Global Information Assurance Certification Paper

GIAC Enterprises
Security Policies & Procedures

Simon J Oliver
GISO – Basic Practical Assignment
Version 1.0 (October 30, 2001)

Contents

Assignment 1: Describe GIAC Enterprises

Description of GIAC Enterprises

GIAC Enterprises is a medical products distributor, shipping a limited range of specialized products direct to customers' homes. They have close working relationships with both the manufacturers of the products they distribute, large managed care payers, as well as with the customers themselves.

The company does business across the Continental USA, primarily from its Head Office facility which has 300 client-facing staff, involved in order processing, telephone support, and reimbursement issues, plus associated support staff. This site also acts as the main data center for the company, hosting the company's internet site and related services, plus file and print servers, and a specialized database/back-office system for processing and tracking orders and insurance claims.

The company also maintains premises in several other states. There is one major branch office, with approximately 50 staff – which has some servers of its own – but which draws most of its computing resources from the Head Office, via a Frame Relay WAN. In addition there are four other small sites scattered across the USA, with three staff each. These sites' IT requirements are relatively modest, and connectivity to Head Office is provided via VPN connections over the Internet.

IT Infrastructure

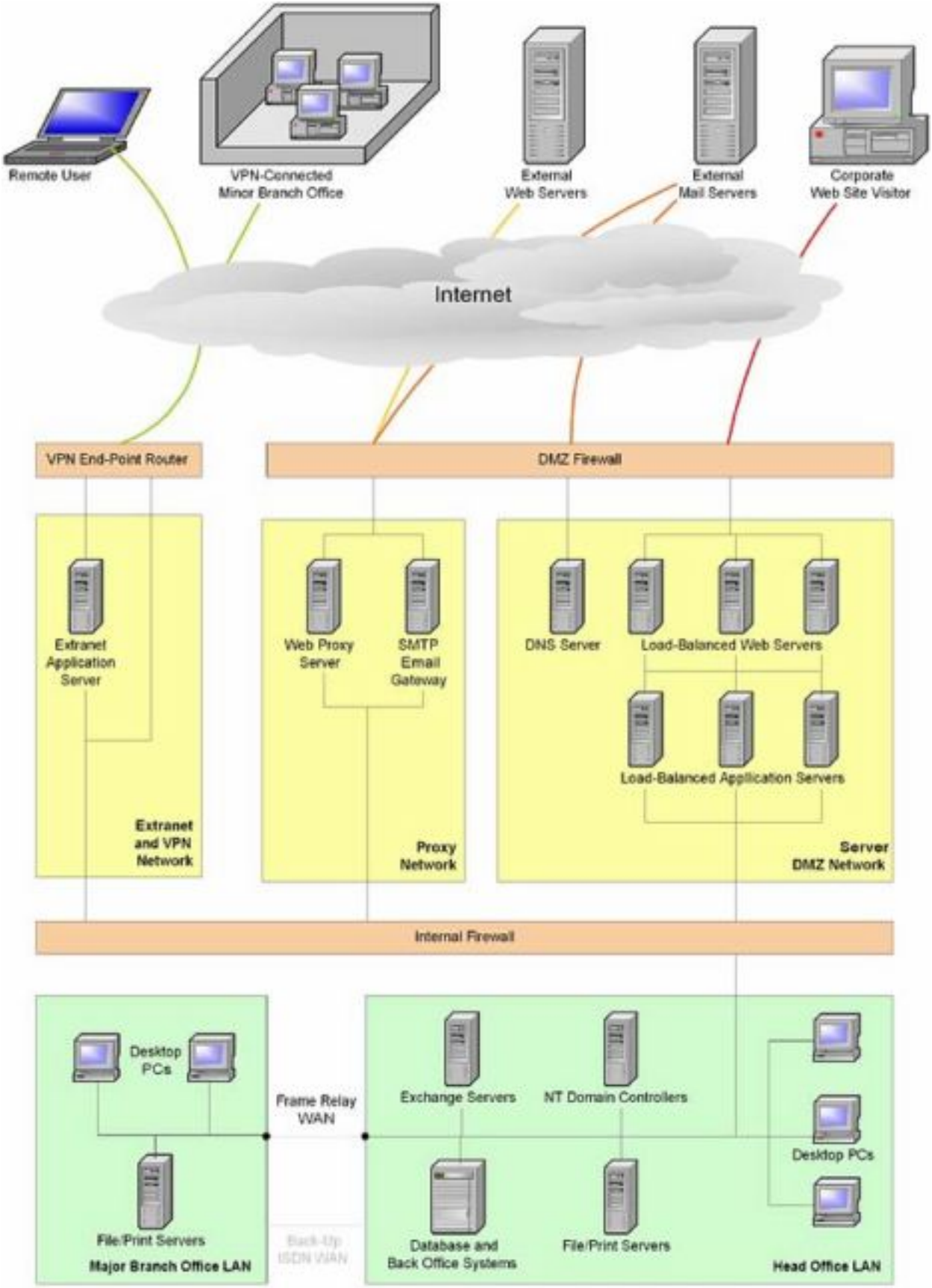
With the exception of a terminal-based AS/400 back-office order-processing system, GIAC Enterprises' IT Infrastructure is based on Microsoft Windows. A conceptual diagram of the company's network is shown on the next page.

At its heart is the Head Office LAN, consisting of approximately 350 desktop PC's, plus 8 Compaq ML300-series servers providing a range of services, all connected via a 100BaseT switched Ethernet network.

At this site, as at all others, all desktop PC's are Intel x86 hardware, running Windows 98, whilst with one exception, discussed below, the servers are x86 hardware, running Windows NT4.0 SP6a, with additional hotfixes as appropriate. Standard services are provided from this LAN, including Domain Controllers, and File and Printer sharing.

The company's core transaction processing system is also housed on this site, and comprises a custom AS/400 application which provides complete order processing and tracking capabilities, plus integrated insurance-claim, accounting and reporting functions.

The Major Branch Office has approximately 60 desktop PC's, plus 2 servers providing local file and print services. It is connected to the Head Office LAN via a full T1 Frame Relay Circuit.



The Head Office site also provides three types of Internet-facing connectivity, each partitioned into separate subnets to enhance security and ease of administration. These are shown towards the top of the diagram on the previous page, and comprise an Extranet/VPN network, a web/email proxy server network, and a web and application server DMZ. These networks are separated from the company's LAN/WAN by a packet-filtering firewall (a Cisco 3600-series router, with IP Filtering capabilities), and from the Internet by one of two devices, as discussed below.

Considering each of these networks in turn, the first is the Extranet/VPN network, which is fronted by a Nortel Contivity 1500 VPN server which provides a connection end-point for IPSec tunnels, whilst blocking all other non-tunneled traffic. It provides VPN and data-transfer services to three distinct user groups: minor branch offices, individual remote users, and business partners. These applications are discussed further in the *Business Operations* section, below.

The Proxy Server network is a mini-DMZ, providing gateway services for in-and-outbound SMTP email, and outbound web and ftp connections for all users – at Head Office and all the branches. Traffic passing through these proxies is automatically scanned for viruses, and other harmful or inappropriate content. This subnet is connected to the Internet via a CheckPoint Firewall, which also protects the main DMZ.

The DMZ's firewalled Internet feed is connected to a suite of hardened web servers running Windows NT4.0, and IIS 4, with load-balancing provided by Resonate Central Dispatch. These devices are dual-homed, and the second NIC on these devices has a non-world-routable IP address, and is connected to a private DMZ subnet which also houses the Application Servers. These are also hardened NT4 devices, running Apple WebObjects, and using that product's built-in load balancing capabilities.

Connectivity from the Web Servers to the Application servers is via an IIS ISAPI plug-in which proxies the user's connection back to the WebObjects boxes. Those non-publicly accessible servers alone have privileges to connect back through the internal firewall to any data sources that they may require, such as the AS/400.

Business Operations

As a specialist medical distributor, much of GIAC Enterprises' business involves the collection, storage and use of Individually Identifiable Healthcare information – i.e., patient medical records, and related shipment data. As a 'covered entity' under the Health Insurance Portability and Accountability Act (HIPAA), GIAC is under a moral and legal obligation to protect that data from unauthorized disclosure. This situation is complicated by GIAC's close relationship with business partners such as manufacturers, Insurance companies, and major Clinics, all of whom have legitimate needs to access some of that data – whether at the level of individual patients, or aggregated.

The smaller branch offices also require cost-effective access to core data systems via remote connectivity, as do remote users such as senior management and sales staff, in order to conduct business when travelling. In both cases, the patterns of application usage and access are broadly similar to that required by comparable users on the Head Office LAN.

In order to meet these data access requirements, GIAC provides the following mechanisms:

- The four minor branches comprise only desktop PC's, and are connected to Head Office via a gateway-to-gateway VPN circuits, using remote Nortel Contivity 100 devices connected to 192kbps SDSL connections.

- Approximately twenty senior management and sales staff are provided with company-owned Laptops, running Windows 2000 Pro. These also connect to Head Office via VPN connections – in this case, these are client-to-gateway connections, over dial-up 56kbps feeds, and utilizing Nortel's custom IPSec Client software, which provides for closer integration with the Contivity system at Head Office than is offered by Windows 2000's native IPSec system.

- The exchange of sensitive business data and/or confidential medical information with business partners is conducted over IPSec-based partner connections from the Contivity 1500 to a compatible connection gateway on the partners' network. A dedicated Extranet server on the VPN network provides various communication mechanisms, such as ftp file uploads and downloads, and web-based custom applications, for this limited audience, without exposing this data to an unnecessarily-large external audience on the public Internet, whilst avoiding the need to directly expose internal systems to business partners. Some of these exchanges are continuous real-time transactions, some are occasional, on-demand updates, whilst others are batched daily or weekly, depending on the specific need.

It should be noted that real-time intrusion detection systems are run on the VPN, DMZ and LAN/WAN networks, in order to monitor, report and potentially control suspicious activities.

Much of the Company's direct contact with patients is via the telephone, in what can broadly be described as a 'call-center' operating environment, driven by the AS/400 application. Email is also widely used for patient and business partner communications, although care has to be taken to avoid transmitting sensitive information in the clear via publicly accessible email servers.

Increasingly, additional real-time customer service and ordering functionality is provided via GIAC's web site. This provides a range of static marketing information, plus password-protected applications which allow patients to order online, and check order status.

Outbound Web access is also a crucial tool for research purposes, and is provided for approximately 20% of the company's staff, across all locations, where there is a business need.

As noted above, GIAC Enterprises is covered by the HIPAA legislation. As such, the company will be required to meet certain deadlines between the Spring of 2003, and early 2004 for being compliant with certain federally-mandated standards concerning patient's rights to privacy of medical information, and the standards of security used to ensure such information remains private. Furthermore, under a somewhat unrelated area of the HIPAA legislation, GIAC will be required to support standard X12 EDI transactions for exchanging medical encounter and claim information with Payers and other partners. At present, such exchanges are conducted using

dedicated dial-up modem connections to a 3rd party clearinghouse/VAN. However, in future, it is likely that these transactions will also be transmitted over a Internet-based VPN.

Aside from the capabilities provided by the AS/400 system, the bulk of the remaining application requirements for the company are covered by the Microsoft Office suite, which is licensed for all users.

Additionally, the Company's IT staff are responsible for desktop support, business continuity and disaster recovery planning, and day-to-day server administration and data back-ups.

Assignment 2: Define Security Policy

Areas of Risk

Given the nature of GIAC's business, and the operational requirements discussed above, several key security issues have been identified which must be addressed by suitable policies and procedures. These include, but are not limited to, the following:

- DMZ system vulnerabilities
- Viruses and related malware
- Laptops and Remote access
- Inappropriate Use of the Internet
- Security Incident Response

Each of these is discussed in more detail below.

DMZ systems vulnerabilities

Overview of Threat

The Company's Internet-exposed systems need to be secured against known vulnerabilities (particularly remotely-exploitable ones) through application of appropriate system architecture and configuration options, and installation of OS and application software patches. Failing this, the machines are likely to be compromised, leading to denial of service, theft of data and/or loss of data integrity, and consequent damage to the company's reputation.

Relevance to GIAC Enterprises

GIAC Enterprises hosts its own DNS, Web Sites, online applications, and SMTP services. As such, these systems are in important communication tool for GIAC systems, directly facilitating over one hundred thousands of dollars in business revenue each day, on average. Furthermore, some of these systems are intended to provide authorized users with access to sensitive information.

In general terms, in the event of these systems being compromised, the systems could be rendered temporarily or permanently inoperable, resulting in a loss of service, and hence revenue, or security measures may be bypassed, resulting in unauthorized disclosures of patient information.

Potential for Damage

High. Depending on the precise vulnerability, and the manner in which it is exploited, there are any number of possible outcomes, including:

- Root compromise of publicly-accessible web servers, allowing web content to be modified or deleted – possibly causing confusion to our customers and/or embarrassment to the company.
- Compromise of application servers allowing application logic to be changed, or authentication tokens stolen or bypassed, resulting in unauthorized access to data

- Installation of a back-door program allowing on-demand access to the systems in future, or a network-scanning worm, either of which allow the company's servers to be used as a base for attacks on external systems: again resulting in embarrassment and/or legal liability.
- Hi-jacking of DNS servers; causing traffic to the company's Internet servers to be directed elsewhere
- Various mail-relay exploits, allowing UCE or malicious emails to be sent to internal or external addresses, possibly with the appearance of being 'official' GIAC mail.
- Denial of service attacks against any or all of our servers causing services to become unavailable to bona fide users.
- Given the importance of our patients maintaining faith in GIAC as a trustworthy supplier, the potential business impact of a compromise of publicly accessible systems is very great. The immediate short-term loss of revenue resulting from unavailability of online ordering systems is small compared to the potential for a longer-term loss of business and goodwill resulting from a loss of customer confidence in our ability to keep their medical records secure.
- Once the HIPAA regulations are in force, there will be legal penalties for breaches of security – including per-incident fines, and jail sentences.

Likelihood of Exploit

High. New exploits are reported daily in forums such as Bugtraq, NTBugTraq, and through organizations such as CERT and SANS (see *References* section for details). Over the past year, it seems the time between discovery of a vulnerability and availability of an exploit tool is decreasing; requiring prompt attention to vulnerabilities as they are revealed, and allowing a larger audience of less-skilled miscreants to attempt to exploit the vulnerability for a longer period of time.

With automated tools, and self-propagating worms (such as Nimda or Code Red), the base of attacking systems can quickly become very large, ensuring that any Internet accessible system is likely to be probed for a vulnerability within a matter of days of the exploit being introduced – even if the basis for targeting the system is purely random, based on IP address. If the underlying vulnerability itself is newly-discovered (which in the case of Nimda and Code Red, it was not) then fewer systems will have been patched and so the pool of infected systems, and hence likelihood of attack, will be even higher.

Mitigation

There are several measures which GIAC can take to protect itself against this threat, although the constant emergence of new vulnerabilities and exploits means that this is an ongoing task:

- Keep up to date with vulnerability disclosures; and evaluate the appropriate response to each as they are released
- Harden all systems prior to deployment, following guidelines from the software vendor or other credible source (see *References* section for some examples)
- Apply the principle of least privilege to ensure that only the minimum required services are running on servers, and they are only accessible to the minimum required set of users.
- Block access to all non-essential protocols and ports at the firewall
- Apply relevant hotfixes and service packs as soon as they are available and tested

- Use a vulnerability assessment tool (such as ISS's Internet Scanner – see *References* section for further details) to establish a baseline of what services are being made available, and to monitor reality against that baseline as requirements evolve, and configuration changes are made
- Deploy an intrusion detection system (such as ISS's RealSecure – see *References* section for further details) to actively monitor the network for suspicious activities
- Architect the network with layers of physical and logic security, in such as way as to minimize the impact of any one breach
- Prepare and rehearse an incident response plan to ensure that in the event of a breach being suspected, there is a well-understood procedure in place to investigate, contain, and recover from it. This will help to minimize the duration and impact of the incident.

Overall vulnerability

The overall risk to GIAC is significant insofar as there is a high likelihood of an un-patched vulnerability being exploited and causing significant harm. However, the risk can be mitigated to an acceptable level by following the strategy outlined above.

Viruses and related malware

Overview of Threat

All computer systems, including those not directly connected to the Internet, need to be protected against malicious applications (a.k.a. 'malware') such as Viruses, Trojan Horses and Worms which can cause loss of functionality and/or data if machines become infected.

Relevance to GIAC Enterprises

Given the preponderance of email- and network-aware threats that have emerged in the past eighteen months, coupled with the tightly-integrated suite of Microsoft applications and servers that GIAC Enterprises uses, there is potential for an unchecked infection to cause massive disruption to business processes.

Potential for Damage

High. In addition to threatening directly-Internet-connected systems in the DMZ, malware also poses a risk to purely internal servers, and client desktop PC's.

Aside from possible data loss as a result of malicious code that deliberately deletes file-systems or files, or otherwise renders systems unusable, it is also quite possible that corporate email servers and or network file servers could be subjected to an effective denial-of-service attack due to bottlenecks caused by massively increased traffic loads as infected systems attempt to propagate to other computers on our network.

The Exchange server in particular is an important component in GIAC's communications architecture, and is extremely vulnerable to significant downtime and data loss, as a result of explosive growth in the system's data store in the event that an uncontrolled email-aware virus is let loose on the company's WAN or LAN.

Likelihood of Exploit

High. There are a large number of viruses circulating at any one time, and as can be seen from AV vendor's bulletins (such as the Norton's SARC website – see *References* for details) significant, at least a handful of brand new viruses appear each month, quite apart from the scores of minor variants on existing viruses that emerge.

Furthermore, the recent growth of web-, network- and email-aware viruses and worms, combined with vulnerabilities in email clients such as Outlook, means that damaging viruses can spread increasingly rapidly, and potentially require little or no user interaction to trigger an infection.

Mitigation

There are several steps that can be taken:

- Deploy anti-virus (AV) software on all desktops and servers
- Patch known vulnerabilities in email clients and browsers
- Ensure that virus signatures/definitions are kept up to date on all machines
- Actively monitor AV vendors' websites for news of new threats
- Harden front-line servers, as discussed above
- Actively filter all in-bound content (emails, attachments, and web downloads) on proxy machines on the network's boundary
- In addition to scanning for known viruses (which may miss new classes of threats for which signatures are not yet available), detect and block major classes of threatening content, such as executables, wherever a clear business need for them cannot be identified.
- Deploy AV products from different vendors at different levels of the network infrastructure (e.g., one vendor on the SMTP Gateways, and another on the Exchange server or desktops). This will provide two opportunities to intercept a new virus, if one vendor releases signatures before another.
- Restrict the opportunities for employees to transfer files onto GIAC's network other than through controlled portals (such as the gateway servers discussed above) which include AV scanning and filtering. In particular, prohibit the transfer of files between home and work machines on floppy disks or CD-ROMs, unless there is clear business need, and appropriate safeguards are in place (AV protection on the home machine, stand-alone AV scanning machines, etc).
- Train all users to understand the importance of data security in general, and AV security in particular. Make sure that users understand to be very skeptical of attachments in emails, and what to do if they believe they may have received or worse still, activated, a virus. However, do not rely unduly on this training; the social engineering in many exploits can lull users into a false sense of security, such that they forget much that they have been taught. Equally importantly, no amount of training will protect users against exploits which target vulnerabilities in browsers and/or email clients to execute code without the users knowledge or consent.
- Institute a clear response procedure to identify and respond to virus outbreaks. Avoiding even a few seconds delay in shutting down affected clients and servers can make a huge difference in the outcome of a virus infection.

Overall vulnerability

Malware poses a very real threat to GIAC's information systems. Given the large number of machines that are potentially vulnerable to a new and malicious program, and the data and service loss that could result, the threat has to be taken very seriously. In view of that, GIAC must be very careful to pursue as many avenues of protection as possible.

Notwithstanding that, and given a healthily cautious approach, and the mitigations discussed above, the vulnerability can be reduced to an acceptable level.

Laptops and Remote Access

Overview of Threat

There are two related issues here: the reliability and confidentiality of connections to the GIAC LAN from public or 3rd-party networks, and the security of the laptop computers which are most often the remote end-points of those connections.

It is essential that we provide reliable, encrypted, authenticated mechanisms to support this to ensure that business operations are not interrupted, and data is only made available to the people and organizations that have a legitimate need. Furthermore, we need to minimize the impact of any security compromises that may occur on the remote end of the connections, and over which GIAC may have little or no control.

Often, the means of establishing remote access connections is from a laptop, with a dial-up Internet connection. We need to take steps to protect these machines from Internet-based threats during the time they are dialed up to the Internet (such as from automatic IP-address scanning worms like Code Red) – not only to protect the devices themselves, but to prevent them becoming a conduit by which the rest of the company may become infected.

Furthermore, the physical security of these devices needs to be enhanced, to reduce the risk of the device being stolen, and ensure that no business-critical data can be taken from the machine's hard-drive by unauthorized users.

Relevance to GIAC Enterprises

As discussed above, under '*Business Operations*', several different user communities need to be able to access some or all of GIAC Enterprises' computer systems from off-site locations.

In addition, several employees have company-provided laptops which they use when travelling on business, not least for the purposes of being able to establish remote access connections to GIAC's LAN/WAN. Typically these are senior executives or sales-support staff – who may have confidential business information and individual's medical information, respectively, stored on their hard drives.

Potential for Damage

Medium-High. As discussed above, GAIC has to protect the confidentiality of the medical records that it holds, as well as its confidential and proprietary business information. If this information were to fall into the hands of an unauthorized user – be it a competitor, a supplier, or

a private individual – a great deal of damage could be done to the company's competitive position, and equally importantly, its reputation with business partners and suppliers. This damage could occur as a result of either an observation of data in transit, a failure in GIAC's authentication and authorization systems (allowing access to the wrong information, or too much information), or as a result of physical theft of a computer – especially a laptop – on which the data resides.

At the same time, this issue represents a balancing act, since the authentication and authorization mechanisms in place need to be reliable and not unduly impede the information flows required by GIAC's business model.

Likelihood of Exploit

Medium. This issue is less likely to be exploitable by an automated attack, or by someone with little technical knowledge. Even in the event of a random laptop theft, the sensitive data will probably be a less significant target than the hardware, and as such may simply be wiped.

This vulnerability is more likely to be a concern when exploited by someone with a specific agenda, looking to access the company's data for it's own sake, or to cause embarrassment to the company.

One aspect of this issue might be considered high-likelihood, however: the possibility that the machine used for remote access might be susceptible to a virus or backdoor that is installed when it is dialed-up to the Internet, and so be used as a point of entry to the corporate network when it establishes a VPN connection. This is a particular concern given the relative difficulty of ensuring that remote machines have adequate AV protection, since they may connect infrequently to the corporate network.

Mitigation

Several approaches can be combined to address these issues:

- Employ the principle of least privilege: ensure that remote access is provided and maintained strictly on the basis of business need, and on both ends is limited to the precise hosts and services that are required. Where possible, use pure 'screen-sharing' technologies such as Windows Terminal Services, to restrict the opportunities for harmful data to flow into the network from outside.
- When connecting to a business partner's network, over which GIAC has no direct control, we should require evidence of the security measures in place at that location (and under HIPAA regulations, may be required to formalize this in a business partner and/or chain-of-agreement)
- Encrypt data in transit using proven authentication algorithms, with strong keys, in implementations that are generally considered robust.
- Authenticate users using strong two-factor methods such as smartcard-based certificates or biometrics.
- Where userid/password authentication is unavoidable, ensure that passwords are strong.
- Security harden laptops before they are issued to employees, and lock-down the configurations to prevent accidental or intentional changes which might weaken security.

- Where feasible, prevent remote access users from connecting to other internet sites from the machines that they use for remote access, and require and ensure that up-to-date AV tools are in place on those machines. This may involve a combination of routing and network settings at the OS level, or installation of personal firewall software.
- Avoid 'split-tunneling' configurations, such that a VPN-connected device is not simultaneously visible directly from the Internet at large, and so cannot act as a router onto the company's private network.
- Implement a network architecture which facilitates and encourages the storage of all sensitive data (whether for laptop users, or LAN/WAN users) in a centralized repository which is logically and physically well-secured – such a backed-up, patched, file server with tight ACL's in a locked server room.
- Deploy tools to strongly encrypt data on laptops, so that where locally stored data is unavoidable, it will be inaccessible if stolen
- Deploy intrusion detection tools on remotely-accessible networks to identify potential misuse
- Train users to appreciate security issues, and keep passwords secure
- Set and enforce policies regarding the way in which remote access will be requested, deployed and used. Review access rights periodically to ensure that they are still appropriate.
- Consider providing security hardware such as tethering kits for laptop users travelling outside of the office

Overall vulnerability

Properly implemented gateway-to-gateway VPN connections provide a relatively strong, secure channel for data to flow between GIAC's sites, and to be exchanged with business partners.

Individual client-to-gateway connections from laptop users (or home PC users) are more of a concern, and need to be tightly restricted in order to maintain a secure environment.

Inappropriate Use of the Internet

Overview of Threat

The Company is accountable for the uses to which its computer systems are put, and especially the actions of its employees in that regard. Care must therefore be taken to ensure that such uses are appropriate in the context of everyday business operations, and will not expose the company to legal liabilities or damage the company's reputation or business relationships.

One risk is that the content may be in-and-of-itself illegal – either in the USA, or in other jurisdictions to or from which employees might transmit it. Examples might include pornography and inflammatory, racist or otherwise extreme, political propaganda.

Another issue is that even when the content is not inherently offensive or illegal, the company may also be at fault for allowing breaches of copyright resulting from the distribution and storage of electronic media using the company's resources – including screensavers, photos, mp3 files, etc.

Most likely, however, is the scenario where offensive content – such as a racist or sexually explicit joke, or a pornographic image – is distributed either internally or externally, and causes

offense to a fellow employee. In those cases the company could be legally liable for allowing sexual or racist harassment of its employees.

Additionally, use of company systems for inappropriate, or non-business related activities may increase the company's exposure to other threats such as viruses, insofar as it involves downloading and installing programs, or visiting non-mainstream, insecure web-sites.

Even where no harm is done to a third party, and the behavior or content does not constitute a threat in and of itself, non-business use of the Internet it can result in a loss of productivity if significant company time is wasted. This may be because of time spent online doing non-business-related tasks, or due to the amount of support personnel time required to correct technical issues caused as a result of installing downloaded software that may not be actually malicious, but may still conflict with legitimate business applications.

Finally it should be noted that the threat may not always be the result of internal abuses. For instance, UCE for 'adult web sites' can in some cases be extremely explicit, and cause significant offence to the recipient.

Relevance to GIAC Enterprises

GIAC has several hundred employees, and like any medium-sized or large company, these represent a diverse group of individuals, with differing standards and agendas.

As such, there is a real risk that at some point the actions of one or more individuals might cause offence, or harm (be it financial, physical, emotional, reputational, etc) to employee, or a person or company outside the organization. The company needs to use its best endeavors to prevent this from happening.

Also, in the aggregate, the person-hours lost to frivolous web surfing and personal email can become significant.

Potential for Damage

Medium-High. As noted above, the company is responsible for the actions of its employees, and cannot a priori guarantee that those people will always act in an appropriate way.

When company resources are misused, the potential exists for GIAC to face legal and financial penalties, and a significant loss of goodwill from customers and business partners.

Furthermore, in addition to the abuses discussed above, it should also be borne in mind that significant commercial harm could be done by a malicious employee deliberately disseminating commercially sensitive information – e.g., to a competitor.

Likelihood of Exploit

High. The Internet in general and World-wide web in particular is still in its infancy, and standards of acceptability, and a means of enforcing them are far from uniform. People's attitudes, and sense of responsibility, towards the medium are also still evolving. The availability of questionable content, combined with the relative speed and ease of distributing it –

particularly through email – mean that in the absence of firm controls and especially in a large organization, someone, somewhere, will do something inappropriate.

Mitigation

A combination of several approaches can effectively mitigate the risks – not least in the event of a serious breach, by providing evidence that the company was not negligent in ignoring the issue, and took reasonable steps to prevent it.

- Establish a clear policy on what is and what is not acceptable
- Undertake training for all employees to communicate the letter and spirit of that policy
- Establish automated email-filtering (such as Baltimore Technology's MimeSweeper range – see '*References*' section for details) to strip out multimedia files or other types of content that can be identified as not business related (in addition to the anti-virus filtering discussed above).
- Implement an access-list based filtering system on web proxy servers, so that users can only access web sites which are consistent with their business need.
- Utilize operating-system level controls (such as Windows NT/2000's concept of policies and access rights) to prevent users from modifying system configurations or installing unapproved software.

Overall vulnerability

In a large and diverse organization, it can be difficult to juggle legitimate business needs with clear guidelines against misuse – especially when trying to implement restrictions on web access or automated email content filtering. In general however, using the measures outlined above, a reasonable balance can be struck most of the time, protecting the interests of the company and its employees, customers and partners, whilst allowing normal business functions to continue.

Security Incident Response

Overview of Threat

Rather than considering a threat per se, this section deals with a related 'area of concern': the need for a rapid, effective and appropriate response when a security breach is suspected.

Information systems Security is a continuous process, as system configurations change, and new vulnerabilities are constantly being discovered, and leveraged by easily-applied exploits that require little expertise and can be used by an increasingly large audience of miscreants.

As such, it is not reasonable to expect that a security infrastructure, however well conceived and implemented, will never be compromised. Therefore, it is vital that well-defined and rehearsed incident response procedures are in place such that any security breach can be defined and contained quickly, in order to minimize the potential for damage, unauthorized access to data, and/or loss of data integrity. The procedures also need to consider the implications and requirements for gathering forensic evidence of the incident in order to prosecute the offenders through the legal system.

Relevance to GIAC Enterprises

The customer and business data that GIAC holds is crucial to its business processes and ongoing operations. As such, the security of that data – and public confidence in that security – is paramount. At the same time, GIAC operates a moderately complex WAN including VPN access from multiple sites, users and companies, in addition to conducting business directly on the Internet.
As such, there is a small but significant risk that GIAC will be exposed to a successful security exploit from either an external or internal source.

Therefore, it is vital that well rehearsed procedures are in place to respond when an incident does occur in order to allow faster resolution with minimal damage.

Potential Benefits

The aim of the response procedures is to mitigate the damage done by other security exploits, such as those discussed above. By planning our responses, we can further reduce our exposure in the event that a breach occurs, and so increase the cost-benefit equation and reduce the effective risks associated with providing inherently risky, but nonetheless business-critical, services such as business partner VPNs and Internet access.

Components of the Plan

A successful plan will need to pay attention to a number of areas:

- Roles and responsibilities: who will be doing what during an incident. This includes not just technical and incident management roles, but also who will be responsible for liaising with law enforcement and/or the public and media as necessary.
- Escalation mechanisms and triggers: who gets involved when, who involves them, and how all parties can be contacted at any time. At what point should law enforcement officials be involved.
- Approach: what are the aims and priorities of the response team, or what are the criteria by which they can be determined on a case-by-case basis. For instance, should the primary goal be to minimize damage or downtime, or is the aim to gather forensic evidence: these goals will not always dictate the same course of action.
- Documentation: how should the investigation be documented, especially where the intention is to seek prosecution of the perpetrator. How should physical evidence be gathered, and a chain of custody established?
- Specific threat responses: in the case of specific identifiable threats, such as an email-aware virus outbreak, what steps should be taken to mitigate the damage, even in advance of the response team being alerted and assembled (e.g., disconnect affected servers from the network, or even just perform a hard shutdown if a graceful solution may mean that tens of thousands of infected emails propagate within the system in the meantime). Making clear the responses that are expected avoids any confusion, or the need to wait on clarification when time may be of the essence.
- Rehearsal requirements: as noted above, the plan should specify how and when practice drills will be held.
- Remediation: the plan should also lay down a mechanism for a formal review of any incidents that occur in order to identify not only shortfalls in the response plan itself, but also

to ensure that the vulnerabilities that were exploited are addressed in a timely manner to prevent a recurrence of the incident.

Furthermore, the plan will need to be readily available and understood by all potential participants, and rehearsed periodically to ensure familiarity, and make sure that everyone understands their role.

Even in the absence of actual incidents to benchmark it against, the plan should also be reviewed periodically, to ensure that it is still consistent with business goals, and new technologies, systems and known exploits.

Security Policies

This section details three security policies for GIAC, based on the risk areas discussed above: DMZ System integrity assurance (to address the issues relating to DMZ Server vulnerabilities), acceptable use of the Internet (to address the risk of inappropriate use), and Security incident response.

Note that these policy documents include references to other documents not included here, such as the *Policy Control Procedures* which discuss how policies are amended and ratified.

1. DMZ System Integrity Assurance

Effective Date and Revision History

This is Version 1.0 of this policy, and is effective January 1, 2002.

Purpose

This document addresses the need to establish and maintain the integrity of GIAC's internet-connected computer systems through a combination of careful design, audit and ongoing monitoring.

Scope of this document

The policy and procedures relate to the Internet Server Farm located in the DMZ between the external and internal firewalls, and are intended to be carried out by the MIS staff and the cross-disciplinary Information Security Management Team.

General Policy

It is the policy of GIAC to take all reasonable cost-effective steps to ensure the integrity of its eCommerce server farm and the underlying data, through an appropriate combination of the following measures:

1) Physical security
2) Network-level security
3) System-level security
4) Application-level security
5) Vulnerability assessment
6) Intrusion detection systems
7) Routine monitoring and reporting
8) Ongoing evaluation of security threats

9) Software and hardware design reviews

Specific Policies

1) Physical security

All publicly-accessible and mission-critical eCommerce systems are to be located inside a physically-secured Computer Room adhering to normal standards for such rooms, including redundant power systems, fire and flood control etc.

In practice, it is intended that this will be the GIAC Computer Room at 100 GIAC Way, and that physical access to the room will be limited in line with GIAC's policy – *Access to Sensitive Areas* – detailed separately.

2) Network-level security

At the network level, security is to be provided by firewalls in front of and behind the server farm, configured to permit only the minimum practical level of access to the servers.

From the Internet, connections should only be allowed to necessary available services, such as http servers, at specific IP addresses at ports. Administrative access should be limited to specific, designated internal IP addresses, routed through the internal firewall.

Firewall systems should be in place and tested as functional, prior to the introduction of the protected systems.

MIS should maintain an up-to-date network topology diagram, and review the architecture with the ISMT periodically to ensure that it remains secure.

3) System-level security

Operating systems should be configured with the minimum necessary services running, and non-default passwords, for the minimum necessary accounts. Account and password information should be noted and stored in a physically secure location.

All available patches should be evaluated and applied where demonstrated stable. The configuration of the system should be documented for each class of server, and recovery/config disks made. A register of installed patches and configuration changes should be maintained for each type of server.

Hosts should not be connected to the Internet-accessible network until the OS has been installed and hardened through application of patches and configuration changes. Once this configuration is complete, and before connection, a reference back-up of the system should be taken.

4) Application-level security

Applications should be installed in line with manufacturers' guidelines for security hardening. Example code and documentation should not be installed on production servers.

Security patches should be installed as soon as they have been demonstrated to be robust, in the opinion of MIS. Version upgrades should be installed in a timely manner to ensure ongoing support by the manufacturers. A log should be maintained of all upgrades and patches that are applied to any of the systems.

Where available, MIS should secure ongoing maintenance agreements with the vendors of all application software, to ensure timely availability of security fixes.

Custom-written applications should be written according to MIS's published Object Model and Security guidelines, and verified for secure design by means of design reviews, discussed below.

5) Vulnerability assessment

Vulnerability assessment is implemented using a suitable tool, such as ISS's Internet Scanner and System Scanner.

Once a baseline configuration has been run, these tools should be run at regular intervals of not more than 14 days, and the results logged. Penetration tests should be run from 3 points: the LAN, the ZMD, and the Internet. These tools should be routinely updated as soon as patches are available from the manufacturer.

The standard configuration of the tools should be recorded, to ensure that the tests are repeatable, and the configuration should be reviewed by the ISMT monthly to ensure that the tests remain appropriate. At the same interval, the entire architecture should be reviewed by the ISMT with the intention of identifying any logical flaws or previously undetected vulnerabilities.

All new vulnerabilities detected by whatever means must be reported Security Officer for assessment. Where there is a de facto significant risk, and easy fix, the Security Officer may choose to schedule the fix immediately. Alternatively, new vulnerabilities should be escalated to the ISMT for risk assessment, and formulation of a management plan.

(The ISMT has a number of responsibilities in this respect which are documented in their Terms-of-Reference document. [Not included in this practical])

6) Intrusion detection

Intrusion detection is handled through a signature-based, real-time monitoring tool, such ISS's RealSecure system. This system should be configured to monitor both network traffic and all network server hosts, and to trigger email and pager alerts to the on-call Security Technician in the event that an exploit is detected.

All such attempts should be logged, and reported to the CIO as part of the regular operational reporting by MIS. Furthermore, the on-call technician should respond to any detected incident in accordance with the separate *Security Incident Response* Policies and Procedures, which include reporting significant incidents to the CIO and CFO immediately upon detection.

This software should be kept updated with all patches and upgrades as soon as they are available from the manufacturer.

7) Ongoing evaluation of security threats

The Security Officer is responsible for monitoring relevant mailing lists and web sites to identify security threats which might affect GIAC's systems. When these have been validated, they should be escalated to the ISMT for evaluation, in the same way as for vulnerabilities identified systematically.

Furthermore, the ISMT should hold a monthly security review meeting, to evaluate the following issues and identify any changes needed:

- Network architecture – performance, reliability, security
- Appropriateness of automated monitoring procedures
- Risk assessment for new threats
- Status of ongoing risk management initiatives

The chair of the ISMT should provide a summary report to the CIO each month.

8) Routine monitoring and reporting

In addition to the weekly vulnerability assessments, MIS should also undertake a daily system availability test. This should evaluate the system from an external viewpoint, testing all major functions against a standard script. In the event of any discrepancies, these should be logged, and action taken to correct the problem.

Secondly, system event logs and major system health metrics such as process count, CPU utilization, and available RAM, should be monitored daily, and automated alarms put in place to alert the on-call technical staff in the event that a metric falls outside of agreed norms.

The eCommerce Director should prepare a monthly report to the CIO which includes the following information:

- Configuration changes
- Security vulnerabilities identified and/or addressed
- Intrusion activity detected, impact and response
- Site usage statistics
- Access speed statistics
- Site availability statistics
- Issues outstanding from design reviews

9) Software and hardware design reviews

Whenever changes are to be made to the architecture, or new applications are being developed, MIS should conduct an internal design review to ensure that the design meets strategic objectives and maintains adequate levels of security through compliance with the published Security Model.

The first review should take place at the end of the design phase, prior to detailed development. A further review should take place early in the testing phase, prior to roll out. The eCommerce Director should then sign off on the application/system prior to it being moved to production, once s/he has ascertained that the system continues to comply with its original design intent, and delivers required levels of security.

The GIAC eCommerce Project Control form includes appropriate sign-offs for the design reviews discussed here.

Responsibilities

All employees are responsible for their own conduct in adhering to this policy in the course of their normal business activities.

In particular, the MIS department staff have front-line responsible for carrying out most of the specific actions outlined here, and discussed in more detail in the specific *DMZ Systems Integrity Procedures* document.

This document also establishes some tasks for the Information Security Management Team, whose activities are more fully documented in a separate *Roles and Responsibilities* document. This standing committee is chaired by the eCommerce Director (in his/her capacity as the Data Security Officer).

The Data Security Officer for the Company is final arbiter in deciding how this policy should be interpreted and for determining the acceptability of any proposed extensions to or exceptions from the policy.

Training, Further Information, and Amendments

Specific training on the issues discussed in this policy is available from GIAC's Training Department, and is a required element of new hire orientation within the MIS department. Periodic in-service training will also be provided for all employees.

Technical enquiries regarding this policy should be addressed to the eCommerce Director.

More general queries about the operation and interpretation of Company Policies in general should be directed in the first instance to the HR department.

Amendments to this policy may be made in accordance with the MIS Department's *Policy Control Procedures*, documented separately.

Enforcement and Penalties

This policy is enforced through use of agreed log files for reporting the outcome of routine tasks and tests, which are subject to scrutiny by the ISMT who will in turn report their findings to senior management.

In the event that an employee is aware of a potential breach of this policy, they are encouraged to report their concerns to their manager. All such information will be treated in confidence, but is essential to ensure the security and integrity of the company's information systems, and hence maintain our excellent reputation with partners and customers alike.

Any breaches of policy will be investigated by the MIS department, in conjunction with the HR department, and appropriate penalties determined according to circumstances. Depending on the severity of the breach, penalties up to an including termination may be considered appropriate.

2. Acceptable Use of the Internet

Effective Date and Revision History

This is Version 1.0 of this policy, and is effective January 1, 2002.

Purpose

Use of the Internet is growing rapidly, and the GIAC Enterprises companies are actively embracing eCommerce. The commercial opportunities that this presents are going to be significant, but there are also significant costs: contrary to popular perception, providing Internet access for a business is not a cheap or simple thing to do – the cost of the connections, plus support, software and so on, can easily run to hundreds of thousands of dollars per year, even for a relatively small company. Furthermore, the largely unregulated nature of the Internet presents some potential risks to our business integrity and the safety and privacy of our patients, employees and business partners.

The policies set out here are not intended to be onerous, and certainly not to unnecessarily prevent anyone from doing their job effectively. Rather, they are designed to enable GIAC Enterprises to fully leverage the benefits that the Internet will bring to our employees and company as a whole, whilst keeping the associated costs within reasonable limits, and maintaining a secure, confidential environment for the benefit of us all.

Scope: What this policy covers

This policy applies to all employees of GIAC Enterprises (collectively, 'the Company'). It addresses employee use of the public Internet and intranet systems on behalf of the Company, or using company-provided equipment, software or connectivity. This includes the World Wide Web, email and all other such online systems and applications, and covers not just use during working hours, but also out-of-hours usage of company-owned PCs, laptops, dial-up accounts etc.

This policy also addresses the related issues of data security, encryption, and digital signatures.

General restrictions on usage

Irrespective of the specific applications and systems being used, there are a number of general caveats that all employees will be expected to observe.

Observing other corporate standards

Apart from certain technical security considerations discussed below, the Internet is essentially just another communications resource that the Company provides for employees to interact with patients and business partners. To that extent, the same common-sense restrictions that govern all other communications media also apply to the Internet. These include, but are not limited to, prohibitions on the following:

- obtaining, distributing or accessing material which is pornographic, discriminatory, or otherwise likely to cause offense;
- obtaining or distributing unlicensed software, or other works, in violation of copyright restrictions;
- making available to inappropriate recipients any privileged or confidential information about company operations, business relationships, or customers.

Personal use of a Company resource

Access to the Internet is provided to employees solely on the basis of legitimate business need, and should not be used for personal, non-business reasons in ways that interfere with any employee's performance of normal duties.

Avoiding or defeating network security and management systems

A variety of security and management systems, such as firewalls and anti-virus software, are deployed across the GIAC Enterprises Wide Area Network to prevent malicious and unauthorized access to our resources. Under no circumstances must employees modify, weaken or circumvent these systems. Where legitimate business requirements require changes to the security systems, this will be planned and managed by the MIS department.

Users accessing the Internet using standard MIS-supplied software with the MIS-configured settings will be in compliance with this requirement.

Running unapproved software or servers

Under no circumstances should users run server software on machines connected to the LAN, or install any software without the explicit approval of the MIS department.

Direct connections to Internet from behind firewall

Employees must not connect their LAN-connected computers directly to the Internet, other than via the standard LAN/WAN connections and routers. LAN-connected machines should not have modem or similar direct connections to the Internet or other non-GIAC Enterprises networks.

Web-centric issues

Audio and video

Except as absolutely required by business needs, employees must not access audio and video feeds online – such as RealAudio/Video or MPEG, AVI and QuickTime movies.
Due to the large amounts of network capacity that these applications consume, and the impact this may have on WAN usability and public access to our web site, even where there is a business need for access, permission must be obtained in advance from MIS, and may only be given on a case-by-case basis.

Disclosure of information

When using the web, employees need to be careful not to divulge confidential or sensitive information to inappropriate parties. In general, such data should never be made available to any web site – this includes divulging company information through completion of online surveys. Where legitimate information is being divulged to a business partner online – such as for online ordering or billing purposes – this should only be done using secure 'https' web sites, so that the data cannot be observed in transit between the two companies.

The recommended way for sharing sensitive data with appropriate external parties is through the GIAC Enterprises secure VPN (see separate *Remote Access Policy* for details).

Chat Applications

Real-time chat applications (such as AOL Instant Messenger and iRC,) present a number of security and confidentiality issues, and usage must be pre-approved by MIS. Under no circumstances should confidential or sensitive information be divulged through this medium

using third-party applications or web sites. This restriction does not apply to authorized use of secure chat applications for communication with customers on the GIAC Enterprises web site.

File downloads and installation

Where users are actively downloading files from the Internet, via ftp or web connections, this must be for demonstrable business reasons.

Due to the possibility of accidentally installing malicious code, back doors into our network, or simply buggy code that damages our systems, employees must not download or install application files without prior approval from MIS. Static reference material, such as pdf files may be downloaded, so long as the file size does not exceed 250K.

Larger downloads require prior approval from MIS, who reserve the right to require the user to schedule the download for outside of peak working hours, in order to minimize bandwidth concerns.

Email

Chain emails, virus warnings etc

Most scare stories, chain letters, and virus warnings distributed freely online are hoaxes and can, and should, be ignored. Users should not forward such emails to users either inside or outside the company, as it wastes network and server capacity.

'Virus warning' messages should only be attended to if they come from known MIS personnel within the company. Furthermore, the sender will have taken responsibility for distributing the message to everyone in the company who needs to know, and so there is no need for individual employees to forward the message. In order to reduce the proliferation of such messages, users must not forward such legitimate virus warning messages to addresses outside of the company.

List servers

These automated mailing lists are a valuable source of information on all matter of topics of professional interest to our employees. However, they can also generate very high levels of traffic which can swamp our mail systems.

Consequently, employees must not subscribe to non-business-related mailing lists, and should elect to receive a once-a-day 'digest' version of the list where practical. Also, where a mailing list is of interest to a number of people within the organization, you are encouraged to have one person receive the messages, screen them for points of interest to others, and forward them when appropriate. This conserves both system capacity, and the time taken to monitor the lists for points of interest.

Internal broadcast emails

In order to reduce the 'noise-level' in all of our inboxes, employees should not indiscriminately distribute 'announcement' emails to large groups of internal users without a reasonable business need to do so, and permission from their manager.

Additionally, in order to reduce the capacity these messages take up, and make it easier for colleagues to spot possible virus-carrying attachments, these messages should be plain text messages, without attachments or graphics.

Other mechanisms such as noticeboards and newsletters are often a better and more appropriate medium for many of these messages, and are less disruptive to workflow.

External bulk email

'Spam' is one of the most destructive and despised forms of Internet communication, and offers little or no commercial benefit, and the potential to do massive harm to the company's reputation. Under no circumstances may employees send unsolicited bulk email.

Selective mass mailings to targeted audiences can make business sense, but must be pre-approved by the MIS Director. Care must be taken to ensure that all such lists are 'opt-in' in nature, provide clear instructions as to how recipients can opt out, and respect any such preferences they express.

Personal email

Employees should only use company email accounts for non-business reasons in an emergency, and should ensure that any such communications are carefully worded and do not in any way appear to be from the Company per se, or to express opinions on behalf of the company. Such emails must be sent as plain text, without file attachments.

Employees must not routinely publicize their Company email accounts for non-business purposes. Furthermore, employees must understand that all emails they send and receive through Company systems are liable to be monitored, or reviewed, in the interests of quality control and security.

File attachments

The company expends a lot of time, effort and money in maintaining the integrity of our data systems, and working to prevent and contain viruses. Nonetheless, after a virus is detected, there is inevitably a lag before our security systems can be updated. And even then, automated systems should not be relied on; our employees are our greatest asset in maintaining vigilance against virus attacks.

Therefore, all employees must take care when dealing with files attached to emails, due to the risk of spreading a virus. The sender may not even realize that their computer has been compromised. Even if the email is from a co-worker, or a person who is known to you, you should be especially vigilant if the email is unexpected, and/or the subject or body of the message is not relevant to recent conversations with that person.

Employees should **never** open attachments in the following circumstances:

- where the email is personal in nature
- where the email is from a non-business contact, or on a non-business-related subject
- where the attachment is, or claims to be, an executable file such as a '.exe' or '.vbs' file

If the message appears to be of a legitimate business nature, but is unexpected, employees should still check with the sender to find out what the file is before they open it.

Due to the risk and uncertainty associated with attachments, and the network capacity that large files can use up, employees should avoid attaching files to external-bound emails wherever

possible. Files over 1MB in size may be sent to external addresses only with the express permission and prior knowledge of the MIS department.

Sensitive data

Email is an inherently insecure medium, and any message to or from recipients outside of the GIAC Enterprises companies can pass through any number of intermediary servers before delivery to the intended recipient. As such, it is relatively easy to eavesdrop on regular email communications.

In view of this, employees may not use regular email to communicate commercially-sensitive or patient-confidential information. The GIAC Enterprises VPN system should be used instead, as it is designed specifically to address these concerns.

Care in wording

As written communications on behalf of the company, email messages represent the company to our patients, vendors and partners, with the same potential for benefit, harm, and legal liability seen in any other written communications from the company.

As such, all employees should take care when wording emails and online messages to ensure that they are writing clearly, concisely and accurately, and otherwise adhering to the applicable company policies relating to disclosure, business ethics and so forth.

Use of encryption

Encryption of email using Outlooks Digital ID features, or third party systems such as PGP, offers a number of benefits for secure communication with business partners, but can also open up a number of network security issues in its own right.

As such, employees must not send encrypted messages through the email system with out the explicit consent of the MIS department. Wherever possible, the GIAC Enterprises VPN facilities should be used in preference.

Communicating online

The following guidelines must be observed when communicating via any online medium or application.

Verify the recipient

Employees should ensure beyond reasonable doubt that they are communicating with the person or company that they believe to be the case, and that the information they are communicating is appropriate for that recipient, given the standard disclosure guidelines.

Use approved, secure online systems

When any proprietary, sensitive or confidential information is being disclosed, employees must take care to verify that secure online systems are used which ensure that eavesdropping cannot occur.

Protect data

In all online scenarios, employees should carefully consider the information that they divulge, to ensure that confidential information about the company, its business or its patients is not accidentally divulged.

Read and understand material

Particularly when entering into any form of online agreement on behalf of the company, such as making a purchase or subscription, employees should take care to read and understand any and all instructions and terms and conditions. Online agreements are just as legally enforceable as other arrangements; employees should verify that they have the authority to enter into such arrangements on behalf of the company.

Act responsibly and in good faith

In all online activities, employees should act in good faith the represent the company to the best of their ability. The same requirements for integrity, professionalism and so forth apply to online communications as much as to any other activity. Employees should always behave with courtesy and consideration for the implications of their actions.

Never assume anonymity

Whatever the precise arrangements of the system you are using, employees should never assume that they cannot be personally identified. Indeed, they should always assume that they can be personally identified and held responsible for their actions, and act accordingly.

Dealing with misrepresentation

If employees find information online – on Company or third-party sites – which they believe misrepresents or otherwise harms the integrity or reputation of the Company, they should not take steps to refute the information, or otherwise take action themselves, but rather should draw it to the attention of their manager, who should in turn discuss the matter with the GIAC Enterprises Corporate Compliance Officer.

Publishing information online

Employees must not directly make available online any information about the company, its operations, or patients, suppliers or partners on third-party servers – such as message boards, chat rooms, personal web sites, etc. – irrespective of whether this information night be deemed harmful or beneficial to the company's interests.

Where employees duties involve the preparation of material for publication on the Company's own web site, they should take reasonable steps to ensure that all information is appropriate and accurate, and represents the company's interests in a positive light. Such content must be submitted for necessary approvals prior to publication, and deployed in a controlled way by the MIS staff. Further information on the approval and deployment processes can be found in the 'Move to Production' procedures, published separately by the MIS department.

Data Security

The security and integrity of the Company's information systems is of paramount importance in today's fast-paced, interconnected economy. As such, as employees have a duty to consider the security implication of their actions, and avoid any activities that they can reasonably foresee might compromise corporate systems. If in doubt, employees should contact MIS for guidance.

At a minimum, employees must keep password and other system access information secure, in order to prevent unauthorized access to our systems. Employees must only access systems for which they have legitimate privileges, and must do so in a manner consistent with their duties.

Employees must not share their password information with other employees, nor use another employee's password to access system resources.

Encryption and electronic signature technology

Digital ID certificates

The use of Digital ID Certificates is becoming increasingly widespread online. They help to identify specific individuals in a verifiable way, and can be used to enter into legally-binding contracts.

Employees are encouraged to discuss the use of such certificates with MIS, if they identify applications where they might be of benefit. However, such certificates should only be obtained and used with the prior approval of the MIS department, and employees must ensure that the personal identifying information in the certificate is correct, and accurately represents their name, job function, and company information. Use of a certificate that is incorrect or misrepresents the employee's identity is prohibited.

Do not enter into agreements online

As noted above, online business agreements are coming to have all the strength in law of more traditional off-line agreements. Therefore employees should exercise due care when entering into such agreements, and should only do so where the execution of such agreements falls within the scope of their normal duties.

File/disk encryption

Except for specific circumstances required by MIS, employees should not use encryption technology to secure files on their personal computers or corporate servers.

Where such technology is used, necessary keys and passwords must be made available for secure storage by MIS, such that they can recover the data even without assistance from the employee themselves.

Electronic records

Employees must understand that in order to comply with legal requirements, and best practice in information system security, all electronic information stored in company systems or on company premises may be subject to monitoring, inspection or audit by other company employees, external auditors, or regulatory or legal investigators with appropriate jurisdiction. As such, employees should not expect any privacy in respect of email, files, or system usage.

Responsibilities

All employees are responsible for their own conduct in adhering to this policy in the course of their normal business activities.

The MIS department is responsible for providing a technical infrastructure to enforce and support this policy, and the eCommerce Director, as Data Security Officer for the Company, is final arbiter in deciding how this policy should be interpreted and for determining the acceptability of any proposed extensions to, or exceptions from, the policy.

Training, Further Information, and Amendments

Specific training on the issues discussed in this policy is available from GIAC's Training Department, and is a required element of new hire orientation for all employees. Periodic in-service training will also be provided for all employees.

Technical enquiries, or requests for specific permissions documented above, should be addressed to the MIS Support Desk.

More general queries about the operation and interpretation of Policies should be directed in the first instance to the HR department.

Amendments to this policy may be made in accordance with the MIS *Department's Policy Control Procedures*, documented separately.

Enforcement and Penalties

These policies will be enforced by a combination of automated monitoring and network-defense tools, combined as necessary with direct audit and personal monitoring of systems.

In the event that an employee is aware of a potential breach of this policy, they are encouraged to report their concerns to their manager. All such information will be treated in confidence, but is essential to ensure the security and integrity of the company's information systems, and hence maintain our excellent reputation with partners and customers alike.

Any breaches of policy will be investigated by the MIS department, in conjunction with the HR department, and appropriate penalties determined according to circumstances. Depending on the severity of the breach, penalties up to an including termination may be considered appropriate.

3. Security Incident Response

Effective Date and Revision History

This is Version 1.0 of this policy, and is effective January 1, 2002.

Purpose

This policy document provides high level guidance on handling and recovering from suspected data security breaches.

Scope

This document outlines procedures to be used by GIAC employees – including, but not limited to MIS staff – in handling actual or suspected breaches of data security on any GIAC network. This includes both virus and worm outbreaks, plus compromises of DMZ or internal servers by unauthorized users.

Overview of Policy

It is GIAC's policy to have a 'Response Team' charged with taking all reasonable measures to respond quickly to any suspected security breaches; evaluate and contain the breach; remove the opportunity for repeat attacks, and restore system functionality as soon as possible.

In the course of resolving issues, wherever feasible, the Team will seek to research and document the attack so as to identify the perpetrator(s) and support any criminal investigation and prosecution that might arise, however rapid containment and minimization of downtime should be the primary objective.

Roles

When a security breach is detected or suspected, the incident should be investigated and resolved by a Security Response Team, comprising three roles, as follows:

- **Incident Manager** – responsible for coordinating the investigation, deciding appropriate technical responses, liaising with other functional areas within the company and incident-management partners such as vendors of affected systems and the ISP; providing technical support to the communications officer; and preparing status reports to the CIO and executive management.

- **Security Technician(s)** – involved in investigating the incident at the network level and system level, and assisting the incident manager in responding.

- **Communications Officer** –responsible for all related communications with the outside world other than affected vendors, including communication with security advisory organizations, business partners, and public relations tasks such as issuing press releases, and responding to enquiries from customers or the media.

At all times, there should be one person designated and available to act in each role, plus a designated and available back-up. A weekly roster of who the designated contacts are should be published on the MIS intranet site.

Actions required

Notification

When an incident is suspected, the Incident Manager and Security Technician should be notified immediately. Typically this will be done by a pager alert from the intrusion detection and security systems, but it may also be done by another member of the MIS team, upon observing anomalies in system operation. The Communications officer need not be notified initially, until the initial assessment has been made.

In the event that the primary contacts for this role are unavailable, the secondary contacts should be contacted. The designated primary and secondary responders should be familiar with these procedures, and also have the necessary skills to be able to carry out the procedures effectively. This is equally true of the communications role as the technical ones; employees tasked with handling the press and public relations in such situations should be skilled and experienced in this area.

Until such time as the team is convinced that the breach has been repaired, they should avoid using in-band electronic communications and email to correspond about, or document, the attack.

All incidents and suspected incidents should be logged using the MIS *Incident Response Management Form*. These logs are to be kept by the Security Officer for future reference and reporting purposes.

When the Response Team is notified, they need to work accurately but quickly through the following phases:

1) Initial Assessment

The Team needs to start by obtaining a quick assessment of what has happened:

- Has there indeed been any detectable breach?
- Is the incident still in progress?
- Where has it come from – internal or external hosts?
- What systems have been affected?
- What damage has been done?
- What is the risk associated with the incident?
- Is the attack a one-off, a precursor to some other attack, or a blind to cover an ongoing attack?

2) Damage Limitation

Once the assessment is complete, the Incident Manager should draw up a short-term damage limitation plan in conjunction with the Security Technician.

Depending on the perceived risk, and nature of the incident, the response might include disconnecting the DMZ/ZMD from the Internet; taking the affected servers offline; reconfiguring software; or making changes to the firewall.

The MIS department may also need to be briefed on any LAN/WAN systems that may have been compromised. This notification should be made by the Incident Manager, in accordance with the relevant MIS department policies.

Where feasible, logs and system trace files should be archived to enable detailed examination once the attack has been contained. All actions taken and information uncovered should be recorded on the Incident Response Management form, and the time and date noted.

If appropriate, the Incident Manager should communicate with internal Operations groups to inform them about any loss of service. However, these communications should only provide minimum necessary details of the incident; at this stage, communication should be on a need-to-know basis.

3) Communications Briefing

Whilst the Security Technician is implementing the damage limitation phase, the Incident Manager should brief the CIO on the incident.

If the CIO and Incident Manager think it likely that the incident will attract public attention, then they should brief the Communications Officer at the earliest opportunity.

The Communications Officer should then work on preparing a suitable response in the event that the incident attracts public attention; indeed, they may decide to prepare a formal press release, depending on the scope of the incident.

If the Communications Officer receives public or press enquiries about security issues, s/he should not comment on any specifics until they have been briefed on the incident by the CIO and Incident Manager.

4) Detailed Analysis and Forensics

Once the attack has been stopped, the incident manager and Security Technician should review the evidence they have gathered, to determine exactly what happened, how, and why. They should verify and amend as necessary their initial analysis, and determine precisely which hardware and/or software systems were affected.

Analysis should be performed using tools and utilities from a known-good source; a CD of relevant tools should be maintained for this purpose. This will ensure that attackers cannot cover their tracks by substituting compromised analysis tools in place of the standard admin tools on the server.

They should archive to CD-ROM any relevant files, logs, network traces etc, in order to provide a permanent record of the attack, as well as documenting the information in the Incident Response Management form.

5) System Recovery

Having determined the full scope of the incident, the Team can then begin to recover the affected systems. Depending on the scope of the damage, this may involve reinstalling software, recreating configurations, or restoring data from back-ups. Reinstallation should be done from original disks, not from possibly compromised installation sets on the affected machines.
At this point, the team should also consider further hardening the perimeter defenses and/or detection tools to avoid a repeat attack.

6) Follow-up

During this consolidation and completion phase, the team needs to do the following:

- Confirm that all services been restored, and are tested as 100% functional;
- Confirm that the weaknesses that were exploited have been addressed;
- Ensure that any internal advisories that were issued are followed up to confirm return of normal service;
- Complete the Incident Response Management form;
- Prepare an Incident report for the CIO and CFO;
- Provide information for insurance and legal claims as necessary;
- Re-evaluate this Incident response procedure, and amend as necessary.

Training, Further Information, and Amendments

Specific training on the issues discussed in this policy is available from the MIS department for all affected employees. Such training must be completed prior to appointment into a role as a potential responder.

Requests for clarification or modifications should be made to the Security Officer.

Amendments to this policy may be made in accordance with the MIS *Department's Policy Control Procedures*, documented separately.

Enforcement and Penalties

This policy will be enforced through review of the incident reports generated in the course of an incident, and in the absence of actual incidents, readiness will be assessed and maintained through drills conducted by the Security Officer at least twice per year.

Any breaches of policy will be investigated by the MIS department, in conjunction with the HR department, and appropriate penalties determined according to circumstances. Depending on the severity of the breach, penalties up to an including termination may be considered appropriate.

Assignment 3: Define Security Procedures

This section documents a procedure in support of the DMZ System Integrity Assurance Policy discussed above; specifically, the procedure for hardening a DMZ server's operating system and applications.

Procedures for security hardening of DMZ Servers

Scope and Background

Effective Date and Revision History

This is Version 1.0 of this procedure, and is effective January 1, 2002.

Related Policies and Documents

This procedure is one of several in support of GIAC's policy document "DMZ System Integrity Assurance". Refer to that document for information on the overall approach to systems security and integrity maintenance.

This document also refers to the 'Hot Fix Master List' – a spreadsheet of vendor's bug-fix and security patches which have been reviewed and approved for deployment on eCommerce systems by the Security Officer.

Affected Operations

These procedures apply to the commissioning of new servers for use in GIAC's eCommerce operations (or re-installation of existing servers), or subsequent changes to the configuration of those servers.

Pure content loads, or loads of application server object files (as distinct from the application server system) itself, do not need to be logged in this system – rather, they should proceed according to the separate *Move to Production* procedures.

Affected Servers

These policies apply to all servers installed for GIAC's eCommerce operations whether for development, testing, staging or production, and whether or not the systems are directly Internet-exposed.

Affected Personnel

The procedures should be followed by whomever is responsible for configuring the servers ready for production, or maintaining servers during their in-service life – whether a GIAC employee or a contractor.

The final production approval for new systems and testing of hot fixes should be conducted by a member of the MIS eCommerce technical staff (other than the person who may have installed the system or fix).

Rationale

The steps documented below are required in order to ensure that all production servers are maintained in a secure state, and unauthorized access through mis-configuration or exploitation of known security vulnerabilities is not possible.

Specific changes below are based on experience in deploying previous generations of servers, combined with the recommended configurations from Microsoft. [See references section at the end of this practical for further information and links to original documentation]

Documentation

When a new server is to be brought into production, a new '*System Preparation Checklist*' should be prepared, and actions recorded on that checklist, as the procedures below are worked through.

Any configuration changes (other than content or on-line application code loads) subsequently made to a system should be recorded in that system's 'Configuration Changes' log.

Additionally, as new security exploits are discovered, and hot fixes released, the Information Security Management Team will be responsible for recommending which fixes need to be applied. Those recommended hot-fixes should be recorded in the Hot Fix Master List, and arrangements made to deploy to the necessary machines. The application of those fixes should then be noted in the 'Configuration Changes' log for each system.

Periodically, service packs will be released by manufacturers to address a number of issues with the software, and which may obsolete one or more hot-fixes. When this happens, the ISMT should review the service pack and decide whether and when to deploy it. The decision should be noted in the Service Pack Master List, and arrangements made to install the Pack. Obsolete Hot Fixes should be noted as such in the Hot-Fix Master List.

Completed checklists and logs are retained by the Security Officer for as long as the equipment continues to reside in the production environment.

Auditing Compliance

This procedure includes details of tests which must be conducted to ensure that the systems are appropriately hardened both when first commissioned, and after any configuration changes. The successful completion of these tests is then indicated in the documentation discussed above.

The Security Officer is responsible for conducting periodic audits (at least once per year) in which a random sampling of logs are inspected and verified against the known history of the systems in question.

Windows NT Hardening

The following modifications should be made on each new or re-installed server prior to making it live, except as noted below. Where a known good pre-configured drive image is available for a similar specification server, that may be used instead.

At each stage, the completed modification should be initialed as completed on the '*System Preparation Checklist*', and any comments noted alongside.

Operating System

Install Operating System and Apply Service Packs

The Server Operating System should be installed and applicable Service Packs applied up to the current standard, noted in the Hot-Fix Master List.

Note the following:

- NTFS file systems should be used on all hard disks.
- The server should be configured as a stand-alone in the GIACDMZ domain

Identify and Apply Required Hot-Fixes

Next, all relevant, approved hot-fixes for the Operating system should be applied, as appropriate to the role of the machine. The list of approved fixes is the 'Hot-Fix Master List'.

Accounts and Privileges

Guest Account

The Guest account should be disabled.

Administrator accounts

Change the name of the Administrator account, to DMZGIAC, and set it to not be allowed to log-in remotely. The password on the account should be set to the current password, which should be stored securely, offline, by the Security Officer.

Set up a dummy Administrator account, with no permissions, and audit its use.

Access Privileges

The whole of the OS partition should be set to allow 'full access' to Administrators, System, and DMZGIAC accounts only.

Miscellaneous changes

Turn off 8.3 name generation

Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\ NtfsDisable8dot3NameCreation to REG_DWORD 1.

Set boot time to zero seconds

In Control Panel | System| Startup/Shutdown.

Hide last logon name

Set HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\DontDisplayLastUserName to string "1".

Set logon message

Set HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\LegalNoticeCaption to string "GIAC Enterprises Server".
Set HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\LegalNoticeText to string "Attempting to log into this System without appropriate permissions from GIAC's eCommerce department is prohibited. Violators are liable to disciplinary action and/or prosecution. All interactions with this system are subject to monitoring.".

Remove shutdown button on logon screen

Set HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\ShutdownWithoutLogon to string "0".

Restrict anonymous network access

Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\ RestrictAnonymous to REG_DWORD 1.

Auditing and Logging

Audit log-on and log-off

In User Manager | Policies | Audit - set system to audit both successful and failed log-on and log-off.

Set logs to overwrite

In Event Viewer | Log | log settings set the maximum log size to 1024Kb, and to overwrite events older than 28 days, for all three logs.

Networking

Set IP address and gateway

In Control Panel | Network | Protocols | TCP/IP Protocol | Properties | IP Address, set the IP addresses for each interface.
Then go to the advanced dialog, and make entries as follows;
For internet servers, set the gateway to the internal side of the external firewall – x.x.x.x.
For LAN-based servers, set the default gateway to the LAN interface to the firewall – x.x.x.x.

Disable IP Routing

In Control Panel | Network | Protocols | TCP/IP Protocol | Properties | Routing, ensure that 'Enable IP Forwarding' is not checked.

Configure DNS and WINS

In Control Panel | Network | Protocols | TCP/IP Protocol | Properties | DNS, set the Host Name and domain.
For Internet servers, running a DNS server, add 127.0.0.1 as the DNS address; for LAN servers, set the DNS server address to x.x.x.x.
In Control Panel | Network | Protocols | TCP/IP Protocol | Properties | WINS Address, set the WINS server to y.y.y.y.

Set Bindings

For Internet servers, in Control Panel | Network |Bindings, ensure that only TCP/IP is bound to the Internet-facing interface.

Disable Non-Essential Services

Non-essential services should be disabled, depending on the intended role of the system. Microsoft indicates the following minimum set of services is required for IIS (per *IIS4 Baseline Security Checklist* – see references for details):

- Event Log
- License Logging Service
- Windows NTLM Security Support Provider
- Remote Procedure Call (RPC) Service
- Windows NT Server or Windows NT Workstation
- IIS Admin Service
- MSDTC
- World Wide Web Publishing Service
- Protected Storage

Server Software

The following pieces of server software may need to be installed, depending on the role of the machine:

IIS

For web servers, requiring IIS, complete the following steps:

- Install from NT Option Pack, Using Custom Install. Install only basic server software, and no examples or documentation
- Establish the server root directory structure under d:\iisroot
- File permissions on the directory structure to allow anonymous access to d:\\iisroot\world and employee-only access to d:\\iisroot\private
- Remove samples, default virtual directories, and web based admin tools
- Remove all DLL handler associations

Resonate Central Dispatch

For front-line web and email server, install the currently deployed version of Central Dispatch to provide load-balancing services. Coordinate with MIS to obtain necessary license codes. Configuration of the host will be pushed down from the server cluster once the machine is added to the cluster.

Apple Web Objects

For Application servers, install the Deployment Version of Apple WebObjects 4.5.1 from CD. Reboot the machine and then apply the latest service pack. Coordinate with MIS for license codes.

Security Applications

The following security applications should be installed on all production servers. See the manufacturers' current Installation Guide (packaged with the software) for further information:

IIS System Scanner

This needs to be installed on all hosts in the DMZ.

IIS RealSecure OS Agent

This needs to be installed on all hosts in the DMZ.

ISS RealSecure Network Agent

This only needs to be installed on a dedicated intrusion detection host on the DMZ network.

ISS RealSecure Monitor

This only needs to be installed on a dedicated Security Console.

IIS Internet Scanner

This only needs to be installed on a dedicated Penetration test system.

Data Sources

For machines requiring data source connectivity, such as application servers, the following steps should be taken to configure it:

- Remove all ODBC Data Sources and Drivers
- Install drivers for specific data sources required from manufacturers' media
- Define appropriate Data Sources based on requirements for specific applications.

Final Review and Testing

Once the steps above are complete, or whenever a configuration change has been made to an existing server, the configuration needs to be reviewed and tested, as follows:

Configuration Walkthrough

A member of the eCommerce technical staff should walk through the configuration (or change) with the engineer who undertook it. Any comments or issues from the checklist should be discussed, and the steps double-checked.

Penetration testing

The system should then be tested using ISS's Internet Scanner from the local subnet. Results should be compared with the baseline established for the network on which the system will be deployed. Any remedial action should be taken, and the test re-run until satisfactory results are found.

Vulnerability Assessment and Security Systems Base-lining

The system should also be subjected to an ISS System Scanner test of known Operating System vulnerabilities. The results should be compared against the baselined results for the network on which the machine will be deployed. Any remedial action should be taken, and the test re-run until satisfactory results are found. The current result set should then be stored within the software as the approved baseline set for this machine.

Server daemon testing

The basic functionality of the specific server daemons on this box should then be tested.

System Imaging

Finally, an image should be taken of the system's drive partitions for subsequent restoration in case of an emergency, or the need to build an identical server. An emergency boot disk should be built, and a backup of the system's registry taken.

Final Signoff and System Integration

Once the checks above are successfully completed, the Checklist for the machine should be signed off by the engineer and reviewer. The system can then be released for content deployment, application and content testing, and eventual move into the production environment.

The system should only be moved into production once all steps above have been successfully completed and verified in the final review. Any exceptions to the procedure should be documented on the checklist, and must be approved by the Security Officer.

References

Further information on topics discussed in this document can be found in numerous places online. Searching on any major search engine online will quickly turn up may references; below I give a few personal favorites, along with some commentary on my personal experience with them.

Hardening of Server Systems

- **Microsoft's TechNet Security sub-site**
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp
  The starting point on Microsoft's site for information about Security policies, procedures and fixes for their products including Windows NT, Windows 2000, and IIS. Also provides a searchable index of Security Bulletins, and associated hotfixes.

- **Microsoft paper on 'Securing Microsoft Windows NT Installation'**
  http://www.microsoft.com/ntserver/techresources/security/Secure_NTInstall.asp
  This document provides an overview of the Security implications of a default install of Windows NT, and provides general guidance on optional configurations that will provide more resilience against attacks.

- **Microsoft's 'IIS4 Baseline Security Checklist'**
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iis4cl.asp
  A work-list for configuring IIS4 securely, in order to address weaknesses in the standard configuration, and minimize the opportunity for exploitation by only providing essential services and access rights.

- **Microsoft article: 'Understanding Internet Information Security'**
  http://www.microsoft.com/ntserver/techresources/security/iissecure.asp
  This article provides an overview of how IIS and Windows NT security models interact; an essential requirement for effectively understanding how to secure content at the user level.

Security Vulnerability Notification and Research

- **Microsoft Product Security Notification Service**
  http://www.microsoft.com/technet/security/notify.asp
  This page has details of how to sign up for email alerts from Microsoft when they release notifications and/or hotfixes for security vulnerabilities in their products. Approximately 100 were released in 2000, and 60 in 2001(to date).

- **NTBugTraq Mailing List**
  http://www.ntbugtraq.com
  A moderated email list-server for disclosure and discussion of Windows-related security vulnerabilities. Effectively moderated by Russ Cooper, postings tend to be informative and focussed, and traffic volume is variable depending on current issues, ranging from a handful per week up to one or two dozen messages per day. Covers not only Windows NT, but other Microsoft operating systems – especially Windows 2000 – and Microsoft applications such as IE, Outlook and IIS.

- **Bugtraq Mailing List**
  http://www.securityfocus.com/archive/1
  Similar to the NTBugTraq list, this moderated list-server has a wider remit, addressing vulnerabilities in the full range of client-server technologies. There is some coverage of Microsoft products, but the bulk of the one or two dozen postings per day address vulnerabilities in Unix and Linux variants. Also a good source of information concerning occasional vulnerabilities in infrastructure products such as routers and firewalls.

- **SANS Alert Consensus**
  http://www.sans.org/newlook/digests/SAC.htm
  A weekly digest of security information and disclosures, customizable by platform or technology, so that you only get to see information relevant to your given technology mix. Whilst perhaps not timely enough to be a sole source of information for mission-critical, front-line systems, it is a valuable resource as a round-up check for those systems, or as a primary source for secondary systems where a less-rapid response is tolerable.

- **CERT Coordination Center at Carnegie Mellon University**
  http://www.cert.org
  One of the most respected sources of information and research on security issues. In addition to the resources on their web site, they publish and a few dozen email advisories per year on major vulnerabilities as they are found, covering the full gamut of technologies. Whilst not all vulnerabilities are necessarily deemed worthy of the a full advisory, and the depth of research means that CERT may not be the first to advise on a vulnerability, those vulnerabilities that do receive an advisory are usually worthy of immediate attention.

- **Symantec Antivirus Research Center (SARC)**
  http://www.sarc.com
  This is the home of the research and response team for Symantec's Norton Antivirus product. As well as being a source for the latest IDEs for that product, it also features a searchable index of thousands of viruses, including detailed descriptions of behavior, symptoms, and removal techniques.

Security Products

- **Internet Security Systems (ISS)**
  http://www.iss.net
  Vendors of a comprehensive range of vulnerability analysis and intrusion detection systems, and home to the X-Force vulnerability research team.

- **MimeSweeper/Baltimore Technology**
  http://www.mimesweeper.com
  Providing a range of email and web content security tools, designed to allow the establishment of network-perimeter gateway/proxy servers that can actively filter content for malicious or inappropriate content.