GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

A CIO's Guide to Managing Security Risk in Web Hosting Contracts: What to ask your Managers and Web Service Provider.

Author: Neil Wainman
Date: 7 May 2002

Abstract

While the universal availability of information is the essential strength of the Web, its mechanisms to ensure confidentiality and integrity still challenge users. The continued success of web based e-commerce now demands trust in its security. [CIO, 2000] This paper considers the security issues that a corporation must address when in a web hosting relationship, using the managed service provision [MSP] model. Resilient design is assumed.

It advises that periodic audit and testing of the MSP web-hosting infrastructure by both internal [MSP and Corporation] and external objective professionals are mandatory to discover and remedy intolerable risks. It outlines some problems and pitfalls which must be avoided in such a relationship. Cost justification is on the premise that low cost with lax security now, will risk loss and costly reparations later.

Principles of Operational Security Risk Management

The risk landscape in operating a web hosting infrastructure is a constantly changing landscape. This requires continual awareness of new threats, vigilance with current systems and excellent standards in system configuration controls to stay abreast of vulnerabilities: For example monitoring of

- discovered exploits, and emergent vulnerabilities
- maturing and new technology changes
- new website functionality
- increasing complexity, eg in encrypted transmissions

Risk is a complex and dynamic mix of threat, vulnerability and likelihood, difficult to assess and not an exact science, particularly in IT security. Assessment therefore needs to be done regularly, consistently, by a competent practitioner to ensure controls eliminate or reduce the chance of a loss in revenue, resource or reputation to tolerable levels. Consider who is doing this assessment and whether they demonstrate the necessary technical, commercial and risk management skills.

There are three basic types of control: avoidance, detection and recovery. For example, could you avoid webpage defacement? If it happened, how soon would you know and what would you do to mitigate the damage?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Reducing the vulnerabilities and threat vectors by design, policy, procedure and configuration controls is fundamental to risk reduction.

Important Terms in any MSP Contract

Exact contract terms probably absolve the MSP from financial responsibility for security issues [See UUNET, 2002 for typical disclaimer] and are notoriously difficult to agree. Assuming a contract exists with your MSP, to ensure control and visibilities required for risk assessments, three terms are of paramount importance;

Firstly: 'that the MSP shall provide physical and logical security to meet or exceed the corporations requirements' [Matlus & Maurer, 2002]

Secondly: 'right of on-site audit' [Sherwood, 1997]

Thirdly: 'right to verify security of infrastructure using the corporation's or independent testing companies mechanisms employing recognised tools, eg penetration, vulnerability and scanning tests'.

Faced with this requirement, an MSP may decline to accept these terms. Alternatively an MSP may side-step this issue by using a pre-selected 'approved' auditing company, with exclusive access rights. In either case, the rigour of the security audit and testing must be verified. Gaining the required visibility and access to gain assurance that configuration is adequate for your security needs, may ultimately fail. [Tuesday, 2002].

An SLA should fundamentally define the nature of your relationship, in order to get the flow of management information and operational interfaces correct. The SLA must address the requirements for robust security metrics and reports, incident handling and testing. [Ferengul, 2002]

Process and Policy

Good security management starts with a risk assessment. Security is never a one off fix, but a continuous improvement process, with subsequent assessments building on previous results and remedial work, in a virtuous circle. Frameworks for overall security management include:

- Information Security Forum [ISF, 2002]
- International Standards Organisation Standard17799 [ISO 17799, 2002]

In particular, ISF has actively addressed the needs of e-commerce with good practice guidelines. It is designed for ease of use [with some software support now available] and stressing the procedural good practice [bottom–up] as well as the risk management

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[top-down] approaches. From the author's experience, this represents a good compromise.

Costing for any potential loss of revenue/resource/reputation is still a largely subjective exercise, with few robust tools and actuarial history to help. However, ISF uses a concept of 'Levels of Harm' based on some financial measures. Similarly, 'business impact' questionnaires can be used to support ISO 17799 risk assessments.

CoBiT [2000] is a widely recognised ['open-source'] standard of practice for assessing the general operation of any IT company. However, assessing an MSP's security practices, should diagnose underlying weaknesses in general IT practice, since the former is often required to underpin the latter, eg change management when a new security patch is required. In this way security assessments give double value.

Security practitioners agree that your security stance is first written in a policy, which has senior management endorsement and awareness amongst operations staff. This is the requirement statement or 'What' for security. The 'how' is then codified in design standards, procedures and guidelines that specify the real operational behaviours.

Unfortunately, weak security arising from poor technology choice and network design is difficult to remedy by subsequent procedures and policies, and redesign with investment is usually needed. Additionally, secure platform and network design will be ineffectual without policies, procedures, and standards, security awareness and security management. The latter involves direct ownership of the security function, by someone with skills and knowledge in the area. Even if standards and procedures are present, are they ignored in practice? One pitfall in any assessment, is to accept a manager's word that procedures are followed [espoused behaviour] when in fact they are not [actual behaviour.]

One real danger is of 'enshrining' as policy your current arrangements. Security policy must evolve with the emergent threats. Hence, you must re-assess the web architecture in line with new threats and commentators warn against simple, 'quick fix' and linear methods in security management. [Kessler, 2000]. Rather an ongoing process of periodic reviews of security elements is required: eg web architecture, policies, standards, and so on.

Outsourcing what you do not understand is dangerous. Ensure that the corporations IT governance, risk assessment standards and security policies are extended to and verified at the MSP. Traditional IT governance is only lately recognising web commerce risk and operations. Plenty of guidance is now available to test your security stance such as that endorsed by the UK Government. [AEB, 2002; Eagle, 2002]. Ensure your corporation's IT operational risk register reports to the boardroom contain specific sections quantifying risk in your Information Security and E commerce offerings. Further, ensure allocation of direct functional responsibility for e-commerce and security to a senior manager, who understands the issues or has professional help to do so.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Correct governance demands contingency arrangements and exit plans, with tested scenarios, to cover business failure, major telecom problems and security attacks. [Benke, 2001] Incidences of corporations needing to use contingency plans are well reported and increasing. [Berinato, 2001]

The essential questions are:

- what framework does your MSP use to assess and control information and IT security?
- can they demonstrate compliance with a recognised standard?
- does this standard meet your own standards and needs?

Insurance

The corporate insurance department should be appraised to consider whether criminal and fraud insurance extends to the MSP, either as a spread risk or a 'self-insured' policy. E-commerce insurance offerings are flourishing following recent denial of service type attacks [Kay, 2000] and financial frauds. Clearly insurance alone will not restore trust or avoid future incidents, but should all other avoidance controls fail it is a mitigation of loss of revenue and reputation.

It's The Law

All MSP contracts should pass through the corporate lawyers who understand the unique exposures that the Web presence generates. In the UK, libellous web pages are a growing concern and the recently strengthened Data Protection Act [1998] sanctions companies with legal proceedings for the inappropriate disclosure of personal information. Some UK lawyer firms issue free regular Information Security bulletins on issues of concern. Company directors are often personally liable. [AEB, 2002] Important laws with e-commerce implications include:

- Data Protection Act [1998]
- Copyright, Designs and Patent Act [1988]
- Regulation Of Investigatory Powers Act (RIPA) [2000]
- Computer Misuse Act [1990]
- Telecommunications (Fraud) Act [1997]

The UK courts have yet to try certain inevitable cases, such as:

- failure to stop your servers being used to attack some other commercial site
- failure to allow law enforcement agencies access to encrypted files when the subject of criminal investigations

© SANS Institute 2000 - 2002, Author retains full rights.

Content Management

Website content assessments are important to understanding the level of security investment required and risk. You should not rely on your MSP for this. The nature of your business may mean you fear espionage and therefore inappropriate disclosures on your web site would damage commercial advantage. Content control and editorship are important for corporate image management but also a prospective hacker might glean helpful information in a reconnaissance exercise, for use in a later attack, including

- key personnel names for social engineering attacks,
- telephone numbers to extrapolate direct dial-in ranges for war dialling
- switchboards and voicemail systems are a particular favourite soft target
- major sites, where possible confidential waste might be garnered

Cases of misleading or falsified content, i.e. falsehoods about share prices have been unwittingly propagated by some Websites, even coming from 'trusted' sources, for example by repeating newswire services on a corporation page

Commercial Management

Due diligence checks on company status and liquidity are advised. MSP revenues are currently down and recent MSP consolidations and failures have led to costly re-hosting exercises by corporations. [Berinato, 2001]

Relationship Management is therefore crucial but out of scope here. Kaye [2002] gives excellent advice on 'win win' relationships in web hosting.

Domain Name Management

This area requires constant vigilance, eg monthly checks and there are various survey and monitoring services.

Spoofing attacks are those in which a legitimate Web presence is manipulated to achieve a security breach. Techniques are subtle and often complicated. It is imperative that the Domain Name Service [DNS] correctly resolves the IP address from the URL format. Attacks can occur where the user is redirected to an alternative site for a given 'correct' URL, following DNS server manipulation. Internet addressing authorities are largely wise to this, employing cross checking techniques on DNS servers to detect unauthorised changes. Procedures for changing public address and naming must include a robust method of authenticating the requirement to change. This is required to ensure social engineering attacks do not succeed, eg where an email supposedly authorising the change is acted on by the ISP/MSP domain administration team.

© SANS Institute 2000 - 2002, Author retains full rights.

Alternatively a user may unwittingly type the URL incorrectly, [eg wrong case or character; or use domain .org rather than .co.uk]. Pranksters or fraudsters out to catch unwary users may have legitimately registered these subtly different URL and domains. Commentators suggest that only better national laws will prevent these registrations in the future. [Anon, 2002]

Also, what and where do you get if you put your company name [and variants] in the top World Wide Web search engines? Does anyone trawl through the major hacker sites, newsgroups and chat rooms on the web for news items where your company or MSP is mentioned?

The lessons here are:

- consider registering similar domain names to your own and having these present pages with links to the correct site, advising users of their error
- check who has registered any near miss types and consider acquiring these or registering these yourself
- think internationally, i.e. check various major Internet Registration naming authorities in the major countries

Independent Penetration Tests

Periodic penetration tests are an excellent way of verifying effective management by the MSP of your Web presence and finding weaknesses that may require attention Good tests will include:

- port scanning for exposed services
- information gathering including DNS issues as above
- system enumeration, eg for operating system used
- system vulnerability tests, eg latest buffer overflow
- application vulnerability tests, such as cross site scripting, field manipulations

These are against the MSP's Internet gateway, using the corporation's public IP addressing and domain names and the site pages themselves. Additional testing should immediately follow major new code or configuration changes, eg to ACL's, firewall rules, page functionality and fields, or content. As exposures can arise at any time, a periodic check is advised.

Many companies offering such a service have largely automated their test and reporting, hence getting added value requires effort. Does the testing cover all the risks your business profile warrants, or is it an 'off the shelf' basic test package. Do they update their tests to reflect new vulnerabilities? Do they recommend any solutions to

© SANS Institute 2000 - 2002, Author retains full rights.

problems they find? Are the results then assessed and ranked by high, medium or low risk; who is then responsible for acting on the results in a timely way?

Design Checks & Standards

The number of differing combinations of the elements of the MSP's infrastructure are probably as numerous as the MSP's themselves.

By doing a thorough review of databases, operating systems, hardware platform and network configurations as individual components and as an integrated whole, then many security holes can be avoided. Review the configurations against latest vulnerabilities as published by security related mailing lists such as Bugtraq or CERT-advisory. [See references]. Lists dedicated to particular platforms and manufacturers abound, however some are poor quality and 'unofficial' where care must be exercised.

Since weak links in the security of any architecture element will attract most attention from malicious activity, an holistic view is best. Here all elements are considered, host and network wise. In particular, changes in one element, eg web server are considered for impacts on all other elements security, eg network.

There is vast amount written about securing public web servers, which give good principles from which to probe the MSP's stance. [for example Kossakowski & Allen, 2000; Stein & Stewart, 2002]. Poor password management [i.e. no regular changes and defaults allowed] and no customised configuration controls, i.e. using 'out of the box' plug and play configurations are absolute dereliction of security duty.

Analysis Tools

These tools allow the enumeration of networks and hosts and testing for known vulnerabilities. Such tools are often the same tools used by hackers, [eg NMAP,] and require expert handling, whether by security staff or a testing partner. They may be useful to verify results from your testing company. Since there are dozens of tools for testing all web infrastructure elements, this can become overwhelming. One approach would be to use one or two [such as NMAP and NESSUS] on occasion. The necessary permissions and awareness are required to avoid damaging any relationships, causing false alarms, or worse, accusations of criminal activity. Another alternative, particularly with many new vulnerabilities being found each day, there is benefit in occasionally using a second testing company. This may allow the cross checking of results, and guard against complacency.

In addition, various 'expert system' commercial security analyst tools are available for checking servers and OS's to ensure the correct level of hardening. What is your MSP using? [Kessler, 2000]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Development Risks

Some believe web security is a problem with software development, but achieving good security is never merely a technical or logical solution. Many vulnerabilities arise from poor coding and web application development. Do not rely on the MSP for this security issue. OWASP [2002], provide a development template to web authors in avoiding security loopholes. This is welcome addition to the more traditional approach of just securing network and operating systems and reducing unnecessarily available services. [see also Stein & Stewart, 2002; Costello, 2002]. Documents provided [OWASP, 2002 & Stein & Stewart, 2002] will assist technical auditors to verify the MSP's [or your website developer] has covered major vulnerability issues such as use of:

- mobile code, eg applets and active elements
- operating systems 'small services'
- platform choices
- poor documentation
- database scripts
- web field manipulations, eg with SQL or UNIcode
- file system naming
- UNIcode measures

There must be clarity in the relationship as to who is ultimately responsible for security standards in web site development.

Pre-release code reviews, staged testing, version and change control becomes mandatory for any new functionality, active content, pages, or updates of source code. If the MSP provides a staging or testing environment, be careful that the controls applied to this are as rigorous as the 'live' environment, eg in password management, systems build and patch level. Find out whether it shares the same infrastructure as the live environment, eg test and live servers on same network segment, since weak security on a test environment might then provide a platform to attack the live hosts.

New forums are attempting to address this lack of formal and accepted standards of development with new architectural models of 'Web Services' which include robust security. [Miller, 2002] Early adopters run risks of unforeseen vulnerabilities.

Firewalls and Routers

Many MSP's prefer to use routers with access control lists [ACL's] as their 'dirty' connection to the Internet with a firewall behind this to further protect the Web servers giving good practice 'defence in depth'. Hence filtering in the other potentially mitigates a configuration mistake in one device.

© SANS Institute 2000 - 2002, Author retains full rights.

With ACL's the first line fundamental control and good practice is to implement filtering of inbound and outbound undesirable traffic and protocols such as pings, [ICMP], traceroutes and sourcerouting.

Then using the firewalls [or possibly routers] packet filtering, at a logical port level, port 80 [http] and 443 [https] are often the only inbound connection requests to be passed for the sites functional needs. Packets destined for port 80 on the web server are allowed to pass, no questions asked.

Stateful inspection firewalls will ensure that the protocol is acting as expected, eg has the correct commands, such as 'put' in http, It also maintains a state table of the sessions at a low level and makes decisions on expected traffic based on the state of connection requests. For example, an outgoing DNS UDP [port 53] packet is likely to be a DNS query, and the firewall on seeing the expected return packet, would let it pass, based on the expectation of a response.

Additional 'proxy' methods may be considered, where sessions are set up from the web server to the firewall and from firewall to service requestor to break the direct connection. Proxy firewalls may have a performance issue, however this is not clear cut as some will support cacheing.

Firewalls will handled the obligatory network address translation; hence, the IP address registered in the public DNS should not be in the MSP's [or corporation's] private IP address range. This ensures your internal address space is hidden from the Internet.

The tendency to have lax internal security controls, relying on, or placing too much faith in firewalls [or in IDS's] is a real danger, as is assuming all employees are honest or that external attacks are now impossible. Assuming only port 80 [HTTP] is ingress enabled, then the Web server is not necessarily safe. Geiger [2001] outlines attacks via HTTP to include:

- malformed URL's exploiting Web server code
- attempting to find default installations of server software or components thereof

These attempt to get file privileges to allow uploads or downloads from the server, for example trojans or customer information files. A common attack here is against poor UNIcode control.

In general, Geiger points out that less than one percent of websites use Secure Sockets Layer, which is one straightforward way of 'raising the bar' against attackers. This gives the browsing client some confidence that the server they are requesting a session with, is in fact genuine.

Intrusion Detection Systems

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Due in part to the fact that attacks are possible via port 80 [http] or 443 [https] intrusion detection is therefore recommended to look for attack 'signatures'. Ideally, your MSP should provide intrusion detection systems in order to meet the service requirement of a secure hosting environment. This IDS should use both network and host based techniques.

In network IDS's, inbound and outbound traffic and connection requests are analysed in a 'stateful' manner down to protocol/packet level. A set of advanced attack signatures also monitors the traffic to detect possible attacks. Probes are placed at strategic points, eg directly in front and behind of the Internet gateways/firewalls. This can be particularly effective stance for older sites [where source code rewrites may be an expense]. Promiscuous probes, [with no direct IP participation in the network] are de-facto standard, with management and control provided from a separate interface, rather than the interface for the network segment. Network IDS is not trivial to manage. Probes need signature updates regularly and techniques to trap 'slow and low' attacks are warranted. Check whether the detection of packet fragmented attacks can de demonstrated. Generating real benefit from IDS's comes after alerts are collected; from the quality of correlation, integration and analysis methods.

All host elements [including firewalls and routers] should have built-in or added-on tools for monitoring of system events, traffic, user accesses and picking up connection requests to disabled ports as seen in scanning attempts. Integrity checks to detect changes on files and directory systems is mandatory in the light of the major threat of website defacement. The question is whether these measures are asserted on the systems, and results collected, analysed, assessed, reported and acted on. Hence, authorisation for any change can be verified by cross-reference to the change management system.

Any activity suspected as not authorised should be flagged, generating an incident in a formal security incident investigation system.

On occasion you may want to test IDS response, non disruptively, by running some tools against the MSP's Internet gateway, your own web sites or servers or databases. Similarly, the regular testing company's activities will be noticed by a MSP that is alert to the threats.

Back Doors

Some of the MSP's staff and probably corporation's Web team, will have privileged system and dedicated network accesses available. These are for support [especially out of hours], development, stage testing and uploading of new content, press release publishing and similar. These may involve ISDN links or modems, RAS's or VPN's. The latter may provide 'tunnels 'through the Internet firewall. This area must be checked to ensure robust user authorisations and password management is operational practice. In addition, protocol controls must be implemented, using ACL's and firewalls on any

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

network or communications links between the corporation and MSP. This defence in depth helps ensure a security breach at the MSP does not leave the corporation's networks open and vulnerable.

Other methods of circumventing firewalls cause concern when guarding confidentiality. What is your MSP's policy on detecting exploits with freely available file sharing programs, use of wireless LANs, DECT voice systems at its facilities, RAS or modems for its own staff or system support needs? The MSP's own real time monitoring equipment, eg environment controls, may have dial-up modem facilities or 'dial-home' facilities on file storage [RAID] systems. Request evidence of comprehensive and regular telephony scans with remedial works, eg modem removal, registration, or password protection with dialback only.

Denial of Service Attacks

Denial of Service is particularly problematic, [Kossakowski & Allen, 2000] requiring procedures, incident handling and contingency arrangements sensitive to its unique features. Whether from single [DoS] or multiple sources [Distributed DoS or DDoS], this attack is the most widespread, increasing in frequency, and potentially the most damaging financially. [Liu, 2002; Helgeson, 2001] Take this one up specifically with your MSP. Should the Internet service provider be a different organisation to your MSP, then seek confidence that the ISP and MSP have contingency plans for DoS.

Distinct hardware/software solutions can specifically detect and counteract the effects of DoS, thus protecting the servers behind and legitimate customers. Deployed at each Internet connection point, these segregate and 'bin' the traffic designed to disrupt legitimate access, whether to bandwidth or servers. Firewalls that are more intelligent may have multiple processing 'levels'. These grant 'easy passage' to trusted connections and authenticated sources, saving time, processing power and session management. Meanwhile, new requests or suspect sources are analysed in detail on a session by session basis down to protocol/packet level. Egress traffic should also be analysed to avoid your own hosts becoming 'zombies' [i.e. used to perpetrate attacks in DDoS scenarios]. This is good Internet citizenship, i.e. the egress filters protect others.

As there are known DDoS attacks, the ISP should actively filter on ports representing such attacks. Unfortunately, DDoS attacks change signature rapidly, so fast deployment of countermeasures are required.

Malware and New Vulnerabilities

The need for daily routines to update hosts/servers, operating systems and applications with code is generally understood as a defence against emergent vulnerabilities and malware, seen with increasing frequency. These routines use special and vendor news posting services as advice to system users of new threats, and maintain anti-virus tools

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

running on essential systems. However, the scope of vigilance may be suspect. The same routines should extend to the firewalls and routers used in the network infrastructure. A recent example would be the DoS threat where any device using SNMP, when receiving deliberately malformed protocol packets, might lose its ability to be managed by SNMP, slowdown or even crash. Similarly, the volume of new vulnerabilities, for which a patch may be required, means that good threat assessments are needed. Otherwise, the need to constantly 'cure' vulnerabilities by adding patches affects overall system availability. Further, since any new system code should be tested before being made live, the operational overheads need to be considered. Hence, there is a need for the MSP and the corporation to communicate closely on change control and threat assessment. Decisions about the risks that the corporation is prepared to tolerate should be recorded.

Shared Infrastructure

Find out if your MSP shares its infrastructure over a number of Web hosting contracts. Should your servers be on the same network segment as another customer of the MSP, then you may be more vulnerable than you thought. For example, the other customer may have a more relaxed security stance. This could lead to a compromise of their system being used to attack your own systems. One example might be that a sniffer is used to detect what your traffic is doing, or scan your own servers. Other risks include a common management infrastructure, eg a 'back-up' network segment, on which you share a connection with other clients of the MSP.

Physical Security

Preoccupation with logical security might lead to neglect of the fundamentals of physical security where 'low tech' attacks are often easier. You have a right to expect world class standards from your MSP covering:

- door entry and access control and monitoring for the site and machine rooms
- personnel screening
- restricted access to machine rooms
- fire suppression
- environment controls with real time monitoring
- independent seamless power arrangements

Summary

Insist on 'show me' rather than 'tell me' to gain confidence that espoused behaviours are actual behaviours in the MSP's security measures. Commission comprehensive audits and vulnerability tests. Consider their attitude carefully; defensive or helpful? Get into relationship with your MSP!

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Anon [2002]. *'Spoofing –Arts of Attack and Defence'* [online] White Paper: Articsoft. April. Last accessed on 12 July 2002 at URL: http://www.articsoft.com/wp_spoofing.htm

AEB [2002]. *'AEB Web Security Guidelines'* [online] Published by Alliance For Electronic Business et al. Last accessed 12 July 2002 at URL: http://www.cssa.co.uk/home/reports/websecfinal.pdf

Benke, D.M. [2001] *'Data Center Contingency Plans: How to Address and Emergency'*. [online] Published by the Web Host Industry Review Inc. Last Accessed on 12 July 2002 at URL: http://thewhir.com/features/contingency_plans.cfm

Berinato, S. [2001]. *'Security Outsourcing Exposed!'* [online] Chief Information Officer magazine, Aug 1. Last accessed on 12 July 2002 at URL http://www.cio.com/archive/080101/exposed_content.html

Bugtraq Computer Security Mailing List [online] Last accessed on 12 July at URL: http://online.securityfocus.com/bid

CERT-advisory. [online] Last accessed on 12 July 2002 at URL: http://www.cert.org/advisories/

CIO. [2000] *'You're in Good Hands… with Web Site Insurers.'* [online] White Paper, Special Advertising Supplement, Chief Information Officer Magazine. 1st May. Last Assessed 12 July 2002 at URL: http://www.cio.com/sponsors/050100_ebiz_story2_side1.html

CoBiT [2000] *'Control Objectives for Information and Related Technology'*: [online] ISACA [Information Systems Audit and Control Association] Last Accessed on 12 July 2002 at URL: http://www.isaca.org/cobit.htm

Costello, S. [2002] *'OASIS Creates Web Services Security Body'* [online]. May 13. Last accessed on 12 July 2002 at URL: http://staging.infoworld.com/articles/hn/xml/02/05/13/020513hnoasis.xml?Template+/stc

Eagle, L. [2002]. *'Key Questions to Ask Your ASP: TruSecure'* [online] May. Last accessed on 12 July 2002 at URL: http://thewhir.com/features/security.cfm

Ferengul, C. [2002]. *'Best Practices in Web Hosting Service-Level Agreements'* [online] Meta Group, Jan 29. Last accessed on 12 July 2002 at URL: http://techupdate.zdnet.com/filters/printerfriendly/0,6061,2843179-92,00.html

Geiger, W. [2001]. *'Proactively Guarding Against Unknown Web Server Attacks'* [online] Published by the SANS Institute. September 12. Last accessed on 12 July 2002 at URL: http://rr.sans.org/web/guarding.php

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Helgeson, R.G. [2001].*' Denial-of-Service Attacks Can be Avoided: Eleven Steps Network Administrators Must Take to Protect Their Systems'*. [online] Secure Computing Magazine. September. Last Accessed 12 July 2002 at URL: http://www.scmagazine.com/scmagazine/sc-online/2001/article/036/article.html

ISF [2002] '*Information Security Forum: Standard of Good Practice in Information Security'* [online] Last accessed 12 July 2002 at URL: http://www.isfsecuritystandard.com/index_ie.htm

ISO 17799 [2002] Collection of free and subscription resources for Security Assessment using the ISO17799 standard. Last accessed on 12 July 2002 at URL: http://www.e-security-e-commerce-security.com/

Kay, E. [2000]. *'No Security Blanket Exists'* [online] White Paper, Special Advertising Supplement, Chief Information Officer Magazine. 1st May. Last Assessed 12 July 2002 at URL: http://www.cio.com/sponsors/050100_ebiz_story2.html

Kaye, D. [2002]. *'Strategies for Web Hosting and Managed Services'*. 1st ed. John Wiley & Sons Inc, New York.

Kessler, G C [2000]. *'Web of Worries'* [online] Information Security Magazine, April. Last accessed on 12 July 2002 at URL: http://www.infosecuritymag.com/articles/april00/cover.shtml

Kossakowski, K & Allen, J. [2000] *'Securing Public Web Servers'* [online] Published by Carnegie Mellon University, Software Engineering institute, April. Last accessed on 12 July 2002 at URL: http://www.cert.org/security-improvement/modules/m11.html#who

Liu, V. [2002]. *'Designing and Deploying Effective Defenses Against Denial-of-Service Attacks'*. [online] Secure Computing Magazine. January. Last Accessed 12 July 2002 at URL: http://www.scmagazine.com/scmagazine/sc-online/2002/article/01/article.html

Matlus, R & Maurer, W. [2002]. Writing Security, Business Continuity into Outsourcing Deals. [online] Published by The Gartner Group, April 1, Last accessed on 12 July 2002 at URL: http://techupdate.zdnet.com/filters/printerfriendly/0,6061,2859358-92,00.html

Miller, SK. [2002] *'Buzzing About Security'* [online] Last accessed on 12 July 2002 at URL: http://www.infosecuritymag.com/2002/jan/departments_news.shtml

OWASP. [2002] *'A Guide to Building Secure Web Applications and Web Services.*' [online] The Open Web Application Security Project. May. Last accessed on 12 July 2002 at URL: http://www.owasp.org/guide/index.shtml

Sherwood, J. [1997]. Managing Security for Outsourcing Contracts. *Computers & Security,* 16, p603-609

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Stein, LD & Stewart, JN. [2002]. *'The World Wide Web Security FAQ.'* [online] Last accessed on 12 July 2002 at URL: http://www.w3.org/Security/Faq/

Tuesday, V. [pseudonym] [2001] *'Major Security Concerns Take Back Seat as ASP and Corporate Lawyers Argue Over Minute Details'* [online] Security Managers Journal. Published by SANS Institute, Sept 3. Last accessed on 12 July 2002 at URL: http://www.sans.org/newlook/resources/SMJ/090301.htm

UUNET [2002]. *'NT Web Hosting Security: Disclaimer.'* [online] Last accessed on 12 July 2002 at URL: http://www.uunt.net/documentation/uunet/ntsecurity.htm

© SANS Institute 2000 - 2002, Author retains all rights.