Global Information Assurance Certification Paper

Version 1.3

Securing Your Site With Limited Resources

Maurice McClain

February 5, 2001

Many administrators feel overwhelmed as they are being tasked to secure organizations without additional resources, and sometimes without a redefinition or reduction in current duties. Often companies will not seriously consider dedicating staff or budget towards security until there has been a serious security breach. This trend seems to hold in spite of highly publicized security issues, in a year when the total number of security incidents tracked by the CERT nearly doubled compared to the previous year. (1) After September 11 terrorist attacks some organizations are reacting with increased resources, but some companies refuse to act, and others simply do not know how to react.

This paper will cover the essential elements to secure a site, offer suggestions on how to present an effective security plan to management, as well as provide numerous ideas on how to extend your defenses. Links to many information security sources are presented that will allow the reader to build on concepts discussed.

The Essentials

While some of the suggestions and strategies discussed later may not be applicable at your particular site, some fundamentals should be common in any Internet enabled business environment. First, define your role in the effort to secure your site. Some administrators feel they do not have the authority to undertake the tasks associated with overall security procedures. The direct approach works well, even if it has to be a question and answer session with key members of the company. Point out the security related areas that you are currently responsible for at the business. If you control the firewall, data connectivity, routers, and virus protection, you are likely the first person your company turns to when there is an incident. Asking for a solid understanding of what is expected from your position will give you a better outlook and characterize your options and limits. Establishing a personal security policy will further define your role, as well as provide an important understanding between the company and yourself. The policy should read in plain terms the techniques you are authorized to use, and penetration testing should be defined clearly. The general idea is to provide a document that lays out the ground rules. The company may grant you permission to use certain security tools, but not all. For instance, it may be okay for you to run a password cracker on the file server, but the same privilege may not extend to the payroll server. This policy also protects you from unexpected events that can happen when performing penetration tests. It is probably a good idea to have more then one member of senior management sign off on this document.

Ensure that you have a properly configured firewall, and remember that the policy rules can be setup incorrectly just like anything else. As most sites do not have a completely closed firewall, you should keep up with the vulnerabilities that affect the open ports on

your firewall. Outside of the base configuration, maintain patch levels on the system. A change procedure process should be setup and a modification sheet should be incorporated into company policy. This allows the firewall administrator to document the why, when, and how. Many times the people who make requests for services have no idea about the holes they are creating, and generally agree that the benefit does not take precedence over the risk. It is your job to explain the risk associated with requested services in plain terms. Telling a business manager that your firewall does not detect spoofed packets, and that port 1601 is not defined to a single host is not laying it out plainly. Log everything, or as much as you can. By reviewing log files, you can pick up reconnaissance patterns, which alert you to a hostile user. Clearly, your options depend on multiple environment configurations, but if possible, alerts should be setup for specific events. An example of this is receiving alerts when someone fails multiple authentication requests at the firewall. Even if they fail authentication, you would probably want to know that they are trying. Control any remote connections to your network and plan them carefully. Many people like the host-to-host, port-to-port approach to limit exposure, but anything short of allowing an entire external network to access all hosts on your internal network starts you in the right direction. Review access logs and create a baseline of important events, false positives, and relevant ports. If you know exactly which ports are allowed into your network, and have a general idea of unfriendly ports, you will learn to spot problems quickly when reviewing the firewall logs. Learning site application behavior and user trends will also allow you to disregard events written to the logs files that are harmless.

Examine your external routers that are managed in-house, and include routers handled by your data provider if located on site. Make sure that the configuration is in line with your general security standards. If you are not familiar with this process have the person who installed the router, document the configuration as well as provide details about any security measures in place. Depending on the type of router you have it may be possible to stop unauthorized traffic at this point, so use any security capabilities available. Your mail server should be setup with anti-virus software. Even if the server is hosted externally or in a DMZ, it should be addressed. The flavor is not important but the anti-virus software should have the ability to examine attachments on arrival and remove potentially harmful file types at the server level. My suggestion is at a minimum disallow .exe, .vbs, and .bat. These file types are often used to introduce hostile code, and many times the file extensions are hidden. An e-mail user will see an attachment like familyphotos.gif, but the file name is actually familyphotos.gif.vbs. Entry points such, as these are popular backdoors into networks. Unless you have a burning desire to be placed on a RBL (real time blacklist) configure the mail server relay settings correctly. Leaving your mail server open to relay attacks will also peak the interest of attackers. If this is open what else? If you are not sure how to determine if your mail server is vulnerable to open relay, the following link provides a quick FAQ about Spam, and allows you to check to see if you are already on a RBL. http://work-rss.mail-abuse.org/rss/ This is just one of the sites that list hosts open to relay. If you want to check additional RBL's you should run a google search for RBL, which will return multiple sites that will allow you to check your mail server. Even if you a think you have a particularly secure mail server, or sufficient network virus protection you should still

provide virus software for desktop clients. It is better to have an incident isolated to one host, then to have it propagate throughout the entire network, or worst yet a business partner's network. This will also provide protection against worms, and viruses that can be downloaded from the Internet, or introduced by media. Since this is likely the last defense, configure the software correctly and be sure to update the definition files weekly. Nearly all virus software products depend on definition files, which can only be created after a virus is discovered. For this reason you should enable heuristics. This smells likes a virus looks like a virus approach may produce some false positives, but it could help prevent a virus outbreak. Examine your backup procedure and make sure it is inclusive to all necessary hosts. Secure some of the tapes at an off-site location, including not only servers but also any devices that could equal downtime for services if they fail. The firewall is a good example of a device that could fail and affect multiple services. You should establish the behavior of devices when they fail. You may have to work with vendors to make this determination, but you do not want to learn in real-time that a critical device like the firewall defaults to allow all traffic in, due to a hardware or software malfunction. Redundant hardware is not always required but knowing how to restore devices will give you a head start in a disaster. After taking one last look to make sure there are no gaping holes, begin creating a company baseline by documenting the existing infrastructure. Gather all of the security related policies, grab a three ring binder and you have a sufficient starting point. This baseline should be used to highlight any improvements made during the process to secure your site.

Communicating a security plan to management

After key fundamentals are complete, you should approach management with a structured plan. This may be difficult or simple depending on the company atmosphere, but companies who remain unprotected seem to fall into one of three categories.

- The decision makers are not aware of the vulnerabilities that exist and the potential for a negative business impact.
- They feel that the existing security infrastructure is sufficient.
- The company understands the need to secure the site but will only dedicate existing staff and funds.

If your site falls into any of the scenarios above your next and perhaps most important step is to effectively communicate a security plan to management. One mistake administrators make when trying to secure a site is by requesting multiple security devices to combat the problem. Many times this approach overwhelms the company with new funding requests. A better method is to explain your overall security strategy and the associated costs. While it is still very difficult to place a return on investment on security measures, you must approach business people in a business manner. If a budget analysis is the bottom line at your company, you may want to research articles focusing on return on security investment. @Stake, a company that focuses on business security, has completed documentation of a ROSI study and plans to work on additional ROSI scenarios. (2) The additional studies will focus on return on investment when operating systems are hardened and incident readiness. Apply these scenarios to your site.

Determine how many man-hours are required to patch servers, and desktops. Present estimates on how long it would take to respond to some of the recent attacks if they had hit your site. This type of data can be used to gauge ROSI.

The presentation should not be a one shot deal. Begin with the first presentation and follow it up with either quarterly or semi-annual reports. The scope of the overall problem can be addressed with numbers provided from multiple sources. While the data you select to present will be unique to your site, below are some numbers that speak to the hostile nature of the Internet.

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2001

Year	2000	2001
Incidents	21,756	52,658

Total incidents reported (1988-2001): **100,369**

The CERT® Coordination Center (1)

The steady rise of incidents shows that the problem cannot be ignored. If the increases in attacks continue more sites will be at risk, and it is likely that many of the sites affected by incidents last year will attempt to fix security problems. Attackers will continue to probe networks looking for weaknesses, and your network might be next. A second statistic that highlights how sites remain unprepared is virus and worm attacks. The costs attributed to these attacks are significant.

Analysis By Incident

Year	Code Name	Worldwide Economic Impact ($ U.S.)	Cyber Attack Index
2001	Nimda	$635 Million	0.73
2001	Code Red(s)	$2.62 Billion	2.99
2001	SirCam	$1.15 Billion	1.31
2000	Love Bug	$8.75 Billion	10.00
1999	Melissa	$1.10 Billion	1.26
1999	Explorer	$1.02 Billion	1.17

Computer Economics (3)

While the costs are considerable the fact that many of these attacks could have been prevented is much more important. Code Red struck on July 19, 2001 and the patch for the vulnerability it took advantage of was released on June 18, 2001. Nimda was discovered September 18, 2001, but the patch was released on August 18, 2001. Maybe one of the worst cases was the sadmind/IISworm which used a 2 year old vulnerability to exploit a seven month old IIS weakness. (4) Provide details on when your site installed the necessary patches for these vulnerabilities, and how many unplanned hours were spent on these tasks. To give site-specific estimates on virus and worms try a cost calculator.
http://www.cmsconnect.com/Marketing/CalcMain.htm

A more aggressive step is to place a clean system with logging capabilities on the external network to record hostile attempts to penetrate your network. Research done by the Honeynet Project states that the average life expectancy is just 72 hours. (5) Based on this you can infer that an unprotected or poorly configured system would be attacked quickly. Determine if your existing internal processes would prevent this from happening or alert someone within 72 hours. Be extremely careful before taking this step. You should be experienced before playing a cat and mouse game with a hacker, and if you like job security be sure, you have permission. If a hacker attacks the IP address of the honey pot you can be sure they will run a scan on the larger block, which will show any vulnerable parts of your network.

Determine if there are any allocated funds dedicated to security in the IT budget. A survey conducted by Metricnet shows that "prior to Sept 11th only 18 percent of companies were spending more then 5% of their IT budget on security. As of Nov. 13, 33 percent had decided to spend at least that much on security." (6) Determine where your company fits in this equation to spark discussion on the importance of defending your data. If funds exist, begin tracking where the money goes and if it is being used in the best manner. If there is no line item for security inquire about the reasoning behind the decision.

The information provided in your presentation should be site specific and cover the following areas:

- Company security baseline
- Steps that you would like to implement
- Estimates on your current incident response time
- Affects and costs of downtime
- Identification of sensitive data sources
- The importance of data integrity to your site
- Customer privacy

The steps that follow will illustrate to management your ability to put into practice a long-term security plan. In many cases, the key steps to accomplish security do not have a traditional monetary value attached, which is a good point to emphasize in your presentation. If possible, incorporate the steps below into your plan.

Establish a working relationship with the staff member in charge of physical security to restrict physical access to servers and network devices as necessary. This not only limits access to the machines, but also will allow you to document access if necessary. Begin working with department heads and the human resource department on security related policies. Achieving buy-in from the manager base will help you realize your overall goal. Discussing end-user services allow you to point out the risk association per service. IRC is an example of this. Many companies unknowingly allow this traffic to send requests outside of their network in direct violation of existing policies. Implementing user awareness training better enforces corporate policies. Repeatedly employees sign on the dotted line but have no idea how to interpret the real life meaning. Other employees are aware that while many companies make a point of having you sign these documents, there is no real enforcement to a significant portion of it. Work with management to create a system audit program, which should include the network, desktops, and servers. If you benefit from desktop standards then you should already have a program blueprint to lay out to end-users. Define in policy what users have the authority to download programs, and change computer settings. Even if you do not have the luxury of desktop standards, you can work with department managers to create an approved application set**.** Some sites allow all traffic out from inside their network, because there are no standard services behind the firewall. Defining the application set will allow you set what traffic is allowed from your network, and make the necessary adjustments at the firewall level. User awareness training, joined with strong policies and unscheduled system audits can be powerful. Very few employees want to become an example for violating polices that are routinely enforced. One process that can eliminate surprises during system audits is to create configuration checklists for server and desktop hosts. After working with other system administrators and management to agree on standards, no host should be placed on the network before being compared against a corresponding checklist. This will ensure system consistency and reduce the number of hosts configured incorrectly. Several checklists are available publicly and an excellent effort to publish checklists by

consensus can be found at: http://www.SANS.org/SCORE Wrap up all of this information into an informative presentation and prepare to act on your recommendations. Offer ongoing reports to make management aware of the current information security status.

Extending Your Defense Capabilities

Well-invested time and planning will only get you so far, and at some point you will have to invest capital to extend you defenses. While it would be nice to have a NORAD type infrastructure it is always not possible, so choose expenditures wisely. There are many directions that you can take from this point based on your particular situation, but below are some ideas.

Penetration Testing

If the site has not undergone a network risk assessment, it is time to perform one. This task could be attempted earlier but unless you are familiar with the latest tools and techniques to probe networks, you will likely need to consult with an independent tester. Even if you have a certain level of knowledge, many companies will place more weight on testing done by a professional consultant. Be sure that the person performing the test is capable and will document the process as well as offer recommendations based on the test. Be highly suspect of a test that comes back with no improvement recommendations. One of the reasons for this test is to address any weak points in the armor. The weakness may not be a huge hole, but could be a procedure or technique that is currently being used. Just about every site could do something better when it comes to information security. An ongoing penetration schedule should be implemented to assure that no newly added services have negatively affected the baseline configuration. Routine testing should be established with the time between audits depending on your site, budget, and other defenses.

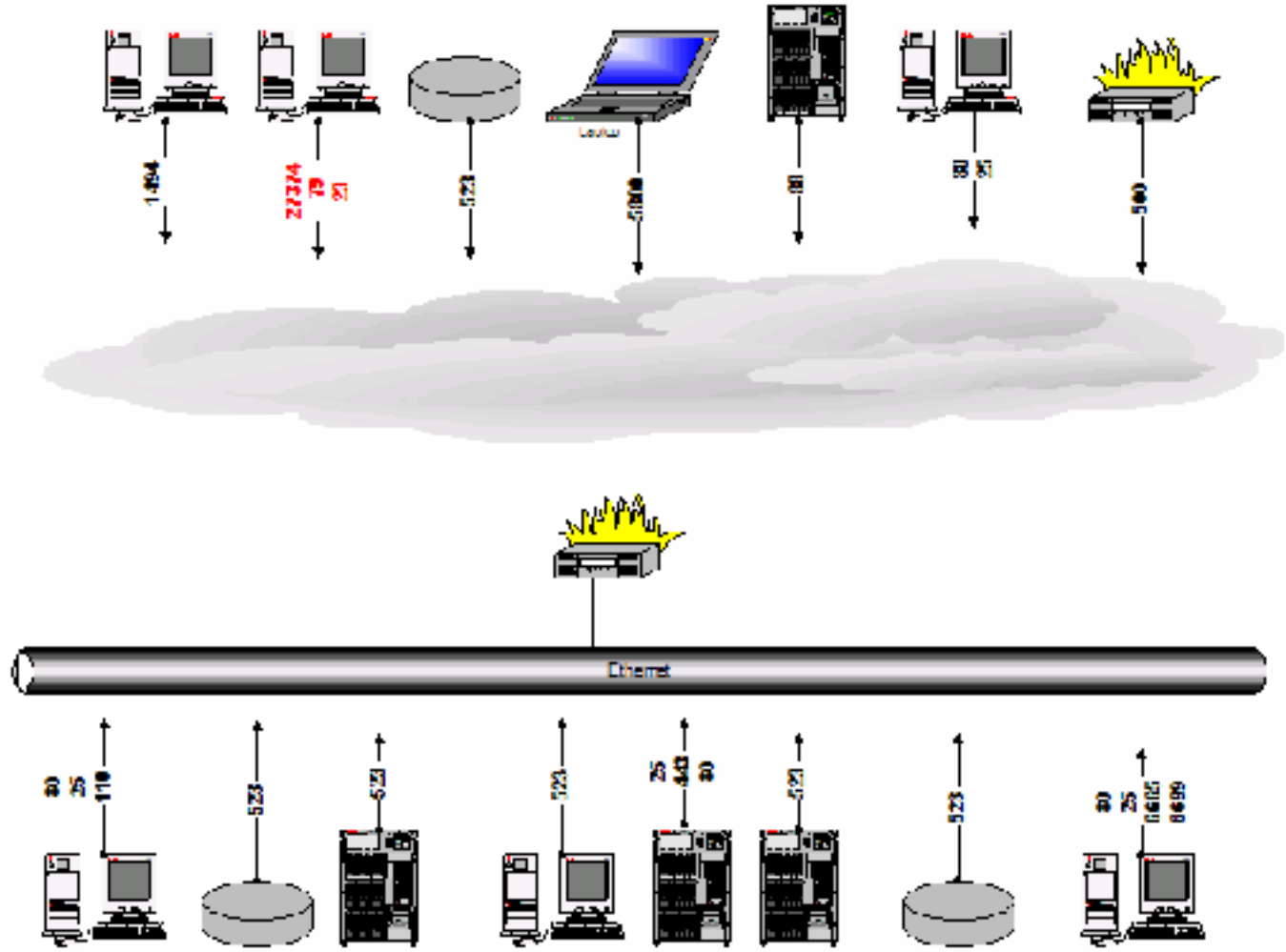
Incident response team

Be prepared to act in the event of an attack. Good documentation on how to respond will help in a high-pressure situation. Appoint the best person to lead the team, which does not always equal you. The roles of each individual should be defined clearly. Basic questions can be answered well in advance of an incident. How long do team member's work on the problem? Do you quarantine the affected hosts? Should we contact the appropriate authorities? Most people would agree that you do not want to deal with these issues in the midst of trying to figure out what went wrong, and how to fix it. After the initial shock of a system compromise, senior company officers will be looking for calm heads that can process the events, react, document actions, and return the site to a production mode quickly. A good resource on how to form an incident response team can be found at http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

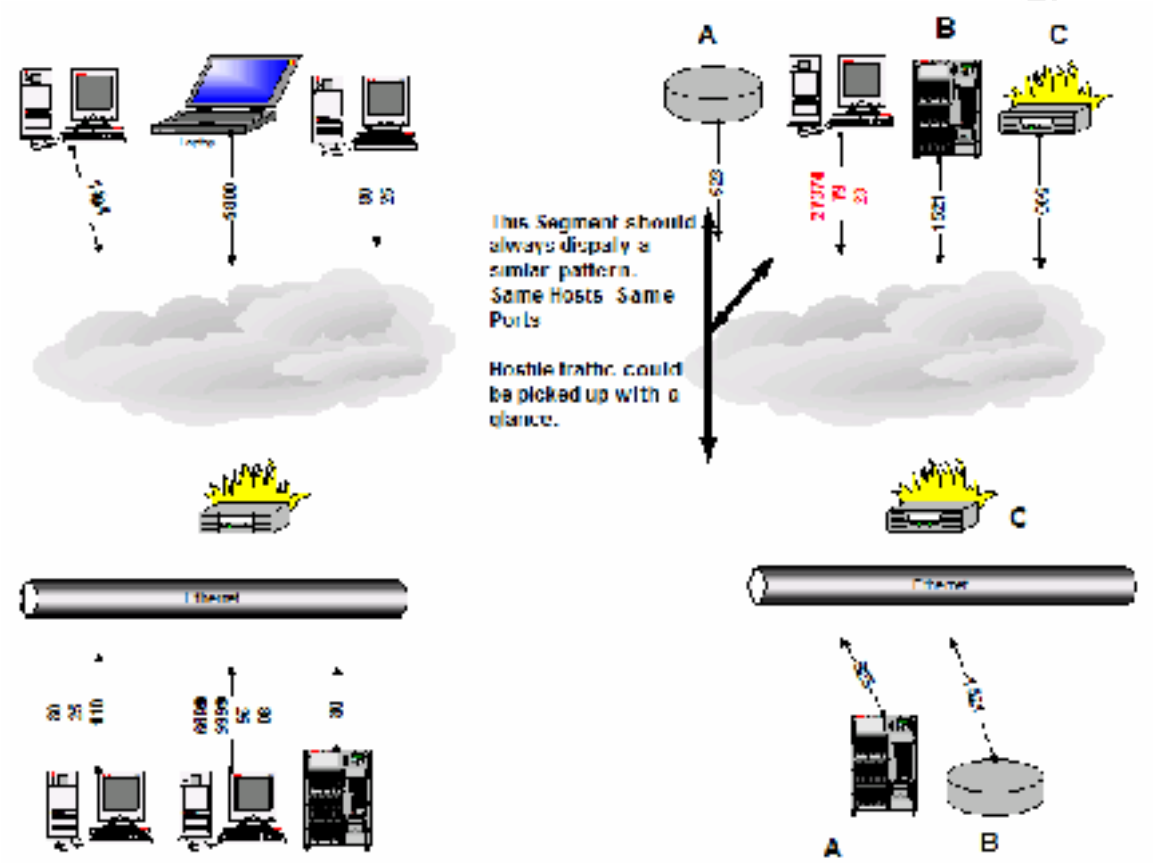
Segment Data Traffic

A technique that could be helpful is separating data services. As businesses extend internal processes to interact with external systems, Internet traffic crossing networks looks like downtown any big city. Different types of packets shooting back and forth, different ports, hosts, and subnets. Most firewalls allow you to look at traffic in real-time via a log and some provide a visual interface. With all of the services crossing through the same point, it is very difficult to notice abnormalities with a glance. Analyze how much bandwidth you need for mail, web browsing, and critical production services. If an alternate data line such as an ISDN or DSL is available route, web and mail services though this line. If you segment specific services for critical business applications on a different data line, you can define the traffic pattern. Many times this traffic is communicating with a fixed host. It could be local clients verifying credit card information with a payment provider, or a database sending and receiving updates from an off site source. These types of transactions can be defined, as they do not typically deviate from a fixed pattern. It would be an advantage to have a clear view to quickly spot abnormal traffic. Below illustrates two contrasting views of data traffic.

Site A - All services passing through a single point. Where is the bad guy?



Site A – Services segmented between and existing T1 and a 2nd DSL line.



IDS

If you tap on the glass, long enough it is bound to break. According to a CIO.com survey of 600 IT professionals only half would know if their company's infrastructure was under attack. (7) Question 2 should have been what do you plan to do about it. Put into operation an intrusion detection system should be the answer. Most administrators agree that no matter how good the perimeter defenses systems could still possibly be breached, because of the complexity and evolving nature of attacks. There is also a school of thought that the initial breach is not always the end game. How you identity the attack, respond to it, and precisely how fast is a very important step in defense. Many attackers probe networks looking for vulnerable systems, sometimes only to launch a much larger attack. The ability to have a system alert you to hostile patterns is invaluable. An IDS system does in minutes what would take a very well trained, attentive person, hours to complete. While there is a large number of products on the market that range from freeware to commercial, you should study up on IDS before you make a decision. You can find a tutorial at: http://www.securityfocus.com/infocus/1520

Audit Application Security during the Development Cycle

Some companies define e-commerce as publishing their internal applications, with little modification to the Internet. Outside of some basic security measures, these applications for the most part are not audited. This is also a problem with consultant provided custom software and pre-packaged applications. One of the first arguments from the developers will be that it will slow down the product cycle, so you will undoubtedly need support from management on this issue. You should point out that it is more cost effective to tackle these issues during development. Some companies will not want to address this issue but give it a shot anyway.

Audit Data Centers

Today many companies outsource various business processes to data centers, for the most part to secure the data. Some data centers attempt to woo company executives with the military look. Servers in former bank vaults, secured with barbed wired fences, and really cool retinal scanners. Security consultant James Foster of Guardent states "nearly every corporate Web site that's ever been hacked was in a data center." Well the key is just because its looks good you need to check under the hood. You should at minimum request data about past security incidents. Ask questions about audit schedules, system patch procedures, and intrusion detection capabilities.

Consolidate logs

Companies continue to add services but the personnel are rarely increased. With VPN deployments creating the bridge to branch office networks, administrators are forced to defend multiple locations. Typically, these sites contain various network hosts that generate events, which are logged. Some sites completely neglect the task of reviewing log files, not because they feel the information in insignificant, but because it is, time consuming. One helpful technique to handle the additional load is to consolidate device log files. To be able to see all of the recorded events from multiple sources in a single view will enable you to cover more ground efficiently. As you become accustomed to scanning log files, an abnormality will pop out quickly. Some of these tools have IDS like features with the ability to send alerts on configured events. There are products on the market with different features and some of these products have overlapping features of other security products. The suggestion is not to use these tools in place of IDS options, but rather as a way to actually maintain multiple log files. Listed below are links to two different approaches of this practice.

*e*Trust Audit - http://www3.ca.com/Solutions/Product.asp?ID=157
Event Reporter - http://www.eventreporter.com/en/Product/

The Inside Threat

While external attackers grab most of the headlines, insiders account for an estimated 85 percent of information theft. (9) Wave the flag on documented data like this to support initiatives you want to implement. Many people consider external threats the larger challenge but hosts behind the firewall should not be ignored. Developing internal access controls that can be audited should be considered. The negative exposure is endless when it comes to internal users since they do not have the perimeter defenses in front of them. Try limiting network rights by user groups, and have a utility in place to alert you when someone attempts to access a restricted file or directory. You might also want to check to make sure no one has installed a sniffer on your network. If you work at a site that allows users to download software and install it locally this could very well be a possibility. Even commercial network traffic products are available for a trial period and they are not very difficult to use. Employees can also do harm with software such as gnutella which can circumvent firewalls. It has been proven that attackers can manipulate this type of connection to attack internal networks. So the point is, spend some time working with the network administrator to get a measurement of the internal risk, and ways to work against it.

Security Training

If you are serious about keeping your site secure continuous training is a necessity. Peeping into group forums and breezing through a few web seminars may be helpful, but when trying to keep up with attackers you have to get solid training from people who do it all the time. Do not underestimate the effort it takes to attain and maintain security knowledge when talking with management. It might also be a good idea to convince key staff to attend a targeted training session about security. The SANS institute offers a good security brief targeted to managers. You can find SANS training and other sites dedicated to security training at the following links below.

http://www.cert.org/nav/index_gold.html
http://www.rsasecurity.com/training/
http://www.SANS.org/newlook/home.php

Quick Tips

- *Subscribe to a security periodical*
  Half the battle is keeping up with the latest vulnerabilities. Getting in the habit of reading security alerts, and scanning security related resources will allow you to react quickly to news that affects your site.

  http://www.sans.org/snb/index.htm
  http://www.securityfocus.com
  http://vil.nai.com/vil/content/alert.htm
  http://www.incidents.org
  http://www.sans.org/newlook/digests/newsbites.htm

- *Keep software and systems patched*
  Many patches take minimum time to complete and some vendors have setup mailing lists to alert customers to fixes. Find similar resources like the examples below that are relevant to your site.

  Oracle Security Alerts
  UNIX and Windows Alert Service
  Microsoft Security Bulletins

- *Lock Down Desktops*
  End-users can turn your firewall into Swiss cheese if you let them. If your firewall by default allows all connections out, be aware of the many possible ways employees can place your site at risk. Locking down the desktop allows you get a handle on what software is installed.

- *Don't publish the system audit schedule*
  If you do not have the luxury of locking down the desktop, users will have the ability to install and more importantly uninstall programs. If you send out a company wide e-mail on Wednesday, shouting that the machines will be audited Monday, most unauthorized programs will be removed by Thursday.

- *Additional e-mail restrictions*
  Limit the size of file attachments. Have you ever wondered what would happen if someone sent multiple e-mails to your mail server with 500Mb attachments?

  You should also block the following extensions:
  com, vbe, dll, ocx, cmd, pif, lnk, hlp, msi, msp, reg, nws, asd, cab, shs, scr, chm, wsf, wsh, eml, hta, vcd, vcf, eml

- *Change the administrator passwords*
  As silly as this seems, some sites keep the same administrator password for years. Even after former administrators and consultants, leave the company.

- *System services and accounts*
  Audit default system accounts and disable unnecessary services.
  When human resources confirm terminations delete user accounts in a timely fashion.

- *Modems*
  Sometimes the Achilles heal of networks, as nearly every computer comes with one. Try to make a case to end the use of external modem connections by offering secure connections you can control though the firewall.

References

1. The CERT® Coordination Center. "Cert/CC Statistics 1988-2001." 10 January 2002. URL: http://www.cert.org/stats/cert_stats.html (2 Feb. 2002).
2. Berinato, Scott. “Alarmed: Coming up ROSI.” What’s the Return On Security Investments? 26 October 2001. URL: http://www.cio.com/security/edit/a102601_rosi.html (2 Jan. 2002)
3. The CERT® Coordination Center. "Cert Advisory CA-2001-11 sadmin/IIS Worm." 10 May 2001. URL http://www.cert.org/advisories/CA-2001-11.html (24 Jan. 2002).
4. Computer Economics. “2001 Economic Impact of Malicious Code Attacks” January 2, 2002. URL: http://www.computereconomics.com/cei/press/pr92101.html (18 Jan. 2002)
5. Honeynet Project. “Honeynet Project Overview” Know Your Enemy. 1 February 2002 URL: http://project.honeynet.org/speaking/ (6 Feb. 2002)
6. Scalet, Sarah. “Will Security Make a 360-Degree Turn?” 6 December 2001. URL: http://cio.com/security/edit/a120601_spending.html (25 Jan 2002)
7. Ware, Lorraine. “CIO Security Worksheet” 12 August 2001. URL: http://www2.cio.com/research/surveyreport.cfm?id=21 (14 Jan. 2002)
8. Pizzo, Stephen. “Health Care’s Napkin Network” Gotcha! Securing Records on a Network. 1 January 2002. URL: http://www.baselinemag.com/article/0,3658,s=2101&a=22257,00.asp (19 Jan. 2002)
9. Ulsch, MacDonnell, Steinert-Evoy, Scott. “Internet Wake-up Call” Are Financial Institutions Ready for Cyber Terrorists? URL: http://www.pwcglobal.com/extweb/indissue.nsf/2e7e9636c6b92859852565e00073d2fd/efc7f78cb183552d8525688d004d3fb0/$FILE/Ulsch_art.PDF (3 Feb. 2002)