Global Information Assurance Certification Paper

Desktop Security in an Outsourced Corporate Environment

Chad Ironside
October 26, 2004

1. Introduction

It is easy to argue that network security is a hot topic among IT organizations worldwide. It is more difficult to describe exactly *how* to secure a company's network. It is the opinion of the author that one of the more difficult tasks for IT organizations, in regards to network and information security, is securing the user desktop. It is a fairly straightforward process to put a server behind a firewall, harden the operating system and apply the necessary patches. It is more difficult to convince the average user why they should or should not stream internet radio at the office, secure a confidential document or install and run file-sharing software on their company-owned computer.

The purpose of this paper is to present a combination of business practices, responsibilities, policies, procedures and tools that effectively secure the user desktop in a corporate environment. I use "desktop" here as a very broad term: for this paper it is defined as anything the user can do from his or her workstation that might jeopardize network and/or information security. In other words, the purpose of this paper is to secure user actions. For example, if the user can spread a virus by opening an email attachment, then an email filter that blocks the infected email is a valid desktop security solution.

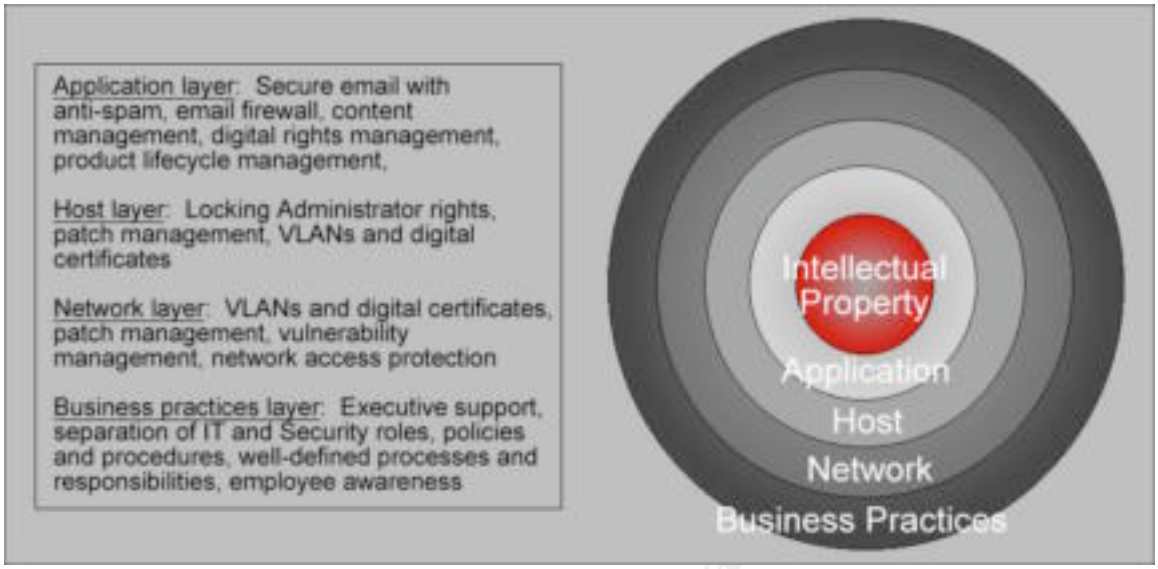
To take the topic one step further, this paper will try to address desktop security in an outsourced environment. An "outsourced environment", for the purpose of this discussion, is defined as a corporate environment where key functions (IT, Human Resources, Finance and Manufacturing, etc.) have been outsourced. Such a company must focus its efforts equally among securing employee and contractor desktops.

Section 2, "Business Practices", describes the executive support, policies, procedures, organizational responsibilities and roles that *must be in place* in order for the implementation of the proper tools to be effective. Section 3, "Desktop Security Tools", describes the tools that can secure the desktop with proper implementation and usage. Section 4 mentions a couple wish list items have either not yet been released or are still being evaluated by the company.

Our company chose the policies, procedures and tools described in this paper due to their ability to meet our specific business needs. Each solution contributes to the overall security of our network and information. Together they create a multi-layered approach to desktop security within our environment. To put it in SANS terms, the paper attempts to secure the desktop using the idea of *defense in-depth*.

Each solution falls aligns within one or more of the layers of defense in-depth, as outlined by in figure 1. There is one significant addition to the defense in-depth strategy outlined by SANS that our company considers necessary for successful desktop security: the business practices layer. Section 2 describes these practices in detail.

Figure 1: Achieving desktop security through defense-in-depth



It is worth noting that companies have dozens of effective practices, policies, procedures and tools at their disposal when trying to secure their networks and information. Although this paper describes one particular combination of solutions, many other combinations may be equally as effective. Ultimately, a company must choose a combination of policies, procedures and tools that address the unique needs of its own environment.

1.1 Company Description

Before I begin discussing the topic, I will first give more detail about the environment we are trying to secure. The company is a mid-sized technology manufacturing company (approximately 3000-5000 employees). The company's most prized assets are the manufacturing patents generated by the Engineering and Product Development organizations. The company keeps its corporate offices, as well as approximately 10 smaller offices (approximately 10-100 employees each), in the United States. This company also has approximately 10-20 small offices world wide. Business demands have dictated the outsourcing of many organizations including IT, Human Resources, Finance, Manufacturing and Facilities.

The employees of this company include highly technical engineers; however it should be assumed that the average user is mostly non-technical. In general, users have no desire to learn how their computers operate; they only see computers as a tool for accomplishing work-related tasks. In regards to hardware/software, the company is a Microsoft Windows environment running mostly Windows 2000 and XP, although there are still a few machines lurking that operate on Windows 98.

Last, assume that before the implementation of desktop security within this company, only basic security controls were in place: firewalls, virus scanning and

NT logins were the only true measures of security. Network and information security were rarely even given any thought before making a decision that impacted the IT infrastructure. In fact, the only exposure that network security received came after virus attacks that brought the network to its knees.

2. Business Practices

The items listed below are business practices that we consider necessary to the success of desktop security. They include executive support, policies, procedures, organizational responsibilities and roles that *must be in place* before desktop security will be successful. Ultimately it is the *tools* that enforce security; however the ability to procure, implement and effectively administer such tools will be unsuccessful without these factors. Several of these items are large enough topics to be entire papers of their own, but are mentioned briefly in order to stay focused on the overall topic.

2.1 Executive Support

To successfully secure the user desktop, a company must first have the proper support of upper management. In addition, executives should have an understanding of network and information security, including the inherent risks. They will make them more comfortable supporting the implementation of measures that aim to mitigate these risks.

The first reason for this support is monetary: the proper tools for securing the network are expensive (our digital rights management solution alone cost close to half a million dollars), and obtaining the funds for these tools will be an uphill battle if management does not understand or agree with what it is you are trying to accomplish. "*Manufacturers Face Difficulty Benchmarking Security Best Practices*", an article written by Dick Hill in August of 2003, states that "if you are required to justify expenses related to security enhancements, then you are among the majority." On the other hand, a management team concerned about network security might go so far as to create a budget specifically for network security, if the risks are clearly understood.

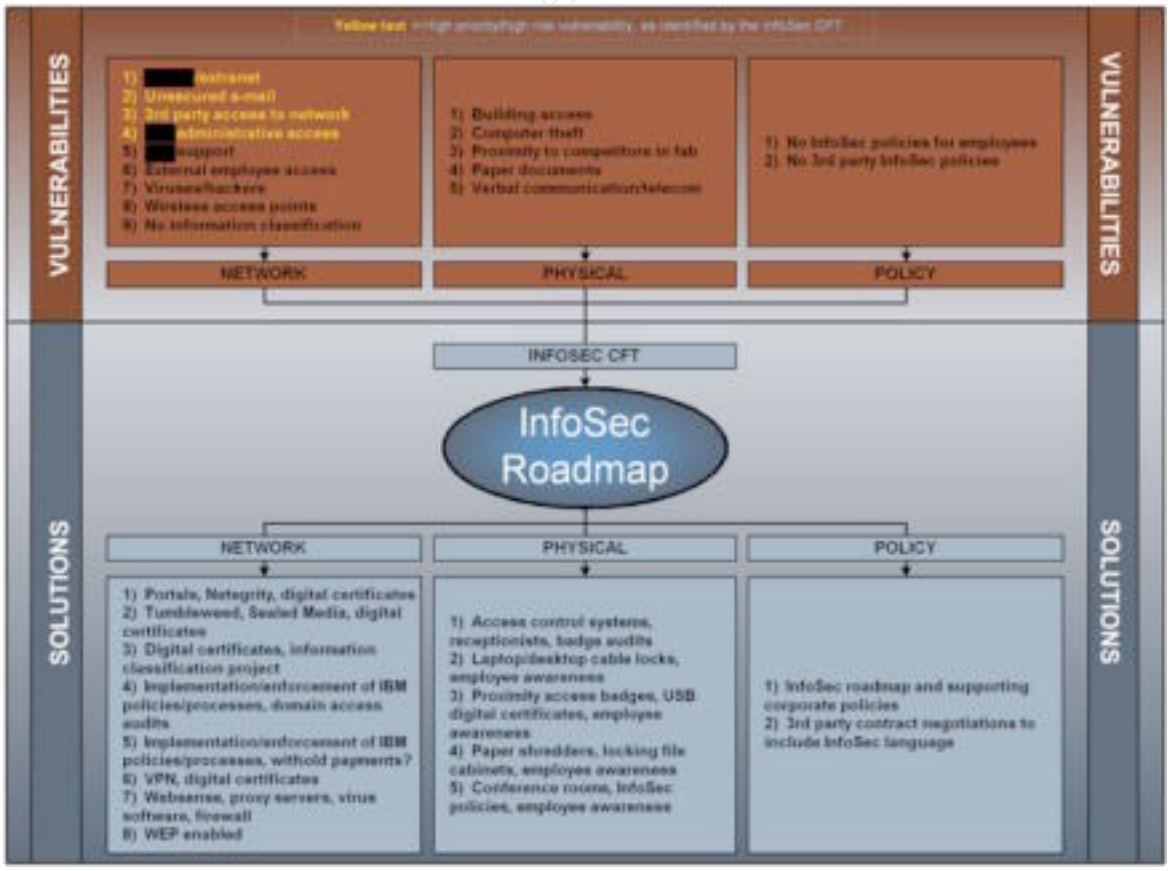
This support may be achieved by illustrating the risks involved with NOT securing the network and information it contains. Associating monetary value with your intellectual property can quantify the risk that would be associated with losing that information. If your company generates patents, estimate the revenue generated by the patent and translate that into a loss in the event of information theft. A strong argument for information security is a recent report created by ASIS, PricewaterhouseCoopers and the U.S. Chamber of Commerce. The report is titled "Trends in Proprietary Information Loss" and was published in September of 2002. The report includes the monetary losses associated with the theft of trade secrets and other proprietary information, and provides losses per incident. The loss runs in the hundreds of thousands of dollars per incident, and

is a good number to use when attempting to quantify the risk of intellectual property theft.

This support may also be achieved by calculating hours of network downtime due to malicious attacks, and then associating productivity and/or loss with these hours. Although no one wishes for a successful attack, if email goes down for one or more business days due to the effective mass-mailing worm, simply multiply the number of workers affected by revenue per employee and hours of downtime to come up with the total revenue loss during the outage. This easily translates to a strong ROI for the intrusion solutions that would have blocked the worm and prevented the unknowing user from opening the attachment in their email.

To increase executive support for network and information security, we created a document that we titled the "Information Security Roadmap". We aligned this document with strategic IT initiatives to gain the support of IT and gain visibility with executives. The document's purpose was to identify major network and information security vulnerabilities, as well as to identify specific solutions that remediate these vulnerabilities. This roadmap was a key first step in increasing awareness of network and information security among company executives and was successful at gaining executive support.

Figure 2: The Information Security (InfoSec) Roadmap



A second reason for executive support directly affects contracts with outsourced providers, suppliers and business partners. A supportive executive team can be convinced to negotiate network and information security standards and policies into provider, supplier and business partner contracts. Any security standards or policies added to contracts become key weapons of enforcement when locking a contractor laptop out of the network due to viruses they brought from their own network. If you executive team includes expert negotiators, these contract clauses can even go as far as helping the company enforce minimum security standards on all contractor computers that connect to the company's network. A lack of security clauses leaves the company no recourse in the event a business partner or contractor compromises the security of the network.

2.2 Separation of Roles: IT & Security

It is important to understand that successful desktop security also depends on the separation of network and information security from the IT organization. IT should be concerned with the implementation and tools that secure the network. This leverages their expertise and is a logical assignment. On the other hand, Security should be tasked with enforcing network and information security, via policies that IT tools support. Security should also maintain its own tools that audit the effectiveness of the IT tools against security policy. This separation acts as a check and balance against IT decision-making and helps maintain the integrity of network security audits.

The Security organization should ideally have at least one resource dedicated to network and information security. Proper management support, mentioned previously, should help the case for the creation of such a position. Ideally this person should be an IT/Information Security Manager involved with the development of information and network security policy as well as the management of security audit and compliance tools. This person should also maintain strong relationships with IT management, the outsourced IT provider and upper management in order to ensure that network and information security concerns are properly addressed in all IT and information-based decisions. When possible, this manager should be supported by a Security Analyst that implements and administers the organization's security tools. This person should be highly technical, and should know the configuration of the network as well as (if not better than) IT in order to be an effective security auditor.

Last, IT should also rely on Security to act as the enforcement arm in regards to rogue users. By doing so, IT leverages Security's authority, as well as its expertise on the hazards and legal ramifications of dealing with sensitive employee issues. As Security already deals with troublesome employees (employee theft, threats to other employees, etc.) they are already have the experience needed to deal with these users.

2.3 Network and Information Security Policies and Procedures

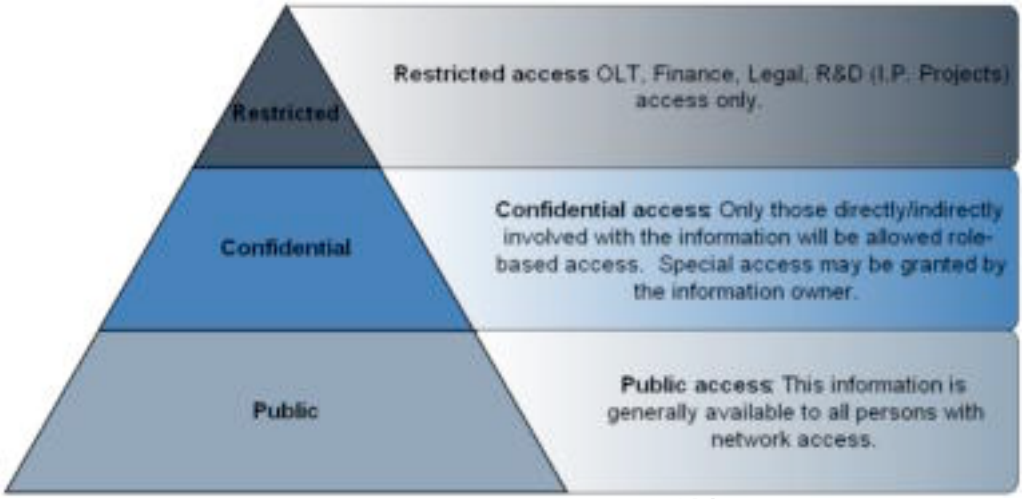
Network and information security policies are the most essential elements of effective desktop security. Effective policies are the corporate standards that dictate user responsibilities in regards to computer use. They define appropriate and prohibited web and email usage (business need vs. surfing for pornography, conducting personal business during work hours, etc.), specify whether users can install unauthorized software, establish appropriate measures to be taken against users that create vulnerabilities, and outline user responsibilities in regards to protecting confidential information and intellectual property. These policies are grouped logically into categories based on business need and may differ by company, however examples are as follows:

1) Communication Systems Use Policy
   This is a general policy that defines communications systems as email, the internet and other electronic systems that allow a user to communicate electronically. It defines user responsibilities in regards to these systems, which includes approved and prohibited uses. It states that users are liable for the effects of any misuse and states that penalties will be imposed in the case of misuse. It might also state that these systems are the property of the Company and are therefore usage may be monitored.

2) Software & Hardware Policy
   This policy states that only specific types of hardware and software are acceptable within the company, and states that no non-approved hardware and/or software may be attached to the network. As with the Communications Use Policy, this policy states that users are liable for the effects of any misuse and states that penalties will be imposed in the case of misuse.

3) Data Classification Policy
   This policy establishes categories for all information within the company, and dictates that all information must be assigned one of these categories. It also states that employees are required to use the appropriate tools to secure the appropriate categories, and dictates where such information must be stored. Examples of categories are Top Secret, Restricted, Confidential, and Public. The International Organization for Standardization (ISO) generates a newsletter that recommends five categories, although our company chose only three to avoid confusion when assigning a category to a file (Restricted, Confidential, and Public). The ISO categories are Top Secret, Highly Confidential, Proprietary, Internal Use Only and Public. Details may be found at http://www.iso17799-web.com/issue6.htm.

Figure 3: Data Classification Policy



A comprehensive list of policies that affect network and information security is listed below. This list is based on ISO 17799 standards. More information may be found at http://www.iso-17799.com/.

1) Global Standards of Business Conduct Policy
2) User Responsibility Policy
3) Security Compliance Policy
4) Proprietary Information Policy
5) Non Disclosure of Proprietary Information Policy
6) Distribution of Software Policy
7) Distribution of Systems Documentation Policy
8) External Party Information Disclosure Policy
9) Outsourcing Security Policy
10) Asset Management Policy
11) Data Classification Policy
12) Trade Secret Policy
13) Incident Reporting Policy
14) Internet Usage Policy
15) Communications Use Policy
16) Email Policy
17) Internet and Intranet Content Management Policy
18) User Account Management Policy
19) Firewall Policy
20) Token Responsibility Policy
21) Remote Access Policy
22) Network Resource Usage and Control Policy
23) Operating System and Application Control Policy
24) Wireless 802.1x Security Policy
25) Privacy Policy

Procedures are written to support these policies, and their goal is to fill in the missing details. When details change, they are updated within the procedures, not the policies. A key point to remember here is an effective policy does not need to be updated – that is the purpose of the supporting procedure(s).

Examples of effective procedures are aligned with the policy examples from above:

1) Communication Systems Use Procedure
   This procedure includes a list of approved communications systems as well as specific prohibited uses (i.e. surfing pornography, gambling, games or hate-related sites; using vulgar language in email, etc.).

2) Software & Hardware Purchasing Procedure
   This procedure includes a list of approved hardware and software. It dictates that all purchases must be approved by IT, and must be made through formal purchasing processes. It may even include hardware/software order forms.

3) Data Classification Procedure
   This procedure establishes the system(s) of record for securing company confidential information and intellectual property. It includes links to training documents and/or information on how to use the system, information on troubleshooting and escalation processes, as well as Service Level Agreements (SLAs) that will be followed in the case the system goes down. It also provides specific details about the policy, including the proper repositories for specific categories of documents, etc.

2.4 Strong IT Processes

Effective desktop security also depends on strong IT practices. To begin, the IT provider must be dedicated to network and information security, which includes providing the necessary resources to troubleshoot critical security issues in a timely manner. Second, Change and Problem Management procedures must be clearly defined and well-executed. If the Desktop Support team runs into a problem rolling out a critical patch using an automated delivery system, they must be willing and able to quickly diagnose the root cause of the problem, then allocate the necessary resources and shift to manual implementation if necessary.

Creating a cross-functional Incident Response Team will help foster dedication to the security cause through team-building and peer support. The team should have well identified roles and members, and should be supported by the proper policies and procedures. Proper representation is also critical – the team should include members of the company's IT and Security management, members of

the outsourced provider's management as well as Desktop Support and Help Desk supervisors. The team should be chartered with the creation, maintenance and implementation of proper Change and Problem Management policies and procedures in the event a critical issue arises. These policies should outline necessary resources in the event a critical issue arises, and should document a clear process for finding root cause and then mitigating the risk or intrusion. Documenting such items will guarantee that resources will be available when an issue arises and will also help ensure smooth incident response.

2.5 IT Responsibilities: Maintaining Inventories, Clear Knowledge of Network Architecture

In order to secure the desktop, IT and Security must maintain an up-to-date inventory of the hardware and software that makes up the user environment. This inventory must be maintained in conjunction with a current document that details network architecture. This information is a reference by which the IT and Security organizations determine the vulnerabilities must be addressed, as well as how many resources will be necessary for tasks such as upgrading software, finding and patching workstations and laptops, dividing the network into appropriate subnets, etc. Such knowledge will also be invaluable in the event of a critical security breach that must be quickly mitigated.

2.6 Employee Awareness

Employee awareness is also important to effective desktop security. Defining network and information security and identifying the associated risks, posting security policies, discussing security systems' affect on employees, speaking to employee groups about security and empowering employees to assist with security are all methods of creating employee awareness. Much of this information can be easily posted and accessed via the company intranet. A "Your Role" page on the Corporate Security site provides employees with an easy-to-access, centralized source of security information. When employees feel involved they are more likely to feel like part of the team, and will be more likely to feel personally responsible for security. If nothing else, such awareness will make employees less resistant to network and information security.

3. Desktop Security Tools

Now we will discuss the tools that have been successful at securing the user's desktop within our company. These tools were chosen using approved processes and in most cases included sufficient due diligence, however much has also been learned through experience. Each of these solutions also contributes to one or more layers of the defense in-depth model.

It must be noted here technology evolves rapidly. Many of the products discussed will be replaced with more-effective versions in a matter of years or even months. Although some tools remain fairly constant, the list that is provided today is different than a list generated five years ago, and will be at least slightly different in another five years. Overall, effective desktop security requires

staying on top of the latest security technologies in order to keep pace with changes in hardware, software and the risks inherent in each.

3.1 Locking Administrator Rights among the General User Population

Prohibiting the user from being assigned Administrator rights is a tool in the arsenal that supports desktop security. This deters users from installing prohibited software (file sharing services, games, hacker tools, etc.) and helps to control the software environment within the Company. The downside is that some security tools require Administrator rights to run properly (for example, Microsoft's Baseline Security Analyzer), but workarounds can usually be found and the tradeoff is therefore still worth the effort.

3.2 Logon Scripts

A well-designed logon script affects desktop security by enforcing compliance with security policies. In this example, the script is designed to pop up as soon as the user logs on to the company network. The window states that all users must agree to abide by the appropriate network and information security policies (identified by name) and provides both an "I Agree" and an "I Disagree" button. If the user selects "I Agree", the window disappears and the user may begin using the computer. If the user selects "I Disagree", the computer shuts down. While this window is active the user cannot perform any other tasks on the machine.

Figure 4: Logon script window

3.3 Patch and Vulnerability Management

It should be no surprise to anyone that Microsoft's products contain vulnerabilities. These vulnerabilities can cause any computer on the network to become a liability if the vulnerability is successfully exploited. Is should therefore be no surprise that a secure desktop environment must follow patch management best practices in order to minimize exploits on Microsoft software (Windows operating systems, IIS, SQL, Office, Internet Explorer, etc.). As a

note, Microsoft provides very good documentation on patch management best practices at its Patch Management Process page.

Effective patch management relies on several factors, as follows:

1) Patch Management Team
   This is a cross-functional team that decides which patches should be installed on the desktop. They base their decisions the criticality of the patch, its effect on the company's environment and it's effectiveness at mitigating the vulnerability associated with the patch. They also determine the method and schedule of delivery for all approved patches. For the most part an automated system is used, however if the patch is highly critical and has issues with automated deployment, the Patch Management Team may look to the Incident Response Team for manual deployment. The Patch Management Team is made up of Company IT management, outsourced IT provider management, Security management and a cross-section of Help Desk and Desktop Analyst (DTA) supervisors.

   As a means of creating awareness amongst employees, the Team may post all approved and prohibited patches and service packs on the intranet. This may cause users to feel more involved in the process.

2) Automated Patch Deployment
   Microsoft recommends their Systems Management Server (SMS) technology as an automated patch deployment system for medium to large companies. This system can detect workstation vulnerabilities, take hardware and software inventories, apply patches automatically and audit compliance with specified patch levels. While this is a good tool, we have chosen a third-party system in order to minimize the tendency to become over-reliant on Microsoft. The tool, called Backweb, automatically detects a network connection and downloads any available updates from the appropriate staging server. Although pushing patches is not the main function of the software, it satisfies our need because it downloads and installs patches silently without affecting the user experience, even when bandwidth is minimal (connection via phone modem, etc.).

3) Patch Compliance Auditing and Vulnerability Management Tool
   As mentioned above, Microsoft's SMS tool has the ability to audit patch compliance enterprise-wide. Microsoft's Baseline Security Analyzer (MBSA) may also be used on a smaller scale to scan single computers or small groups of computers. This, however, requires that the user has Administrator rights and is therefore not recommended for use among the user population (although it is still a good troubleshooting

tool for the Help Desk and or Desktop Analysts). Although both SMS and the MBSA are effective under the right circumstances, both are Microsoft products and could potentially the integrity of any Microsoft patch compliance audit.

The patch compliance audit tool chosen by our company is ip360 (nCircle). This system allows the organization to scan ALL devices (routers, hubs, Sun/AIX/Windows/Unix/Linux servers, desktops, etc.) for patch compliance issues as well as other vulnerabilities (open ports, unnecessary services, file and drive sharing, etc.). It allows the organization to establish baseline risk profiles for all network servers, appliances and clients (workstations/laptops). The tool then audits all machines against this baseline and can generate reports that show which machines are not in compliance. It takes these reports one step further and goes into detail about the steps that must be taken to fix identified vulnerabilities. If the installation of a Microsoft patch is necessary, it provides links directly to the appropriate Microsoft patch download page. Ip360 also includes a ticketing system that tracks compliance to the baseline and will alert the appropriate Desktop Analyst via email if a specific machine must be patched and/or updated to meet the baseline requirements.

This tool allows Security to have an independent patch/vulnerability audit and compliance tool with high levels of automated functionality, making vulnerability and patch management easy. Furthermore, its appliance-based architecture allows the organization to quickly scale the solution as new subnets are added or reorganized, and eliminates the need to install a monitoring service on all of the devices it scans.

Figure 5: Vulnerability Management Report

3.4 VLANs and Digital Certificates

In the past, this company was one large, happy network. It was also a *vulnerable* network. All data, regardless of importance, was stored on the same group of file servers and the only access controls in place for all employees, contractors and business partners were NT rights. Recently the network was reorganized into VLANs, or Virtual Local Area Networks (a good, albeit somewhat dated, page that discusses VLANs in detail is posted by UC Davis). By doing so, we were able enhance network access controls by dividing users into employee, business partner (contractors, outsourced providers, suppliers, etc.), customer and guest VLANs. We are further able to segregate groups of users by job function, which helps us to control access to confidential information and intellectual property. For example, an employee in HR gets access to the Company HR VLAN while an engineer working on patents gets access to highly confidential documents stored in the Engineering VLAN. Salesmen that come to present the latest technologies plug into the Guest VLAN, which allows only internet access.

Figure 6: Logical VLAN Structure

Our company chose to implement RSA digital certificates (machine based, not user based) as a means of controlling VLAN access. We developed naming conventions for the certificates that separate employees from contractors, and further separate employees into functional groups (HR, Engineering, IT, etc.). As mentioned above, guests that do not have a certificate matching any of the approved certificates are deposited in the Guest VLAN. We also developed an automated process by which a DTA may request the appropriate certificate for a machine, and the appropriate IT or Security Manager may vet, or approve, the certificate. All this is done via a web browser. The certificate is then installed by the DTA using a script and the computer is allowed onto the appropriate VLAN.

Although a whole paper could be written on the proper implementation of digital certificates, I will mention only a few key items here. First, when automating the process of certificate generation, make sure to configure your tool to create only

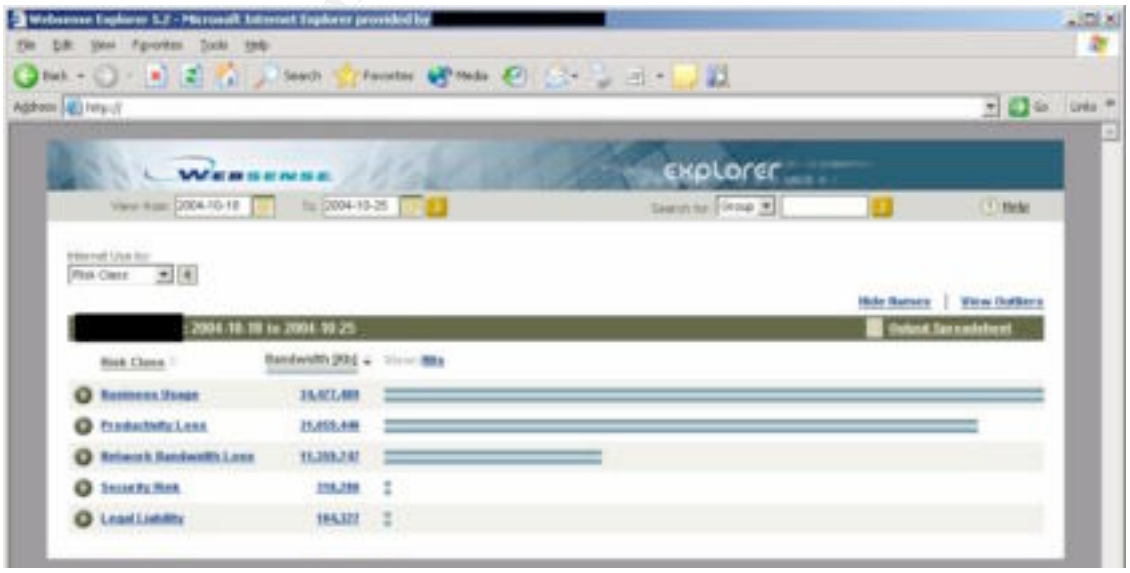
non-exportable machine-based certificates. Otherwise, a technical user will be able to copy the certificate on to other machines. A second task is to make sure and choose only key individuals to vet, or approve certificates. Third, keep the Certificate Authority (CA) on a separate physical machine from the Registration Authority (RA), and store your root CA offline. Finally, nCipher Hardware Security Modules provide effective access controls in relation to the CA and RA via plastic keys that contain certificates. You can choose how many keys are necessary to access the CA/RA (2 out of 5, 3 out of 8, etc.). Make sure, however, that you create enough keys that there are always enough resources available in the even the CA/RA must be accessed in a hurry.

3.5 Employee Internet Management

Our company also chose to implement an internet management tool called Websense Enterprise Employee Internet Management (EIM). This tool allows us to filter http (port 80) traffic and effectively block users from accessing prohibited websites. When the user attempts to access such a site, they are redirected to a web page that describes the violation as well as provides links to the supporting policy and procedures. Examples of blocked sites are web mail, hate and crime-related, gambling, games, pornography, guns and hacker tools.

This tool further allows the Security organization to monitor and report on internet access. In particular, if internet access is slow, we are able to run a report on users utilizing the most bandwidth and can identify those using large portions of bandwidth (i.e. users streaming audio or video). We can even run reports that tell us how much time a user spends on the internet as well as which sites they have visited. We then escalate user violations to the user and their HR Manager. We have created escalation templates that contain standard language for violation escalations.

Figure 7: Websense Internet Traffic Report



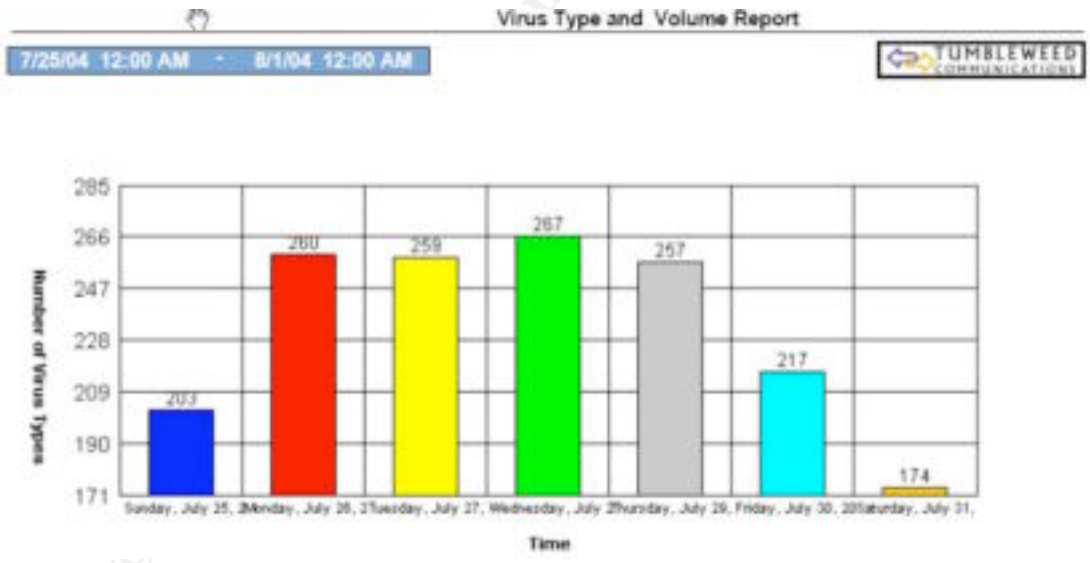
Another benefit of these tools is its ability to block specific protocols entirely. Examples include FTP, Instant messaging, Telnet, Remote Access (PC Anywhere, Citrix, GoToMyPC, etc.), streaming media and P2P file sharing protocols. Although we do not block them all, we have the option of doing so in the event we discover a specific vulnerability exploiting that protocol.

3.6 Email Filters

Tumbleweed provides our company with effective an effective email filtering tool called Email Firewall. This solution allows us to filter inbound and outbound email for viruses and other malicious code, spam, inappropriate language and confidential information. We can generate policies within the application that automatically enforce the prohibition of email from specific domains, as well as email containing certain language or attachment types. We utilize these tools in the following manner:

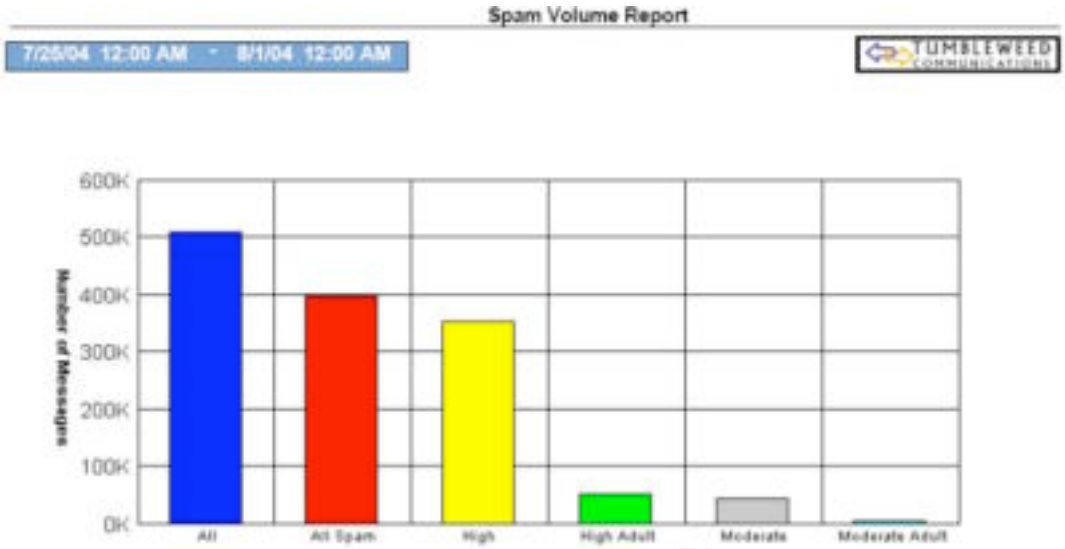
1) Inbound mail
   We utilize the filters to remove viruses and malicious code from all inbound mail. In an average week this tool blocks over 4000 viruses.

Figure 8: Weekly Virus Volume



We also use this tool to block spam. In an average week we block over 400,000 spam messages, which is over 80% of all inbound mail.

Figure 9: Weekly Spam Volume



2) Outbound mail
We utilize the filters to block outbound mail containing offensive language, inappropriate attachments (pornography, death/dismemberment, unsecured confidential information and/or intellectual property, etc.) and escalate user violations to the user and their HR Manager. We have created escalation templates that contain standard language for violation escalations.

Tumbleweed also provides us with a tool called Secure Redirect (the referenced site calls it "Secure Messenger" for some unknown reason). This tool encrypts email, securing the user's *transmission* of our confidential information and intellectual property over the internet. A user must simply enter the word "secure mail" into the subject of an outbound email and the contents are automatically redirected to a secure web server. The recipient receives a link to a secure SSL session, by which they retrieve the contents of the email from the secure web server. Before retrieving the message, the user must first create an account on the web server that allows them to authenticate and retrieve secure email in the future.

3.7 Digital rights Management

The Tumbleweed tools described above allow us to secure confidential information during transmission. What will still needed after this tool was in place was a system that could control access to our confidential information and intellectual property regardless of where it resides – on our network, on a competitor's computer in another state, or on a CD sent to an engineer in Shanghai. SealedMedia provided us with a digital rights management solution that does just that.

The SealedMedia solution allows us to "seal" common document types: MS Word, Excel and PowerPoint; Adobe PDF; html files; .gif and .jpeg. We can specify what rights a user has to a specific document by allowing or denying editing, cutting and pasting, printing, video capture (screenshots), saving in unsealed format, etc. Furthermore, we can set expiration dates on specific documents, or can even specify the number of times the user may open the document. Most importantly, we can add/change user access and rights to a specific document in real time. For example, a document is emailed to an employee in Germany and the sender forgets to grant access to the recipient. The recipient requests access when they discover that they cannot access the document. The recipient should become able to access the document within seconds of the sender granting the appropriate rights (assuming the recipient has internet access), regardless of the physical distance between the two individuals.

We designed custom services with the implementation of this tool that automatically seal documents saved within particular directories on the company network. This allows us to effectively build our directory structure based on the Data Classification Policy described in section 2.3 and *enforce* the structure by automatically sealing documents within the appropriate folders. For example, if an employee in Finance drops a financial spreadsheet into the "Finance Restricted" folder, it is automatically sealed to allow only *Restricted* access to the document.

The SealedMedia solution utilizes user accounts and passwords to protect documents. It will integrate with an organization's LDAP servers so that users on the company network may use their same NT login account to access sealed documents.

4. Future Functionality

Security software companies are constantly developing improved network and information security products. Below is a quick list of tools that we believe can only increase effective desktop security in our environment, but have not implemented within the company.

4.1 Product Lifecycle Management

Given the large amount of manufacturing-related intellectual property that is generated by our company's Product Development organization, we are currently evaluating the Windchill product lifecycle management tool. This solution allows us to control access to the product development lifecycle. The system acts a central repository for all product development projects, allowing access to multiple file types (CAD drawings, project plans, etc.) through a single application – the web browser. This solution further allows the company to manage revision control by automatically tracking all updates to a particular document. Windchill also controls access to the files by prohibiting the user from saving copies of the files anywhere but in the central repository. For example, a user is able to

access a CAD drawing within the repository, as well as view and edit the file as necessary. They may not, however, save the file in any location except the repository from where it came.

Such a system would allow the company to identify and centralize our intellectual property. It would provide revision control as well as access , which would have a positive impact on information security.

4.2 Network Access Protection

The Longhorn release of the Windows 2003 Server platform will include a new set of operating system components that can evaluate the overall health of a client attempting to connect to the network, and deny network access to that client if certain thresholds are not met. These components, called Network Access Protection, will be able to check for certain virus and Microsoft vulnerability patching levels and deny client access unless pre-determined thresholds are met. This technology will apply to any client attempt to connect directly or via the company's VPN, and will require clients running Windows XP. The components will integrate with third-party software (virus scanning tools, vulnerability management tools, etc.) to effectively diagnose clients and remediate when necessary.

Assuming that this tool allows the organization to set thresholds against which the components run continually, this tool will provide the company with strong controls against client-based vulnerabilities. It's ability to control VPN and direct network access is important as well. If it allows the organization to set thresholds and enforce these thresholds using automated processes, this tool may be able to successfully help us secure proactively stop vulnerabilities before they are able to gain network access .

5. Conclusion

The business practices, policies, procedures and tools described above have been effective at securing the desktop in the outsourced environment described in the Introduction. We have seen downtime due to vulnerability exploits, viruses and other malicious code decrease; and significantly decreased the amount of spam arriving in user mailboxes. We have seen employee misuse of the network, internet and email (internet surfing, inappropriate email, saving large amounts of mp3s on file servers, etc.) decline and have almost completely eliminated the amount of unauthorized software that resides on user desktops. Employee awareness is up in regards to information security, and the amount of unsecured intellectual property leaving the network has decreased while the use of secure email has increased. We are currently working with other organizations in the company to promote widespread enforcement of our Data Classification Policy, and have found an increasing number of organizations to be highly receptive to this plan.

We must stress the belief that our actions have been successful due to *defense in-depth*. Each piece of the puzzle contributes to effective desktop security by adding layers to the defense in-depth model. Given the complexity of securing the desktop, a successful security strategy *must* rely on this model to be comprehensive and effective. All of the business practices, policies, procedures and tools described in this paper are interdependent and rely on each other to be successful.

Furthermore, we do not believe that our network and information will *ever* be 100% secure. We realize that no environment is impenetrable – even the most secure environments will be the victim of at least minor attacks. The key to being successful is minimizing the risks involved with desktop security as well as minimizing the impact on business continuity should an attack or exploit be successful. Even if an attack successfully breaches your environment, network security is still considered successful if it can remediate before the exploit causes network downtime or employee productivity.

It is my hope that the reader will use the knowledge gained from this paper as helpful information in the effective implementation of desktop (a.k.a. user behavior) security within their own organization. Please, however, do not assume that my paper includes an exhaustive list of effective policies, responsibilities, roles or tools. There are many factors not mentioned that may be equally as effective in different business environments. It is up to those responsible to choose a combination of factors that will help to achieve desktop security in their own environment.

References

Cole, E., Fossen, J., Northcutt, S. and Pomeranz, H. SANS Security Essentials, Track 1: Defense In-Depth, SANS Institute, 2004. 11-14.

Hill, Dick. "Manufacturers Face Difficulty Benchmarking Security Best Practices". ARC Insights, August 6, 2003: 3. http://public.arcweb.com/cybersecurity/Shared%20Documents/2003-31M.pdf.

ASIS Foundation, PricewaterhouseCoopers and the U.S. Chamber of Commerce (2002). "Trends in Proprietary Information Loss, Survey Report September 2002", 2002. URL: http://www.asisonline.org/newsroom/surveys/spi2.pdf.

International Organization for Standardization. "ISO17799 News – Issue 6: Information Classification Criteria", ISO17799 News. URL: http://www.iso17799-web.com/issue6.htm.

International Organization for Standardization. The ISO 17799 Directory. URL: http://www.iso-17799.com/.

Microsoft Corporation. Microsoft Baseline Security Analyzer, August 16, 2004. URL: http://www.microsoft.com/technet/security/tools/mbsahome.mspx.

Microsoft Corporation. Patch Management Process, August 6, 2003. URL: http://www.microsoft.com/technet/security/guidance/secmod193.mspx.

Microsoft Corporation. Systems Management Server. URL: http://www.microsoft.com/smserver/default.asp.

Backweb. Backweb Home Page. URL: http://www.backweb.com/index.cfm.

nCircle. IP360 System Overview. URL: http://www.ncircle.com/index.php?s=prod_ip360.

University of California at Davis. VLAN Information, December 18, 1998. URL: http://net21.ucdavis.edu/newvlan.htm.

RSA Security. Digital Certificates. URL: http://www.rsasecurity.com/node.asp?id=2604.

RSA Security. Access Management. URL: http://www.rsasecurity.com/solutionsTertiary.asp?id=1097.

RSA Security. RSA Keon Certificate Authority. URL: http://www.rsasecurity.com/products/keon/datasheets/KCA_DS_0403.pdf.

NCipher. Hardware Security Modules. URL: http://www.ncipher.com/hsms/.

Websense. Websense Enterprise. URL: http://www.websense.com/products/about/Enterprise/.

Tumbleweed. Tumbleweed Email Firewall. URL: http://tumbleweed.com/products/emailfirewall.html.

Tumbleweed. Tumbleweed Secure Messenger. URL: http://tumbleweed.com/products/secure_redirect.html.

SealedMedia. SealedMedia products & services. URL: http://sealedmedia.com/products/default.asp.

PTC. Windchill. URL: http://www.ptc.com/appserver/it/icm/cda/icm01_list.jsp?group=201&num=1&show=y&keyword=37.

Microsoft Corporation. Network Access Protection Platform Architecture, October 20, 2004. URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/naparch.mspx.