points. A formal new tape rotation should be instituted. A compatible or duplicate tape drive should be available in both Site1 and Site2. A test of the backup/data recovery should be performed at least once per year at each site. Active investigation, consideration of alternatives and implementation at both Site1 and Site2 has begun.

Data security, privacy security and disaster recovery should be regarded as a process and not a destination. This security audit was designed to identify and correct both recent changes and major issues. Maintaining quarterly reviews of your security and disaster recovery plans must entail adjusting to business changes, adjusting to known threats, and implementing best practices to safeguard your data. Monitoring your network, your endpoint devices and practices is essential to maintaining data security and mitigating developing risks. Through a process of continual review and enhancement, your systems security and ability to respond to disaster will continue to increase.

Quarterly Information Security Audit
CompanyX

January 2007

Personal computers used by CompanyX were inspected as part of a quarterly security audit performed by Bright Ideas. Your IBM mainframe was not included in this security baseline. Please consult with your software vendor and IBM Business Partner regarding the security of this system. Additional information was gathered through interviews with CompanyX officers, and informal discussions with staff. A significant amount of raw data related to the security baseline has been provided to CompanyX as documentation of the results related to individual computers.

The goal of the information security audit was to:

Assess existing and needed security measures to protect the business information of the CompanyX and privacy of existing and potential customers regarding daily operation and disaster recovery.

In short, I found your security and disaster planning to be adequate. Suggested changes are noted below. This security audit is part of an ongoing effort to verify and maintain information security. Changes made during previous security audit were assessed for effectiveness and consistency of application. No significant new threats were discovered. The implementation of blur filters on monitors accessible to the public improves the privacy of displayed data.

Your data security is critical to maintaining business information and protecting the privacy of current and potential customers. While there is no such thing as total data security, many steps can be taken to manage the risk. Your information security is only as strong as the weakest link in a security chain. Mitigation of risk is accomplished by applying best industry practices, correcting configuration errors, and upgrading components as needed. The goal in managing data security and mitigating risk is to provide multiple layers of defense. The layers should offer protection, recognition of breaches in defense and an audit trail for analyzing successful attacks. Because the threats to your data are ever evolving, network security must be seen as a process and not a destination.

Your stateful packet inspection firewall should be recognized as a strength of your existing network security. Firewall logs and alerts are routinely emailed to CompanyX personnel and reviewed for unusual activity. Unsecured PC's or high value targets on your LAN are blocked from Internet access at this level. The video recorders in both Site1 and Site2 were blocked from internet access at the firewall. The implementation of SonicWall's Intrusion Prevention Service, Gateway Antivirus and Anti-spyware service is a valuable addition to your network defense. These add-on SonicWall security services must be renewed by

July, 2007. An optional firmware update to the SonicWall required to implement the new Daylight Savings Time is expected to be available in late spring 2007.

Using a firewall to appropriately limit access to the network from the outside is only the first step in securing your network. No wireless network, laptop use or VPN access was found. A diagram of physical connectivity should be developed and audited on a routine basis.

You currently depend on the Norton Internet Security (NIS) program suite to alert you of malicious traffic on your local network. Because malicious traffic or programs can still enter your network, Norton Internet Security will remain an important element of your security plan. NIS is updating and scanning the computers on your network appropriately. All computers were configured to perform a full scan on a daily basis, rather than a weekly basis. Some computers will require the renewal of NIS in coming weeks. The NIS software will provide sufficient notice and prompt you repeatedly to renew your subscription.

A SYSLOG server provides a source of forensic data following any successful attacks against your data systems. This server was working properly. It did experience an undetected failure for a period of several days. A process to routinely test its function was reviewed. The implementation of a second, redundant SYSLOG should be implemented when pending computer upgrades are performed. This can be accomplished using free software and an older computer.

Secured envelopes containing all needed administrative passwords and logins for all systems, both internal and external, should be kept at secured off site locations.

A baseline of network devices, IP addresses, network shares and service presentation was established. No unexpected devices or shares were found. All expected shares were found. Appropriate backups of network device configuration were made.

It is critical to secure the operating system against known threats by applying appropriate patches provided by the manufacturer. All systems are normally brought to current standards using the Microsoft Update service. Some machines experienced problems installing several patches. Nearly identical systems were succesfully patched. Frequently, these types of problems are related to a single computer and/or a single patch. They are often the result of conflicts among, software installed on the individual computer, the Microsoft Update Service and the software patch itself. All needed patches were downloaded from Microsoft and installed manually. Occasional failures of this type are not uncommon. but a pattern of problems should be a concern. The timeliness and effectiveness of Microsoft Update should be monitored. Relatively inexpensive alternatives to this service are available should problems persist. Problems using Windows 2000 and the Microsoft Update Service (instead of Windows Update Service) seem most severe, yet inconsistent. Because a relatively small number of patches were required for Windows 2000 systems during the quarter preceeding this audit, it is difficult to determine if prior

changes in process have been effective in improving the automated patching of Windows 2000 systems. Should similar problems acquiring Microsoft Automatic Updates become evident during the next quarterly audit, active investigation into alternatives should begin. All operating systems used at your facilities are currently supported by Microsoft.

The new evening shutdown process (leaving all computers turned on and logged out from all user accounts) implemented for all computers at Site2 seems to be working as desired. Secondary administrative accounts were created on some computers as needed.

All systems were scanned for rootkit infestation. No rootkits were found. All computers were scanned for viruses and spyware infection. No unexpected Browser Helper Objects (BHO) were found. Minor adware infections were found and removed on one computer. The Broadcast PC adware software was found and removed from the User9 computer. No other malware was found. No unexpected software was found to be installed. User logins were audited on each computer with no problems found. Archival data on the User6 computer (retained from it's prior use as a file server) was securely deleted.

Mozilla FireFox 1.5 was automatically updating as expected. Mozilla FireFox 2.0 was installed on selected computers as a test because support for FireFox 1.5 will be phased out late spring 2007. Assuming FireFox 2.0 causes no unexpected problems, FireFox 1.5 should be upgraded to 2.0 during the next security audit. The use of FireFox greatly mitigates the threat of spyware infection from simple browsing. The combination of IDS/IPS at the firewall and FireFox greatly reduces your probability of system compromise due to spyware. The addition of Webroot's Spysweeper subscriptions, especially on high internet usage workstations, such as CompanyX officers, would also improve your spyware defenses.

Several minor changes were made which do not significantly impact your network security, but they do improve the efficiency of your network operations. There has been some divergence from the standard hosts file used to resolve names on your local network. A revised, standard hosts file was placed on each computer for consistent name resolution. The registry changes made to computers at Site2 has eliminated the problems of Master Browser Wars. This problem was caused by the lack of a domain controller on your LAN. Normally, the domain controller serves as the master browser on a network. When a domain controller is not on a network, the various computers engage in a process known as a Master Browser War to determine which computer should be in charge of the network. The implementation of KeySoftwarePackage2 in Site2 caused a dramatic increase in the number of Master Browser Wars. This produces large amounts of unnecessary network traffic and causes large numbers of events to be written into the event logs on the hard disk. The Registry changes reduced this unnecessary logging and network traffic. A similar process should be implemented on the Windows 2000 computers in Site1 during the next security audit.

Your organization is taking basic data backup processes for your PC systems seriously. However, some elements to ensure a quick, successful recovery are missing. Baseline backups of key PC systems must be performed on a routine basis. Data stored at an insecure site should be encrypted. Two generations of monthly backups should be maintained, providing multiple restore points. A formal new tape rotation should be instituted. A compatible or duplicate tape drive should be available in both Site1 and Site2. A test of the backup/data recovery should be performed at least once per year at each site. Active investigation and consideration of alternatives has been completed. These changes to backup processes will be implemented at both Site1 and Site2 when the pending new computers are installed..

Data security, privacy security and disaster recovery should be regarded as a process and not a destination. This security audit was designed to identify and correct both recent changes and major issues. Maintaining quarterly reviews of your security and disaster recovery plans must entail adjusting to business changes, adjusting to known threats, and implementing best practices to safeguard your data. Monitoring your network, your endpoint devices and practices is essential to maintaining data security and mitigating developing risks. Through a process of continual review and enhancement, your systems security and ability to respond to disaster will continue to increase.

Quarterly Information Security Audit
CompanyX

April 2007

Personal computers used by CompanyX were inspected as part of a quarterly security audit performed by Bright Ideas. Your IBM mainframe was not included in this security baseline. Please consult with your software vendor and IBM Business Partner regarding the security of this system. Additional information was gathered through interviews with CompanyX officers, and informal discussions with staff. A significant amount of raw data related to the security baseline has been provided to CompanyX as documentation of the results related to individual computers.

The goal of the information security audit was to:

Assess existing and needed security measures to protect the business information of the CompanyX and privacy of existing and potential customers regarding daily operation and disaster recovery.

In short, I found your security and disaster planning to be very good. Suggested changes are noted below. This security audit is part of an ongoing effort to verify and maintain information security. Changes made during previous security audit were assessed for effectiveness and consistency of application. No significant new threats were discovered. Reviews of your security and disaster recovery plans must entail adjusting to business changes, known threats, and best practices to safeguard data and privacy.

Your data security is critical to maintaining business information and protecting the privacy of current and potential customers. While there is no such thing as total data security, many steps can be taken to manage the risk. Your information security is only as strong as the weakest link in a security chain. Mitigation of risk is accomplished by applying best industry practices, correcting configuration errors, and upgrading components as needed. The goal in managing data security and mitigating risk is to provide multiple layers of defense. The layers should offer protection, recognition of breaches in defense and an audit trail for analyzing successful attacks. Because the threats to your data are ever evolving, network security must be seen as a process and not a destination.

Your stateful packet inspection firewall should be recognized as a strength of your existing network security. Firewall logs and alerts are routinely emailed to CompanyX personnel and reviewed for unusual activity. Unsecured PC's or high value targets on your LAN are blocked from Internet access at this level. The implementation of SonicWall's Intrusion Prevention Service, Gateway Antivirus and Anti-spyware service is a valuable addition to your network defense. These add-on SonicWall security services must be renewed by July,

2007. An optional firmware update to the SonicWall required to implement the new Daylight Savings Time is available but was not applied at your request.

Using a firewall to appropriately limit access to the network from the outside is only the first step in securing your network. No wireless network, laptop use or VPN access was found. A diagram of physical connectivity should be developed and audited on a routine basis.

You currently depend on the Norton Internet Security (NIS) program suite and McAfee VirusScan Plus to alert you of malicious traffic on your local network. Because malicious traffic or programs can still enter your network despite your protective firewall, these security suites will remain an important element of your security plan. These programs are updating and scanning the computers on your network appropriately. The McAfee VirusScan Plus package was installed on all Windows 2000 computers because the NIS update would not run on the older Windows 2000 systems. McAfee has integrated smoothly into your operations. The software firewall included in the McAfee product does a better job of masking PC's on your network from general network scanning than the NIS product. The practical outgrowth is to make the computers protected by McAfee harder to detect on the network and therefore reduce the risk of attack against apparently invisible systems. All computers were configured to perform a full scan on a daily basis, rather than a weekly basis.

At this point in time, your greatest risk comes not from a direct assault on your network from outside. Your greatest risk is from compromise of a system behind your firewall which can steal passwords or send information back out using "normal" data traffic such as web access or email. Such a compromise might result from a successful exploit of a known defect in the Windows OS or an application running on your systems. Incoming email and encouraging or forcing the user to view an infected web page are commonly used to gain initial access to your system. Therefore, aggressive use of IPS, antivirus and desktop firewalls is key to securing your data. You may want to consider periodically raising the Sonicwall alert settings to show even low priority events. Raising the alert settings will likely increase the daily email alerts to three or four times normal numbers. The routine audits of systems are also critical.

A SYSLOG server provides a source of forensic data following any successful attacks against your data systems. This existing server was working properly. A process to routinely test its function was reviewed. A second, redundant SYSLOG was implemented on an existing workstation in response to an earlier undetected interruption of the primary SYSLOG server. Both SYSLOG servers will function in the background of your operations. These SYSLOG servers use different operating systems in order to complicate hacking them.

Secured envelopes containing all needed administrative passwords and logins for all systems, both internal and external, should be kept at secured off site locations. I understand this is in process and largely completed pending a formal review.

A baseline of network devices, IP addresses, network shares and service presentation was reviewed. No unexpected devices or shares were found. An additional computer was found. This new computer will be put into service when all programs have been installed. All expected shares were found. Appropriate backups of network device configuration were made.

It is critical to secure the operating system against known threats by applying appropriate patches provided by the manufacturer. All systems are normally brought to current standards using the Microsoft Update service. Once again several machines experienced problems installing several patches. Once again, no clear pattern exists in identifying machines likely to fail in the automatic update process. There does not appear to be a month to month failure pattern on any specific computer. Nearly identical systems were successfully patched alongside machines which failed the patch. Some systems required multiple attempts to manually apply needed patches and others were successfully patched on the first manual attempt. All needed patches were downloaded from Microsoft and installed manually. All operating systems used at your facilities are currently supported by Microsoft.

Occasional failures of this type are not uncommon, but a pattern of problems should be a concern. The consistent and timely application of Microsoft patches has been a recurring issue within your organization. Furthermore, the development of"Patch Tuesday" and "Exploit Thursday" time lines for utilizing known defects to take over desktop systems reinforces the need to apply patches in a timely manner. The timeliness and effectiveness of Microsoft Update should be monitored and active investigation into alternatives should begin. One solution is to login as administrator and manually visit the Microsoft Update site on the second Wednesday of each month. If current patterns persist, you will need assistance in successfully patching a few systems each month. Another solution is to implement an alternative patch management system which still uses the official Microsoft patches. A third party patch management solution will cost $1200-$1500 to implement the first year and have recurring annual fees of approximately $400.

All systems were scanned for rootkit infestation. No rootkits were found. All computers were scanned for viruses and spyware infection. No viruses or trojans were found. No unexpected Browser Helper Objects (BHO) were found. A minor adware infection was found and removed on one computer. The Broadcast PC adware software was found and removed from the Worker8 computer. Using a nonadministrative login on Worker8 will help prevent this type of infection. No other malware was found. No unexpected software was found to be installed. User logins were audited on each computer with no problems found. Secondary administrative accounts were created on some computers as needed Archival data on Employee3's previous computer (retained from it's prior use as a file server) was detected but retained. This data is not shared on the network.

Your administrative passwords have not been changed in over a year. You should consider changing them. There is an ongoing need to maintain good

separation between the administrative password of your PC's and of your network devices. You must continue to use different passwords on the LAN and on the network devices. In small organizations such as yours, the tendency is to consolidate those passwords to simplify management. To do so would be a mistake. The LAN administrative passwords currently in use have not been changed in a long time. This increases the likelihood that unauthorized persons may have acquired administrative passwords. I understand the small size of your organization makes the widespread sharing of such information likely. You must assess the risks and change passwords as needed. Some organizations routinely change administrative passwords every 180 days or more often. Sealed envelopes containing administrative passwords should be kept securely onsite and offsite. These files should be reviewed and updated quarterly, or more often as changes dictate. Changing administrative passwords should be considered with the departure of any employee. Employees showed appropriate respect for safeguarding passwords.

Mozilla FireFox 2.0 was installed because support for FireFox 1.5 is being phased out. The use of FireFox greatly mitigates the threat of spyware infection from simple browsing. The combination of IDS/IPS at the firewall and FireFox greatly reduces the probability of system compromise due to spyware. The addition of Webroot's Spysweeper subscriptions, especially on high internet usage workstations, such as CompanyX officers, would also improve your spyware defenses.

Several minor changes were made which do not significantly impact your network security, but they do improve the efficiency of your network operations. There has been some divergence from the standard hosts file used to resolve names on your local network. A revised, standard hosts file was placed on each computer for consistent name resolution. The McAfee firewall on the Worker24 machine at Site2 was improperly configured resulting in over blocking legitimate and needed network connections. The McAfee firewall was reconfigured to allow needed network resources. The registry changes previously made to computers at Site2 has largely eliminated the problems of Master Browser Wars. This problem was caused by the lack of a domain controller on your LAN. Normally, the domain controller serves as the master browser on a network. When a domain controller is not on a network, the various computers engage in a process known as a Master Browser War to determine which computer should be in charge of the network. This produces large amounts of unnecessary network traffic and causes large numbers of events to be written into the event logs on the hard disk. The Registry changes reduced this unnecessary logging and network traffic. These changes were also made on the Windows 2000 computers in Site1. A fix for the changes to Daylight Savings Time was applied to computers running Windows 2000.

Your organization is taking basic data backup processes for your PC systems seriously. Email received and stored only on local hard disks was at risk. Email is now being backed up and sent to centralized storage where it is transferred to tape storage nightly. Redundant hardware for key systems at both Site1 and Site2 is available. Critical data is being archived on a backup internal

hard disk and the entire system is being backed up to a tape drive nightly. Compatible tape drives are available and in use at both branches. The disaster recovery plan in Site1 has been tested. Baseline backups of key PC systems are performed on a routine basis. Data stored at an insecure site should be encrypted. Two generations of monthly backups should be maintained, providing multiple restore points. A formal tape rotation should be instituted. Logging of backup errors should be formalized and consistent between the branches. Despite these many improvements, some elements to ensure a quick, successful recovery are missing. The Symantec Ghost program should be installed on each SoftwarePackage2 computer to facilitate a speedy recovery of the primary hard disk. Estimated cost is $40 per SoftwarePackage2 server. This software makes a disk image including all local configuration issues which can be restored in a matter of minutes, rather than 4-5 hours.

Data security, privacy security and disaster recovery should be regarded as a process and not a destination. This security audit was designed to identify and correct both recent changes and major issues. Maintaining quarterly reviews of your security and disaster recovery plans must entail adjusting to business changes, adjusting to known threats, and implementing best practices to safeguard your data. Monitoring your network, your endpoint devices and practices is essential to maintaining data security and mitigating developing risks. Through a process of continual review and enhancement, your systems security and ability to respond to disaster will continue to increase.