Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Network Security and the SMB

Network security is an issue for all businesses. The challenges faced by small-to-medium size businesses (SMBs) are unique and significant. Taken together, the ongoing threat to network security and myriad challenges to SMBs necessitates a unique and comprehensive approach to risk management, auditing and best practices. This paper is intended as a guide for service providers and consultants seeking to enhance the security posture of SMBs, which acknowledges the unique challenges that SMBs face. What is more, this pape...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Network Security and the SMB

A Guide to Risk Assessment, Auditing and Implementing Best Practices

© SANS Institute 2005, Author retains full rights.

Matt Hawley
Practical Assignment Version 1.4c – Option 1
GIAC Security Essentials Certification (GSEC)
October 29, 2004

© SANS Institute 2005 Author retains full rights.

1.0 INTRODUCTION

1.1 Abstract

Network security is an issue for all businesses. The challenges faced by small-to-medium size businesses (SMBs) are unique and significant. Taken together, the ongoing threat to network security and myriad challenges to SMBs necessitates a unique and comprehensive approach to risk management, auditing and best practices.

This paper is intended as a guide for service providers and consultants seeking to enhance the security posture of SMBs, which acknowledges the unique challenges that SMBs face. What is more, this paper is intended to assist the interested SMB owner in understanding network security threats and remedies and proposed solutions offered by service providers/consultants. A sufficient network security posture is possible for SMBs – even in the face of constraints they face – with good strategy and diligence. The following is not a comprehensive step-by-step, but a guide and overview.

1.2 Network Security and the SMB

While larger businesses have substantial resources with which to identify and defend against network security threats, all businesses face the same significant and constant risks. A large business can afford to dedicate staff time to network security, or hire an outside firm, or both, but SMBs (generally) cannot. The issue at hand is that SMBs rely on technology and networks as much as any business.

What is needed is a methodology for assessing risk, auditing networks, systems and processes and implementing best practices – in a SMB context. Fortunately there is a tremendous amount of information available to SMB technology staff and/or the technology service providers that work with SMBs.

In terms of that wealth of information, relying on single sources is unwise. Just as defense-in-depth (arraying multiple defenses, at different layers, in creating a security posture) is critical practice, aggregating available information and focusing on commonalities yields the best results. What is more, information borne out of the collaboration of respected, knowledgeable and vendor-neutral individuals, groups and organizations is *most* desirable in securing networks (vendor-provided information still has much potential use though; particularly in configuration).

2.0 NETWORK SECURITY – THREATS & REMEDIES

2.1 Threats

The Internet is a pervasive and important part of our lives. At home and in business the networked nature-of-things is clear. Increasingly, business functions and profitability, as well as personal data communications, are dependent on network traffic moving freely and without delay. There are, however, significant threats to that flow of data. As

© SANS Institute 2005 Author retains full rights.

reliance on data and networks increases – and the consensus is that it will – the value in, and ability of, malicious actors to disrupt network communications increases.

There are myriad threats that all Internet users face. From worms and trojan horses (malicious code that *usually* arrives through e-mail) to software exploits (allows hackers to damage or control a computer via an unpatched vulnerability) – and everything in between – there are all sorts of potential compromises.

The CERT Coordination Center (CERT/CC) described the main types of network security exploits in a 2003 presentation:

- Trojan Horse/Malicious Code [a.k.a Viruses]: designed to damage a computer, or take control of it for illegitimate purposes;
- Network Sniffers: used to capture network traffic, notably usernames, passwords and electronic mail;
- Scanners: [automated (to varying degrees)] tools that examine a network for vulnerabilities;
- Distributed Attack Tools: akin to sniffers, but with a wider scope and ability to effect larger numbers of hosts/computers; and
- Denial of Service Tools: used to disrupt access to network resources such as servers and web sites. [1]

It is important to understand the generalized threat types, but there is more to understanding network security vulnerabilities. As the capabilities and features of network and computer services and applications expand, so do the associated security challenges. The problem is complex and requires a comprehensive response; Howard F. Lipson, Ph.D of the CERT/CC explains:

> Perhaps the greatest threat to the Internet today is the abysmal state of security of so many of the systems connected to it. There are many contributing factors, including commercial off-the-shelf (COTS) software, in which the number of features and rapid time to market outweigh a thoughtful security design. New vulnerabilities are continually being discovered in such software. The widespread use of many COTS products means that once a vulnerability is discovered, it can be exploited by attackers who target many of the thousands or even millions of systems that have the vulnerable product installed. A lack of security expertise by most Internet users means that vendor security patches to remove the vulnerabilities will not be applied promptly, if at all. As a result, systems with unpatched vulnerabilities can be easily compromised, in large numbers, by motivated attackers, who will then use these systems as launching points to concentrate an attack against better-protected systems and to hide the tracks of the attacker.[2]

Sobering statistics are easily found. Twice a year, Symantec publishes an Internet security threat report; findings include:

- The average time between the public disclosure of a vulnerability and the release of an associated exploit was 5.8 days.
- The Symantec Vulnerability Database documented 1,237 new vulnerabilities between January 1 and June 30, 2004.
- On average, 48 new vulnerabilities per week were disclosed between January 1 and June 30, 2004.

© SANS Institute 2005 Author retains full rights.

- During this period, 96% of disclosed documented vulnerabilities were rated as moderately or highly severe.
- In the first six months of 2004, 70% of disclosed vulnerabilities were considered easy to exploit.
- During this period, 64% of vulnerabilities for which exploit code is available were considered high severity.
- In the first half of 2004, 479 vulnerabilities, or 39% of the total volume, were associated with Web application technologies.[3]

2.2 Defense In Depth

Defense-In-Depth (DiD) is a key concept in network security. DiD posits that no single defense is adequate in network security. Progress towards an improved security posture involves understanding threats and vulnerabilities and arraying a multiple, layered (and evolving) defense.

What does it mean to say that no one defense is adequate? And how does a SMB correlate the expensive defense systems and processes in place at large businesses with their limited resources – particularly when the threats and vulnerabilities are essentially the same?

Primarily, SMBs must understand DiD conceptually. The Information Assurance Group of the National Security Agency tells us that there are three key areas of DiD: People; Technology and Operations.[4] It is useful to think of DiD as a three-legged stool (take one away and the stool topples).

To a SMB this means that their people (or person) must be part of the security solution, not the problem. How much specialized knowledge is required for the SMB's staff? If there were a one-size-fits-all answer to this question then network security would be easy, but it's different for each SMB. The *people* part of DiD needs to be considered in regards to risks (which will be covered later).

Technology is the hardware and software in place. This equipment must be properly specified, designed, configured, deployed, maintained and disposed of if a sufficient security posture is to be maintained. Degree of success in terms of the technology aspect of DiD is best measured in auditing – and executed in best practices (both auditing and best practices are covered in future sections).

Finally, operations must be considered. How is the SMB using technology? Are sufficient network security safeguards in place to prevent intrusions, exploits and data loss and preserve confidentiality, integrity and availability (CIA)? Operations is measured through a combination of risk assessment and management, auditing and best practices.

© SANS Institute 2005 Author retains full rights.

Having just introduced *CIA*, it is now appropriate to define those, and some other, key network security terms:[5]

> *Confidentiality* – The need to ensure that information is disclosed only to those who are authorized to view it.
> *Integrity* - The need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
> *Availability* - The need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.
> *Authentication* - The process of confirming the correctness of the claimed identity.
> *Least-Privilege* - The principle of allowing users or applications the least amount of permissions necessary to perform their intended function.
> *Non-Repudiation* - The ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

2.3 Insider Attacks

Most are familiar with and understand the idea of external attacks. Less understood, however, is the concept of inside attacks. Inside attacks are: "defined as a crime perpetrated by, or with the help of, a person working for or trusted by the victim."[6] Insider attacks are one of the most vexing network security problems because they exploit the needs of usability and access for network users. It is one thing to keep people out, another to control who gets in and out, but something altogether different to apply controls to people inside the network.

There is much that can be done, but it requires, as do most effective network security measures, forethought, care and diligence. The particulars of discovering insider attack vulnerabilities and applying controls can be found in future sections.

2.4 SANS Top 20

With something as important and complex as network security there must be a reference point – something to look to for guidance and a place to start. The SANS Top 20 is just that reference point. For those not familiar with SANS a bit of an introduction is in order:

> SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.[7]

© SANS Institute 2005 Author retains full rights.

As the SANS web site explains, the vast majority of worms and successful cyber attacks are made possible by vulnerabilities in a small number of common operating systems. To help solve these sorts of problems SANS teamed with the National Infrastructure Protection Center to produce a list of the most critical network security vulnerabilities. (It is actually two lists; one of the most common Windows vulnerabilities and a similar list of potential UNIX and Linux exploits.) SANS explains that the list is a consensus list of vulnerabilities that require immediate attention. Furthermore, The Top 20 is a living document subject to revisions over time.[8]

How is the SANS Top 20 relevant for the SMB? It is extremely valuable in setting priorities and establishing a network security baseline. If a SMB does anything in regards to network security (and they should!), they must ensure that the Top 20 is addressed. If a SMB owner or technology services decision-maker does not get a *good* answer when they ask their system/network administrator or technology service provider about the SANS Top 20, they need to ask someone else.

2.5 First Steps

Now is the time to (hopefully) become skeptical. Skeptical of what you may ask? Of *everything* is what the experienced network security practitioner would say – of what I have written thus far and what follows certainly.

Many in the network security field joke that they have a *healthy* paranoia. It is indeed true that looking at everything as a threat is useful in the security field (to a point, of course). Just as a salesperson is always looking for the next sale, so should a network security practitioner (and perhaps the SMB owner) be looking for the next exploit.

Considering the source of information when attempting to combat network security threats is key. Just as the reader of this paper should be carefully evaluating my statements and sources, so should they ponder the motivations of informational and prescriptive materials.

The value of academic and non-commercial information is immeasurable. While certainly valuable in administering hardware or software, vendor-provided information has its limits and should not be considered the primary, and certainly not the sole, source. Consensus-based guidance and information should always take precedence in making network security decisions. No source is perfect or complete, but the absence of the *profit-motive* is very important.

2.6 A Journey, Not A Destination

Because network security threats, vulnerabilities and exploits are constantly evolving and expanding, so must any organization's response. This paper concentrates on the *how* of securing networks in a SMB context, but the *why* is just as important.

© SANS Institute 2005 Author retains full rights.

First, successful attacks cost the SMB money. When a computer virus clogs a network or a trojan horse inserts spam-bots and PCs slow to a crawl, a business can come to a standstill. The specifics of what does not get done while the exploit is in progress vary, but the financial impact is always the same – more than the SMB can afford. Exploit descriptions, examples and incredible dollar figures abound, but the truth that any SMB using computers and networks needs to be protected should be self-evident.

Second, the highly networked nature of business, and the world, allows for tremendous opportunities, as well as great risks. As with a chain, a network is only as strong as its weakest link (and the Internet is a network of networks). Keeping networks and computers secure means that SMBs must be part of the solution, not the problem.

> In the past, information security was not often seen as essential or even relevant to smaller businesses in both developed and developing countries. Now, the interdependence of different communication infrastructures and business models mean that all businesses are potentially interconnected. So it is imperative that everyone play their role in the global culture of security.[9]

It is possible to achieve a sufficient network security posture; getting there is well described by the National Cyber Security Partnership:

> Just as with other purchases, good information security requires both initial effort and ongoing checks. You need to do your research before buying security software, hardware or services. While you should expect the technology to work well, you still need to carry out the right checks to ensure that it's working correctly. Appropriate features must be set and adapted to work with your existing computers, software and network connections. Many security vulnerabilities are created when people install a new application and simply leave all the default settings in place, making them much easier for unauthorized users to manipulate.
>
> It may seem complicated or overwhelming at first, but over time your actions should become so familiar and automatic that they constitute a 'culture of security'. No one expects people running small businesses to review software code or understand the intricate workings of hardware. But you can and should read the relevant information, ask pertinent questions and get explanations of issues that don't seem clear. By taking the initiative and showing that security is important to your business, you can go a long way to making sure that your information systems develop in a secure way. In some cases, for example when making significant changes to your information systems, you may need expert assistance in the initial configuration and deployment of the system. But it's essential to keep asking the experts what they are doing and why, and to satisfy yourself that the choices made reflect your business needs and improve the information security of your business.[10]

3.0 Network Security & SMBs

3.1 Differences Between SMBs & Large Businesses

It is not realistic for the SMB to examine computer code or deploy comprehensive real-time network monitoring – they do not have the staff or expertise. That caveat, however, does not exempt the SMB from applicable network security best practices. In effective

© SANS Institute 2005 Author retains full rights.

network security, a compromise between the risk a SMB is exposed to and expense in protecting against that risk must be struck.

The simple fact is that large businesses have more, and sometimes more sophisticated, assets to protect. A large e-commerce site may have hundreds of thousands of saved customer profiles – many with stored credit card numbers. The potential negative consequences for a breach of network defenses are tremendous. Accordingly, large businesses take (hopefully!) significant steps to improve information and network security.

3.2 "Can't Happen To Me . . . "

It is quite possible that a SMB owner has read to this point and would agree that network security is important, yet still offer objections to devoting resources to developing a sufficient security posture. Seems counter-intuitive, but it is possible given the expenses involved.

Having objections, reasons, excuses – call them what you will – does not, however, make the problem go away. How the issue of network security is framed is key to moving forward in a positive direction.

Instead of offering example upon example of instances where SMBs were hit by a virus or had their network or servers compromised, the salient question is: what can the SMB afford to lose? For example, if the SMB uses e-mail as part of their business, can it afford to:

- lose all its saved contacts?
- lose all its past/saved e-mail messages?
- lose the ability to send and receive e-mail?
- have its address book(s) hijacked and used to flood virus-laden e-mails to others (particularly its *customers*)?

This example can be applied to any technology or process a SMB uses.

According to Microsoft, feeling exempt from threats because of size is dangerous in ways that might not seem obvious:

> Many small business owners believe that they do not need to worry much about security. "After all," they reason, "who would want to target my business when there are so many bigger targets out there." While it is true that small businesses are not directly attacked as often as larger, there are three flaws with this reasoning. The first reason is that small businesses often end up as part of larger attacks, such as mass worm outbreaks or efforts to harvest credit card numbers. The second reason is that because security is becoming tighter than ever at larger companies, small business networks look increasingly tempting to attackers. And the third reason is that this assumes that all attacks come from the outside.[11]

© SANS Institute 2005 Author retains full rights.

Another important reason that SMBs should be actively concerned with network security is that hackers will automate scans that search for vulnerable targets and will go after whatever they find to be accessible – regardless of business size.

3.3 Thinking Like A Hacker

Understanding your enemy is the first step to protecting yourself. And knowing the general steps a hacker takes in attempting to gain access to a network or system is important. The following are seven (generally accepted) steps a hacker takes:

1. Perform a footprint analysis
2. Enumerate information
3. Obtain access through user manipulation
4. Escalate privileges
5. Gather additional passwords and secrets
6. Install backdoors
7. Leverage the compromised system[12]

What do these steps mean to the SMB though? A brief explanation of each step and its potential impact is useful now:

The footprint analysis step is emblematic of the differences between SMBs and large businesses. To perform a footprint analysis the hacker must first decide on the desired target; this usually means identifying a domain name of a site of value/interest. Chances are the SMB won't make the cut in this calculation, so the SMB risk here is relatively low. However, if an automated scanner happens to find a vulnerable site – and that site belongs to a SMB – then an attack could commence. A key step to avoiding discovery is having a properly configured firewall (this is covered later in the Audit and Best Practices sections).

Next, a hacker will enumerate information about the site. He/she will attempt to find out everything possible about such things as operating systems/versions in use and open ports and what information probes might yield. Taking all the appropriate security/lockdown steps described in the SANS Top 20 will provide a high level of protection, while still allowing functionality (although an audit should still be performed to identify vulnerabilities).

Obtain(ing) access through user manipulation is the hacker's next step. There are two primary methods a hacker uses here: 1) social engineering (using interpersonal skills to get people to give information they would not otherwise volunteer) and 2) brute force attacks (using automated means of guessing passwords after having determined a user account name and with access to the system in question). Both of these issues can be effectively dealt with via security policies (covered later in the Best Practices section).

To escalate privileges, the hacker must take advantage of mis-configurations in a system to change their access level from the user-level account to a root or

© SANS Institute 2005 Author retains full rights.

administrator level account (once successful, they will have full control). Defense in this regard means having properly configured and patched systems.

The next step in the attack is gather(ing) additional passwords and secrets. The hacker now seeks any additional information that might give them further (or maybe future) control of the system in question. Ensuring proper configuration and patching, as well as such things as strong passwords, is key here (again, part of policies and best practices).

The hacker might have, or believe they have, limited time to access the system and will install backdoors to allow for future access. An implanted backdoor represents a significant breach and there is little a SMB can do at this point (save discovery and elimination). Well-designed policies and infrastructure may limit the damage a hacker can do by limiting access to other systems. Without, however, such things as file-integrity checking to detect changes to system files or some type of network monitoring to detect anomalous traffic, the attack will do damage.

Finally, the hacker leverage(s) the compromised system. At this point the hacker is most likely operating as an administrator on the compromised system and having his/her way (at this point the system must be taken off-line and appropriate remediation steps must be performed).

4.0 Risk Assessment & Management

4.1 What Is Risk Assessment and Management?

There are significant numbers of network security threats to SMBs and the threats will only increase. It is impossible to be completely protected from every threat. Reconciling those two interrelated, but opposite statements, is the realm of risk assessment and management.

The process of understanding threats and determining what action to take is critical for SMBs. Without an intelligent – and adequate – response to network security threats SMBs risk, among other things:

- lowered employee morale;
- loss of revenue and profits;
- downtime and loss of productivity; and
- possible damage to reputation and standing amongst customers.

Assessing risk is the first step to a better network security posture. But how do you start?

Knowing what you have is the first step to risk assessment (and management). Inventorying all technology systems and components allows for the calculation of the three components of risk: threat, vulnerability and cost. Risk is generally expressed as the following equation:

© SANS Institute 2005 Author retains full rights.

Risk = Threat x Vulnerability x Cost[13]

Considered generally, the components of risk break down as follows:

- Threat: something (negative) that could happen
- Vulnerability: likelihood that the threat will occur
- Cost: the dollar value of the loss if a vulnerability is exploited

Risk assessment and management is a complex and sophisticated field and area of study. The previous equation and explanation just scratch the surface. To discuss this field in-depth is beyond the scope of this paper.

4.2 The Business Case For Risk Assessment and Management

What is important is that with limited resources a SMB can only mitigate certain threats. In this regard, knowledge is power. Without a thorough examination of assets, their value to the business and an understanding of what a business is willing to lose, the chances that anything effective will happen in regards to network security are low.

Without risk assessment, network security threats can seem overwhelming. Overwhelmed SMBs generally resort to some combination of two strategies: applying controls they have heard about and can afford and/or dismissing threats as things that happen to other people. The latter seems hard to believe, but it is often true, and the former leads to a false sense of security.

An example of where SMBs apply risk assessment and management is useful before moving on to auditing.

Virtually no business leaves its doors unlocked after business hours. Real effort is put into deciding how much to spend on locks and doors and ensuring that they are installed and work properly. In this instance, a SMB perceives a threat (an intruder entering their place of business after hours), acknowledge that they are vulnerable (it is reasonable to think that this might happen to me) and understand the cost (the potential loss of merchandise, etc.). To mitigate the risk, the SMB applies controls (good locks and strong doors) (and some do even more . . .).

The above example also helps us understand the various responses to risk:

- Acceptance
- Mitigation (controls)
- Transfer

Whether consciously or not, every business decides on one of the responses above.

© SANS Institute 2005 Author retains full rights.

4.3 Understanding The Risk Equation

In the risk equation if any of the factors are close to or equal to zero, then the risk is zero. If one of the factors is of any significance however, then risk exists and a response must be chosen. Specifically, the SMB owner can 1) accept the risk (e.g. do nothing); 2) mitigate the risk (apply controls; e.g. deploy an intrusion prevention device at the network edge) or 3) transfer the risk (e.g. purchase insurance). Sometimes a combination of numbers two and three are chosen. (A non-technology example of a combination-response would be a Floridian who applies various hurricane-proofing building methods *and* purchases hurricane-related insurance.)

4.4 Risk Assessment and Management Is An Ongoing Process

Risk assessment and management is something that must be understood by the SMB owner and SMB technology service providers. The danger of one-size-fits-all strategies are that they either under-protect or over-protect – either of which is costly to the SMB. Intelligent and on-going (incorporating changes as they occur) risk assessment and management is the key to a sufficient network security posture.

What is more, risk assessment and management must be an ongoing process. SMBs face competition from various sources and know that to survive they must continually improve their product (to continue or expand their customer base) and improve their cost structure (to achieve or enhance profitability). The ongoing and evolutionary nature of risk assessment and management is no different.

5.0 AUDITING

Author's Note: A Basic SMB Network Security Assessment Check-List can be found in Appendix A

5.1 Why Audit?

Without auditing, risk assessment and management is merely a thought exercise. To effectively apply the principles of risk assessment and management there must be an understanding of the assets involved. Much like the old adage 'You can't solve problems you don't know about' says, without conducting full and regular audits a sufficient network security posture cannot be realized.

Virtually all business-people have some understanding of a financial audit, even if they have never been subject to one. These same business-people, however, may not know what an information/network security audit is, or understand its importance. As the importance of information and technology grows for businesses – large and small – so must the understanding of why it is critical to protect these assets.

5.2 SMB Auditing Constraints

Network security auditing, in the SMB context, is a different thing than for large businesses. The scale of auditing is just different for large businesses. Just as a large

© SANS Institute 2005 Author retains full rights.

business has significant resources devoted to managing large numbers of desktop computers, user accounts, network switches and routers and enterprise servers, so must it devote similar/proportional resources to network security auditing.

SMBs cannot hire large consulting firms to conduct comprehensive network audits. It is simply not possible given their resources. What SMBs do need is assessment, evaluation and recommendations that understand their constraints and needs – and fit their resources.

5.3 An Effective SMB Network Security Audit

Auditing is not just looking at all the devices present and examining them for such things as patch and hot-fix status and whether unnecessary services are disabled (although such is critical). Key to an effective network security audit is determining whether effective security policies are in place.

Without clear and comprehensive policies, employees and management do not know what their responsibilities are, nor is effective enforcement possible. Having SMB-centric security policies in place – from how the phones are answered and what information is given to caller (no matter who they *say* they are) to how change management is implemented on custom-built software – matters a great deal. (Security policy is also discussed in the next section on best practices.)

Asking the right questions is key to an effective and successful SMB network security audit. For example, an auditor that is asking questions about Access Control List management on routers and how often Intrusion Detection logs are reviewed does not understand how a 10-person small business uses technology. Examples of better questions are: does everyone have anti-virus software running (and how is it updated?) and has their installation of Microsoft Small Business Server been examined for unnecessary services and current patches and hot-fixes?

5.4 SMB Audit Process

As we can see, the mindset and approach that an auditor takes in regards to the SMB is critical – understanding the implications of resources disparities is very important. There are lessons that can be taken from large business audits though; procedure is key.

The first step to an effective and thorough network security audit is pre-audit preparation. A thorough site survey is critical. The auditor must ensure that they have accounted for equipment, personnel, processes and procedures before beginning an audit.

Past security issues, breaches and near-misses must also be accounted for and understood. Mistakes and problems from the past should be a part of the auditor's thought process during the audit, as that will yield the best recommendations later.

© SANS Institute 2005 Author retains full rights.

Scope must also be considered before the audit commences. Not having a solid understanding of what will be examined will lead to confusion later. The SMB owner may not have the resources to conduct a comprehensive audit of equipment, policies *and* business practices. Clearly defining the audit's scope and delineating the boundaries between related audit areas will help avoid potential conflicts. What is more, it will create a better understanding of interrelationships and what the SMB owner can, and cannot, expect from the audit.

The audit should not disrupt business activities. Obviously there will be some change from the normal day-to-day for the business, but the auditor must understand that some penetration and vulnerability tools can be disruptive. While these tools and tests are often very important for larger networks, they can be overkill for SMBs. (If it is deemed necessary to run such tests, it is probably best to do so in the evenings or on weekends. Any downtime caused by audit activities will likely sour the SMB owner on the process.)

After the audit is finished the auditor should brief the SMB owner on any problems that are found that need *immediate* attention. Short of any *critical* issues, it is time for the auditor to carefully review audit findings and report back to the SMB in a timely fashion.

Any post-audit report must be clear, succinct and have achievable fixes. Audit findings that recommend expensive new systems, along with important and affordable remediation, will likely be ignored. Such an outcome should be avoided at all costs as a SMB that has conducted a network security audit has taken a critical step towards better security – and represents a tremendous opportunity in improving network security as a whole.

5.5 Audit Tools

There are a number of tools available to the network security auditor. First and foremost, an open mind and attention to detail are the most important *tools* an auditor employs during a network security audit.

Many tools exist to assist the auditor in assessing the state of the network, its components and vulnerabilities. A complete treatment of free and commercial network security auditing tools is beyond the scope of this paper. However, an understanding of the wealth of tools available and their proper use is important.

The following sources should be consulted (as a starting point):

- NIST [14]
- CERT/CC[15]
- The Center for Internet Security[16]
- CERIAS[17]
- INSECURE.org[18]
- Microsoft[19]

© SANS Institute 2005 Author retains full rights.

6.0 BEST PRACTICES

Author's Note: the Basic SMB Network Security Assessment Check-List found in Appendix A may be useful in determining best practices.

6.1 What Are Best Practices?

According to the CERT/CC, a security best practice is "any action, procedure, or technique, that provides assurance that a control objective will be achieved."[20] It can be said that anything one does is a "practice," so everything a SMB does either contributes to the security of their business – or detracts from it. As the old saying goes: you are either moving forward or falling behind.

6.2 Why Are Best Practices Important?

The Internet Security Alliance does an excellent job of explaining why best practices are important for every size business:

> It is important to understand that neither the size of your company nor the type of your business guarantees protection from an attack. If you use the Internet, you are vulnerable. If you follow the recommended best practices contained here, you will be substantially less vulnerable.[21]

(Author's Note: the above referenced publication is (highly) recommended reading for any small-to-medium-size business-person.)

Another quote from ISAlliance's Guide is useful:

> Many attacks on Internet and network systems have no particular target. The attacker simply sends a large broadcast that uses any unprotected system as a staging point from which to launch an attack. Using computers without basic protections like firewalls, anti-virus software, and user education not only affects your own business, but many other businesses as the virus is spread around the Internet.
>
> Your system's lack of protection makes you a target: it can destroy your computer, your network, and can contribute to a virus distribution that slows or halts portions of the Internet. All of us who use the Internet have a responsibility to help create a culture of security that will enhance consumer and business confidence. But most importantly, failing to heed best practice advice could hurt your company significantly.[22]

6.3 Frameworks from Standards Organizations

There are many best practices guidelines and frameworks available from which SMBs can choose. These frameworks are best suited for the *not-small* SMB (say 25-1,000 employees) and most likely one with some type of in-house information technology staff (or staffer). The following are good places to begin research on network security frameworks and information security standards organizations:

- ISO 17799 (International Organization for Standardization)
- CoBIT (Control Objectives for Information & Related Technology)

© SANS Institute 2005 Author retains full rights.

- NIST 800 Series (National Institute for Standards and Technology)
- FIPS 199 (Federal Information Processing Standards)
- FFIEC Handbooks (Federal Financial Institutions Examination Council)
- ISSA-GAISP (Information Security Association – Generally Accepted Information Security Principles)
- IITIL (IT Infrastructure Library)
- BITS (Banking Industry Technology Secretariat)
- NERC (North American Electric Reliability Council)[23]

6.4 Transforming Audit Deficiencies

For a SMB to derive value from a network security audit deficiencies must be addressed. There are two key ways for turning the problems and weaknesses found in the audit to solutions and strengths.

First, and most important, problems must be solved. From the lack of a policy on how employees answer the phone (to avoid being fooled into giving out sensitive information) to disabling unnecessary services on a server – and everything in between – changes to address vulnerabilities must be made.

Next, and almost as importantly, how the problems came to be must be addressed. Whether through misconfiguration, lack of knowledge – whatever – the climate or culture in which the vulnerabilities arose must be addressed. This does not mean, however, that anyone should start pointing fingers or assigning blame. Just as everyone has a role in achieving a sufficient security posture, no one is immune from blame when things are not up to snuff. Besides, pointing fingers and laying blame is looking backward and network security is first and foremost about the future.

6.5 Relevant Best Practices

The key to achieving a sufficient network security posture for SMBs is to absolutely, positively, make sure that the basics are covered. The SANS Top 20 mentioned earlier is an important baseline of network security. The idea being that if the vulnerabilities in the SANS Top 20 are *not* addressed, then a SMB, or any business for that matter, has not achieved even the bare minimum in regards to network security. Along those same lines, the ISAlliance has an excellent list of (SMB-relevant) best practices that should be considered.

1. Use strong Passwords and Change Them Regularly
2. Lookout for E-Mail Attachments and Internet Download Modules
3. Install, Maintain, and Apply Anti-Virus Programs
4. Install and Use a Firewall
5. Remove Unused Software and User Accounts; Clean Out Everything on Replaced Equipment
6. Establish Physical Access Controls for all Computer Equipment
7. Create Backups for Important Files, Folders and Software
8. Keep Current with Software Updates
9. Implement Network Security with Access Control
10. Limit Access to Sensitive and Confidential Data[24]

© SANS Institute 2005 Author retains full rights.

The above is just a list of key network security best practices. If at all possible, the SMB owner, or their technology staff(er), should carefully review the ISAlliance's Guide so as to translate the recommendations to their particular situation and specific needs. In the event that an outside provider is being used, the ISAlliance's 10 Best Practices should be included in whatever proposal or plan is offered.

6.6 Security Policies

The importance of policies in the area of network security cannot be overstated. A key best practice is to define what is acceptable, and what is not. Ambiguity is one of the bigger stumbling blocks when it comes to achieving a sufficient network security posture. Furthermore, the development, implementation and maintenance of policies must work for each SMB.

The degree to which things are enumerated in policies – both in terms of what types of policies are written and level of detail – will be different for each SMB. For example, a larger SMB (~500 employees) may want to have separate policies for acceptable use of desktop computers, internet access, e-mail and interaction over the phone. The development, training and compliance issues related with so many policies may not work for the smaller SMB (say, 25 employees) and they may wish to write a single, comprehensive policy.

Network security policy is a rich field and further discussion is beyond the scope of this section, and paper. Interested parties should investigate the following online resources; SANS;[25] Network Working Group (RFC 2196);[26] Cisco;[27] and Symantec.[28]

6.7 The Danger of False Economy

In implementing best practices a balance between unnecessary expense and false economy must be struck. Unfortunately, there is not a clear and objective standard for SMBs to reference when determining which best practices to employ.

SMBs must bring together various sources of information to make the best decision they can about how they spend their money in regards to network security. Again, the importance of risk assessment and management is clear. Without an understanding of the *bad* things that could happen, any action taken runs the risk of being excessive or inadequate.

Good sources of information are objective web sites and publications (the Internet Security Alliance is a good place to start); local and national industry-specific groups (which may produce guides that relevant); local and regional chambers of commerce (to find similar businesses who have implemented network security controls and possible workshops) and, finally, technology service providers.

© SANS Institute 2005 Author retains full rights.

6.8 Consider Support

So, now the SMB:

1) understands they are vulnerable;
2) believes that network security is important;
3) has assessed their risks;
4) has completed an audit; and
5) has developed a best practices plan.

Is there anything else they *must* do before implementing changes?

Yes. There is another key issue to consider: support/maintenance. How will changes and improvements be monitored and maintained? Will companies that are supplying the hardware, software and services be around in one month, six months, a year, or longer? There are a number of questions that a SMB should ask (or get good answers from their service provider) before expending scarce resources; they include:

- how long has the vendor been in business?
- how long has the vendor been involved in the particular area?
- how accessible is support (for you or your service provider)?
- is self-service support available (i.e. knowledgebases, FAQs, interactive FAQs)
- does the vendor track your purchase/relationship?
- do any of your peers have experience with the vendor?
- does the vendor cater to SMBs, or are they an afterthought?
- are hotfixes and patches easy to obtain?
- what is the vendor's track-record/policy on updates? (i.e. what's free, and what's not?)

7.0 VALUE

7.1 Demonstrating Value

Demonstrating the value of network security in the SMB context is difficult. It is a challenge even when discussing large businesses with significant assets. The problem lies in proving a negative – that preventing something from happening (a network security breach), rather than *causing* it (implementing a new e-commerce system), is where value lies.

It is now useful to revisit the area of risk assessment and management, specifically: risk assessment. While attempts by SMBs to calculate the value of information assets and potential losses is an inexact science at best, the imperative remains.

7.2 Loss Expectancies

Inaction, as we have seen, is not an acceptable course. In working towards a sufficient network security posture the value of assets, their potential loss or unavailability and control costs must be considered. SMBs must identify their assets and apply two key

© SANS Institute 2005 Author retains full rights.

calculations in deciding what security steps to take: Single Loss Expectancy (SLE) and Annualized Loss Expectancy.[29]

SLE is expressed through a standard formula which includes: Asset Value (AV) (what the asset was purchased for or its value to the business) and Exposure Factor (EF) (the degree to which an asset is damaged as a percentage (10% = minimal damage; 100% = complete destruction of the asset).

$$SLE = AV \times EF$$

Annual Loss Expectancy, or ALE, is a determination of how many times in a year the SLE is anticipated.[30] In the SMB context, it is really up to the individual business to determine whether it is reasonable to believe that a threat is ongoing. Or, in other words, the business activity that engenders the threat can be curtailed or eliminated – or sufficient network security controls can be put in place (or nothing can be done and the ALE remains high). ALE is a product of SLE and the Annual Rate of Occurrence (ARO)

$$ALE = SLE \times ARO$$

7.3 Understanding SLEs and ALEs

What are some actual SMB examples of these formulas? First, let's say that there are human assets and information assets. Broadly stated, human assets are the business knowledge and wisdom, customer familiarity and productivity of SMB people. Information assets are business databases, trade secrets and the availability and smooth functioning of such things as networks, servers, E-Mail and computers (and even telephones!).

A blended event example would be a virus that infects all the computers of a SMB and clogs the network with unauthorized traffic rendering the network unusable. In this instance both the human assets were affected (the computers they rely on were not available and they could not work) as well as the information assets (the computers would not be available until the virus was eliminated).

More importantly – and harder to assign a number to – is the possible damage to the reputation and good standing of the business. To the extent that the business was unavailable to its customers (and suppliers and partners), damage may be done to the future prospects of the business. In highly competitive environments the damage to a company's reputation can be very damaging indeed. If customers have options and doubt the availability of a product or service, they will find another provider. This is especially true if the availability question could impact *their* business and ability to deliver to customers.

An information asset example is a hacker compromising a server and stealing sensitive customer information (which could include credit card numbers). The damage to human assets in this instance is relatively low, but the damage to reputation could be

© SANS Institute 2005 Author retains full rights.

tremendous. Even though credit card companies limit customer liability for fraud to $50.00, the impact on customer confidence is significant. And with the importance and prevalence of e-commerce and credit card transactions growing every year, companies that can gain and hold customer confidence will be best positioned for success.

8.0 THE SECURITY LIFE-CYCLE

8.1 A Process, Not An Outcome

Security, like success, is a process not an outcome. Of course the "success" reference is a well-worn cliché, but it is no less relevant to a discussion of network security and the SMB. If network security threats were static then vulnerabilities could be fixed and risk would be nil – but we know that to be false.

Because the number and nature of threats is increasing and evolving, so must our response. The only other option is to not use technology and find a way to function in the business world without the advantages and speed that much of technology confers.

As this paper has tried to address, there is a process to network security. That is to say, a place to begin and a way to proceed. Note: I did not close that loop and say *a place to end*.

A sufficient network security posture is best achieved when network security is integrated in all business activities. The National Institute of Standards and Technology (NIST) explains the importance of the life-cycle approach to network security: "Security, like other aspects of a computer system, is best managed if planned for throughout the computer system life cycle."[31]

8.2 The Computer System Life Cycle

NIST describes five steps/phases in the Computer System Life Cycle: Initiation; Development/Acquisition; Implementation; Operation/Maintenance and Disposal.[32] The following is a SMB-relevant description of each phase.[33]

Initiation: Every business function, process or system begins somewhere. When a business opportunity or need is discovered and work begins, network security should be considered.

Development/Acquisition: As assets (computer hardware, software, WAN connectivity . . .) are sourced, specified, designed, programmed, developed, or otherwise decided on, network security should be part of the process.

Implementation: Prior to deployment, a function, process or system must be examined and tested for vulnerabilities – and problems must be fixed.

© SANS Institute 2005 Author retains full rights.

Operation/Maintenance: As the function, process or system is used it will no doubt change over time. It is critical that as updates are made that network security best practices are maintained.

Disposal: When a function, process or system has reached the end of its useful life it must be disposed of in a way that does not expose the SMB (or its customers) to risk.

9.0 CONCLUSION

While the process is daunting, information and network security is possible and affordable for SMBs.

As the importance and use of technology rises for businesses of all sizes it is reasonable to expect that threats will experience a similar increase. The pace of change is indeed fast and many SMBs will find it hard to keep up. This difficulty, however, is no excuse for inaction – there is much at stake, even for SMBs. Each SMB must examine the value of technology and make appropriate investments to protect their assets. The threats are real, vulnerabilities many and no one is immune. What matters is how the SMB responds.

The expanding and evolutionary nature of the threats necessitates approaching network security as a journey – not a place of departure and a destination point. SMBs know that each day brings competitive and customer challenges and opportunities – as they use technology more and more, so must they include network security threats in their daily calculus.

Besides examining the question of network security and the SMB, this paper has tried to describe the wealth of information available on the Internet. There are two sources that stand out: the Resources area of the SANS Institute web site[34] and the ISAlliance's web site.[35] I recommend that anyone concerned with network security and the SMB bookmark and visit those pages often. For your convenience, here are the addresses:

http://www.sans.org/resources/

http://www.isalliance.org/

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

10.0 APPENDIX A: BASIC SMB NETWORK SECURITY ASSESSMENT CHECK-LIST

DESKTOP COMPUTERS

- are computers base-lined for security before deployment?
  - BIOS password?
  - unneeded groups/users removed?
  - Windows: MBSA?
- are personal firewalls present (or host-based intrusion detection)?
- are dial-up modems secured (if attached to a phone line)?
- is anti-virus software present and functioning?
- are anti-virus definitions up-to-date?
- are patches and security hot-fixes up-to-date?
- are passwords secure?
  - or, two-factor authentication with simple, rotated, passwords?
- is authentication-after-idle in place? (what is timeout?)
- is there a failed login limit?
- groups with privilege profiles vs. many users with many privilege profiles?
- is Administrator access disallowed?
- are sensitive files encrypted?
- is anything logged?
- what is backed-up?
- do computers have remote administration enabled/capabilities?
- are there external storage devices? (USB memory keys, external HDDs?) (is that data secure?)
- is computer case lockable(ed)?

The above are only some basic questions that should be asked; the following offer specific information:

Linux (The Linux Documentation Project)[36] (Debian)[37], (Red Hat and Mandrake)[38] (SUSE)[39]
Apple/Macintosh[40], and[41], and[42]
Windows NT Workstation and 2000 Professional[43]

NETWORK

Edge

- is network equipment physically secure?
- how is network traffic filtered at edge?
- is a firewall in place?
- is firewall certified by an independent authority?
- are access control lists (ACLs) in place?
- what is the ports allowed policy?
  - allow all, deny some?
  - deny all, allow required?
- how often are ACLs updated?
- at what (OSI) layers does the firewall filter?
- are management interfaces secure?
- is SSH used?
- are passwords secure?
- is firewall firmware up-to-date?
- is firewall operating system up-to-date?
- is spam filtered?
- are dangerous attachments disallowed?
- are VPNs used?
- what access to tunneled users have?

© SANS Institute 2005 Author retains full rights.

- are unauthorized outbound connections disallowed?

Core

- # of switches vs. # of hubs?
- are switches managed securely (SSH)?
- how is SNMP implemented/managed?
- is there VLAN segmentation?
- are new users registered?
- are insecure computes denied network access/quarantined?

Wireless

- what security protocols are in use (802.1X? 802.11i?)?
- is rogue Access Point (AP) detection in use?
- are APs physically secured?
- how are APs managed?
- is there a management VLAN for APs?
- is network traffic encrypted?
- are users/packets authenticated? against what?
- is there an isolation VLAN for wireless traffic?
- is there an internal firewall to segregate wireless users?
- what can wireless hosts access?
- are clients Infrastructure-mode only?
- is wireless access public? if so, what edge protections are in place?

The above are only some basic questions that should be asked; the following offer more specific information:

Check Point (vendor site)[44]
Cisco Routers and PIX Firewalls[45]; (vendor site)[46]
HP (vendor site; network security how-to guide)[47] (vendor site; wireless LAN how-to guide)[48]
Juniper/Netscreen (vendor site)[49]
SonicWALL (vendor site)[50]
WatchGuard (vendor site)[51]

Note: some vendors do not offer generalized security information, if a vendor is not listed above please see their web site and search based on your particular product/model.

POLICIES

- what policies are in place?
- how are policies developed?
- how are policies maintained?
- how are policies enforced?
- are regulatory requirements being met?

For more information on polices a good place to start is the SANS Security Policy Project[52]

SERVERS

- is server physically secure?
- is server public-facing?
- if public-facing, is it in a DMZ?
- if not public-facing, private or public IP address?

© SANS Institute 2005 Author retains full rights.

- is anti-virus software present and functioning?
- are anti-virus definitions up-to-date?
- are patches and security hot-fixes up-to-date?
- are passwords secure?
- is user/group schema secure?
- is authentication-after-idle in place? (what is timeout?)
- is there a failed login limit?
- check for unnecessary services
- host-based intrusion detection
- file integrity monitoring
- sensitive file encryption?
- is telnet or FTP enabled? if so, why?
- is logging enabled,? for what events?
- are logs reviewed regularly?
- has the server been scanned for vulnerabilities?
- what are the server's trust relationships?

The above are only some basic questions that should be asked; the following offer specific information:

FreeBSD[53]
HP-UX[54]
Linux (The Linux Documentation Project)[55] (Debian)[56], (Red Hat and Mandrake)[57] (SUSE)[58]
Solaris[59]
Windows NT Workstation and Server/2000 Professional and Server/2003 Server[60]

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

11.0 WORKS CITED – USEFUL RESOURCES

[1] CERT Coordination Center. "Overview: Incident and Vulnerability Trends." URL: http://www.cert.org/present/cert-overview-trends/module-4.pdf (20 October 2004).

[2] Lipson, Howard F.. "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues." URL: http://www.cert.org/archive/pdf/02sr009.pdf (20 October 2004).

[3] Symantec. "Symantec Internet Security Threat Report – Trends for January 1, 2004 – June 30, 2004." Volume VI. Page 4.

[4] The Information Assurance Group of the National Security Agency. "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments." URL: http://www.nsa.gov/snac/support/defenseindepth.pdf (20 October 2004.)

[5] SANS Institute. "SANS Glossary of Terms Used in Security and Intrusion Detection." Updated May 2003. URL: http://www.sans.org/resources/glossary.php# (20 October 2004).

[6] Einwechter, Nathan. "The Enemy Inside The Gates: Preventing and Detecting Insider Attacks." SecurityFocus.com." URL: http://www.securityfocus.com/infocus/1546 (20 October 2004).

[7] SANS Institute. "About The SANS Institute – Press Room." URL: http://www.sans.org/aboutsans.php (20 October 2004).

[8] SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." URL: http://www.sans.org/top20/ (20 October 2004).

[9] CyberPartnership.org. "Information security issues and resources for small and entrepreneurial companies: A business companion to the 2002 OECD Guidelines for security of networks and information systems: Toward a culture of security." URL: http://cyberpartnership.org/Biac%20SME%20Guide.pdf (20 October 2004). Page 4.

[10] ibid, Page 7.

[11] Microsoft. "Why Security Matters." URL: http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/why_security_matters.mspx (20 October 2004).

[12] Schultze, Eric. "Thinking Like A Hacker." URL: http://www.shavlik.com/Whitepapers/Thinking%20like%20a%20hacker.doc.pdf (20 October 2004).

[13] TruSecure Corporation. "Business-Driven Security: A Risk Mitigation Approach." September 2002. Page 6.

[14] Wack, John and Miles Tracey. "DRAFT Guideline on Network Security Testing. Recommendations of the National Institute of Standards and Technology." NIST Special Publication 800-42. URL: http://csrc.nist.gov/publications/drafts/security-testing.pdf (20 October 2004).

[15] CERT Coordination Center. "CERT Security Practices." URL: http://www.cert.org/security-improvement/practices/practices.html (20 October 2004).

© SANS Institute 2005 Author retains full rights.

[16] Center for Internet Security. “Benchmarks/Tools.” URL: http://www.cisecurity.org/benchmarks.html (20 October 2004).

[17] Center for Education and Research in Information Assurance and Security. “COAST Projects.” URL: http://www.cerias.purdue.edu/about/history/coast/projects/ (20 October 2004).

[18] INSECURE.ORG. “Top 75 Security Tools.” URL: http://www.insecure.org/tools.html (20 October 2004).

[19] Microsoft. “Enterprise Security Tools.” URL: http://www.microsoft.com/security/guidance/tools/default.mspx (20 October 2004).

[20] CERT Coordination Center. “Which Best Practices are Right For Me?” Version 1.0. URL: http://www.cert.org/archive/pdf/secureit_bestpractices.pdf (20 October 2004).

[21] Internet Security Alliance. “Common Sense Guide to Cyber Security for Small Business.” URL: http://www.isalliance.org/resources/papers/Common_Sense_sm_bus.pdf (20 October 2004). Page 4.

[22] ibid. Page 4.

[23] CERT Coordination Center. “Which Best Practices are Right For Me?” Version 1.0. URL: http://www.cert.org/archive/pdf/secureit_bestpractices.pdf (20 October 2004).

[24] Internet Security Alliance. “Common Sense Guide to Cyber Security for Small Business.” URL: http://www.isalliance.org/resources/papers/Common_Sense_sm_bus.pdf (20 October 2004). Pages 9-32.

[25] SANS Institute. “The SANS Security Policy Project.” Resources. URL: http://www.sans.org/resources/policies/ (20 October 2004).

[26] Network Working Group. “Site Security Handbook.” Request For Comments 2196. URL: http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc2196.html#sec-2 (20 October 2004).

[27] Cisco. “Network Security Policy: Best Practices White Paper. White Papers. Document ID: 13601. URL: http://www.cisco.com/warp/public/126/secpol.html (20 October 2004).

[28] Symantec. “ Importance of Corporate Security Policy.” Security Response. URL: http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html (20 October 2004).

[29] Wilson, Marcia. “Calculating security ROI is tricky business. “July 24, 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,83207,00.html?SKC=security-83207 (20 October 2004).

[30] SANS Institute. “1.3 – Internet Security Technologies.” GSEC Courseware; Track 1 – SANS Security Essentials and the CISSP 10 Domains. Page 355.

[31] National Institute of Standards and Technology. “An Introduction to Computer Security: The NIST Handbook.” URL: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (20 October 2004). Page 74.

[32] ibid. Pages 75-6.

[33] [While the underlined headings are taken from the following source, the text that follows is my own.] National Institute of Standards and Technology. “An Introduction to Computer Security: The NIST

© SANS Institute 2005 Author retains full rights.

Handbook." URL: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (20 October 2004). Pages 75-6.

[34] SANS Institute. "Resources Page." URL: http://www.sans.org/resources/ (20 October 2004).

[35] Internet Security Alliance. "Home Page." URL: http://www.isalliance.org/ (20 October 2004)

[36] The Linux Documentation Project. "Home Page." URL: http://www.tldp.org/ (20 October 2004)

[37] Debian. "Debian Security Audit Project." URL: http://www.debian.org/security/audit/ (20 October 2004)

[38] Center for Internet Security. "CIS Level 1 – Benchmark and Scoring Tool for Linux." Version 1.1.0 (Benchmark), 1.4.2-1 (Scoring Tool). October 2003. URL: http://www.cisecurity.org/bench_linux.html (20 October 2004).

[39] SuSE. "Business Customers – Security." URL: http://www.suse.com/us/business/security.html (20 October 2004)

[40] Apple. "Apple Product Security." URL: http://www.info.apple.com/usen/security/index.html (20 October 2004)

[41] Ernest Orlando Lawrence Berkley National Laboratory. "Procedures for Securing Systems: Macintosh." Computer Protection Program. URL: http://www.lbl.gov/ITSD/Security/systems/mac.html (20 October 2004).

[42] SecureMac.com. "Home Page." URL: http://www.securemac.com/ (20 October 2004)

[43] Center for Internet Security. "Center for Internet Security Benchmarks and Scoring Tool for Windows XP Professional, Windows Server 2003, Windows 2000 and Windows NT." [Multiple versions available.] URL: http://www.cisecurity.org/bench_win2000.html (20 October 2004).

[44] Check Point Software Technologies Ltd. "Security Center." URL: http://www.checkpoint.com/securitycenter/index.html (20 October 2004).

[45] Center for Internet Security. "CIS Level 1/Level 2 – Benchmarks and Audit Tool for Cisco IOS Routers and PIX Firewalls." Version 2.2. September 2004. URL: http://www.cisecurity.org/bench_cisco.html (20 October 2004).

[46] Cisco. "Security and VPN." URL: http://cisco.com/en/US/products/hw/vpndevc/index.html (20 October 2004).

[47] HP. "Define a network security policy." Solutions – how-to guides. URL: http://www.hp.com/sbso/productivity/howto/security/index.html (20 October 2004).

[48] HP. "Set up a wireless LAN." Solutions – how-to guides. URL: http://www.hp.com/sbso/productivity/howto/wireless_lan/index.html (20 October 2004).

[49] Juniper Networks. "Security." Solutions. URL: http://juniper.net/solutions/security/ (20 October 2004).

[50] SonicWALL. "Small-to-Medium Business." Markets. URL: http://www.sonicwall.com/industries/smmdbus.html (20 October 2004).

[51] WatchGuard. "Resource Center." Products. URL: http://www.watchguard.com/products/infocenter.asp (20 October 2004).

© SANS Institute 2005 Author retains full rights.

[52] SANS Institute. "The SANS Security Policy Project." Resources. URL: http://www.sans.org/resources/policies/ (20 October 2004).

[53] Center for Internet Security. "CIS Level 1 – Benchmark and Scoring Tool for FreeBSD." Benchmarks/Tool. Version 1.0.4 (Benchmark) 1.5.5 Scoring Tool. September 2004. URL: http://www.cisecurity.org/bench_freebsd.html (20 October 2004).

[54] Center for Internet Security. "CIS Level 1 – Benchmark and Scoring Tool for HP-UX." Benchmarks/Tool. Version 1.1.0 (Benchmark) 1.4.2-1 (Scoring Tool). October 2003. URL: http://www.cisecurity.org/bench_hpux.html (20 October 2004).

[55] The Linux Documentation Project. URL: http://www.tldp.org/ (20 October 2004).

[56] Debian. "Debian Security Audit Project." URL: http://www.debian.org/security/audit/ (20 October 2004)

[57] Center for Internet Security. "CIS Level 1 – Benchmark and Scoring Tool for Linux." Version 1.1.0 (Benchmark), 1.4.2-1 (Scoring Tool). October 2003. URL: http://www.cisecurity.org/bench_linux.html (20 October 2004).

[58] SuSE. "Business Customers – Security." URL: http://www.suse.com/us/business/security.html (20 October 2004).

[59] Center for Internet Security. "CIS Level 1 – Benchmark and Scoring Tool for Solaris." Version 1.3.0 (Benchmark), 1.5.0 (Scoring Tool). August 2004. URL: http://www.cisecurity.org/bench_solaris.html (20 October 2004).

[60] Center for Internet Security. "Center for Internet Security Benchmarks and Scoring Tool for Windows XP Professional, Windows Server 2003, Windows 2000 and Windows NT." [Multiple versions available.] URL: http://www.cisecurity.org/bench_win2000.html (20 October 2004).

© SANS Institute 2005 Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**