INTERNET SECURITY ALLIANCE

Common Sense Guide to Cyber Security for Small Businesses

Recommended Actions for Information Security
1st Edition – March 2004

Internet Security Alliance Officers

Dr. Bill Hancock, Chairman, ISAlliance and Senior Vice President for Security, Cable & Wireless

Doug Goodall, Vice Chairman, ISAlliance and CEO, RedSiren Technologies

John Shaughnessy, Vice Chairman, ISAlliance and Senior Vice President Visa, U.S.A.

Yoram Maliniak, Secretary and Treasurer, ISAlliance and Director, Knowledge Management & Information Security, Raytheon

Dave McCurdy, Executive Director, ISAlliance and President, Electronic Industries Alliance

Rich Pethia, Director, CERT Coordination Center, Carnegie Mellon University

Internet Security Alliance Sponsors and Members

American International Group (AIG)
Automatic Data Processing
Boeing Company
Cable & Wireless
Ceridian
Coca Cola Company
Equant
Federal Express
Frank Russell Company
Harris Corporation
Intuit
Mellon Financial Corporation
Mitsubishi
National Association of Manufacturers (NAM)
NEC
Nortel Networks
Northrop Grumman
Qualcomm
Raytheon Company
Red Siren
Sony Corporation
Symantec
TATA Consulting Services
VeriSign, Inc.
Verizon
Visa, U.S.A.

Authors

Carol Woody, Carnegie Mellon University
Larry Clinton, Internet Security Alliance

Best Practices – A Twelve Step Program to Cyber Security

A. Introduction

1. I'm Very Busy; Do I Really Need to Read This?
2. Real World Examples---This Could Happen To You
3. Does This Publication Apply to My Specific Business?
4. Why Would Anyone Attack Me?
5. OK, Maybe I Should Do More, but What is This Going to Cost Me?
6. How Can I stay Updated on What I Should be Doing to Secure My Business?

B. Specific Practices and the Dirty Dozen Examples of Actual Small Businesses Hurt by Cyber Attacks

1. **Use Strong Passwords and Change Them Regularly**
   Case One: Ex-Employee at Building Contractor Uses Old E-Mail Access to Spy for Competitive Attack

2. **Look Out for E-mail Attachments and Internet Download Modules**
   Case Two: MyDoom Worm Hits Thousands of Small Businesses Hard

3. **Install, Maintain, and Apply Anti-Virus Programs**
   Case Three: Consultant Fails to Keep Software Updated, Winds up Infecting and Losing His Customers

4. **Install and Use a Firewall**
   Case Four: Hotels and Wireless Internet Connections Need Firewalls

5. **Remove Unused Software and User Accounts; Cleanout Everything on Replaced Equipment**
   Case Five: Small Telecom Firm Loses Business When Security Breach Is Made Known to Prospective Clients

6. **Establish Physical Access Controls for all Computer Equipment**
   Case Six: Accounting Firm Has Backups Threatened by Fire

7. **Create Backups for Important Files, Folders, and Software**
   Case Seven: Small Manufacturer Loses Major Government Work Due to Software "Time Bomb"

8. **Keep Current with Software Updates**
   Case Eight: Diners Have Supply Chain Interrupted; Inn Loses Reservation System when Software Not Updated

9. **Implement Network Security with Access Control**
   Case Nine: Cyber Blackmail Goes Mainstream

10. **Limit Access to Sensitive and Confidential Data**
    Case Ten: Credit Union Employee Uses Personal Information for Financial Gain

11. **Establish and Follow a Security Financial Risk Management Plan; Maintain Adequate Insurance Coverage**
    Case Eleven: On-Line Retailer Misunderstands Insurance Coverage, Gets Wiped Out by Attack

12. **Get Technical Expertise and Outside Help When You Need It**
    Case Twelve: Venture Capitol Firm, Law Firm Try to Get by Without Tech Assistance -- Regret Decision

C. References/Sources

D. Contributors

INTRODUCTION

I'm Very Busy; Do I Really Need to Read This?

Yes. Many small and medium-sized businesses are under the mistaken impression that their size, or the minimal security steps they have already taken, will protect them from cyber attacks. This assumption is both inaccurate and dangerous.

Attacks on information systems operated by small and mid-sized companies are growing rapidly and having severe impacts on business operations. One survey showed that about **one out of every three small businesses** was affected by the recent "MyDoom" virus. That is **twice** the proportion of large enterprises that were hit by the same virus.

Widespread anonymous attacks with colorful names like "Code Red," "Blaster," and "So Big" have generated increasing publicity as their negative effects on all types of business have grown. Insurance estimates show that as late as 1996 the amount of money that business lost to cyber events was perhaps less than a billion dollars a year. Current estimates put business losses as high as several **billions of dollars each week** to various forms of cyber attacks.

Obviously, larger firms have more to lose in terms of absolute dollars. However, the narrower profit margins under which smaller businesses typically operate make it all the more important that they become pro-active in protecting their information systems. Think of what would happen if your business computer data were not backed up on a regular basis. How badly would the loss of your business computers affect your ability to conduct normal business?

How much would it cost to repair?
How much data would be lost beyond replacement?
How much would this data loss cost your company?
Can you afford this kind of down time and inconvenience?

Real World Examples --This Could Happen to You

Thanks to a series of computer attacks a company once valued at $1million dollars is now selling off its customer lists. "My business is gone. M y wife's business is gone. Now I just hope we can hang on to our house," says the disgruntled former owner

As quoted in Computer World Magazine. Fuller description of this case is provided with Best Practice #11.

This booklet contains examples of many different types of small and medium-sized businesses that have been harmed significantly by various cyber attacks. Not all the damage was as severe as the example above. In fact some companies were able to defend themselves very well. However, these are not hypothetical cases. They are stories of actual small companies that were reported in the media, listed on the FBI Website, or reported directly to the Internet Security Alliance during the research that led to the writing of this publication.

Although the examples are spread throughout the book, they do not apply directly to each specific suggested practice. Computer attacks do not work that way. Often an attack can be the result of a combination of faults. What is striking is the range of businesses nationwide that have been hit. These examples include small manufacturers, building contractors, credit unions, hotels, diners/restaurants, coach and limo services, trucking companies and a range of professionals and consultants including law firms, accountants, and venture capitalists.

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.

Does This Publication Apply to My Specific Business?

One likely reason that smaller enterprises are being hurt by such a dramatically higher percentage than larger firms is that many larger companies, with greater economies of scale, are making systematic attempts to manage the risk to their information systems. For this they use large information technology departments that small businesses cannot afford.

This document is intended to be read by non-technical managers at companies which have more than a single computer, but which lack a sophisticated in-house information technology department.

Sole proprietorships, with just a single computer, might be best served by referring to the ISAlliance *Common Sense Guide for Home and Individual Users*. That document offers fairly extensive advice targeted to very small operations.

The ISAlliance *Common Sense Guide for Senior Managers* is designed for companies which do have a sophisticated in-house information technology department. All of these documents are available free of charge at the ISAlliance Website (www.isalliance.org).

The number of employees and annual revenues is not really the best criteria for distinguishing the target audience for this *Guide for Small Businesses* versus the *Guide for Senior Managers*. A construction company, for example, might have a large number of employees and large annual revenues, but only a small head office with one person working part-time to keep the computer network up and running. The *Guide for Senior Managers* might be overkill for such a company. By contrast, a small bank, with fewer employees and lower annual revenues than this hypothetical construction company, would surely want to use the *Guide for Senior Managers*, either on its own or in conjunction with this current *Guide for Small Businesses,* due to the complex statutory legal and regulatory environment associated with the banking industry.

Why Would Anyone Attack Me?

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.

This guide provides a simple and easy-to-understand road map towards cyber security. We encourage you to read this, act upon it, and protect your business and others. Do not be one of the losers in terms of time and money. Be proactive rather than reactive.

OK. Maybe I Should Do More, But How Much Is It Going to Cost Me?

In December 2003, the US Department of Homeland Security in coordination with private industry held the first National Cyber Security Summit. At this event the Internet Security Alliance was asked to produce this publication, *A Common Sense Guide to Cyber Security,* a best practices publication specifically targeted to small businesses.

Rather than basing its work on its past writings, the ISAlliance instead initiated a series of focus groups in coordination with the US Chamber of Commerce, the National Association of Manufacturers, the National Federation of Independent Businesses, and the Electronic Industries Alliance. Nearly 100 small businesses became involved in the development of this publication, helping to guide it toward the specific needs of the small business community.

Cost, both in terms of time and money, was the dominant theme of these discussions.

As a result, this publication attempts to not only suggest appropriate steps to be taken, but also addresses the issues of time, money, and technical skill required, as well as the consequences of not adopting best practices. Moreover, each suggestion breaks down the implementation of the suggested practice, explaining how to get started and what additional steps are required.

Each small business needs a security plan as much as it needs a marketing plan. You should immediately check the security component of your IT budget. Have you budgeted adequately for all 12 practices? If not, then it's time to add in the missing elements. On an annual basis, your costs may be heavily software-driven for maintenance and upgrades. On a longer-run, systems acquisition basis, necessary security features need to be budgeted up front in both hardware and software terms. While we realistically understand that improved security may come in stages, the goal of this publication is to bring you through *all* the stages. It is in the best interest of your business to follow them completely.

How Can I stay Updated on What I Should be Doing to Secure My Business?

The ISAlliance is a collaborative effort among Carnegie Mellon University's Software Engineering Institute (SEI); its CERT® Coordination Center (CERT®/CC); the Electronic Industries Alliance (EIA), a federation of trade associations; and private and public member corporations. The ISAlliance mission has always been clearly defined: To use the collective experience of the members of the Internet Security Alliance to promote sound information security practices, policies, and technologies that enhance the security of the Internet and global information systems.

We have not given specific vendor recommendations, as this is really beyond the scope of the ISAlliance mission. We recommend that you use anti-virus programs, for example, but we don't recommend any particular vendor of such programs. Some of these vendors may do a better job than others. The trade press publishes frequent reviews of the various products available—perhaps these will help your computer person decide on which product to use. Or your computer person could perform an in-house evaluation of the various products available.

We have tried to stick to generalities that will stand the test of time, so that this document doesn't become immediately dated, while at the same time trying to be as up-to-date as possible.

Finally, we encourage small businesses to join the ISAlliance. Associate membership in the ISAlliance is specifically designed and priced for small businesses. Membership entitles your company to updated information about current and emerging threats and vulnerabilities that may affect your system as well as a range of discount programs intended to make cyber security more affordable. You can get more information on membership at www.isalliance.org.

Practice 1 Use Strong Passwords and Change Them Regularly

Cost: Minimal - No additional investment

Technology skill level: Low to medium

Participants: Everyone using the electronic facilities

Why do it?
Passwords are an easily implemented method of limiting access to your electronic work environment. Passwords that are harder to discover will discourage many kinds of intruders. Smaller businesses often have higher employee turnover rates, which increase the need to change the passwords regularly. Since you may not know if a password has been guessed, change it at least every six months and preferably every three months, and do not allow reuse of old passwords.

For each computer and service you use (online purchasing, for example), you should have a unique password. By not reusing a password a compromise in one area will not open access to other areas. You should not write passwords down or share them with anyone. But if you do need to write them down, store the paper in a secure location such as a locked file cabinet (not under your keyboard where anyone can find them).

Every user of the computer system should have a unique account and be responsible for controlling their password. This provides a means of directly linking actions on the network to a specific individual.

Poor Passwords Give a False Sense of Security
Without limited access, all contents of a networked device can be seen, changed, and destroyed by anyone with network access. If your network is connected to the Internet (and very few are not these days) your information may be accessed from anywhere in the world.

Even with passwords, protection is limited. Computer intruders use trial-and-error, or brute force techniques, to discover passwords. By bombarding a login program with all the words in a dictionary (which takes only a few minutes), they may "discover" the password. If they know something about you, such as your spouse's name, the kind of car you drive, or your interests, clever intruders can narrow the range of possible passwords and try those first. They are often successful. Even slight variations, such as adding a digit onto the end of a word or replacing the letter o (oh) with the digit 0 (zero), will not protect passwords from discovery (e.g., 24THErd).

Getting Started
A password should be complicated so it cannot be easily guessed. Do not use dictionary words, names, or minor variations of these. Consider using a combination of letters, both upper and lowercase, numbers, and punctuation marks. Lengths can vary (a minimum of six characters; longer is better). Construct the password using a pattern so that you can remember it whenever you need it without having to write it down to jog your memory.

Educate employees to always change default passwords and initial access passwords as soon as possible. Policies should be established to require strong passwords and mandate a frequency of change. Employees should be educated about the need for strong passwords as soon as they are hired and reminded to change them regularly.

Additional Steps
Set up the electronic environment to require strong passwords by mandating length and structure complexity. Automatically expire passwords to enforce a frequency of change policy.

- **Case One**

Ex-Employee Uses Old E-Mail Access to Spy for Competitive Advantage

A California man pleaded guilty to illegally accessing the computer system of his former employer and reading e-mail messages of company executives for the purpose of gaining commercial advantage at his new job with a competitor.

The guilty party had been an employee at a contractor in Chino, California. After leaving one firm to go to work for a competitor, he used his Internet access to his former employer's office to gain access to computer systems on more than 20 occasions. He read e-mail messages of his former employer's executives to gain knowledge of their business opportunities and provided this information to his new employer seeking a competitive advantage. The original employer lost thousands of dollars in business before the FBI was able to stop the illegal activity.

Source: *US Department of Justice, September 2002*

Practice 2 Look Out for E-Mail Attachments and Internet Download Modules

Cost: Minimal - No additional investment

Technology skill level: Low to medium

Participants: Everyone using the electronic facilities

Why should I be careful?
One of the most common methods of transferring computer viruses is by embedding them in attachments that accompany e-mails or materials downloaded from attractive websites. Recently, attackers have become adept at capturing address books and embedding viruses in attachments that appear to come from people you know. Companies should have strict policies about what can and cannot be downloaded or opened on their systems.

You share important information via e-mail and attachments allow us to send reports, copies of files, spreadsheets, photos, cartoons, music, etc. You update and expand the software on computers using sources on the Internet and vendors encourage this practice by passing on some of their delivery savings if we use this mechanism. Website designers take advantage of built-in capabilities to check your machine to make sure you have the needed software tools to access their content, and if anything is missing they automatically arrange for the installation for you. All of this is quick, easy, and saves you from dealing with a lot of technology mumbo-jumbo.

Anyone who writes a software program can distribute it on the Internet through the Web or by sending you a copy attached to e-mail. You are at the mercy of the program author when running it on your computer. Any task that you can do on your computer, this program can also do. If you delete a file, send e-mail, or add or remove a program, your newly installed program can do this too. And an intruder can do these tasks, unbeknownst to you, through the program you have just installed and run.

What Happens if I Am Not Careful?
E-mail text, e-mail attachments, and download modules are excellent conduits for malicious code. By opening an e-mail attachment or accepting a downloading install option, the code is copied into your technology environment (sometimes in temporary files that you cannot easily see) and can attack your system through vulnerabilities (see Practice 8).

Malicious code that lodges in your computer will usually attempt to spread itself to other computers using e-mail attachments. If your computer is compromised, everyone in your electronic address book will receive e-mail from you with an attachment that can attack his or her system. The volume of e-mail alone can strangle a network to a halt. In addition, the malicious code can corrupt and delete files and software running on your system.

If you do not take steps to prevent it, software to spy on your Internet usage will be loaded on your computer to track the websites you use and report on web-accessed accounts. Key tracking software to intercept, store, and transmit the sequences of key types for accounts and passwords can also be installed on your machines.

Getting Started
Educate all e-mail users to do the following:
1. Do not use the "preview" function for e-mail contents.
2. Do not open an attachment that the anti-virus software has indicated is malicious (see Practice 3)
3. Do not open e-mails (delete them instead) from someone you do not know, especially if the subject line:
    - Is blank or contains strings of letters and numbers that are nonsense
    - Tells you of winning a contest you never entered or money you should claim
    - Describes the details of a product that you might like
    - Notifies you of a problem with instructions to install software on your machine
    - Notifies you of a billing or account error for a service you do not use.
4. If you know the sender or decide to open the e-mail, check to make sure the contents along with the names of attachments and the subject line make sense.

Additional Steps
Set up your browser to alert you to Internet module downloading and do not accept them from sites you do not know, especially if e-mail from an unknown recipient has sent you to the site.

Delete and do not forward chain e-mails (similar to chain letters) and do not use the unsubscribe function for services to which you did not subscribe initially since this only alerts an attacker that a active address has been located and makes you a more valuable target.

Deactivate the use of java scripting and Active-X in your browser and only activate them temporarily for specific web pages.

When you are considering buying a software program, look for a clear description of the program and its features and make sure the source of this information is reputable.

- **Case Two**

MyDoom Worm Hits Thousands of Small Businesses Hard

The MyDoom e-mail worm and its variants spread rapidly, accounting for 30% of all e-mail traffic at its peak in early February 2004. The worm arrived as a well-disguised e-mail attachment, which, if opened, could install a backdoor that would allow unauthorized access to an affected computer, which might be utilized in a variety of harmful ways in the future. Research shows nearly 1 in 3 small businesses have been affected by MyDoom and 1 in 6 larger enterprises. In addition, MyDoom can spread through popular file sharing networks such as Kazaa. Total cost to business from the effects of MyDoom already run into several billion dollars and are still climbing.

Source: *BBC, March 2004*

Practice 3 Install, Maintain, and Apply Anti-Virus Programs

Cost: Low – Site licenses are available

Technology skill level: Low to medium depending on selected approach

Participants: Everyone using the electronic facilities

Why do it?
Anti-virus programs are a low-cost means of protecting your systems and information from external threats. Viruses (malicious code embedded in files) exploit vulnerabilities within the technology environment, and the number of identified vulnerabilities has doubled annually since reporting was initiated in 1988. Vulnerabilities exist in every aspect of the hardware and software available in today's marketplace. The most widely publicized viruses are transmitted via e-mail attachments, and infection is initiated when they are opened (see Practice 2).

Viruses can infect a computer in many ways: through floppy disks, CDs, e-mail, websites, and downloaded files. When you insert a floppy disk, receive e-mail, or download a file, you need to check for viruses.

Anti-virus (AV) programs look at the contents of each file, searching for specific characters that match a profile or pattern--called a virus signature--known to be harmful. For each file that matches a signature, an AV program typically provides several options, such as removing the offending pattern or destroying the file or e-mail attachment that contains the virus. When AV program vendors learn about a new virus, they provide an updated set of virus signatures which must be loaded onto each machine to catch new problems. Automatic update options can be activated for individual machines.

What Happens without Anti-Virus Protection
Intruders have the most success attacking any computer when they use viruses as the means for gaining access. Installing an AV program and keeping it up-to-date are among the best defenses. When a machine is infected, software can be disabled and data destroyed, and the affected machine will attempt to infect other machines, consuming available communication bandwidth, choking networks, and overloading servers. Protection is needed at each machine.

Getting Started
Install anti-virus software on every machine and keep the signature files current through automatic or manual updates at least weekly. Renew the automatic update capability annually as required to maintain a current virus signature file on every machine.

DO NOT connect to the Internet without first activating an AV program.

Educate all computer users to remove or destroy infected files identified by the AV software. Make sure they know how to remove their machine from the network and who to call for help if they suspect an infection.

Educate all e-mail users not to open e-mail attachments from unexpected and unknown sources (see Practice 2) to avoid unleashing a new virus not yet blocked by the AV program.

Additional Steps
Enable the AV program to automatically check every file source on each machine when it is used (CD, floppy, etc.).

Require periodic AV examinations of all files on a regular basis, preferably weekly, to catch problems missed at other checkpoints.

- **Case Three**

Consultant Fails to Keep Software Updated; Winds up Infecting, and Losing, His Customers

A New Jersey utility consultant operating as a sole practitioner bought a new computer to better manage his growing business. The salesperson told him the new computer came with anti-virus applications already installed. Unfortunately, the consultant did not realize he needed to update this protection on a regular basis. Without the new virus definitions, his system became infected. His address book was used to spread viruses to his customers through bogus e-mails, resulting in several of his clients terminating their business relationship with him.

Source: *Reported to Internet Security Alliance while researching this booklet, February, 2004*

Practice 4 Install and Use a Firewall

Cost: Moderate – Software is free but effective tuning takes time

Technology skill level: Moderate to High depending on selected approach

Participants: Technical support

Why do it?
A firewall performs much the same job as a security guard at a public building. It examines the messages coming into your system from the Internet as well as the messages you send out. The firewall determines if these messages should continue on to their destination or be stopped. The firewall "guard" can greatly reduce the volume of unwanted and malicious messages allowed into your network, but it takes time and effort to set one up and maintain it. Firewalls can also prevent many forms of undesirable access to your network.

The hard part is defining the rules--what is allowed to enter and exit your system. If you let nothing in and nothing out (*deny-all* firewall strategy), communication with the Internet is effectively disconnected. Since that is not practical for most small businesses, additional work is required. Some firewall products let you easily review each information message (packet) so that you can decide what to do with it. When you are shopping for a firewall, look for this review feature because it can be quite helpful. Practically speaking, it is not easy to decide which traffic is acceptable and which is not. Get technical assistance (see Practice 12) to help you identify normal usage for your organization and establish rules to block all other network traffic.

Firewalls can also be used to enforce an acceptable use policy by blocking content access to websites considered inappropriate by the business, such as pornography and gambling.

What Happens without a Firewall?
With nothing in place to check information coming into and out of your network, you are totally reliant on each individual user to practice good e-mail and download habits (see Practice 2) to protect the network from viruses and worms. If you are using a high-speed Internet connection such as DSL or cable, you are also dependent on the other subscribers to your service.

Without a firewall, potential attackers can quickly scrutinize each available computer on the network to locate vulnerabilities (see Practice 8) and attack.

Getting Started
Install an individual firewall on every machine and set it up to block traffic for all services except those specifically used on the machine (see Practice 5).

Educate your employees as to the value of the firewall so they will help you refine the rules instead of disabling it when a change in the implemented rules is needed. While the firewall rules are being crafted, there will be instances of over-blocking, making the use of some computer services more difficult.

Additional Steps
Get technical help to establish one or more firewalls for the network based on the configuration. Establish a security policy to be implemented by rules in the firewall that will define what is wanted and unwanted content within the network. Provide a process for adjusting the security policy for approved exceptions.

Educate employees as to the value of a centralized solution and establish a mechanism for monitoring and changing the rule over time to meet new needs of the organization.

- **Case Four**

Hotels and Wireless Internet Connections Need Firewalls

"Most hotels offer secure broadband services, but do not know enough about security issues to ask their providers questions," a broadband security expert told CNN. "A guest of company A could hack into a conference held by company B, their competition, stealing valuable corporate data and leaving the hotel open to liability," CNN reported.

Many laptops have a default setting that enables a person to share files with other computers. Unless this is shut off, hackers can easily get in when a traveler logs on to a wireless network. Personal firewalls can be used as a deterrent. These are software-based, and simple versions can be downloaded free off line.

Source: *CNN.com, February 2004*

Practice 5 Remove Unused Software and User Accounts; Clean Out Everything on Replaced Equipment

Cost: Minimal - No additional investment

Technology skill level: Low to medium

Participants: Technical support

Why do it?
Computer systems are delivered with a myriad of options, many of which you may never use. Also, the installation process is designed for ease and not security, so functions that are major security problems are often activated, such as remote file sharing.

Software that is no longer used will not be maintained and should be removed from the computer systems so that it cannot be used as a way for attackers to harm your systems.

Every user of the computer system should have a unique account that limits access to the data and software they need to do their job (see Practice 1). When they leave or change functions, the access capabilities need to be terminated or adjusted to meet the new job. Standard management techniques, such as separation of duties, need to carry into the electronic environment to limit the risk of one individual causing harm to the business.

A tremendous volume of data can be stored on disk drives, and this information is not removed when the files are deleted. Additional data is stored in temporary files used by software on the computers. Anyone can retrieve this information by accessing the disk through another computer. For equipment that is removed and repurposed, discarded, given away or sold, the disk space must be overwritten to avoid sharing confidential and sensitive data.

If it's not in the way, can't I just leave it alone?
Unused software and user accounts are not like books gathering dust on the coffee table. Each has the potential for allowing an attacker to gain access to the system. With access the attacker can take confidential information such as credit cards and customer names and damage and destroy files and programs. Attackers can also use your systems as a base to attack others, and these victims can sue you if their losses are high.

Control of computing access needs to be managed just as carefully as cash since the loss of important information can be as detrimental to a business as the loss of money. If unused accounts belonged to former employees, they can keep current on your business and steal or destroy confidential information by continuing to use their system access.

As you upgrade equipment, the data stored on the replaced machinery does not go away. Utilities are available to retrieve deleted files and information from reformatted disks.

Getting Started
Remove accounts for terminated employees when they leave. When firing someone, remove the computer access before notifying them and arrange for a monitor while they are on premise.

Establish a policy that unneeded software not be installed on company computers (i.e. games, free download software, music players, etc.).

Establish a process for removing data on all computers hard drives when equipment is repurposed, discarded, donated, and sold. Use a utility program to remove all information by overwriting all available disk space.

Additional Steps
Uninstall software that is no longer in use and archive data files that are no longer used. The less clutter on the system the easier it will be to manage backups (see Practice 7) and keep software on the system at a current update level (see Practice 8).

While it may be convenient, it is very risky to rely on vendor defaults for your system. Default functions are attractive targets for attackers --the likelihood of availability is high since most installers will choose the default. Reduce your visibility as a target by explicitly selecting only the computer functions you need at installation. If you do not know what a function is, check the help information and make sure it is something you need before turning it on. A little time at the start can save you from major trouble later.

- **Case Five**

Small Telecom Consulting Firm Loses Business When Security Breach is Made Known to Prospective Clients

A telecommunications-consulting firm with 8-10 employees reached a business agreement with a security consultant for joint work. To confirm, the security consultant sent a letter to the president of the company via e-mail. The president never got the letter.

Instead, the consultant received a note back with his original e-mail saying; “Don’t do business with this company. We are a government organization made up of DEA and FBI agents. This e-mail has been sent to you confidentially. If you disclose any of this information we will prosecute you.” Since the consultant was in the security field, he easily determined the warning was bogus and contacted the State Attorney General’s Office and the FBI.

The consultant also terminated his agreement with the telecommunications firm, which threatened to sue him, a threat that never materialized. It turned out the bogus e-mail was from a disgruntled former employee who had built the company’s e-mail server. Before leaving the company, the former employee arranged to have all e-mails to the president of the company forwarded directly to him. He has not been prosecuted.

Source: *Reported to Internet Security Alliance while researching this booklet, February 2004*

Practice 6 Establish Physical Access Controls for all Computer Equipment

Cost: Minimal

Technology skill level: Low to medium

Participants: Everyone using the electronic facilities

Why do it?
No matter how good the passwords (see Practice 1) and security controls on the computer, laptop, or PDA, if someone else has physical access to it they can circumvent the security and use or destroy anything on the device. Electronic devices should not be left unattended inside or outside the office, especially while a user has an account logged on and active.

Cleaning and maintenance staff, visitors and employee family members can download malicious code (see Practice 2) or accidentally change and destroy files and programs while using the computers. Locking the device to a table or wall is not sufficient protection for the data and software stored on it.

If network access plugs (called network drops) are active in open areas such as empty offices, conference rooms and reception areas, outsiders can plug in a device to compromise the network.

Loss of Physical Control is Loss of Security
Anyone with physical access to your electronic device, including repairmen, technical support, and family members, can bypass installed controls and see, change, and destroy data and programs on your computer. If your device is connected to the network, the data and programs on other computers on the network are also at risk. Installed controls will slow them down but not stop them, similar to the protection provided by door locks against a determined thief.

Getting Started
Establish policies for employee's acceptable use that requires:

1. Logging off or applying a screen lock to their computer before leaving it unattended even for a short break
2. Assigning employee responsibility for computer access and equipment taken offsite
3. Limiting employee and family member's personal use of company computers
4. Limiting the use of personal machines on the company network
5. Establishing employee liability when personal acceptable use has not been followed.

Make sure all equipment is protected against power surges with power strips.

Lock down equipment located in highly trafficked areas.

Store unused equipment in locked areas and arrange a sign-out process through an individual responsible for the key.

Educate employees about the policies and walk around the office periodically to make sure policies are being observed.

Additional Steps
Get technical help to implement authentication of all portable devices when they are reconnected to the network.

Lock empty office and conference rooms where active network access plugs are located when not in use.

Review contracts with technical support and repair services to include liability for equipment and information stored on equipment that is turned in for work.

- **Case Six**

Accounting Firm Makes Both Physical and Electronic Copies—But Business Is Threatened by Fire

A New Jersey accountant had his office in a building that also housed a small trucking firm. The accountant had dutifully made electronic backups of his clients' tax returns and put another copy in his filing cabinet along with the rest of his important documents. He also arranged with another accountant to hold additional copies of each other's files.

Unfortunately, the trucking firm had a fire that wiped out most of the building and caused the accountant to lose both the electronic and physical copies of all his records. He was able, however, to maintain his business only because he had provided for another copy to be stored off site.

Source: *Reported to Internet Security Alliance while researching this booklet, February 2004*

Practice 7 Create Backups for Important Files, Folders, and Software

Cost: Moderate to Expensive (depending on the level of automation and sophistication of selected tools)

Technology skill level: Medium to high

Participants: Technical support and Users if individuals must handle their own backups

Why do it?
If an intruder corrupted your computer systems or destroyed software programs, files and folders on the system, could you continue to operate your business effectively? Will your insurance coverage compensate for the lost business of several days while the computer systems are repaired and information is rebuilt manually? Many general insurance policies no longer cover cyber losses. Backups are another form of insurance to help you recover when an intruder attacks or a disaster such as fire or flood harms your technology environment.

Copying files, folders, and software onto some other media (like a disk or CD) provides a source for recovery if it is needed. Manually creating copies can be tedious, and automated options are available. You may already have some of the content in another form, such as software programs that were initially loaded from CD.

Backups should be created any time there is a change to the original content. Select the backup option based on expense (both time and equipment), available time for creating the backup, and recovery time restoring the original from the backup copy. Copies can be created on any form of removable media including floppy disk, CD, ZIP disks, or removable disk drive. Redundant computers can be structured to continuously build a duplicate at the same time as the original for immediate recovery.

Backup copies should be stored in a secure location, preferably offsite to avoid loss to the same disaster that destroys the original. Physical control of backups is as important as physical control of the originals (see Practice 6).

If Backups are not available
Since no protection practices work 100% of the time, it is highly likely that an intruder will successfully attack and harm your technology environment or some type of disaster will destroy some of it. Without a means of recovery, reconstruction can be time consuming and crippling to a business. Even with a backup, the recovery process can be challenging, but at least it is possible.

Getting Started
Backup all files on an established schedule. To select appropriate frequency for backups, remember that changes to the original between the time of backup creation and loss would have to be applied manually.

Retain backups over a period of time to allow for fixing a problem that is not discovered right away. Special backups such as calendar year-end and fiscal year-end should be saved for several years.

Periodically test the backup process by restoring the contents to an alternate location and checking it for accuracy.

Additional Steps
Get technical assistance (see Practice 12) to automate as much of the normal backup process as possible to make sure it always happens. Make sure the backup process creates a date and time log so the contents of the backup can be validated. Create copies on multiple types of media (file server copy and removable disk copy) to provide as much restoration flexibility as possible.

Confirm that the automated process is occurring by periodically restoring the contents and verifying its accuracy.

Check your insurance policies to make sure your data and information systems and intellectual property are covered as well as your physical property.

- **Case Seven**

Small Manufacturing Company Loses Major Government Work Due to Software "Time Bomb"

A northeast manufacturing firm captured contracts worth several million dollars to make measurement and instrumentation devices for NASA and the US Navy. However, one morning workers found themselves unable to log on to the operating system, instead getting a message that the system was "under repair." Shortly after, the company's server crashed, eliminating all the plant's tooling and manufacturing programs. When the manager went to get the back up tapes, he found they were gone and the individual workstations had also been wiped out.

The company's CFO testified that the software bomb had destroyed all the programs and code generators that allowed the firm to customize their products and thus lower costs. The company subsequently lost millions of dollars, was dislodged from its position in the industry, and eventually had to lay off 80 workers. The company can take some solace in the fact that the guilty party was eventually arrested and convicted.

Source: *The CERT Coordination Center, Carnegie Mellon University, 2001*

Practice 8 Keep Current with Software Updates

Cost: Moderate – Software maintenance fee plus staff time to install and verify

Technology skill level: Medium to high

Participants: Technical support

Why do it?
Software vendors routinely provide updates (also called patches) to fix problems and enhance functionality within their products. In addition, many of these patches fix vulnerabilities that could be used by viruses and other attacks to harm your computer and its contents. By keeping software up-to-date, software malfunctions and opportunities for system compromise are minimized.

Vendors often provide free patches for downloading from their websites. Software vendors may provide a recall-like service, similar to receiving a recall notice for your car. You can receive patch notices through e-mail by subscribing to mailing lists operated by the vendor. Through this type of service, you can learn about potential problems before they occur and, hopefully, before intruders have the chance to exploit them.

Sometimes a patch fixes one problem but creates another. When this happens, the repair cycle may have to be repeated until a number of successive patches completely fix a problem.

If Patches are not Installed
Software is not shipped defect free. Vendors rely on their customers to tell them when something unexpected happens while using their software. By not installing patches, you are missing the fixes to problems discovered by others.

Code defects make your software vulnerable to malicious code attacks. These attacks can corrupt and delete files and remove protection mechanisms such as anti-virus software (see Practice 3) and firewalls (see Practice 4) to increase future vulnerability. Attackers can use your computer as a base for bombarding others with unwanted e-mail that appears to be from you.

Intruders find out about vulnerabilities the same way you do--by monitoring e-mail lists and subscribing to automatic notification services. The longer the vulnerability is known, the greater the chances are that an intruder will find it on your system and exploit it.

Getting Started
When you purchase a program, see if and how the vendor supplies updates. Learn how the vendor provides answers to questions about problems with their products. Consider purchasing extended warranty support if it is available. If patches are not supplied, find out when a new release is available and consider upgrading if vulnerability fixes are included.

Locate and apply vendor software updates, especially patches for known vulnerabilities, as soon as possible. Consult the vendor's website to see how to get timely e-mail notices about patches. Subscribe to a vendor mailing list for notification of problems and fixes.

Additional Steps
Some vendors provide programs that automatically contact the vendors' websites looking for new patches to their software. These programs can tell you when patches are available, and can download and install them. You tailor the program's update features to do only what you want--for example, reporting that a new patch is available but giving you the option to defer its download and installation.

If you learn of a vulnerability and no patch is available, consider using different software until the original program is fixed.

- **Case Eight**

Diners Have Supply Chain Interrupted/North Carolina Inn Has Reservation System Crashed—Both Failed to Update Software

A small string of diners in Maryland that had come to rely on e-mail to deal with its suppliers found itself knocked off line for four days by a virus attack. Although the company tried to download the patches to address the specific problem, it found it was unable to because it had not put in patches for earlier software problems.

Similarly, an Inn on the Outer Banks of North Carolina found it was also unable to make repairs to its system in response to an attack because it had not kept up maintenance. It found its online reservation system knocked out for a period of days, and employees became distrustful of the rest of the computer system for fear it too had become corrupted.

Source *USA Today, August 2001*

Practice 9 Implement Network Security with Access Control

Cost: Moderate to High depending on the options selected

Technology skill level: Moderate to High

Participants: Technical support and all network users

Why do it?
Though your organization's technology environment is often referenced as "the network," in reality it is a collection of pieces assembled in a certain way to meet the technology-specific needs of your organization. Good network security requires access protection for each component on the network including firewalls (see Practice 4), routers, switches, and all connected user devices. Otherwise, anyone who could reach your network could locate and compromise network components and services. In addition, remote and portable devices should be required to authenticate themselves to the network to limit who can see and access the network services such as databases, shared files and printers.

A firewall (see Practice 4) provides a buffer between the components of your network and the external environment. Other techniques, such as proxy servers and network address translation (NAT) add further protection limiting the information an outsider can learn about the components in your technology environment making it more difficult for attackers to find vulnerabilities.

The more access restrictions you can legitimately place on your network using blocking capabilities within the firewall and other similar services, the easier it will be to keep it secure.

Special Considerations
Good access control is critical for wireless access since use of this type of connectivity is less visible. It is not uncommon for someone sitting in a car in the parking lot to be able to access an unsecured wireless network and jeopardize everything on the entire network. You may have a wireless or remote access (dial-in) connection to your network and not realize it, since many vendors install them to provide remote support capabilities. Point-of-sales devices and inventory devices communicate to central servers via wireless.

The ability to reach and use services on your network from outside (called remote access) is extremely valuable for traveling employees, suppliers, and customers. Remote access also allows technology vendors to provide support for critical network services quickly without having to travel to your site. Employees can and do add remote access devices (dial-in) directly to their computer so they can work from offsite. Use of this type of network access requires careful control, or anyone who happens to find the access point using simple scanning tools can get into the network and compromise or destroy information.

Instant messaging, chat sessions, and music-sharing capabilities establish other routes (peer-to-peer) into the network, bypassing many of the traditional network security mechanisms. These options are a growing conduit of malicious code and must be used carefully.

What Happens without a Good Network Security?
Attackers are constantly bombarding components accessible from the Internet with query functions looking for weaknesses. Unprotected devices are compromised within minutes after connectivity is established especially when Internet access is available through cable modems, digital subscriber lines (DSL), or other high-speed connections. A compromised device puts all other devices on the network at risk since it can be used as an inside base for locating weaknesses and attacking other components on the network.

Not all attackers are external to the organization. Employees can compromise fellow employee machines using tools readily available from the Internet when there is poor network security. These tools allow them to spy on others' actions, view information outside of their job function, stalk and harass others, and plant inappropriate content on others' machines.

Getting Started
Access to each component on the network should be limited to protect it from improper access and harm. Basic access protection can be implemented using strong passwords (see Practice 1).

Establish procedures to turn off the file and printer sharing feature on each computer (see Practice 5) unless it is in use, particularly when accessing the Internet using cable modems, digital subscriber lines (DSL), or other high-speed connections.

Instruct employees to disconnect from the Internet by turning off the online session and turn off their computer when it is not in use.

Access to network protection devices such as firewalls (see Practice 4), switches, and routers should be further limited to only those individuals responsible for the maintenance and support of these components. Knowledge of the passwords for each component should be limited to two people--a primary and backup. A vendor providing component support should exercise the same level of caution (see Practice 12).

Do not select the option on web browsers for storing or retaining user name and password.

Require authentication for wireless and remote access.

Additional Steps
Consider the use of smart cards or other hardware tokens for remote access to network-critical components, especially the firewall, switches, and routers. Educate employees in the use of these devices along with the rationale for their use, and assign the responsibility to the employee in the event of loss or destruction.

Get technical assistance (see Practice 12) to establish intrusion/detection monitoring to make sure the network is being used as expected without internally - or externally - generated interference.

- **Case Nine**

Cyber Blackmail Goes Mainstream

Once perpetrated predominantly against wealthy individuals or major corporations to extract large payouts, cyber blackmail has now become prevalent even in smaller business. Office workers are now widely reporting being the targets of an extortion scam that seems to target almost anyone with an e-mail address. The e-mail demands that the recipient make an on-line payment of a small sum of money, usually $20-$30 dollars. If the recipient fails to comply, the sender threatens to attack the company's computer system and wipe out sensitive files or upload child pornography. Unsuspecting victims often opt to pay the extorter rather than risk the possibility of attack or embarrassment. Consequently, many instances of cyber extortion go unreported and investigations are not conducted.

Source: *Reuters, 2003*

Practice 10 Limit Access to Sensitive and Confidential Data

Cost: Moderate to High depending on the options selected

Technology skill level: Moderate to High

Participants: Technical support

Why do it?
E-mail should only be viewed by those to whom it is sent. Data files should only be accessed by individuals who have received specific permission. Since you cannot trust everyone in the world to act appropriately on his or her own, control mechanisms are required to enforce restrictions.

If the data is stored in files, folders, and databases within your network, you can control who can see and use the contents with an access control list, or ACL. ACLs define who can perform actions on a file or folder such as reading and writing.

When access to information cannot be tightly controlled, such as e-mail or a credit card transaction over the Internet, this information can be concealed through a mathematical process called encryption. Encryption transforms information from one form (readable text) to another (encrypted or scrambled text). The encrypted text appears to be gibberish and remains so for people who don't have the formulas (encryption transformation scheme and the decryption keys) to turn the encrypted text back into readable text. The encryption mechanism must be sufficiently complex or someone with electronic tools could guess the formulas and defeat the encryption.

What Happens without Good Data Security?
Good network security (see Practice 9) is not enough to assure data protection. A wide range of people such as full, part-time, and temporary employees, as well as contractors and vendors, will have legitimate access to your network but should not have unrestricted access to every piece of information on the network. When anyone can access your network, they can see every communication that passes among the devices on your network and view and modify or destroy the contents. Snoopers will initiate programs to search your network communications for credit card numbers, social security numbers, and financial information for criminal intent. They will search for passwords to databases, applications and other networks to expand their access capabilities.

Getting Started
Educate employees to use care in sharing sensitive and confidential information electronically.

Do not use real information for any testing of new processes.

Do not use public or Internet café computers to access online financial services accounts or perform financial transactions.

Do not disclose personal, financial, or credit card information to a little-known or suspect website.

Additional Steps
Ensure that your browser supports strong encryption (at least 128-bit). Get technical assistance (see Practice 12) to establish automatic encryption, when possible, for all electronic communication that passes outside of your network, and notify the sender when information cannot be sent encrypted.

Get technical assistance to establish ways to encrypt sensitive and confidential information that is stored and shared on the network.

Turn off the caching feature for the browser so sensitive and confidential information is not stored in unprotected temporary locations.

Establish ACL's for access to all shared files, folders, and databases to assure that access is only available to those who should have permission. These will have to be maintained over time as staff changes. Further limit who can update and delete data and files for greater protection.

- **Case Ten**

Credit Union Employee Gets Private Customer Information and Uses It for Personal Gain

The US Justice Department has prosecuted a woman who worked at a Sacramento, California, Credit Union. The woman used her firm's computer to obtain customer account information including names, social security and driver's license numbers, and addresses to open accounts in the names of others and incur unauthorized charges. Some of the credit card accounts were opened on the Internet. After the phony accounts were established, the defendant made numerous purchases totaling well over $50,000.

Source: *US Department of Justice, March 2003*

Practice 11 Establish and Follow a Security Financial Risk Management Plan; Maintain Adequate Insurance Coverage

Cost: Moderate – a risk management methodology is free

Technology skill level: Low to Moderate

Participants: Representatives of all levels of the organization and technical support

Why do it?
In order to be effective, security must be consistently applied across the organization. For example, the use of very tight technology controls with lax or non-existent organizational security policies does not provide protection. The best way to validate your security is through the application of a security risk management methodology. In a structured sequence of activities, participants at multiple levels of the organization work together to devise a plan that makes sense for the needs of the organization based on its use of technology. To be comprehensive, this planning process must consider the following areas:

1. security awareness and training for all technology users
2. organizational security policies and regulations
3. collaborative security management (partners, third-parties and contractors)
4. contingency planning and disaster recovery
5. physical security
6. network and data security

In the rush of daily activities it is easy to overlook the need for such things as employee security training, contingency planning, and disaster recovery. You may not even be aware of the level of dependency your organization has developed on technology and the potential impact that a failure of one or more components will cause. By developing a security risk management plan, these dependencies will be highlighted and mitigation steps can be identified to reduce the potential impact of technology compromise or failure.

What Happens Without Security Risk Management?
Without a plan, you will have to react to technology compromise or failure when it happens. Your options for response will be limited by what you can find when the problem occurs. Also, you will not be in a good position for negotiating the cost of technical assistance or the level of expertise provided. The outage will be longer than necessary as you scramble to figure out what to do before acting to correct the problem.

Getting Started
Review your disaster recovery and contingency plans.

Identify the impact to your business should you experience an extended power outage, flood, or major storm.

Additional Steps
Apply a security risk management methodology design for small business, such as OCTAVE®-S, to identify important technology assets, threats to these assets, and develop a security plan for your organization. As part of the methodology you will compare your existing security practices with established best practices to identify areas where your organization is vulnerable and mechanisms for addressing the gaps in your existing security practices.

Get technical assistance (see Practice 12) to perform a vulnerability assessment on your technology environment to assist you in identifying vulnerabilities that pose a major risk to your important technology assets and identify mechanisms for reducing their possible impact.

- **Case Eleven**

On-Line Retailer Misunderstands Insurance Coverage, Gets Wiped Out by Attack

Thanks to a series of computer attacks, an on-line retailer once valued at over $1 million is ruined. The worst damage was done when the attacker spammed his clients contending the firm was a front for pedophiles (his wife operated a day care center). Direct losses, denial of service, replacing data, customer attrition and PR costs crippled him. Since this was an inside job no reasonable technical measures would have protected him, but appropriate risk management including insurance might have. Unfortunately, the president of the company had misunderstood that his cyber-risk exposures were not covered by his standard property and casualty policy. Standard insurance policies do not cover cyber-risks.* "My business is gone. My wife's business is gone, now I just hope we can hang on to our house," said the disheartened former owner.

Cyber insurance, which is now available, might have saved this company. Of course, taking out a separate cyber policy would have added to his operating expenses, but it might have allowed his company to survive the financial consequences of the cyber attack. Some organizations, including the Internet Security Alliance, have arrangements in place wherein substantial premium credits on the cyber-insurance premium can be provided to its members who comply with best practices such as those outlined in this booklet.**

Source: *CSO Magazine, December 2001*
* Ernst & Young, 2003 Global Information Security Survey
** Internet Security Alliance/AIG risk management protection program (www.aignetadvantage.com);
Cyber-Risk Profiler℠ (http://www1.nuserve.com/CyberRiskProfiler)

® OCTAVE is registered in the U.S. Patent and Trademark Office

Practice 12 Get Technical Expertise and Outside Help When You Need It

Cost: Low to High depending on the services needed

Technology skill level: Medium to High

Participants: Company Management and Technical support

Get the Right Kind of Help
Because you have a business to run and technology security is not something you can afford to have consume all or most of your time, good technical assistance can be a valuable asset. Employees, friends, and family with a technical interest can help you get started, but you need someone with security training and experience to tie all of the individual activities together into a working security protection mechanism for your organization. Even this is not guaranteed protection, since new opportunities for compromise are identified daily.

Unlike most software tools and hardware components, technology security cannot be learned by trial and error. Security is not static and must be reassessed frequently to identify when changes within the organization and new threats require an adjustment to some or all of the protection mechanisms.

Great care must be taken in selecting who will handle the technology security for your organization. Trust but verify! Those entrusted with security will be aware of your technology weaknesses and how to take advantage of them. Make sure they can explain to you what they are doing and why. They must be able to demonstrate the steps they are performing to implement the security practices in this guide. In addition, they must be able to show how their actions are working for you to resist attacks, recognize intrusions, and recover as needed.

What Happens without Good Technical Expertise
Hardware and software components are designed for easy installation and use. A wide range of information sharing capabilities are available but should not be used without careful consideration. Additional time and effort is required to implement security, but without it your network can be compromised and your information taken or destroyed without your being aware of anything unusual.

In addition to the Internet attackers attempting to compromise all types of devices for unknown purposes and data snoopers looking for ways to steal personal and financial data, others such as your competitors, current and former employees, and family members may be seeking ways to learn more about your business, employees, and customers. Whether their reasons for snooping are nosey or malicious, the outcome to your organization will be a loss of your business reputation, potential harm to customers, potential fines and penalties, and loss of time while you explain why you let this happen.

Getting Started
Ask the individuals handling your technology support how they are addressing the security practices in this booklet and if they need additional assistance.

When considering outside assistance, evaluate the following:

1. review past work experience
2. review partial client list and ask for references from current customers
3. ask how long the company has been in business
4. ask who, specifically, will be assigned to do your work and their qualifications and relevant certifications
5. ask how they provide support, what is done at your site, and what is done offsite
6. ask how offsite access is controlled

Make sure you have made arrangements for all of the security practices described in this booklet. If internal staff is handling some of the technical work with the assistance of a consultant, make sure everyone knows what they are to do and how they will work together.

Make sure you have included minimum performance requirements, monitoring mechanisms, and a termination process before establishing any technical security support.

Additional Steps

Through organizations such as the Chamber of Commerce, National Association of Manufacturers, National Federation of Independent Businesses, the Internet Security Alliance, and other peer groups and conferences, ask others about their approach to security and what they feel has been successful.

Establish periodic reviews of your security service, whether it is being handled internally or externally (annually at a minimum and preferably once a quarter) to determine if existing support is sufficient and identify needed improvements.

- **Case Twelve**

Venture Capital Research Firm and Law Firm Try to Get by Without Good Technical Assistance—Regret the Decision

A three-person venture capital research firm realized how dependent their business was on the Internet when their e-mail went out due to a virus just before two of the partners were due to take extended business trips. Although the firm received over 600 e-mails a week and used the web as its sole source of promotion, it felt it could not afford a full-time tech expert. The partners had to cancel the business trips fearing they would lose their customers if they could not keep in touch. It took three frantic days of calling around before they found an expert to talk them through their problems.

An Albany NY law firm with about 20 computers lost its network administrator and failed to replace him for six months. When the firm finally brought in consultants, they found a variety of vulnerabilities. In addition, updates had not been applied to the server, the anti-virus software had not been updated, and the license had expired. After the technical consultants turned in their analytical report, but before they had begun to repair the situation, the law firm was hit by a virus. Many of the PCs were affected and hundreds of files were compromised.

Source: *Reported to Internet Security Alliance while researching this booklet, February 2004*

C. References/Sources

- Six facilitated focus groups with small business representatives, *January-February, 2004*
- ISAlliance *Common Sense Guide for Senior Managers* (www.isalliance.org)
- Small Business Cyber RiskProfile[SM] Risk Assessment Tool (http://www1.nuserve.com/CyberRiskProfiler)
- Cyber-Risk Insurance and Risk Management, American International Group (www.aignetadvantage.com)
- Cyber Security Tip ST04-0003, National Cyber Alert System (www.us-cert.gov/cas/tips/ST04-003.html)
- ISAlliance *Common Sense Guide for Home and Individual Users* (www.isalliance.org)
- Remembrance of Data Passed: A Study of Disk Sanitization Practices, *IEEE Security and Privacy*, January/February 2003.
- Computer World Magazine, August 2000
- USA Today, August, 2001
- CSO Magazine, December 2001
- The CERT Coordination Center, Carnegie Mellon University, 2001
- U.S. Department of Justice Press Releases: September, 2002; March 2003
- Reuters, 2003
- CNN.com, February 2004
- BBC, 2004

D. Contributors

Scott Algeier, US Chamber of Commerce
Peter Barrett, Business Performance Technology, LLC
Joe Beacom, Landstar
Brian Cilley, Netstruxion
Wendell Craven, Digital Trends Corporation
Lee Eisen, The Strathmore Group
Kai Tamara Hare, nuServe
George Hickey, Glasswalker
Marc Jones, Visionael
Tom Kellermann, The World Bank
Doug Landoll, Veridyn Inc.
Charles LeGrand, The Institute of Internal Auditors
Ted LeRoy, Frontrunner Network Systems
Jeff Recor, Olympus Security
Steve Roberts, University of Florida Fredric G. Levin College of Law
Larry Thomas, Landstar
MacDonnell Ulsch, Janus Risk Management, Inc.
Caroline Van Hollen, Internet Security Alliance

Copyright 2004 ©. Carnegie Mellon University and Internet Security Alliance. All rights reserved.

Join the ISAlliance today and...

BE FIRST

Fight security breaches from the moment they're discovered instead of waiting to find out if you've been hit.

BE SECURE

As an ISAlliance member, you'll improve your security posture, mitigate cyber threats, and ensure continuity of business operations.

BE HEARD

The ISAlliance increases your access to lawmakers, regulators, and news media, advocating your interests and amplifying your viewpoints.

BENEFITS OF MEMBERSHIP

Each membership level includes an increasing number of certificates to the CERT®/CC Restricted Knowledgebase as well as an increasing discount on conferences, publications and CERT®/CC courses. *Note: Multinational organizations generally join at the Sponsor level. For more information on Sponsor level benefits, please visit us at www.isalliance.org.

ASSOCIATE MEMBERSHIP US$5,000/year

This service suite is designed primarily for smaller businesses that may have a very small IT department but are still interested in keeping fully abreast of emerging cyber security threats, and wish to communicate regularly with larger companies and CERT professionals about how they can improve their own cyber security program.

Associate benefits include:

- **Associates receive one CERT/CC certificate allowing access to the full range of CERT services.**
- **Associates receive regular "Special Communications" about threats, vulnerability, and upcoming attacks through the Internet. This critical information is often provided well in advance of its dissemination to the public.**
- **Associates are able to search the vast CERT/CC knowledgebase of vulnerability and threat information and trend data.**
- **Each month, Associate Members meet via a secure conference call with CERT experts and other ISAlliance Sponsors and Members to discuss emerging issues in the cyber field. On these calls CERT experts are available for company specific questions. Associates can also access CERT/CC expertise on-line.**
- **Associates are entitled to a full 15% discount off AIG cyber insurance rates granted to ISAlliance members who also commit to fulfill the ISAlliance best practices regime.**
- **Associates are entitled to a discount off state-of-the-art CERT training programs.**
- **Associates receive ISAlliance publications such as the Best Practices compilations, "The Common Sense Guide to Cyber Security for Small Businesses," "The Common Sense Guide for Senior Managers," and "The Common Sense Guide for Home Users," free of charge.**

BENEFITS OF MEMBERSHIP

FULL MEMBERSHIP US$25,000/year

Full ISAlliance membership is designed for medium to large sized firms that appreciate the multiple factors involved in developing a secure information network. Full Members are invited to participate in all the technical, public policy, standards and practices, and international programs offered by the ISAlliance.

Full Membership benefits include:

- **Full Members receive 5 CERT certificates enabling several people within the organization to have access to the range of CERT services.**
- **Full Members receive almost daily "Special Communications" from CERT/CC about threats, vulnerability, and upcoming attacks through the Internet.**
- **Full Members also receive enhanced technical services, such as intermittent "Executive Communications" (about 6-10 a year), which identify immediately threatening cyber events.**
- **Full Members of the Alliance are entitled to participate fully in ISAlliance Committees by exercising voting rights and recommending projects and policies to the Board of Directors.**
- **Full Members are also entitled to participate in ISAlliance International programs including sponsorship opportunities.**
- **Full Members are entitled to a full 15% discount off AIG cyber insurance rates granted to ISAlliance members who also commit to fulfill the ISAlliance best practices regime.**
- **Full Members are entitled to a discount off state-of-the-art CERT training programs.**

www.isalliance.org

2500 Wilson Boulevard
Arlington, Virginia 22201-3834
United States of America
+1 703 907 7799

+1 703 907 7799
2500 Wilson Boulevard
Arlington, Virginia 22201-3834
United States of America

www.isalliance.org