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.

# Security Incident Handling in Small Organizations

ep through  the processes before, during, and after a security incident,  along with literature, vendor, and tool resources....

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn
More

# Security Incident Handling in Small Organizations

Author: Glenn Kennedy

Advisor: Jim Purcell

© SANS Institute 2008, Author retains full rights.



© SANS Institute 2008, Author retains full rights.

## Security Incident Handling in Small Organizations

A challenge exists when attempting to provide the Small Business (SB) owner with a workable procedure and resources for security incident handling. Considerable research has been accomplished, with a focus on the steps necessary to create and organize an Incident Handling Team in large organizations, but the resources required for such a project do not scale down to anything usable by the Small Business community. This paper reviews current best practices in the security community, and proposes a compromise that scales these steps into something workable and acceptable to the SB community. The paper also references SANS checklists to assist the SB owner step through the processes before, during, and after a security incident, along with literature, vendor, and tool resources.

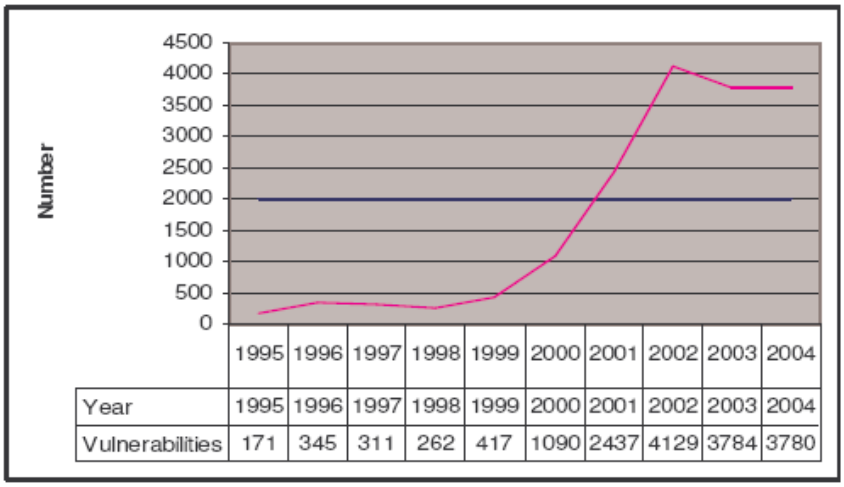
### Analysis of the Problem

Small Business is the backbone of the economy in the United States. They "represent 99 percent of all employers, employ 52 percent of all private workers, and provide 51 percent of the private sector output." (Klomp, 2001). With Small Businesses representing this magnitude of the business environment in the United States, it is easy to see why small business security is of considerable importance to the U.S. economy.



© SANS Institute 2008, Author retains full rights.

Over the years from 2000 to 2005, the reported computer system vulnerabilities have increased by 347%, as indicated in the following graph (Carnegie Mellon).




In 2007, the Government Accountability Office (GAO) published GAO-07-705 "Cybercrime," highlighting the threat to U.S. Business, and calling for Federal action to mitigate the threat.

"Cybercrime is a threat to U.S. national economic and security interests. Various studies and expert opinion estimate the direct economic impact from cybercrime to be in the billions of dollars annually. The annual loss due to computer crime was estimated to be $67.2 billion for U.S. organizations, according to a 2005 Federal Bureau of Investigation (FBI) survey. The estimated losses associated with particular crimes include $49.3 billion in 2006 for identity theft and $1 billion annually due to phishing." (Government Accountability Office (GAO) Cybercrime, p. 2)

These reports make clear the magnitude of the threat, and recent federal legislation including Sarbanes-Oxley and HIPAA;



© SANS Institute 2008, Author retains full rights.

have raised the bar for publicly traded firms and the health industry. In the U.S., most medium-sized and enterprise scale organizations have responded with addition of full-time security staff and the formation of Incident Handling teams, in accordance with recommendations from publications like the National Institute of Standards and Technology (NIST) publication SP800-61 Revision 1. (National Institute of Standards and Technology (NIST), 2008)

The remaining challenge is these techniques remain far outside the economic and organizational capability of small business in the U.S. The typical small business owner may understand the threat but feel he or she is powerless to fund or provide such mitigation. With the magnitude of the threat, it is important the security community direct attention to the needs of the Small Business owner, and provide economically and organizationally practical steps for the monitoring and mitigation of these threats.

## Definition of Incidents

An *event* is any observable occurrence in a system or network. Events include a user connecting to a file, a server receiving a request for a Web page, a user sending electronic mail, and a firewall blocking a connection attempt. *Adverse events* are events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malicious code that destroys data. A computer security



© SANS Institute 2008, Author retains full rights.

*incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. The terminology for these incidents is helpful to the small business owner for understanding service and product offerings.

*Denial of Service* - An attacker directs hundreds of external compromised workstations to send as many ping requests as possible to a business network, swamping the system.

*Malicious Code* - A worm is able to quickly infect several hundred workstations within an organization by taking advantage of a vulnerability that is present in many of the company's unpatched computers.

*Unauthorized Access* - An attacker runs a piece of "evil" software to gain access to a server's password file. The attacker then obtains unauthorized administrator-level access to a system and the sensitive data it contains, either stealing the data for future use or blackmailing the firm for its return.

*Inappropriate Usage* – An employee provides illegal copies of software to others through peer-to-peer file sharing services, accesses pornographic or hate-based websites or threatens another person through email.

## Definition of Small Business

The Small Business Administration defines a small business as one that is "independently owned and operated and which is not dominant in its field of operation." (Small Business Administration). It further goes on to define a series of



© SANS Institute 2008, Author retains full rights.

employee counts and revenue for various categories of small businesses. For the purposes of this paper, the definition is further restricted to a standard of "under 100 employees in the United States and under 50 employees in the European Union (Wikipedia, 2004). The paper is also of direct relevance to what are termed "microbusinesses" with less than 10 employees.

## Vulnerabilities, Threats and Risk

Security management makes a distinction between vulnerabilities, threats, and risk. *Vulnerabilities* are an inherent security weakness in an element of hardware or software. These are frequently a software vulnerability brought about by immature software development methodology, which allows "evil" attackers to formulate or craft input data in a manner that yields unexpected results. Many such vulnerabilities might well exist in software, hardware or systems, but never be exploited for any number of reasons.

Vulnerabilities typically include:

1. Physical security of work areas, computers, and servers
2. People Issues – weak vetting, social engineering
3. Password Issues
    a. Use of default passwords
    b. Non-existent use of passwords
    c. Weak passwords
4. Flaws in the operating system – Microsoft Windows, Mac OS, UNIX
5. Flaws in the application software – MS Word, Excel, etc



© SANS Institute 2008, Author retains full rights.

6. Network protection issues – lack of firewalls
7. Data Integrity – lack of backup, offsite storage and restore capability

A *threat* is an instance of a tool or technique used by an "evil" attacker to exploit one or more vulnerabilities in a system for personal or organizational gain. These threats originally came from "hackers' experimenting with computer systems for personal learning, with perhaps the equivalent of "soaping a window" as the highest threat level. Increasingly, these threats are orchestrated by criminal organizations for identity theft or international city-states for military and economic warfare (Federal Bureau of Investigation).

In many cases, Small Businesses are often affected by large global attacks, such as mass worm outbreaks, and with security becoming tighter at larger enterprises; small business networks look increasingly tempting to attackers.

The Small Business owner should be aware of the terminology associated with these range of threats:

*Spam* or unsolicited commercial e-mail messages, wastes bandwidth and time. The sheer volume of it can be overwhelming, and it can be a vehicle for viruses. Much of it is of an explicit sexual nature, which creates an uncomfortable work environment and, potentially, legal liabilities if companies do not take steps to stop it.

*Spoofing* means creating packets that disguise the originating address to look as though they have come from somewhere else, a technique used primarily in one-way denial of



© SANS Institute 2008, Author retains full rights.

service (DoS) attacks. E-mail spoofing means forging an e-mail message so the *From* address does not indicate the true address of the sender.

*Phishing* is increasingly becoming a tactic of choice for hackers and organized crime. Typically, an attacker sends an e-mail message that looks very much like it comes from an official source (such as a bank or financial institution). Links in the message take one to a website that also looks like the real thing. The goal of the scam is to trick one into giving away personal information, sometimes for Spam lists, sometimes so that the perpetrators can steal account information or even identity.

*Viruses* are programs designed to replicate themselves and potentially cause harmful actions. Viruses in e-mail messages often masquerade as games or pictures and encourage users to open and run them. Viruses try to replicate themselves by infecting other programs on the computer.

*Worms* are similar to viruses in that they try to replicate themselves, but they are often able to do so by directly exploiting a vulnerability in a system without end-customer action, like opening an email.

*Trojan Horses* are malicious programs pretending to be benign applications. They do not replicate like viruses and worms but can still cause considerable harm. Often, viruses or worms are smuggled inside a Trojan horse.

*Spyware* refers to small, hidden programs that run on the computer and are used for everything from tracking online activities to allowing intruders to monitor and access the



© SANS Institute 2008, Author retains full rights.

computer. Typical sources of Spyware are downloaded music from file-sharing systems, free games from sites not trusted, or other software from an unknown source.

*Information disclosure* is exposure of information to individuals who normally should not have access to it. For example, a user on the network might make certain company proprietary files accessible over the network that should not be shared.

*Denial of Service* (DoS) attacks are computerized assaults launched by an attacker in an attempt to overload or halt a network service. Such an attack may cause a server to become so busy attempting to respond that it ignores legitimate requests for connections.

*Elevation of privilege* is a process by which a user misleads a system into granting unauthorized rights, usually for the purpose of compromising or destroying the system. For example, an attacker might log on to a network by using a guest account, then exploit a weakness in the software that lets the attacker change the guest privileges to administrative privileges.

The vulnerabilities or the threats by themselves do no harm to a computer system. It is when a threat coincides with or overlaps a vulnerability that *risk* occurs to the small business. When there is risk, an "evil" attacker may *exploit* that risk and trigger an *incident*.

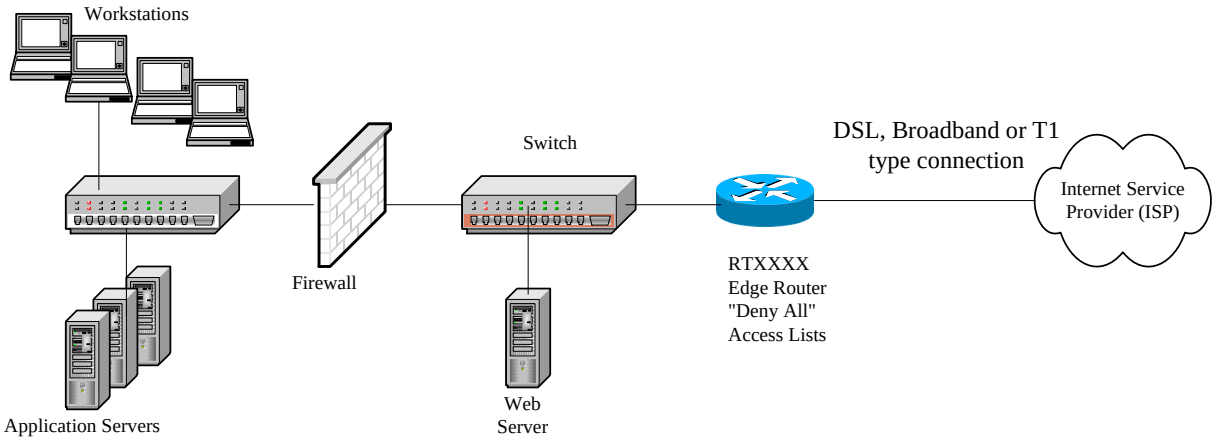


© SANS Institute 2008, Author retains full rights.

## Small Business Technology Environment

These vulnerabilities, threats, and risks exist in a technical environment that appears foreign to the small business owner. A brief and simplified view of the components will assist in understanding the mitigation steps and more intelligently assessing service offerings from computer support organizations.

When we link two or more computers together using network cards and cables (or a wireless setup) a local area network (LAN) is created. All the computers on the network can share data and




e-mail as well as access shared resources like printers, modems, or broadband Internet connections. This block diagram indicates a typical small business architecture, and will assist to providing a framework for the following discussions. Link two or more LANs together over a broadband or DSL-type connection, and a wide area network (WAN) has been created. When one of these connections is to an Internet Service Provider (ISP), the small business network is now connected to the Internet, and here is where the trouble begins. Until the business is connected to a public network, it



© SANS Institute 2008, Author retains full rights.

is reasonably safe from external threats. Hooking up to the public Internet is connecting the previously safe small business network to the entire global span of the Internet. This process of communication involves some terminology that will assist the SB owner.

*Packets* - Information travels across networks in small chunks called packets. The packet has the data plus an address that tells the network where to deliver that data. Everything going over the Internet is broken down into packets, including Web pages, e-mail messages, and downloads. Large amounts of data like graphics and large files are broken down into a series of packets and reassembled at the destination. As these packets travel over the Internet, they are exposed to eavesdropping at many of the locations where they jump from one system to another.

*Addresses and Ports* - Every computer on the network is assigned a unique number called an Internet protocol (IP) address. The IP address uniquely defines that computer on the network and provides directions for packets to reach their destinations. IP addresses work much like street addresses. Part of the address identifies the destination network, and part of the address identifies the actual computer at the destination.

With the IP address uniquely identifying a network and computer, the system still needs to identify the application program within the computer that is the ultimate destination. This is accomplished by assigning what is called a *Port* number to each piece of software. For example, port 80 is the port for Web servers, and port 25 is the port that is used to send e-mail. So,



© SANS Institute 2008, Author retains full rights.

all packets traversing the Internet are addressed to a network, computer, and port.

*Firewalls* separate one portion of a network from another and allows only authorized network traffic to pass back and forth. Reference the block diagram and identify the firewall located in between the outer or "public" segment of the network and the inner or "private" portion. Firewalls examine the packets that flow in and out of the network to make sure that they are legitimate, filter out suspicious packets, and hide the identities of computers within the private network to make it harder for criminal hackers to target individual computers

*Servers* are computers located on the network dedicated to storing data, sharing printers and handling one or more applications,. Servers do not support individuals utilizing them as workstations.

## Traditional Incident Handling Methodology

The NIST SP-800-61 [NIST] publication is perhaps the most authoritative reference for incident handling in the U.S. In this publication, the incident response process has several phases, from initial preparation through post-incident analysis. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are



© SANS Institute 2008, Author retains full rights.

implemented; furthermore, no control is foolproof. Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can act to mitigate the impact of the incident by containing it and ultimately recovering from it. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents. The major phases of this incident response process are: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity.

Incident response methodologies typically emphasize preparation – not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is so important that it is now considered a fundamental component of incident response programs. The incident response team's expertise should be valuable in establishing recommendations for securing systems.



© SANS Institute 2008, Author retains full rights.

These SP-800 procedures are well thought out, and well documented. The challenge they represent is that no small business has the technical capability, staff or funding to implement them. To address this issue, the following section will provide a recommendation for a scaled version.

## Modified Small Business Approach

This section makes several assumptions about the Small Business environment and the risk\cost tradeoff the owner is willing to make. The approach assumes we are addressing a small or micro business with a staff of a few up to 100 employees. It also assume the organization is too small to have a dedicated Information Technology (IT) staff, and probably relies on one or more "computer savvy" internal staff for support, or outsources those requirements to a local computer vendor or consultant.

Given the lack of IT staff, or the resources to implement a security or Incident Handling team, the approach recognizes the owner is willing to trade off speed of incident detection and arguably a lowered incident handling capability in return for a more realistic resource and staff costs. Given these tradeoffs, this approach moves much of the Small Business IH effort from being evenly distributed over the four steps of the NIST SP-800, to focus on the first step – Preparation. The efforts required in the remaining three steps will need to be outsourced to one or more members of a team defined by the small business owner prior to an incident. The following are considered the minimum essential steps of this scaled approach.



© SANS Institute 2008, Author retains full rights.

***Develop and Publish a Security Policy*** - A security policy sets guidelines that define an organization's approach to security. A policy differs from a plan in that a plan is a call to action, while a policy defines the goals of a plan.

The company security policy will actually be a collection of several different policies, which might include guidelines on employee Web and e-mail use, administrative access, and remote access.

Its important to remember a policy is useful only if it is enforced. The company should not create policies that are stricter or more complicated than they are willing to enforce. Also, a policy is not set in stone, but is a living document, and must be allowed to grow so that it can accommodate new threats, new technology, and new ways of thinking. Although each organization's security needs are unique, most security policies address a handful of common elements.

- Objectives: This section clearly states the reason the security policy exists.
- Scope: This section identifies the people and systems affected by the policy.
- Protected Assets: This section identifies the assets that the policy protects. Mail servers, databases, and websites are common business assets that need to be protected. Think of this section as an expanded discussion of the objectives.



© SANS Institute 2008, Author retains full rights.

- Responsibilities: This section of the policy identifies the groups or individuals responsible for implementing the conditions of the policy.
- Enforcement: This section of the policy discusses the consequences for violating the policy.

SANS has an excellent library of policy templates designed to get you up and running quickly.

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

Use these resources to develop company policies in at least the following areas:

- Appropriate Usage Policy: Outlines the overview of system ownership, expectation of privacy and proper usage.
- Information Protection Policy: Provides guidelines to users on the processing, storage, and transmission of sensitive information.
- Virus Protection Policy: Provides baseline requirements for the use of antivirus software as well as guidelines for reporting and containing virus infections.
- Password Policy: Provides guidelines for how user-level and system-level passwords are managed and changed.
- Firewall Security Policy. Describes, in general, how firewalls are configured and maintained, and by whom.
- Remote Access Policy: Outlines acceptable methods for remotely connecting to the internal network, such as whether



© SANS Institute 2008, Author retains full rights.

employees are allowed to connect to the network from their home computers.

After the policies are created, distributed, discussed, and signed, engage a local third-party computer support firm to implement an appropriate usage banner on the opening screen of all the company systems. While this step may seem unnecessary, it has proven critical when Human Resource issues arise down the road. A copy of a typical banner in located in the resource section at the back of the document.

***Protect Company Desktops and Laptops*** - If the company takes only three precautions to help safeguard the computers the business, make them the following:

- Configure company computer operating system and application software for automatic updating.
- Insure the company has virus protection software and automatic signature update subscriptions. Viruses do replicate, and copy themselves, and even send themselves to e-mail addresses in a contacts list. Virus-infected computers can spread the virus throughout the company and cause serious downtime and data loss. The company also risks infecting the computers of clients and customers they communicate with via e-mail.
- Enable individual computer firewall software.



© SANS Institute 2008, Author retains full rights.

***Keep Company Data Safe*** - Implementing a regular backup procedure is a simple way to help safeguard critical business data. Much of the misfortune that small businesses experience can be blamed on outside forces—a poor economy, a natural disaster, a decision by a key employee to leave. Those who survive the down times are typically those who minimized their risks by taking basic precautions. One of the most basic precautions of all is protecting critical business data.

Visualize walking into the office one morning and discovering that all sales records, customer contact information, and order history had disappeared. How long would it take to recover? How much disruption and delay would occur? What would it cost?

Data loss can and does happen. It can result from hardware failure, flood, fire, security breach, or just an accidental deletion of an important file. Whatever the cause, taking precautions to reduce the impact is like an insurance policy, enabling the business to get back up and running quickly.

Test backups frequently by actually restoring data to a test location. In this way, the company can:

- Ensure backup media and backed-up data are in good shape.
- Identify problems in the restoration process.
- Provide a level of confidence that will be useful during an actual crisis.

Periodically move a backup copy to an offsite location (owner's home, bank safe deposit box, etc.) to prevent a disaster from destroying the required recovery resource. It is far too



© SANS Institute 2008, Author retains full rights.

common to find the small business data backups stored next to the servers.

Encrypt sensitive data when it is outside the company. Encryption complements other access control methods and provides an added level of protection for securing data on computers that may be vulnerable to theft, such as mobile computers or files shared on a network.

***Use the Internet Safely*** - Unscrupulous websites, as well as pop-ups and animations, can be dangerous. Set rules about Internet usage to protect the business—and employees. The business must publish a policy on appropriate Internet usage. Though the Web can be an incredibly useful workplace tool, it can also cause significant workplace havoc that can result in lost productivity. Setting some rules protects the business and its employees.

Such a policy should address at least the following:

- Whether employees are allowed to browse the Web for personal use as well as business purposes
- When employees can use the Web for personal use (for example, lunch hours, after hours)
- If and how the company monitors Web use and what level of privacy employees can expect
- Web activity that is not allowed: Spell out unacceptable behavior in detail. In many companies this behavior includes activities such as:



© SANS Institute 2008, Author retains full rights.

- Offensive content downloads
- Threatening or violent behavior
- Commercial solicitations (non-business related)
- Other illegal activities

Beyond malicious activities instigated by outsiders, businesses can be put in a vulnerable position by employees who engage in illegal or undesirable Web activity during work hours and from company-owned computers.

***Protect the Company Network*** – The small business owner must develop a mental "Defense-in-Depth" mindset to mitigate the lack of IT staff present. The owner must understand the depth of the today's threat, and periodically re-evaluate possible threat vectors and results against their network.

For example, remote access to a network may be a business necessity, but it is also a security risk that needs to be monitored closely. Using strong passwords and be especially cautious about wireless networks. Nobody likes to think the worst—that around every corner someone is snooping into company business affairs. However, if a company operates a network and has information that should remain confidential, a little paranoia will serve well.

*Set up firewalls* – Use a computer support firm to configure a firewall for the firm. A firewall controls access to and from the network or computer, blocking intruders from accessing a private network and controlling what employees can access outside



© SANS Institute 2008, Author retains full rights.

the network. Perimeter firewalls protect all the computers on the network. They also offer an additional layer of defense because they can effectively make all network computers "invisible" to the outside world.

*Use strong passwords* - most small businesses use passwords to authenticate identity, whether on computers, cash registers, or alarm systems. Although more sophisticated authentication systems exist, such as smart cards and fingerprint or iris scans, passwords are most common because they are easy to use. Unfortunately, they are also easily misused. Hackers have automated tools that help them crack simple passwords in minutes. Crooks may also use social engineering to get employees to divulge passwords. Educating staff about the importance of passwords is the first step in making passwords a valuable network security tool. Employees should regard their passwords the same way they would an office key. Employees should avoid weak and easy-to-guess passwords that include

- Their real name, username, or company name
- A common dictionary word that makes them vulnerable to "dictionary attacks," in which a program attempts to use words found in a dictionary to log on to a system
- Common passwords, such as "password," "admin," "letmein," or "1234"
- Commonly known letter substitutions, such as replacing "i" with "!" or "s" with "$"
- A password that someone else knows



© SANS Institute 2008, Author retains full rights.

- Using no password at all, which makes it easy for other employees to just walk up to an unsecured computer and log on
- Any password that they write down

*Use Wireless Security Features* - Wireless networks use a radio link instead of cables to connect computers. As a result, anyone within radio range can theoretically listen in or transmit data on the network. Freely available tools allow intruders to "sniff" for insecure networks. Security features are built into Wi-Fi products, but manufacturers often turn the features off by default to make network setup easier. If the company uses wireless networking, make sure the computer vendor turns the security features on and uses the security and access features that will make the network more secure. Also consider these tips:

- Restrict wireless access to office hours or whenever staff expects to use the network.
- Filter out casual intruders by setting access points to restrict network access to specific computers.
- Use the encryption built into the wireless access point to encode information as it travels across the network and prevent any non-authorized party from reading or changing data.

*Close unnecessary network ports* - Network traffic for various applications are identified using numbered ports. In order for an application's traffic to get through a firewall, the firewall must allow traffic on that port. To strengthen the



© SANS Institute 2008, Author retains full rights.

network's security against unauthorized access, have the computer support firm close unused or unnecessary ports by using perimeter firewalls, with a default "Deny All" approach.

*Protect Company Servers* – Company servers hold the organization-critical information and capability, and it is easy to understand why keeping them safe from attack is mission-critical. When servers are compromised, the entire network and organization is at risk. While some server attacks are merely annoying, others can cause serious damage. In a small business, there may not be more than one or two servers, but no matter how few or how many servers the business is running, the network relies on them. They serve the applications, Web pages, or e-mail the team needs to do their jobs. They store valuable and confidential information resources. They provide a means for customers to communicate with, or perhaps even purchase goods or services from the company. When the servers are down, the company loses productivity, and jeopardizes customer relationships to the point of taking an economic hit.

*Keep servers in a safe place* - Businesses must make sure that servers are not vulnerable to physical calamities. Locate these machines in a locked, well-ventilated room, not in a hallway or under a desk. Servers should never be used as workstations, and server rooms should have no windows and a single door that can be locked. Server cases should also be locked to prevent tampering with internal components. Know which employees have keys to the server room. Keep a record of the serial numbers of servers and mark the machines with company



© SANS Institute 2008, Author retains full rights.

information so that they can be identified and recovered if stolen.

*Practice least privilege* - The principle of least privilege dictates that users should be given only the permissions they need to do their jobs, but no more permissions than that. Rather than giving users Administrator access, provide user access to specific programs only and to define which user privileges are allowed on the server. This ensures that users cannot make changes in areas that are critical to server or workstation operation. It also prevents users from installing software that may introduce a virus or spyware to their computers, which in turn can compromise the integrity of the entire network.

*Understand security options* - Today's server operating systems are more secure than ever, but the powerful security settings found in products are good only if they are used appropriately and monitored aggressively. Consider hiring an outside consultant to help appropriately protect company servers.

***Secure Line-of-Business Applications*** - Make sure that software critical to the business operations is fully secure. Internal and external vulnerabilities can lead to lost productivity—or worse. Many companies rely on specialized business programs for accounting tasks, running point-of-sale systems, tracking inventory, and managing supply chains. These programs—sometimes dubbed line-of-business (LOB) applications—typically run on a server and operate in conjunction with a



© SANS Institute 2008, Author retains full rights.

database. This integrated setup offers great advantages. Multiple employees can work with an LOB program and access the database information—all at the same time. However, there are also security risks to such setups. Customer information, sales figures, profit and loss statements, and other vital business data located on a network server are vulnerable to intruders. Moreover, the company may not want all employees to have access to all kinds of data. The challenge is to create a security plan that protects LOB program data integrity and privacy, yet also supports efficient data access and collaboration.

***Training*** – The previous steps discussed need to be complemented by an environment where the employees of the small business have been trained in security awareness. Assuming the previous steps have been taken, the weakest link in the security chain will be the human one. While security certainly can never be the 100% topic of discussion in a company, periodic refreshers about the dangers of social engineering, dumpster diving, physical security and password safeguarding need to be made part of the company culture.

## Specific Next Steps

After this discussion, and the focus on NIST Step 1 – Preparation, it is reasonable to ask "What Next?" The following critical steps must be reviewed by the small business owner and remediation taken wherever there is a current deficiency.



© SANS Institute 2008, Author retains full rights.

1. Use the SANS templates and create a company security policy with specific appropriate usage statements. Have all employees read, understand, and sign a copy of the policy.
2. Have a member of staff inventory the major components of the company computer systems and create a spreadsheet with manufacturer, model number and serial numbers. Confine this list to major computer components and do not try to track keyboards, mice, etc. Consider attaching a company asset tag to all tracked equipment. Purchase cables, locks, and encryption software for all company laptops.
3. Have the third-party computer support company you selected implement a warning banner on all systems.
4. Have the same support company configure all desktops and servers for automatic software updates, and review the anti-virus software to be sure the systems are downloading signature updates.
5. Retain a different third-party computer support company to install and configure a perimeter firewall with a default "deny all" ruleset. The concept behind involving a second firm, and utilizing the company accountant in these steps, is to help assure that no single entity might compromise the company security. Have this firm create a high-level block diagram of the company's network, with key network addresses and ISP information. This diagram will prove invaluable



© SANS Institute 2008, Author retains full rights.

in discussions with other firms or troubleshooting during an incident. The nature of this network information means it must be well secured.

6. Have the third-party company that installed the firewall demonstrate to you how to physically disconnect the network from the Internet, and be sure the required cables are labeled so they be easily located during an incident.
7. Have your company accountant confirm that data backups are occurring and have them conduct a test restore of some data. Also ask they confirm that copies of backup tapes are periodically moved offsite.
8. Review with employees the policies on appropriate usage of the Internet and what constitutes allowable and disallowed Internet usage.
9. Physically inspect where the company has servers located and assure they are physically safeguarded in a locked area. Have the third-party support company configure the servers to enforce company password policy in terms of strong passwords and password change interval.
10. Have the third-party company that installed the firewall review any wireless access points and be sure that encryption is being used and that default passwords and IDs have been changed.



© SANS Institute 2008, Author retains full rights.

11. Review with your company accountant the status of key application software in terms of correct versions, physical safeguarding of original discs and support subscriptions.
12. Develop a simple tracking document or spreadsheet to show the security training provided to employees.

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2008, Author retains full rights.

## *Incident Handling Steps for the Small Business*

**Step 1 - Preparation**

1. **Create a company security policy**
2. **Inventory major components of the company computer system**
3. **Implement a warning banner on all systems.**
4. **Configure all desktops and servers for automatic software upgrades**
5. **Install and configure a perimeter firewall with a default "deny all" ruleset.**
6. **Create a block diagram of the company's network**
7. **Know how to disconnect the network from the Internet during an incident.**
8. **Confirm that data backups are occurring**
9. **Brief staff on appropriate usage of the Internet**
10. **Inspect server location**
11. **Review any wireless access points**
12. **Review key application software**
13. **Track security training provided to employees.**

**Step 2 - Detection and Analysis of an incident.**
The first warning to the small business will come in the form of malfunctioning computers. Staff will complain of unusual slowness of the computers, a defaced web site, pop-ups occurring on the computers, or unusual messages on desktops or servers. When this occurs, the owner must be notified and he or she moves to Step 3 in the process.

**Step 3 - Containment, Eradication, and Recovery**
The owner will need to make the first assessment of this step. They are making the decision to either pull the physical connection to the Internet or allow the connection to remain in place. Once that disconnect decision is made, the containment and eradication will involve a local computer support company.

**Step 4 - Post Activity**
Review of lessons learned - an extremely valuable piece of the process. After containment and eradication is completed, the owner meets with senior staff, trusted advisors and the computer support vendor(s) to review possible vulnerabilities or recommend new steps to be implemented.



© SANS Institute 2008, Author retains full rights.

## The Final Steps of Incident Handling

In order to scale the NIST procedures for the small business, the concentration has been on preparation and prevention, which this author strongly believes is in the best interest of the small business owner. However, that belies the fact that an incident will occur at some point in the history of the business. What is the recommendation to the owner for the steps when that occurs?

Step 2 in the NIST strategy is the Detection and Analysis of an incident. By definition of our small business organization, they will not have elaborate Intrusion Detection tools in place to detect security incidents. The first warning to the small business will come in the form of malfunctioning computers. Staff will complain of unusual slowness of the computers, pop-ups occurring on the computers, or unusual messages on desktops or servers. Customers may also call in about a defaced web site. When this occurs, the owner must be immediately notified, and he or she moves to Step 3 in the process.

Step 3 is the Containment, Eradication, and Recovery of the incident. In the Small Business, this step will need the involvement of both the owner and the previously identified computer support company. The speed and asynchronous nature of an incident, coupled with no internal IT staff, means the owner will need to make the first assessment of this step without the benefit of technical help. He or she must make an instinctive call about the relative risk to the company of an intruder having control of their computer systems. They are making the decision



© SANS Institute 2008, Author retains full rights.

to either pull the physical connection to the Internet or allow the connection to remain in place. If they pull the connection, no further threat from the outside exists, but their employees have lost email and the Internet and customers have lost access. If they leave the connection in place while troubleshooting, they retain some capability while risking further intrusion. This is not an easy decision, and it requires the owner to talk to senior staff and trusted advisors to make this decision before any future occurrence. Once that disconnect decision is made, the containment and eradication will involve a local computer support company. Their staff can review firewall logs, initiate virus scans and if necessary rebuild complete systems. This process will be time consuming, expensive, and certainly frustrating … prevention is far better than the cure.

Step 4 - Post Activity is the review of lessons learned, and is an extremely valuable piece of the process. After containment and eradication is completed, the owner should meet with senior staff, trusted advisors and the computer support vendor(s) to review possible vulnerabilities or recommend new steps to be implemented.

## Areas for Future Research

The small size of these organizations, dictates they are unlikely to ever afford full-time Information Security staff. This provides one possible area of future investigation into small "appliance-type" automated hardware solutions that implement all of the referenced policies, and are based on a



© SANS Institute 2008, Author retains full rights.

heuristic technology that will recognize intrusion attempts, thwart such activity and notify the small business owner. While it is doubtful such technology would be 100% effective, a small, automated solution of this nature would provide much of U.S. small business with sorely needed improvement in their security posture.

Another possible solution is the emergence of managed security services with offerings focused on the small business market. If such services were readily available, and perceived as affordable, they would represent viable alternatives in this arena.

## Conclusion

After review and discussion with small business owners, a reasonable solution has been created for scaling the NIST Incident Handling framework down to the range required. The critical element is a full understanding by the small business owner that he or she is accepting a certain degree of risk in return for not expending the funds for full-time IT security staff and an Incident Handling Team. It is also incumbent on them to review the computer service providers in their area and establish a relationship prior to an incident and an on-call service when an incident is detected.



© SANS Institute 2008, Author retains full rights.

## Resources & Tools

Training and Security Policy Templates

SANS Policy Project: http://www.sans.org/resources/policies/

SANS Training: http://www.sans.org/sans_training.php

SANS Operational Checklists

http://www.sans.org/score/checklists.php

Microsoft Security Guide for Small Business

http://download.microsoft.com/download/3/a/2/3a208c3c-f355-43ce-bab4-890db26
7899b/Security_Guide_for_Small_Business.pdf

Microsoft Rootkit detection tool

http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx

Anti-Virus Resources

Norton AntiVirus: www.symantec.com/smallbiz/nav/

McAfee VirusScan: www.mcafee.com/

Microsoft Malicious Software Removal Tool: visit www.microsoft.com/downloads/ and type “Malicious Software Removal Tool” into the Search box



© SANS Institute 2008, Author retains full rights.

Banner Text Sample

| |
|---|
| This is an Acme Computer System. This computer system, including all related equipment, networks and network devices including Internet access, are provided only for authorized Acme use. Acme computer systems may be monitored for all lawful purposes, including: ensuring that their use is authorized, management of the system, to facilitate protection against unauthorized use, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized Acme entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this Acme system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution, and evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring. |

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2008, Author retains full rights.

## References

Carnegie Mellon University Software Engineering Institute. (2005) . *CERT® /CC Statistics 1988-2005.*

Government Accountability Office. (2007) . *Cybercrime - Public and Private Entities Face Challenges in Addressing Cyber Threats* (GAO publication No. GAO-07-705)

Federal Bureau of Investigation. (2006) . *FBI, Internet Crime Complaint Center 2006 Internet Fraud Crime Report.*

Klomp, J.M. (2001) Security problems for small companies. *SANS Institute 2001, November 6, 2001.*

National Institute of Standards and Technology. (2008) . *Computer Security Incident Handling Guide.* (NIST publication 800-61 Revision 1)

SANS. (2008) . Templates. Retrieved October 4, 2008, from: http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

Small Business Administration. (2008) . *Small Business Size Standards*. Retrieved November 1, 2008, from: http://www.sba.gov/services/contractingopportunities/sizestandardstopics/size/index.html

*Wikipedia: The free encyclopedia*. (2004, July 22). FL: Wikimedia Foundation, Inc. Retrieved October 11, 2008, from http://en.wikipedia.org/wiki/Small_business



© SANS Institute 2008, Author retains full rights.

Last Updated: May 20th, 2013

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| SANS Malaysia @ MCMC 2013 | Cyberjaya, MY | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| SANS Pen Test Berlin 2013 | Berlin, DE | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| Industial Control Systems Security Training - Houston | Houston, TXUS | Jun 10, 2013 - Jun 15, 2013 | Live Event |
| Security Impact of IPv6 Summit 2013 | Washington, DCUS | Jun 14, 2013 - Jun 16, 2013 | Live Event |
| SANSFIRE 2013 | Washington, DCUS | Jun 14, 2013 - Jun 22, 2013 | Live Event |
| SANS Canberra 2013 | Canberra, AU | Jul 01, 2013 - Jul 13, 2013 | Live Event |
| 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 |
| SANS Mumbai 2013 | Mumbai, IN | Jul 22, 2013 - Jul 27, 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 San Francisco 2013 | San Francisco, CAUS | Jul 29, 2013 - Aug 03, 2013 | Live Event |
| SANS SEC 560: Network Penetration Testing @ Bangalore 2013 | Bangalore, IN | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| SANS Boston 2013 | Boston, MAUS | 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 Thailand 2013 | Bangkok, TH | Aug 19, 2013 - Aug 31, 2013 | Live Event |
| SANS Virginia Beach 2013 | Virginia Beach, VAUS | Aug 19, 2013 - Aug 30, 2013 | Live Event |
| Mobile Device Security Summit 2013 | OnlineCAUS | May 30, 2013 - Jun 06, 2013 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |