Global Information Assurance Certification Paper

THE RIGHT STUFF:

A GUIDE TO BUILDING AN ISSP PERSONAL KNOWLEDGE BASE

Abstract

> A knowledge base is a centralized repository for information. (WhatIs?Com[1])

In 2001, Robert Taylor wrote "Keep Current with Little Time"[2], in which he offered a list of useful websites for overworked ISSPs. My goal in this article is to update and substantially expand his list. My intention, as was Taylor's, is to offer suggestions for the beginning ISSP; the list of resources may also help the established IT professional who must keep up with security issues in addition to general systems support duties.

The ISSP knowledge base, like a personal library, includes books, periodicals, and – nowadays – an extensive list of Web resources. As ISSPs, we rely on an inventory of professional information that keeps expanding and changing with technology, industry events, and our careers. We tend to give away outdated books and throw out old magazines and newspapers. Due to the mutability of the Web, we must regularly review our Web resources, to ensure they still meet our needs – for that matter, to ensure they still exist.

I Defining the Right Stuff

> Start with what they know, build on what they have. (Kwame Nkrumah[3])

Figuring out what resources to gather can easily overwhelm anyone; the quantity of materials available to someone with open Web access is impossible to encompass. The Computers and Internet sections at Borders or Barnes and Noble offer a mind-numbing array of books; computer-related magazines absorb as much as one-sixth of the space a bookstore reserves for all magazines. Perhaps the simplest place to begin is with what you already have and what you already know, then add what you need to know. This exercise can lead to an understanding of what you do not have and do not know. This, in turn, helps you decide what additional resources you need. The Web has become such a ubiquitous presence in 21st century culture, that nearly all professional non-Web resources (books, journals, magazines, even daily newspapers, radio stations, and television programs) include URLs for "more information." These websites include hyperlinks to several more resources. So you begin by looking at the resources already in your knowledge base, selecting topics you need to understand better, checking out a

---

[1] http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci753399,00.html, "knowledge base – a searchCRM definition," WhatIs?Com, TechTarget, 2003; Last updated on: 06 Jul 2001.
[2] http://www.sans.org/rr/catindex.php?cat_id=48, Robert Taylor, "Keep Current with Little Time," SANS Reading Room, 19 September 2001.
[3] http://web.utk.edu/~wrobinso/560_lec_commun-analysis.html, Kwame Nkrumah (1909-1972, first leader of post-colonial Ghana), as attributed by William C. Robinson, "Community Analysis," University of Tennessee, Knoxville, 2003.

few of the websites listed, following interesting links to other interesting links to still more inter….

A second method – and probably most often used by over-worked IT people – is to start with a problem that needs solving "yesterday." A vendor's product is acting strangely; the morning news announced a new email virus sweeping the Internet; a buddy mentioned a new firewall trick over a couple beers last night …. You have a question; the World Wide Web has *all* the answers.

It becomes far more efficient to depend on a relative handful of websites for most of your resources than to go to a search engine every time you have a question. But which sites? If you had the time, you would organize your personal knowledge base according to job duties and search out websites that fit those categories and look at, maybe, the top ten or twenty. You have to figure out 1) if the site is actually relevant, 2) if it is easy to navigate, and 3) if its information is accurate. Other considerations might include response/load time, frequency of page updates and amount of visual (or aural) "clutter." For someone with attention deficit disorder (like me), all the fancy graphics, animations, flashing text, flowing banners, music, and sound effects are so much annoying, distracting mental static; I need clean, clear, quiet pages. (It is amazing how much junk a properly configured Web browser and firewall can bounce!) All these qualities are subjective; only you can decide if a particular site will be useful, and it takes time and experience with a site to make that judgement.

Over the long term, your knowledge base will grow through recommendations from other sources, through your own Web searches and through the evolution of the Web itself. You will discover that websites change, as technology, content focus, and site ownership change; some sites will become inactive – still on the Web, but no longer maintained – and their information will become outdated; some suddenly disappear altogether. Your own responsibilities and interests will change, as well. Nevertheless, there is a core of IS security websites that will (almost) always remain in your knowledge base.

The bulk of the ISSP's knowledge base must come from the Internet. It is the only "delivery system" that can provide timely warnings about threats against their systems. On the other hand, keeping up with *all* the ISS resources on the Internet is impossible. There are two ways to handle this problem, either in a structural, logical way or in an ad hoc, incidental way.

Following the structured method, you first define your job responsibilities, perhaps in terms of the nine tracks of security training offered by the SANS (SysAdmin, Audit, Network, Security) Institute,[4] or the "ten domains of the common body of knowledge,"[5] from the International Information Systems Security Certification Consortium $(ISC)^2$ or according to the hardware and software one is protecting. The SANS approach is practical/technical and is organized by such topics as perimeter protection, intrusion detection, audit, forensics, and security policies. The $(ISC)^2$ is somewhat broader:

[4] http://sans.org, "SANS Institute – Computer Education and Information Security Training," The SANS Institute, 2003.
[5] https://www.isc2.org/cgi-bin/content.cgi?category=8, "Common Body of Knowledge, $(ISC)^2$.

access control, disaster recovery, physical security, law. The hardware/software approach relies on vendor knowledge bases and technical support pages; but the vendor sites will lead inevitably to other, vendor-neutral sites. In a large corporation or government agency, an IS tech's responsibilities may be specialized to some degree; in small organizations with only one or two IT people, their responsibilities may cover all areas of information security.

In conjunction with defining functional duties you must also measure the importance of the operating system platform(s). Historically, a pure Microsoft Windows environment had little need for UNIX/Linux resources and *vice versa.* Nowadays, few "pure" shops remain; even the specialist in UNIX/Linux needs to know something about Microsoft insecurities. Linux is evolving into a robust enterprise technology, to the extent that Red Hat now has Enterprise Linux and Fedora[6] and Novell is buying SuSe[7].

The second step is to determine how timely various kinds of information must be. In this respect, the three major sources of information are books, periodicals, and the Internet. Each source has a role in the ISSP's working library: books cover fundamentals and principles; periodicals highlight the dynamics of IS technology and policies; the Internet delivers focused, critically timely data.

The third step is to collect recommendations from resources already in hand: books, people, magazines, etc.

The final step is to look at the recommended resources, to decide if they are helpful to you.

Using the ad hoc method, you simply start with the question you need answered, decide what website is the likeliest to produce a viable answer, then follow promising links until you find the answer. You collect books and magazines almost incidentally, as you recognize topics you need to know more about. Even following the adhoc process of creating an ISSP knowledge base, you will consider how each source of information can best serve your needs.

The fundamentals of information systems do not change much: the nature and relationships of bits and bytes, input/output, processing and storage are the same now as they were in Eniacs' day. Even with the advent of greater capability and sophistication, much of the old technology remains useful: html has not entirely replaced ASCII, nor has streaming audio/graphics replaced text. Books about specific operating systems and applications are timely enough for all but the most forward of bleeding-edge technologists. Books that cover various areas of IS security are also useful in pointing out the theory of good security practices and discussing types of risks and threats. They will not be current with the lastest attacks, but they do cover most "popular" types of attacks and proven counter-measures. An excellent beginning for gathering Web resources is a study guide for (almost any) certification. Vendor product

---

[6] http://www.redhat.com/solutions/migration/rhl, "redhat.com – Red Hat Enterprise Linux Migration Center," Red Hat, Inc., 2003.

[7] http://www.novell.com/news/press/archive/2003/11/pr03069.html, "Novell: Novell Announces Agreement to Acquire Leading Enterprise Linux Technology Company SuSE Linux," press release, Novell, 4 November 2003.

certification guides generally point to vendor websites, but “vendor-neutral” certification guides are more egalitarian in their selections.

Periodicals cover current concerns, both actual events and future trends. They can evaluate new technology and products, analyze legislation, attempt to predict what is coming in the future – in short, provide useful information about the dynamic aspects of IS. Novell recently announced plans to acquire SuSe, who produces a popular distribution of Linux, and develop NetWare products to run on the Linux kernel[8]. By the time this information reaches book form, it is too late to make any strategic decision as to whether to move completely over to Windows or to begin migrating to Linux. On the other hand, I do not care about this *today*; I need to know if I have to go patch-hunting for the latest Novell vulnerability. Likewise, SCO’s recent attempts to highjack Linux[9] will be irrevelant to tactical operating decisions by the time someone writes a book about it, as well as irrevelant to my daily routine. Periodicals also provide tips, tricks, and hacks that can make a daily task more efficient or effective; these often are “secrets” buried too deeply in user manuals for harried IT staff members to dig out, or a bit of programming someone tinkered up to take advantage of a poorly implemented “feature.” They also include a URL “to learn more” at the end of nearly every article; many magazines have added a regular “Interesting websites” feature, as well.

In some respects, the Internet is becoming the superset of all information resources. The Web, Usenet, and IRC can provide the same information as print materials, usually with greater timeliness and in immediately relevant doses. Electronic versions have mirrored many print periodicals for several years, and cyber-books are becoming increasingly available. Vendors, organizations, and even individuals maintain Web archives of information, all of it efficiently accessible through search engines. Usenet is a vast collection of discussion groups (by one count, over a hundred thousand![10]), organized by topic. Go to the appropriate newsgroup, present the problem, in a few days get several suggested solutions. Chatrooms provide even quicker feedback, as well as instant virtual water-cooler conversation, when one is stuck at work in the middle of the night. In the last year or two, the Web has dramatically changed from millions of sites offering narrowly defined services – electronic magazines, newsletters, bug reports, specific vendor products – to millions of sites offering a huge range of resources, making it nearly impossible to neatly categorize such sites. The Web has evolved so far as to incorporate the best features of the Usenet; many sites include discussion groups, which are usually moderated and kept “on topic.” (Some also support chatrooms.) My focus, like Taylor’s, is to get someone started. By exploring these sites and following interesting links, ISSPs should be able to develop the best resources for their work and interests.

Part III (“(Some of) the Right Stuff”) offers a sample of resources that a new (or “part-time”) ISSP should find useful as a starting point. With time and experience, this list will be modified to suit individual needs. However, many of these resources will remain in

---

[8] Novell, Ibid.
[9] http://www.infoworld.com/reports/SRscosuit.html, “InfoWorld Special Report: Linux under siege: Tracking the course of SCO’s lawsuit,” (various authors), IDG News Service, 2003.
[10] http://www.newsfeeds.com, “Welcome to Newsfeeds.com,” Newsfeeds.com, 2003.

the working library of even the most experienced ISSP. I focus, as Taylor did, on Internet resources, but I also offer some thoughts about print media; as noted above, they are also valuable to an ISSP. Unlike Taylor, who favored hacker sites, I give more weight to the law side of the security culture.

A note concerning "hackers": mainstream computer users tend to carelessly apply the term "hacker" to anyone who criminally breaks into government or company computer systems; books and news articles have popularized this view. However, hackers are people who simply do computer things in unorthodox ways. According to WhatIs?Com, "Hacker is a term used by some to mean 'a clever programmer' and by others, especially journalists or their editors, to mean 'someone who tries to break into computer systems.'"[11] Infoplease defines "hack" as (among other things) "to devise or modify (a computer program), usually skillfully"[12]. Crackers, a sub-group of the hacker community, do unorthodox things for unauthorized purposes, not necessarily with malice aforethought. As WhatIs?Com puts it, "A cracker is someone who breaks into someone else's computer system, often on a network, …[and] intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there…."[13] The distinction seems fuzzy when exploring "whitehat" (good guys) and "blackhat" (bad guys) websites, but it is important to keep in mind. Hanging out in blackhat virtual communities can be quite educational. When a vendor does not give me a back door into the computer of the CFO, who dropped dead yesterday, I will try nearly any means to get the information he thought was too sensitive to trust to the network servers. Knowing the state of the hacker's art also may help me protect my systems from new exploitations. On the other hand, other far more talented and experienced IS security professionals can spy on such groups far more effectively than I can; the whitehats will tell me what to watch for and how to protect against it. (The trend in book publishing is shifting; see the comments by who is editor of O'Reilly and Associates new "Hack" books.[14])

II Finding the Right Stuff

> Knowledge is of two kinds: we know a subject ourselves, or we know where we can find information upon it. -Samuel Johnson, 1755.[15]

The World Wide Web has not only continued to expand, but has evolved as well. A significantly greater variety of media – pictures, animation, .wav, radio, MP3, streaming video – is available, and individual websites are constantly adding new features. A typical "professional" site may carry news, newsletter subscriptions, blogs, SIG forums, webcasts, chat rooms, links to similar sites, and even moderated newsgroups. This makes websites exceedingly difficult to categorize. A website that once was simply the

---

[11] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212220,00.html, "hacker – a searchSecurity definition," TechTarget, 2003, Last updated on 24 Sep 2003

[12] http://www.infoplease.com/ipd/A0467007.html, "Meaning of hack," Infoplease, Pearson Education, 2003.

[13] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html, "cracker – a searchSecurity definition," TechTarget, 2003, Last updated on 14 Oct 1999.

[14] http://hacks.oreilly.com/pub/a/oreilly/hacks/whyhacks.html, "Why the Hacks Series," O'Reilly and Associates, Rael Dorfest, O'Reilly and Associates, 2003, October 2003.

[15] Boswell, S. The Life of Samuel Johnson,

cyber version of a monthly magazine has become a portal to massive amounts of data in half-a-dozen formats and a knowledge base in its own right.

Where the Web excels is in automatic and nearly instant delivery of warning. Several agencies, organizations, and vendors maintain orderly distributions of alerts about attacks, malware releases, vulnerabilities and critical IS security news. Perhaps the greatest strength of the Web is the ability of search engines to ferret out specific information throughout a virtually limitless storehouse of resources. It has, however, a few disadvantages. Searching that infinite storehouse often returns an overwhelming number of pages to rummage through. Marketing schemes, which help pay for the Web, often cause search engines to organize the results they return based on criteria having nothing to do with the end user's objectives.[16] (This can be mitigated by restricting a search to first-order domains such as .org and .gov or by excluding .com.) Because the Internet is a kind of anarchy, there is no authority to enforce any standard of truth in the information or even order among the users. Likewise, no single authority can deter, prevent or punish malefactors.

ISSPs must decide what stuff is right for their purposes. Therefore, the following is a only sample selection of available resources, rather than a definitive list. In discussing these resources, I hope readers can determine for themselves what they need and how to find it. I have stopped short of listing Internet resources for specific security tools; there are far too many. Most websites include links to a variety of such tools; many websites offer several such tools in one place. In many instances, the URL I discuss is merely an entrance to ultimately hundreds of additional sites.

My experience suggests that an ISSP knowledge base should contain the following types of resources: 1) a selection of general references; 2) books on the systems I am protecting, on the particular aspects that I am responsible for, and on information and computer security in general; 3) a handful of trades and professional periodicals which support my work and keep me informed on news, issues and developing technologies; and 4) copious Internet-specific resources. Internet resources include security alerts and advisories (notification of vulnerabilities and malicious attacks), standards, law, international issues, vendor knowledge bases, moderated discussion forums, SIG portals, and software tools (COTS, as well as freeware and shareware).

A growing trend on the Web is free "registered user" schemes. Every site listed here offers additional benefits to registered users; most require registration to take an active part in site-sponsored activities (posting to a discussion group, voting in polls, asking for help or subscribing to email products). On the other hand, registration is still free (unless otherwise noted). Registration requires, at a minimum, a username, password, and email address; some sites also ask for demographic data, such as age, gender, and job title. Newsletters, especially from vendors, often include sales pitches. It is important to weigh the amount of time wasted going through the irrevelant material in order to get to useful information.

Three major challenges of the Internet are its virtually limitless supply of information, the mutability of that supply, and its anarchic structure: we cannot touch every pertinent

[16] http://www.searchenginewatch.com/webmasters/index.php, "Search Engine Submission Tips", SearchEngineWatch.Com, 2003.

piece of information, we cannot trust the information to remain the same, and we cannot automatically trust the veracity of any piece of information. Search engines return results biased by marketing objectives, are only as efficient as our queries, and cannot make value judgements; Web portals will lead to only a selected number of additional resources; linked sites may be less reliable than the referring site. Our opinions as to the usefulness of a particular resource depends on our needs and on both our trust in the source of a recommendation and our direct experience using a resource.

III (Some of) the Right Stuff

> "Oook!" said the Librarian, instantly." [who is, in fact, an orangutang] (Pratchett)[17]

In the course of writing this article, I looked at several hundred Web pages. In order to keep this a manageable length, I include here only my top three to five resources.

General References

I rely heavily on three non-IT references in all my work: an (abridged) encyclopedia, a big dictionary, and a thesaurus. Most word processing applications include a dictionary/ thesaurus function, but I have found it to be of limited usefulness. An excellent, all-around online resource is Bartley.com. The "Reference" page lists 35 books covering general information (encyclopedia, dictionaries, etc.), quotations, English usage, religion and mythology – even *Gray's Anatomy*, Emily Post's *Etiquette*, and Fannie Farmer's *The Boston Cooking-School Cook Book*.[18]

Information Please[19] is another cyber reference shelf. It provides information from an almanac, several atlases, dictionary, and encyclopedia. Another dictionary/ thesaurus site is Merriam-Webster Online[20]; a paid subscription gets one to advertisement-free pages for its unabridged editions and other services, but basic word lookup is free.

The encyclopedia is admittedly of limited use when investigating IT topics (to say nothing of IT security), but a one-stop reference is an enormous time saver, when the IT jargon gets ahead of me. These IT-centric resources can stand in good stead:

WhatIs?com[21] is a wonderful website maintained by TechTarget for word hounds of IT information. A search for a definition of an IT word or phrase returns not only the definition (and its source), but a selection of related "Best Web Link Categories," news articles, technical advice, and vendor products. An especially nice feature is its search engine; WhatIs?Com returns alternative Web sources for definitions, whether it has a definition or not. (Note, however, that the list of sources is topped by "sponsored links," i.e., advertising, and many definitions are from other TechTarget sites.) I use this site often enough to keep it on my Web browser's "Personal Toolbar." A similar "general IT

---

[17] Pratchett, Terry, Soul Music, *Death Trilogy*, p. 392, Victor Gollancz, London, England, 1998.
[18] http://www.bartleby.com/reference, "Reference: Dictionary, Encyclopedia, Thesauri, Usage, Quotations, and more," Bartleby.com, 2003.
[19] http://www.infoplease.com, "Information Please," Infoplease, Pearson Education, 2003.
[20] http://www.m-w.com, "Merriam-Webster Online," *Merriam-Webster Dictionary*, 2003.
[21] http://whatis.techtarget.com, "WhatIs.Com," TechTarget, 2003.

information" site is Webopedia,[22] which is a part of Internet.Com. It is not as complete as WhatIs?Com, but adequate for most purposes.

A sub-category of dictionaries is the "Jargon File," aka the Hacker's Dictionary. Several websites host a version. My favorite is archived by the Universiteit van Amsterdam (University of Amsterdam) in Holland,[23] because it is the easiest to navigate; it also seems to be the best maintained of the several that Taylor listed.[24] Most hacker jargon is included in Whatis?Com's search index, if not in its dictionary directly, but Webopedia is not as inclusive.

Sometimes it helps to know who you're looking at. Several sites provide WHOIS lookup services which list registration information of Internet domain names. ARIN (American Registry for Internet Numbers)[25] covers the US and has links to the registries for Latin America (Latin American and Caribbean Internet Addresses Registry – LACNIC), Europe and Africa (Réseaux IP Européens Network Coordination Centre – RIPE NCC)[26] and Asia-Pacific Rim (Asia Pacific Network Information Centre – APNIC).[27] RIPE includes a list of all ISO-3166 regional identification codes (239, at current count), including Antartica (.aq), Pitcairn (.pn) and the Vatican (.va). The two-letter designation is not always obvious: for example, .hr is Croatia, because its local name is Hrvatska.

Three other resources that belong in the "General Reference" category are Web browsers, search engines, and newsreaders (plus, perhaps, IRC software). One can argue that these are tools, not resources, yet they are such a fundamental part of getting around the Internet that they deserve attention. The manner in which they present content is an important, though often subliminal, kind of information itself. Since these "tools" are somewhat off-topic, I discuss them in Appendix A: Internet Tools.

Security Alerts and Newsletters

The "Alerts" or "Security Advisories" section of an ISSP knowledge base is the most critical. We simply cannot keep up with every threat to the Internet, and we do not really have time to sort through *all* the alerts to find the ones relevant to our systems; we really do not have the time and energy to waste on guessing whether any given warning truly warrants our attention. We need a brief selection of absolutely reliable websites which can send us automatic notification of security issues important to us. By subscribing to appropriate mailing lists, we automatically receive relevant email messages about newly discovered vulnerabilities and attacks.

---

[22] http://www.webopedia.com, "Webopedia: Online Dictionary for Computer and Internet Terms," Jupitermedia Corporation, 2003.
[23] http://www.science.uva.nl/~mes/jargon, "Jargon 4.2 node: Jargon File 4.2.0 dated Jan 31, 2000," Eric Raymond, ed., Faculteit der Natuurwetenschappen, Wiskunde en Informatica, de Universiteit van Amsterdam, 2000.
[24] Taylor, p.4.
[25] ftp://ftp.arin.net/netinfo/iso3166-countrycodes, "Some Codes from ISO 3166," ARIN.
[26] http://www.ripe.net/ripencc/mem-services/general/indices/index.html, "RIPE NCC Local Internet Registries: Country Index," RIPE NCC.
[27] http://www.apnic.net/info/reference/lookup_codes_text.html, "List of ISO 3166 codes and corresponding RIRs," APNIC Pty. Ltd., 2003, Last modified 19 November 2003.

A primary source of alerts are the Computer Emergency Response Teams (CERTs). They serve as clearing houses for any untoward Internet activity in many parts of the world. The primary CERT in the U.S. is run by Carnegie-Mellon University.[28] The organization of European sites is a little complicated. The Trans-European Research and Education Networking Association (TERENA) is the technical association which is responsible for the international telecommunications (including the Internet) infrastructure.[29] A task force of TERENA, the TF-CSIRT (Task Force-Computer Security Incident Response Teams) coordinates the activities of member European CSIRTs through a variety of conferences, training programs, accreditations, and periodic reviews. The Trusted Introducer maintains a hyperlinked list of all the European CIRTs it knows about, classified as to their accreditation status: listed (simply known), accreditation candidates (undergoing the accreditation process), or accredited (successfully completed accreditation).[30] Australia supports two collaborative organizations (the National Information Technology Alert Service and the National IT Incident Reporting Scheme) who jointly maintain AusCERT. [31]

Another excellent security alert site is Bugtraq, maintained by Security Focus. As Security Focus puts it, "BugTraq is a full disclosure moderated mailing list for the *detailed* discussion and announcement of computer security vulnerabilities: what they are, how to exploit them, and how to fix them." [32] Full disclosure means the vendor responsible for the vulnerability may not be aware of it before it is published here. Moderated means humans try to ensure that the posting is relevant and reasonable. Detailed means the descriptions and discussions about a vulnerability may be very technical. Security Focus supports over 30 daily mailing lists[33] and three weekly newsletters.[34] Because I come from the business administration side of IT, I lack the engineering background to make effective use of BugTraq alerts. I do pay attention to the "Focus on Microsoft" mailing list, because – whether I understand the technical details or not – it tells me about problems I need to address.

A careful selection of newsletters and digests is also important; these focus on important events, as well as warnings, in the segments of IS that we are most concerned about. Every website listed in this article emails at least one daily or weekly newsletter; most simply report news, often well-larded with product blurbs. Digests from the CERTs and other watch dogs are weekly summations of the vulnerabilities and malware discovered that week. They are slightly more likely to include URLs for patches or advice on work-arounds, simply because enough time has passed since the initial warning to devise countermeasures.

---

[28] http://www.cert.org/nav/alerts.html#summaries, "CERT Coordination Center Alerts," Carnegie-Mellon Software Engineering Institute, Last modified: 17 December 2003.
[29] http://www.terena.nl/about, "TERENA -- About TERENA," TERENA, Last modified 14 November 2002.
[30] http://www.ti.terena.nl/teams/index.html, "Trusted Introducer / CSIRT Teams," S-Cure (Amersfoort, NL), 2003: Last updated: 03 June 2003.
[31] http://national.auscert.org.au, "AusCERT – Australia's National Computer Emergency Response Team," AusCERT.
[32] http://securityfocus.com/archive/1, "SecurityFocus BugTraq Mailing List," Security Focus, 2003 (click on "About This List").
[33] http://securityfocus.com/archive, "SecurityFocus Mailing Lists Archive," Security Focus, 2003,
[34] http://securityfocus.com/newsletters, "SecurityFocus Newsletters," Security Focus, 2003.

The SANS Institute sends out three weekly bulletins, covering the most critical IS vulnerabilities, important IS news, and privacy issues.[35] Security Focus newletters are weekly digests of reports on Microsoft, UNIX, and Linux.[36]

Vendor-specific alerts are also critical. While operating systems and applications are more susceptible to vulnerabilities and attacks, the drivers and firmware that make hardware work also carry risks; furthermore, as software is updated, hardware may require updated drivers .

Portals and Forums

> Portal is a term, generally synonymous with gateway, for a World Wide Web site that is or proposes to be a major starting site for users when they get connected to the Web or that users tend to visit as an anchor site…. Some major general portals include Yahoo, … Netscape … and … AOL.com. Examples of niche portals include Garden.com (for gardeners), Fool.com (for investors), and SearchNetworking.com (for network administrators). (WhatIs?Com)[37]

> [Forum}: An online discussion group. Online services and bulletin board services (BBS's) provide a variety of forums, in which participants with common interests can exchange open messages. (Webopedia)[38]

The value of portals and forums is the concentration of resources which are accessible from one site. Portals offer extensive links to related sites; forums offer an extensive community of experts and practitioners at one site. Many websites that began life as electronic versions of periodicals have evolved into virtual emporiums of information. Web technology makes adding hyperlinks to related sites such a trivial task that it is nearly impossible to find a website that does *not* include such links. Maintaining moderated forums is more labor-intensive, but special-interest forums (as captive audiences for sales and marketing efforts) provide enough value to the website owners that they, too, have become ubiquitous. I make the distinction here based on what the website's ultimate goal is (or at least, what I understand its goal to be) and my subjective judgement on the ratio between "vendor-neutral" information and product-oriented information. Because I use software that blocks advertising, my judgement is probably skewed toward including sites that include more advertising than I actually see.

The websites that I consider to be the most valuable IS portals are the SANS Institute and the U.S. National Institute of Standards and Technology (NIST); they are extensive, reliable, and open. Some useful "dot-com" portals – commercial websites, selling products or advertising – include O'Reilly and Associates, InfoSysSec, and VNUNet. AntiOnline is an excellent IS forum; TechTarget Network is a collection of forums worth visiting.

---

[35] http://www.sans.org/newsletters, "SANS Institute – Computer Security Newsletters," SANS Institute, 2003.
[36] http://securityfocus.com/newsletters, "SecurityFocus Newsletters," Security Focus, 2003.
[37] http://whatis.techtarget.com/definition/0,,sid9_gci212810,00.html, "portal – a whatis definition," TechTarget, 2003.
[38] http://webopedia.com/TERM/f/forum.html, "forum – Webopedia.com," *Webopedia*, Jupitermedia Corporation, 2003.

For someone new to information security, the SANS Institute is the first place to go. SANS has been active in computer security since 1989.[39] Its home page features its Computer Security Training Events Calendar,[40] but the conferences merely scratch the surface of all that SANS provides. From the beginning SANS has sponsored research and education in an open, cooperative environment, which has led to consensus standards in many areas of information security. It publishes three weekly newsletters, which summarize the most important information about vulnerabilities and security news. The Reading Room[41] contains over a thousand articles: case studies, white papers from security experts, and research papers by certification candidates. The Internet Storm Center (ISC)[42] provides near-realtime reports on various types of suspicious Internet traffic, news bites, and "infocon," a color-coded assessment of the Internet's general health. S.C.O.R.E. is a joint project with the Center for Internet Security (CIS) to develop security standards and best practices.[43] S.C.O.R.E.'s home page lists benchmarks and scoring tools for various operating systems, checklists for a variety of hardware devices and software, several incident handling forms for both computer security and intellectual property (i.e., incidents that may have compromised a system's data content). Although SANS is one of the oldest organizations to offer IS training, it did not begin its certification program until 1999. SANS supports itself through the the fees charged for conferences, training, and training materials. All other information, policy guides, news bulletins, consensus standards, etc. are openly available on its website; furthermore, SANS encourages all security professionals to participate in any of its research projects.[44] My only disappointment with the SANS website is its lack of hyperlinks to other security-centered websites; on the other hand, every paper in the Reading Room includes extensive links on specific topics.

NIST is the U.S. federal agency most directly involved in Internet technology and sandards and the most accessible. I have discussed it in detail with other U.S. government IS websites.

InfoSysSec quotes Yahoo! editors: "The most comprehensive computer and network security resource on the Internet for Information System Security Professional."[45] InfoSysSec maintains three closely related websites: InfoSysSec.com, InfoSysSec.net, and InfoSysSec.org.[46] (They are so closely related, they look identical.) The home page is a true portal. It provides very little of its own content, but lists hundreds of links to other IS resources: news, alerts, patches, specific malware programs, IT glossaries, forums, tools, and other IS sites. A sister site, Security News Portal, collects IT news from numerous sources.[47]

---

[39] http://sans.org/aboutsans.php, "SANS Institute About the SANS Institute," SANS Institute, 2003.
[40] http://sans.org, "SANS Institute," SANS Institute, 2003.
[41] http://www.sans.org/rr, "SANS InfoSec Reading Room," SANS Institute, 2003.
[42] http://isc.sans.org, "Internet Storm Center," SANS Institute, 2003.
[43] http://www.sans.org/score, "S.C.O.R.E. – Security Consensus Operational Readiness Evaluation," SANS Institute, 2003.
[44] http://www.sans.org/projects, "SANS Institute: Security Projects," SANS Institute, 2003.
[45] http://www.infosyssec.net/index.html , "Hacking and Hackers -- Computer Security Programs Downloading Search Engines Portal Nwes," InfoSysSec Security Portal, 2002.
[46] http://www.infosyssec.com/infosyssec/advertise.htm, "Advertising that targets the real IT security professionals," InfoSysSec Security Portal, 2002.
[47] http://www.snpx.com/pagetwo.html , "Security News Protal,…Page Two," SecurityNewsPortal.com., 2001.

AntiOnline[48] is a computer and network security forum that is also a portal. It hosts a large archive of security text files, a security downloads area, a calendar of security events, and a version of the Hacker's Dictionary. Among its lists are: newsletters (over 100), security certifications (21 from nine organizations – by no means a complete list), and degrees in security from (U.S.) colleges and universities (17 at current count). It includes news items and sponsored products. While it covers security issues in general, it has a distinctly Linux flavor. It is owned by Enterprise IT Planet.Com (which in turn is owned by Jupitermedia[49]). EITPlanet is far more market-driven, but it also covers IT news and supports forums and resources in storage and networking, as well as in security. AntiOnline has been around for a while, and its webmasters are active in both policing the membership and keeping the site relevant to its members. It is possible to lurk without becoming a member, but registration is required to take an active part in the site; this includes posting to the forums, voting on threads (and other members' continued participation), and submitting tips and tutorials. While the forums are not subject to an assigned moderator, the AntiOnline community as whole keeeps everyone on reasonably good behavior. Among the hundreds of IS websites I have visited, AntiOnline is unique: it is sustained almost entirely by its very active membership, and it shares both the advantages and disadvantages of Usenet. You can enjoy the community and obtain very useful information, but it may take some time and effort and you cannot expect everything you find here to be reliable. (Another Jupitermedia portal worth looking at is Wi-FiPlanet.com; it is a portal for the wireless industry.[50])

New Order, a computer security portal/forum in Slovakia (remember my remark about knowing who you are looking at?), is similar to AntiOnline. It supports an active international community interested in a wide range of topics besides information security. Several newsletters are available in a dozen European languages, although the site's "native language" is English. It boasts "4242 link and files" in its "file archive and links database.[51]

TechTarget Network[52] is a closed media company forum, which means advertising ranks high among its company priorities and all hypelinks point to other TechTarget sites (or advertisers). Nevertheless, it produces useful information in 17 specialized IT forums, organized by applications (CRM and SAP); "core technologies" like database, networking, and security;[53] and platforms, including Linux[54] and Windows.[55] Each area provides news, expert advice, upcoming TechTarget conferences and webcasts, products and vendors, polls and surveys, white papers, newsletters, career services, and a host of other resources. TechTarget also supports WhatIs?Com; one needs to note which definitions are provided by "sponsored" links or related TechTarget sites, then decide if the definition is biased accordingly.

---

[48] http://antionline.com, "AntiOnline – Computer Security," EnterpriseITplanet.com's AntiOnline, Jupitermedia Corporation, 2003.
[49] http://www.internet.com/corporate/about.html, "About Jupitermedia," Jupitermedia Corporation, 2003.
[50] http://wi-fiplanet.webopedia.com, "www.Wi-FiPlanet.com," Jupitermedia Corporation, 2003.
[51] http://www.neworder.box.sk, "New Order – the computer & networking security portal," Box Network team, 2002.
[52] http://searchtechtarget.techtarget.com, "SearchTechTarget – Welcome," TechTarget, 2003.
[53] http://searchsecurity.techtarget.com, "SearchSecurity.com," TechTarget, 2003.
[54] http://searchenterpriselinux.techtarget.com, "SearchEnterpriseLinux.com," TechTarget, 2003.
[55] http://searchwin2000.techtarget.com, "SearchWin2000.com," TechTarget, 2003.

A similar portal/forum in Britain is VNU Net.[56] It organizes its information by "centres": news, product reviews, downloads, advice, and career help. General subjects include security[57] and "Your Business"[58] (which posts additional security-related articles). Unlike TechTarget, it does include occasional links to outside sources. Among other publications, it offers seven free trade magazines[59] (five for IT professionals) and the British edition of *PC Magazine*.[60]

ZDNet,[61] a Ziff Davis online magazine when Taylor included it,[62] is now a portal/forum owned by CNet Networks,[63] along with several other technology-related websites. CNet integrates "an extensive directory of more than 200,000 computer, technology, and consumer electronics products with editorial content, downloads, trends, reviews, and price comparisons"[64] through online magazines, radio ("pushed" webcasts, actually[65]), and technology forums. *ZDNet*, TechRepublic[66] (home for several forums), and CNET News.Com[67] (instant news) are the most useful in covering IT (although they are not specifically focused on IS). CNET itself is primarily about product reviews, as is *CNET Shopper*[68]. (Ziff Davis Media still publishes *Computer Shopper*, which is the print version of *CNET Shopper*, mostly a directory of IT product vendors and advertisements, with some editorial content.)

InformIT[69] is a less useful website; I include it as an example of what to avoid. It focuses on technical resources for IT professionals: databases, "creative media" technologies, networking, operating systems, programming, Web development, wireless, and others. However, it is owned by Pearson Educaton, Inc.; most of the information it offers comes out of Pearson products: books, magazines, or other Pearson websites. The difference between TechTarget and InformIT is attitude. TechTarget labels its products clearly; I have no doubt anywhere on the website about the source of any material. It took me a while to figure this out at InformIT. The most useful link is to Safari Books Online.

For a change of pace, visit DigiCrime, Inc.[70] Not exactly a portal, it makes equally light of security and cybercrime. Please read the disclaimer,[71] before passing judgement on its merits.

---

[56] http://www.vnunet.com, "vnunet.com Homepage," VNU Business Publications Ltd., 2003.
[57] http://www.vnunet.com/News/Security, "vnunet.com Security," VNU Business Publications Ltd., 2003.
[58] http://business.vnunet.com, "vnunet.com SME Business Innovation Centre," VNU Business Publications Ltd., 2003.
[59] http://www.vnusubs.co.uk, "VNU Subscriptions," VNU Business Publications Ltd., 2003.
[60] http://www.pcmag.co.uk, "PC Magazine Online," VNU Business Publications Ltd., 2003.
[61] http://www.zdnet.com, "Information resources for IT professionals – ZDNet," ZDNet, CNET Network, Inc., 2003.
[62] Taylor, p. 1.
[63] http://www.cnet.com, "CNET.com," CNET, CNET Networks, Inc., 2003.
[64] http://www.cnet.com/aboutcnet/company/index.html, "Company Profile," CNET Networks, Inc., 2003.
[65] http://www.cnetradio.com, "CNET Radio Direct," CNET Networks, Inc., 2003.
[66] http://www.techrepublic.com, "TechRepublic – Real World. Real Time. Real IT." TechPublic, CNET Networks, Inc., 2003.
[67] http://news.com.com, "CNET News.com – Technology news and business reports," CNET Networks, Inc., 2003.
[68] http:// http://shopper.cnet.com, "Comparison shopping from qualify online and local stores," CNET Networks, Inc., 2003.
[69] http://www.informit.com, "InformIT – Your Online Guide to Tech Reference," InformIT, Pearson Education, 2003.
[70] http://www.digicrime.com/dc.html, "DigiCrime, Inc." DigiCrime (Kevin McCurley).

Government and Law Resources

Standards of information security ultimately flow from government. In the U.S. legislation, case law, regulations, and Executive Orders define policies and permit or restrict practice, regardless of what the technology itself can or cannot do. A great deal of research and development by various federal government agencies created and has fundamentally shaped the Internet; the needs of "national security" have had an equal impact on information assurance. Sites hosted by government agencies are not as open as commercial sites; some pages and services are restricted to government personnel; yet the publically available informaton is no less valuable. While Taylor included a few of the following websites, he did not present them as government resources.

The National Institute of Standards and Technology (NIST) website is both portal and forum for information security and information technology standards. The first place to look at is the Computer Security Resource Center (CSRC),[72] which is the website of the Computer Security Division (CSD) of the NIST Information Technology Laboratory (ITL). The CSD sponsors research, symposiums, education initiatives, and publications dealing with computer technology and information security. The CSRC site lists NIST news items, current projects, and links to the five program areas of research and development that the CSD is participating in. Its site links to a "Vulnerability and Threat Portal" (labeled "ALERTS" on nearly every page within the ITL)[73], which provides statistics, latest vulnerabilities reported, links to alerts by CERT, SANS, NIPC (formerly the National Infrastructure Protection Center, now the Information Analysis Infrastructure Protection [IAIP] division in the U.S. Department of Homeland Security[74]), and its own ICAT database of vulnerabilities (which is derived from CERT's CVE database). A list of links to Incident Handling teams includes CERT sites for Australia, Germany, and Europe, in addition to an assortment of U.S. teams (most of which are closed to the public). There is also a search engine for vulnerabilities by vendor, software, or keyword and for NIST CSRC resources by keyword.

Beyond vulnerability information, NIST CSRC publishes a wide array of documents pertaining to standards, proposals, R&D progress and results, and miscellaneous topics. The important series for ISSPs are Special Publications (SPs), Federal Information Processing Standards Publications (FIPS), and – to a lessening degree – the "Rainbow Series" of computer security. The best-known of this 37-volume series is "The Orange Book," officially titled *Trusted Computer System Evaluation Criteria*, which spells out the criteria for meeting seven levels of computer security for the Department of Defense and other U.S. agencies. This is the document responsible for the commercial "C2" standard for secure computer systems. However, the International Common Criteria for Information Technology Security Evaluation (the Common Criteria)

---

[71] http://www.digicrime.com/disclaimer.html, "DIGICRIME IS A JOKE!!!" the "Thief Scientist" (Kevin McCurley).
[72] http://csrc.nist.gov, "NIST Computer Security Division 893 and CSRC Home Page," National Institute of Standards and Technology, U.S. Department of Commerce.
[73] http://icat.nist.gov/vt_portal.cfm, "NIST Vulnerability and Threat Portal," National Institute of Standards and Technology, U.S. Department of Commerce.
[74] http://www.nipc.gov/incident/incident.htm, "National Infrastructure Protection Center (NIPC) – Incident Report," Information Analysis Infrastructure Protection, U.S. Department of Homeland Security.

have superceded it.[75] As a result, the "Common Criteria Evaluation and Validation Scheme" provides several resources for anyone interested in the Common Criteria and their implementation.[76] NIST and the National Security Agency have created the National Information Assurance Partnership to handle the process of converting U.S. standards to the international Common Criteria; the NIAP welcomes participation from the private sector, as well as other government agencies.

Another excellent resource is the Department of Energy's (DOE) Computer Incident Advisory Capability (CIAC). Besides a long list of current security issues, CIAC provides a pageful of "U.S. Federal and Security Information Sites,"[77] organized somewhat by entity (governmental, educational, etc.) or service (databases, CERT). It does not provide automatic emails to parties outside of the federal government (they email only to .gov and .mil addresses), but the material in those emails is contained on the website. You will find them at the "C-Notes" page[78] and the Bulletins page.[79] Other resources include the DOE-IS Webserver with tools and guidelines,[80] a selection of security tools developed by CIAC,[81] and a site dedicated to Microsoft security issues.[82]

FedCIRT, the Federal Computer Incident Response Center has become part of the Department of Homeland Security. At the moment, it maintains its own website,[83] but it will be moving soon. It provides various information about incidents: prevention, reporting, analysis, and response. (One can navigate more easily from the Site Map page.[84])

A government-sponsored CERT called US-CERT was established in September 2003. It works closely with the original CERT at Carnegie Mellon University. Like NIST, US-CERT invites active participation by the public in many of its projects.[85] In addition to the working groups, progress reports, and security alerts, US-CERT maintains a reading room of security-related papers, a webcast page, records of the recent Cyber Security

---

[75] http://www.nstissc.gov/Assets/pdf/nstissam_compusec_1-99.pdf, "nstissam_compusec_1-99.pdf," National Security Telecommunications and Information Systems Security Committee, National Information Assurance Partnership, National Institute of Standards and Technology, U.S. Department of Commerce.
[76] http://niap.nist.gov/cc-scheme/GuidanceDocs.html, "CCEVS WebPage," NIST, Last updated 27 December 2003.
[77] http://www.ciac.org/ciac/related_sites.html, "U.S. DOE-CIAC: Federal and Security Information Sites," Computer Incident Advisory Capability, U.S. Department of Energy.
[78] http://www.ciac.org/cgi-bin/cnotes, "CIAC C-Notes," Lawrence Livermore National Laboratory/DOE, 26 February 2001(?)
[79] http://ciac.llnl.gov/cgi-bin/index/bulletins, "CIAC Bulletins," Lawrence Livermore National Laboratory/ U.S. Department of Energy, 26 February 2001
[80] http://doe-is.llnl.gov/DOESecurityResources.html, "DOE Computer Security Resources," Lawrence Livermore National Laboratory/ U.S. Department of Energy, Last modified: 22-Feb-2002.
[81] http://www.ciac.org/cstc/CSTCHome.html, "U.S. DOE-CIAC: CSTC (Cyber Solutions Tool Center)," Lawrence Livermore National Laboratory/ U.S. Department of Energy, 26 February 2001
[82] http://www.ciac.org/ciacNT/index.html, "U.S. DOE-CIAC – Windows NT Information," Lawrence Livermore National Laboratory/ U.S. Department of Energy, 26 February 2001
[83] http://www.fedcirc.gov, "Federal Computer Incident Response Center," U.S. Department of Homeland Security.
[84] http://www.fedcirc.gov/generalInfo/siteMap.html, "Sitemap," U.S. Department of Homeland Security.
[85] http://www.uscert.gov/workwithus, "US-CERT: Working whith US-CERT," U.S. Department of Homeland Security, last updated December 13, 2003.

Summit, and (federal government) news items. Currently, it provides links only to DHS and Carnegie Mellon CERT websites.

The military flavor of incident response is reported at the DOD's CERT[86] and DISA's IASE sites (the Defense Information Systems Agency's Information Assurance Support Environment).[87] Like DOE's CIAC, these sites do not send out alerts to any but .gov and .mil email addresses; for that matter, a noticeable fraction of the material here is not accessible to the public. However, items available only to government or military employees are clearly marked; some material is available to contractors if they hold a DOD PKI certificate. The IASE in particular provides an enormous number of documents. "Policy and Guidance" contains executive orders, legislation, FIPS, public law, and documents from every branch of the military, the General Accounting Office, and NIST.

Information security, in all but technical respects, is closely connected to the law, both domestic and international. The best reference for legal issues is Lexis/Nexis, which began life thirty years ago[88] as a subscription-based caselaw research service. While the full scope of its services are still available only through paid subscription, it provides several free services to "solo and small-firm attorneys" through lexisONE[89], including a valuable directory of IT security/law websites (accessible through Legal Website Directory/Computer Centers)[90] and a very extensive list of resources about "Cyberspace and Internet Law."[91] The list includes links to Internet Security websites, a selection of security mailing lists, and a few online security stores (although these appear to be oriented more toward spy toys than to security products). The Computer Center page also includes links to Cryptography and Encryption and First Amendment and Privacy pages.[92] In addition to the U.S. resources, Lexis/Nexis provides legal research in Europe, Asia/Pacific, Argentina, and Chile,[93] although I cannot say whether the information security resources are as extensive as they are for the U.S.

The Electronic Frontier Foundation[94] is the ACLU of the Internet. Its purpose is to defend the rights of individuals to free speech, privacy, and "fair use" of electronic products from incursions by either government or industry. It currently covers some 30 topics including, for example, electronic voting machines,[95] the Digital Millennium

---

[86] http://www.cert.mil, "DoD-CERT Online," U.S. Department of Defense.
[87] http://iase.disa.mil/index2.html, "IASE Public Home Page," Information Assurance Support Environment, Defense Information Systems Agency, Revised 15 December 2003.
[88] http://www.lexisnexis.com/about, "About LexisNexis," LexisNexis, 2003.
[89] http://www.lexisone.com, "lexisONE," LexisNexis, 2003.
[90] http://www.lexisone.com/legalresearch/legalguide/computer_center/computers_antivirus_security_introduction.htm, "Computer Security," LexisNexis, 2003.
[91] http://www.lexisone.com/legalresearch/legalguide/practice_areas/cyberspace_internet_law.htm#7, "Cyberspace & Internet Law," LexisNexis, 2003.
[92] http://www.lexisone.com/legalresearch/legalguide/computer_center/computers_center_index.htm, "Computer Center," LexisNexis, 2003.
[93] http://www.lexisnexis.com/about, "About Lexis/Nexis," LexisNexis, 2003.
[94] http://www.eff.org/about, "EFF: About," Electronic Freedom Foundation, last updated 22 December 2003.
[95] http://www.eff.org/Activism/E-voting, "EFF: E-voting archive," Electronic Freedom Foundation.

Copyright Act (DMCA),[96] and anti-terrorism laws.[97] It produces a newsletter, EFFector,[98] and a library of discussions, conference proceedings, and Congressional hearings in MP3 format at "Radio EFF."[99]

CERIAS, at Purdue University, lists almost 40 additional websites which pertain to the legal aspects of information security.[100]

Operating Systems

Most sites issuing generic security alerts (that is, for any operating system and application) provide enough information to identify sources and versions of the software with the vulnerability. Links to patches may or may not be provided. Few of these sites will offer specific security products for specific application or operating system software. That requires vendor support and commercial websites which market a varying array of products to endusers.

UNIX/Linux are "open source" operating systems. Although "dialects" of the same operating language, the various commercial implementations of UNIX (IBM, HP, SCO), various distributions of Linux (Red Hat, Slackware, SuSE, Debian, etc.), and even freeBSD implement the "open" source code differently. Anyone using a commercial distribution will start at the vendor's website, which will lead to support pages for their products, which will lead to security advisories and mechanisms for reporting a suspected vulnerability, which may (or may not) lead to the pages for patches, updates, and downloads.

A useful site for Linux Security is Linux Security.Com.[101] Although supported by a Linux consulting company, it is not as driven by advertising as most publication sites (but it does insert product blurbs). Most of the site presents news from many independent sources (USAToday, ZDNet, Tech News World) and commentary from individuals and journalists. It issues two weekly security newsletters: *Linux Advisory Watch*, which covers vulnerability reports, and *Linux SecurityWeek*, which covers other security-related news.

Another Linux Security site, at LinuxInsider, covers the Linux "industry," but news items all come from E-Commerce Times (who owns LinuxInsider).[102]

A leading contender for prime UNIX/Linux IT resources is the Open Source Development Network, (OSDN).[103] OSDN does not address security, *per se*, but it sponsors eleven Web

---

[96] http://www.eff.org/IP/DRM/DMCA, "Intellectual Property - Digital Millennium Copyright Act (DMCA) Archive," Electronic Freedom Foundation.
[97] http://www.eff.org/Privacy/Surveillance/Terrorism/antiterrorism_chill.html, "Chilling Effects of Anti-Terrorism," Electronic Freedom Foundation.
[98] http://www.eff.org/effector, "EFFector Newsletter Archive," Electronic Freedom Foundation.
[99] http://www.eff.org/radio, "Radio EFF," Electronic Freedom Foundation.
[100] http://www.cerias.purdue.edu/tools_and_resources/hotlist/details.php?id=57, "CERIAS – Electronic Law\Dedicated Sites," CERIAS and Purdue University, last updated 27 September 2003.
[101] http://www.linuxsecurity.org, "Linux Security – The Community's Center for Security," Guardian Digital, Inc., 2002.
[102] http://www.linuxinsider.com/perl/section/security, "Linux News: Security," ECT News Network, 2003.
[103] http://www.vasoftware.com/osdn.php, "VA Software: OSDN," VA Software, Inc., 2003.

forums that specialize in various open source topics. Geocrawler[104] is an archive of listserv material, organized by type, including half-a-dozen security lists.[105]

Microsoft has several IS-related websites, although one gets to most security-centric pages through the more general technical support pages. There is a security homepage, but it is a bit skimpy at present (December 2003), not much more than a work in progress.[106] Other MS sites are the Support page (which provides the Knowledge Base search engine and access to other support pages),[107] "Community newsgroups" (Microsoft's version of Usenet – click on "security" in the left frame to open the list of security-related groups), product forums,[108] downloads and updates,[109] and the TechNet security area.[110] There are additional resources: technical articles on various security topics, security bulletins (newsletters), product white papers (read "marketing"), related Microsoft sites, and links to other organizations.

Other, more independent Microsoft resources include *Windows and .Net Magazine*[111] and Windows-help.net[112] (maintained by InfinitiSource, a Windows shareware business[113]). The major publishers (see "Periodicals" below) of PC magazines provide fairly reliable information, although they are covering a much broader audience than ISSPs.

A handful of other sites illustrate some of the difficulties in selecting reliable resources. Just as you must know your enemy, you must know your resource. All these sites aim to sell something to someone (space to advertisers or products to visitors), but none of them push Microsoft products. Annoyances.org[114] takes its name from the O'Reilly and Associates series on Microsoft's imperfections and aims to take some of the sting out of those imperfections. However, the most recent news item on its home page is dated from March 2003 and mentions expanding the capacity of the annoyances.org servers; this may have become an unsupported website since then. On the other hand, there is a great deal of still-relevant information here and visitors continue to post to the discussion groups. (Note that Annoyances.org is owned by Creative Element, a consulting and design company.[115]) WindowSecurity.com[116] is one of a family of network administration sites maintained by Internet Software Marketing Ltd.; the site is a well organized portal of news, articles, alerts, product reviews, and related links. However, Internet Software Marketing Ltd is located in the

---

[104] http://geocrawler.com, "Geocrawler.com," Open Source Development Network, 2002.
[105] http://geocrawler.com/lists/3/Security, "Geocrawler.com – Security—Mailing List Archives," Open Source Development Network, 2002.
[106] http://www.microsoft.com/Security, "Security," Microsoft Corporation, 2003.
[107] http://support.microsoft.com/default.aspx, "Microsoft Help and Support," Microsoft Corporation, 2003.
[108] http://www.microsoft.com/communities/products/default.mspx?gssnb=1, "Microsoft Product Communities: Find a Community for a Microsoft Product or Technology," Microsoft Corporation, 2003.
[109] http://support.microsoft.com/default.aspx?scid=fh;EN-US;DOWNLOADOVER, "Downloads and Updates," Microsoft Corporation, 2003.
[110] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp, "Security," Microsoft Corporation, 2003.
[111] http://www.winnetmag.com, "Windows & .Net Magazine Network," Penton Media, Inc., 2003.
[112] http://www.windows-help.net/index.shtml, "Windows-Help.NET," Windows-Help.NET, 2003.
[113] http://www.infinisource.com, "InfiniSource – The Internet's Premier Resource Center," InfiniSource, Inc., 2003.
[114] http://www.annoyances.org, "Annoyances.org," Creative Element, 2003.
[115] http://www.creativelement.com, "Welcome to Creative Element," Creative Element, 2003.
[116] http://www.windowsecurity.com, "Microsoft Windows security site: intrusion detection, anti-virus, firewalls, and more!" WindowSecurity.com, Internet Software Marketing Ltd., 2003

Seychelles;[117] the products it reviews or advertises may come from anywhere in the world (for example, the URL for Kaspersky Lab anti-virus software points to a Russian website).[118] IsoftMarketing disputes allegations made by the editor of *W2Knews*, a Sunbelt e-publication, and makes a few of its own allegations.[119] Sunbelt, for its part, claims to be "the World's first and largest e-zine designed for NT/2000 System Admins and Power Users that need to keep these platforms up & running."[120] Who do you believe? How much time can you afford to investigate the integrity of websites that promise you solutions to the myriad problems you face every day? (I like WindowSecurity, despite its owner's physical location and occasional incomprehensible links; it is organized, its material makes sense to me, and it does not tout only its own products.)

Conferences, Training, Certification

Conferences are a great way to keep up with continuing education and industry developments. They are also a refreshing change of pace – *if* you can get away from work. Vendor training in new products can be an efficient way to master them (and usually counts toward CE credits). Gaining certification can improve careers, if carefully chosen. Now that information security has become so important, it seems as if *every*one is pushing some kind of paper, and for every certification offered, there are probably hundreds of companies offering training courses or books for it. Taylor listed almost 30 conferences. I include here the handful I think are most useful to any ISSP; the rest are listed in the Appendix, with updated addresses. I have added some websites that offer useful certification and/or training.

The most valuable security conferences for me have been those hosted by the SANS Institute. The major reason is that SANS makes a point to be vendor-independent; it teaches principles and best practices rather than devices or software. (The one exception is UNIX/Linux and Windows operating systems. Both are pervasive in government and business, and each has its own ways of doing [or not doing] security.) SANS has been in the security business for over a decade and does a great deal more than host informative, practical (and intense) conferences. The list of upcoming SANS conferences and the training available at each is posted on its home page.[121] SANS has added certification to most of its courses in the last couple years, which costs extra.

The Computer Security Institute (CSI) has hosted an annual security conference for the past 30 years;[122] it has recently added NetSec, a conference specifically on network security. Publications and online services are available to members only, but training is open to anyone; memberships cost $224 a year for U.S. residents, as of this writing.

---

[117] http://www.isoftmarketing.com/aboutus.htm, "Welcome to Internet Software Marketing Ltd. – Online Network Administrator Portal," Internet Software Marketing Ltd.
[118] http://www.avp.ru/products.html. (No further information is available; the site is written in Cyrilic.)
[119] See http://www.isoftmarketing.com/reply_to_sunbelt.htm "Our Response to Sunbelt's w2knews article about our websites", Stephen Chetcuti, Internet Software Marketing Ltd., for IsoftMarketing's comments, and http://www.w2knews.com/index.cfm?id=452 "Some 'Tech Websites' Are Not What You Think They Are", Sunbelt W2Knews Electronic Newsletter, 17 November 2003 for the original article.
[120] http://www.w2knews.com/about-us.cfm, "W2Knews," Sunbelt Media Services, 2003.
[121] http://www.sans.org, "SANS Institute –Computer Security Education and information Security Training," SANS Institute, 2003.
[122] http://www.gocsi.com/events, "Computer Security Institute,"

USENIX/SAGE is one of the oldest professional UNIX organizations. Its calendar of events and conferences is at its Events page.[123]

MIS Training Institute offers conference and online training in audit and information security;[124] it offers one annual security exposition and several infosec training conferences. It also offers training programs in a variety of business topics to the European[125] and Asian/Pacific[126] communities.

RSA Security hosts an annual data security/crypto conference;[127] the next one will be in San Francisco at the end of February, 2004. RSA also offers almost a dozen training courses in their products and in information security; the "Information Security: From A to Z" (offered in partnership with Hill Associates) is a series of 15 two-hour sessions that promises to prepare participants for CompTIA's Security+ and the (ISC)2's SSCP certification exams.[128]

Despite its name, Black Hat is a company about "digital self defense." It offers training in various aspects of security, briefings, consulting, and tools. Its products are generally vendor-independent, but it has added Windows briefings to its offerings. See "Briefings"[129] for a list of conferences and training opportunities and the Black Hat media kit[130] for a detailed history and mission of the company.

Defcon.org is a hackers website. It lists several hack-related conferences with short descriptions at its "Other Conventions" page.[131]

Opportunities for vendor-neutral security certification are expanding. There is SANS and its GIAC program,[132] which includes both training and certification. There is the International Information System Security Certification Consortium [$(ISC)^2$] and its CISSP and SSCP;[133] it runs three-day review seminars in preparatoin for the CISSP and is beginning to offer domain-specific online courses. Computing Technology Industry Association (CompTIA), a global trade group for IT companies and professionals, has developed several vendor-neutral, IT-related certification programs,

---

[123] http://www.usenix.org/events, "USENIX – Events Calendar," USENIX/SAGE, Last changed: 18 December 2003.
[124] http://www.misti.com/northamerica.asp?page=4&subpage=2&region=1&disp=about, "About MIS Training Institute," MIS Training Institute, 2001.
[125] http://www.mistieurope.com/MIS/about.asp, "Audit and Information Security Training," MIS Training Institute, (2001?).
[126] http://www.misti.com/asia.asp, "Welcome to MIS Asia," MIS Training Institute, 2001.
[127] http://www.rsasecurity.com, "RSA Security – Identity and Access Management e-Security," RSA Security Inc., 2003.
[128] http://www.hill.com/partners/rsa , "Hill Associates – RSA Live E-Learn Events," Hill Associates, 2003.
[129] http://www.blackhat.com/main.html, "Black Hat Briefings Upcoming Conferences," Black Hat, Inc, 2003.
[130] http://www.blackhat.com/images/bh-about/bhmediakit.pdf, "bhmediakit.pdf," Black Hat, Inc, 2003
[131] http://www.defcon.org/html/links/other-conventions.html, "other Conventions & Events," Dark Tangent, 2003, last updated on: 7 November 2003.
[132] http://www.giac.org/GIAC_Cert_Brief.pdf, "Global Information Assurance Certification, Objectives and Curriculum," Northcutt and Corcoran, p.6, SANS Institute, 2003.
[133] https://www.isc2.org/cgi/content.cgi?category=3, "(ISC)2," $(ISC)^2$, 2003.

including the Security+.[134] Although it does not train candidates directly, it provides lists of approved study materials and training partners. Most of the websites already mentioned in other sections of this article provide training or links to training sites. IT professionals in the federal government will find security training available from a number of agencies: Information Resources Management College (a DoD-supported educational institution)[135], Graduate School of the U.S.D.A (also open to non-government employees),[136] and the National Security Agency,[137] among others.

Vendors have trained customers in the administration and maintenance of their products for many years. IT products have become so powerful "out of the box," that customers become frustrated and unhappy when they cannot make the product work as advertised; training is the most effective way to mitigate this problem. For example, Cisco certification is particularly important for three reasons: 1) of course, someone trained in the arcane technology of routers is not as likely to leave the customer's network wide open, 2) routers are a primary security tool for any WAN, and 3) Cisco is the virtual "gold standard" in router hardware. Cisco offers an extensive array of specialties and levels of expertise; certifications are oriented toward product or function (both, at the expert level).[138] Microsoft has added a new Security specialty for MCSAs (two security exams) and MCSEs (three security exams).[139] Sun Microsystems offers certification in Solaris, Java, Sun ONE middleware, and network storage.[140] Hewlett-Packerd's training and certification program is sales-oriented,[141] but training in the Integration and Operating Systems tracks focus on HP platforms and software (such as OpenView) as well as Windows and HP flavors of UNIX and OpenVMS.

Certification in Linux, which is technically "free" software, developed by a global community of volunteers, is difficult to find. Red Hat tests its RH certified technicians and certified engineers on live systems, in addition to the traditional multiple-choice exams.[142] CompTIA offers Linux+.[143]

---

[134] http://comptia.com/certification/security/default.asp, "CompTIA Security+ Certification," The Computing Technology Industry Association, Inc., 2003.
[135] http://www.ndu.edu/irmc, "NDU – IRM College,"
[136] http://grad.usda.gov/index.html, "Graduate School, USDA," Department of Agriculture, ?
[137] http://www.nsa.gov/isso/index.html, "The NSA/CSS Infosec Page," Information Assurance Directorate, National Security Agency, Revised 3 June2003.
[138] http://cisco.com/en/US/learning/le3/learning_career_certifications_and_learning_paths_home.html, "Career Certifications and Paths – Cisco Systems," Cisco Systems, Inc., 2003.
[139] http://www.microsoft.com/traincert/mcp/default.asp, "Microsoft Certifications," Microsoft Corporation, 2003.
[140] http://training.sun.com/US/certification, "Sun training and certification programs," Sun Microsystems, Inc., 2003.
[141] http://h10017.www1.hp.com/certification "HP Certified Professional Certification Program," Hewlett-PackardCompany, 2002.
[142] http://www.redhat.com/training, "redhat.com – Red Hat Linux Training, Certification, RHCT, RHCE," Red Hat, Inc., 2003.
[143] http://comptia.com/certification/linux/default.asp, "CompTIA Linux+ Certification," The Computing Technology Industry Association, Inc., 2003.

Tools

I stated earlier in this article that I would not include resources for security tools. However, a few resources for "meta-tools" need mentioning. In addition to the specific software programs that test or fix specific security aspects of a system, there are tools that address the overall environment of a system. In particular, policy templates and system benchmarks are important, because they provide, on the one hand guidelines for security practices, and on the other a means of measuring the adequacy of a system's overall security.

SANS, CIS, and NIST CSRC are good starting points for this kind of resource. The SANS Security Policy Project,[144] provides a forum for developing security policies and includes several resources on site and a dozen or so links to other websites that offer similar information. CIS (Center for Internet Security) specializes in benchmarking the "technology specific controls" available in a wide range of computer system products.[145] NIST is a portal for *Special Bulletins*, *FIPS*, and other government-sponsored standards and laws.[146]

InfoSysSec is an excellent portal for all kinds of tools; its home page lists over a hundred links to tools, books, vendors, and hacker sites.[147] Three more sources for specific tools are books: the *SANS Security Essentials with CISSP CBK* by Cole, Fossen, Northcutt, and Pomeranz; *Practical UNIX and Internet Security* by Garfinkel and Spafford; and *Hackers Beware* by Eric Cole. All provide appendices of URLs and all are available from Amazon.Com, Barnes & Noble, and Borders Books. There is one caveat for all four sources listed here: the hyperlinks may not contain current information, may not be relevant anymore and may no longer even exist. This is especially true of the books, but InfoSysSec is not entirely accurate, either (it also mixes sponsored links indiscriminately with unpaid links).

Vendors:

The best resources for product support are, of course, product vendors. Vendor-neutral sites may be more likely to publish vulnerabilities and attacks sooner than the vendors, but the vendors are more likely to have the best counter measures. Ad hoc work-arounds may be offered by either the independents or vendors, until a vendor-validated patch is published. The vendor will also supply updated software and drivers for new hardware, operating system versions, and application software.

Vendors routinely include their website address on the box and in the various reading material packed with the product. If these are not available, a search on the product or vendor generally yields several websites; many of them will point to product reviews, opinions, and other not-quite-so-helpful pages, but these are easy to bypass.

---

[144] http://www.sans.org/resources/policies, "SANS Institute – Security Policy Project," SANS Institute, 2003.
[145] http://www.cisecurity.org, "Center for Internet Security – Standards," Center for Internet Security. 2003.
[146] http://www.csrc.nist.gov/publications, "C S R C – Guidance / Publications / Library," CSRC-NIST last updated: December 13, 2002.
[147] http://www.infosyssec.com , "Hacking and Hackers," InfoSysSec, 2002.

Online Periodicals

Most of the following sites began as traditional magazines, added online versions, then expanded into all the "bells and whistles" of the World Wide Web: archives to past issues, links to other sources, search engines, polls and surveys, blogs, webcasts, online training, conferences, white papers, advertising, discussion groups, continuous news updates, etc. Many of the resources following were listed by Taylor, with little explanation as to what they are. I have reorganized the list by publisher, added some descriptions and included a broader range of prodominately "magazine" websites. (Titles marked with an asterix, "*", are from Taylor.)

At the top of Taylor's list is *Wired** magazine,[148] which has been published since 1993 by Condé Nast. Its target audience is anyone interested in anything cyber: technology, science, people, law, privacy, business, politics, culture – if it's on the wire(/less), it's in the mag.

Two major publishers of IT-related magazines are Ziff Davis Media and IDG (International Data Group). Ziff Davis targets individuals more than job titles; IDG targets titles more than individuals. That said, they both cover information technology broadly enough that readers will find valuable resources for both work and home. While most of these magazines do not concentrate explicitly on the security of systems and information, security is playing an increasingly important role in editorial content.

Ziff Davis Media's flagship publication is *PC Magazine*. It features extensive lab tests, comparative analyses, and reviews of computer products, as well as news and views. While its primary focus is on *personal* computer users, much of its material is useful in a corporate setting as well. Despite heavy advertising content, it claims to be "the independent guide to technology." Based on my experience, I tend to trust that claim. *PC Magazine* is available online,[149] as well as in print. In addition, Ziff Davis offers trade magazines free for "qualified" subscribers: the two most useful are *CIO Insight* ("Strategies for IT Business Leaders"[150]) and *eWeek* (a "*PC Magazine"* for enterprise computing),[151] both are available online. *CIO Insight* covers information as managed resource; *eWeek* has a section that concentrates on systems security.

International Data Group (IDG) claims to be "the world's leading technology media, research, and exposition company."[152] In addition to *PC World*,[153] which competes directly with Ziff Davis's *PC Magazine*, IDG publishes *Macworld* [154] for Macintosh users (in the U.S., Australia, United Kindom, and six other European countries[155]). However, its primary market is enterprise

---

[148] http://www.wired.com, "Wired News," *Wired* magazine, Condé Nast, 2003.
[149] http://www.pcmag.com, *PC Magazine*, Ziff Davis Media Inc., 2003.
[150] http://www.cioinsight.com, "CIO Insight," *Ziff Davis CIO Insight*, Ziff Davis Media, © 2003.
[151] http://www.eweek.com, "eWEEK.com," *eWEEK Enterprise News and Reviews*, Ziff Davis Media, 2003. Security information is at http://www.eweek.com/category2/0,4148,1237860,00.asp.
[152] http://www.cxo.com, "CXO Media, Inc. Resources for Management," IDG, Inc., © 2003.
[153] http://www.pcworld.com, "PCWorld," *PC World*, IDG, Inc., © 2003. Privacy and security are at http://www.pcworld.com/resource/browse/0,cat,1529,sortIdx,1,00.asp.
[154] http://www.macworld.com, "Macworld: The Mac Product Experts," *Macworld*, Mac Publishing, LLC., © 2003.
[155] http://www.macworld.com/info/aboutus, "Macworld: About Us," Mac Publishing, LLC., 2003.

computing: *ComputerWorld**, for "IT management;"[156] *InfoWorld*, for "CTOs;"[157] and *Network World*, for LAN/WAN/WLAN managers.[158] Of particular note are *CSO* (a monthly)[159] for IT security officers and *CIO* (biweekly),[160] for senior information officers. All are published in several languages; all have websites; all offer free e-newsletters. *TechWorld*,[161] focusing on infrastructure and networking, is a new online-only magazine.

CMP specializes in technology and health care. [162] Among its products of interest to ISSPs are *Security Pipeline*,[163] a magazine for IT professionals responsible for the "secure enterprise," and the security sections of *Network Computing*,[164] *InformationWeek*,[165] and *Network Magazine*,[166] a monthly that covers technology architecture. *Sys Admin* is a monthly for UNIX/Linux systems administrators;[167] it does not divide out security from other material, but then a major part of a sysadmin's job is security-oriented. CMP has integrated much of the material in its magazines online at "TechWeb," its Business Technology Network.[168]

101communications is a relatively new publisher of several IT magazines.[169] Two of its products cover "the government IT community," which includes agencies at all levels of government, government IT contractors, and IT employees. *Federal Computer Weekly** (which it acquired) is a weekly trade magazine. [170] E-Gov Institute[171] sponsors conferences and seminars on emerging government IT issues; it also publishes the semi-monthly *E-gov Digest*,[172] which covers "electronic government." Another weekly government IT magazine is

---

[156] http://www.computerworld.com, "Computerworld," Computerworld Inc., 2003. Security section of Website is at http://www.computerworld.com/securitytopics/security?from=left.
[157] http://www.infoworld.com, "InfoWorld Homepage," *InfoWorld*, InfoWorld Media Group, 2003. Security section of Website is at http://www.infoworld.com/techindex/security_1.html.
[158] http://www.nwfusion.com/index.html, "Network World Fusion," *NetworkWorldFusion*, Network World, Inc., 2003. Security topics can be found under the "Enterprise Networks" and "SMB Networks" tabs; the URLs are http://www.nwfusion.com/topics/security.html and http://www.nwfusion.com/net.worker/topics/security.html, respectively.
[159] http://csoonline.com, "CSO Magazine for Chief Security Officers and senior security executives," *CSO*, CXO Media Inc., 2003.
[160] http://www.cio.com, "@CIO.com – CIO Magazine and more online," *CIO*, CXO Media Inc., 2003.
[161] http://www.techworld.com, "Techworld.com," *Techworld*, IDG, 2003.
[162] http://www.cmp.com, "CMP," CMP Media, LLC, 2003.
[163] http://www.securitypipeline.com/about.jhtml , "Security Pipeline: About Us," *Security Pipeline*, CMP Media, LLC 2003.
[164] http://www.nwc.com/core/core7.jhtml, "Technology Guide: Security," *Network Computing*, CMP Media, LLC, 2003.
[165] http://informationweek.securitypipeline.com, "Security Pipeline," *security pipeline*, CMP Media, LLC, 2003.
[166] http://www.networkmagazine.com, "Network Magazine – Technology Architecture for the 21st Century," *Network Magazine*, CMP Media, LLC, 2003.
[167] http://sysadminmag.com, "Sys Admin Magazine," CMP Media, LLC, 2003.
[168] http://www.techweb.com, "TechWeb: The Business Technology Network," *TechWeb*, CMP Media, LLC, 2003.
[169] http://www.101com.com, "101communications LLC: Enabling Technology Professionals to Succeed," 101communications LLC, 2003.
[170] http://www.fcw.com, "FCW.com Home," *Federal Computer Weekly*, FCW Media Group, 2003.
[171] http://www.e-gov.com, "The E-Gov Institute," 101 Communications.
[172] http://www.e-gov.com/egov_digest, "e-gov Digest," *e-gov Digest*, 101 Communications.

Government Computer News;[173] it is published by Post/Newsweek. Both are good resources for tracking federal IT laws and standards, as well as news and technology affecting government and government IT consultants.

*Cipher** is a bimonthly e-newsletter by the Technical Committee on Security and Privacy (TCSP) of the IEEE Computer Society.[174] The site mostly covers calls for research papers for upcoming IT security conferences, conference reports, a conference calendar, a list of useful links,[175] reviews of good IT security books (books by SANS gurus Ed Skouris and Eric Cole are among the recent reviews[176]), and newsbits, submitted by TCSP members. As befits the IEEE, *Cipher* topics are highly technical.

Elsevier, a Dutch publisher, produces *Computers and Security*,* a journal for Technical Committee 11 (computer security) of the International Federation of Information Processing.[177] The journal is supported by a website (Compsec Online[178]), which provides news and views on computer security issues with a European focus – a valuable resource for any ISSP working for a global concern.

*Securiy Management** [179] is the monthly publication of ASIS International,[180] a global professional organization that focuses on all aspects of security: physical premises, employee safety, information, law, privacy, etc. Although it is not entirely IT-related, it is an important resource for ISSPs, because information security does not live in technology alone; we need to be aware of environmental factors, as well. Despite its global membership, it is somewhat biased toward U.S. issues, particularly legislation, law, and regulation.

*Information Security** magazine is now a TechTarget publication available as hardcopy or online.[181]

*SC Infosecurity News** is an online news service supported by *SC Magazine* (SC for "secure computing"), which claims to be "the largest circulation information security magazine"[182]; it's available in editions for the U.S./North America, Britain/Europe, and Asia/Pacific regions. Taylor's reference to the URL http://www.westcoast.com (for West Coast Publishing) is now redirected to *SC Magazine*, UK edition.[183]

---

[173] http://www.gcn.com, "Government Computer News (GCN) home," *Government Computer News*, Post-Newsweek Media, Inc., 2003

[174] http://www.ieee-security.org/cipher.html, "Cipher: The Newsletter of the IEEE Computer Society Technical Committee on Security and Privacy," IEEE, 2003.

[175] http://www.ieee-security.org/Cipher/InterestingLinks.html, "IEEE Cipher: Interesting Web Links," IEEE, 2003.

[176] http://www.ieee-security.org/Cipher/BookReviews.html, "IEEE Cipher Book Announcements and Reviews," IEEE, 2003.

[177] http://www.elsevier.nl/inca/publications/store/4/0/5/8/7/7, "Computers and Security," *Computers and Security*, Elsevier Advanced technology, 2003; Last updated 23 December 2003.

[178] http://www.compseconline.com, "Compsec Online," Elsevier.

[179] http://www.securitymanagement.com, "Security Management Online," *Security Management*, 2003.

[180] http://www.asisonline.org, "ASIS International: Home Page," ASIS International.

[181] http://infosecuritymag.techtarget.com, "Information Security Magazine," *Information Security*, TechTarget IT Media, 2003.

[182] http://www.infosecnews.com, "Information Security News," *SC Informationsecurity News*, West Coast Publishing, 2003.

[183] http://www.westcoast.com/cgi-bin/redirect.pl, "Secure Computing Magazine – West Coast Publishing," *SC Magazine*,' West Coast Publishing, 2003.

*Security Advisor** is one of several publications by The Advisor Network[184] which focus on "how-to" subjects, mostly related to database/groupware applications. In addition to the magazines themselves, there is a wealth of information, tips, and techniques in the nearly 70 "Advisor portals and zones."

*2600 Hacker's Quarterly** is a magazine (and website) for/about hacking and phreaking (phone system cracking).[185] Whatis?.com explains 2600 as "the frequency in hertz … that AT&T formerly put as a steady signal on any long-distance telephone line that was not currently in use," which is also the frequency used to carry voice.[186] Most long distance carriers now use a different frequency for the "free [not in use] line" signal, but the term is still used as a slang term for phreaking and for computer cracking in general. *2600 Hacker's Quarterly* treads the thin line between legitimate free speech and freedom of information issues and less reputable hack/crack/phreak issues.

The National Center for Supercomputing Applications* (NCSA) is concerned with developing a "high-performance cyberinfrastructure for scientists, engineers, and society"[187] as a partner of the National Science Foundation's TeraGrid project. It has an impressive history in the development of supercomputing and has been a major contributor to the growth of the Internet through its release of NCSA Mosaic in 1993.[188] I am uncertain about why Taylor included NCSA. It does not supply any resources of immediate interest to ISSPs and does not appear to publish any periodical, although the website does include news.

Online Sources for Books

Books tend to become outdated almost as soon as they reach the bookstores, but they provide a vital structual component to an ISSP's library. I suspect that most of an ISSP's knowledge is acquired "OJT, while under fire" – that is, learned piecemeal, only as much and as quickly as a particular problem requires. Books (and training) provide an integrated "whole subject" view that puts our bits and pieces into context. I have never managed to read a book in its entirety, but I have read major parts of most of the ones I own, and I constantly refer back to the good ones. Unlike the Internet, a book is a portable, manageable handful and a familiar resource.

Internet "sources" for books are booksellers, publishers, and special-interest websites. Booksellers are great for "one-stop shopping." The disadvantage, for me, is they offer thousands of titles to rummage through; even using keyword searches can produce exceedingly long lists. On the other hand, publishers restrict their offerings to the books they (or affiliates) publish, a much more efficient way to find books, if you trust the publisher. The special-interest websites offer books from several publishers, but focus on selected subjects; they frequently offer more than just books, such as news items, letters, online magazines, discussion forums, etc.

---

[184] http://securityadvisor.info, "Security Advisor – securityadvisor.info," *Security Advisor*, Advisor Media, 2003.
[185] http://www.2600.com, "2600: The Hacker Quarterly," *2600: The Hacker Quarterly*, 2600 Enterprises, Inc., 2003.
[186] http://whatis.techtarget.com/definition/0,,sid9_gci211496,00.html, "2600 – a whatis definition," WhatIs?Com, 2003; Last updated on: 20 Jul 2001.
[187] http://www.ncsa.uiuc.edu/AboutUs, "NCSA: About NCSA," NCSA, University of Illinois at Urbana-Champaign, 2003;Last updated 4 November 2003.
[188] http://www.ncsa.uiuc.edu/AboutUs/Overview/Historythe1990s.html, "NCSA: History," NCSA, University of Illinois at Urbana-Champaign, 2003; Last updated 23 December 2003.

Fatbrain, Taylor's only resource for books, was once a very efficient online portal for technical books (computer, engineering, medicine, etc.), which did not much care who ultimately sold you the books. As a part of Barnes & Noble (B&N), it is no longer so egalitarian. However, B&N offers a very broad selection of IT books, typically at a 20% to 30% discount. Books are searchable by subject area, publisher, series ("*…Bibles*," "*… for Dummies*," "*Inside …*," "*…Unleashed*," etc.), price range, and format (hardback, trade, mass, audio, large-print). It does not offer security as a listed subject area, but a couple keyword searches turn up a lot of books: "computer security" returned over 5,000 hits; "information security" resulted in over 3,000 items. These numbers overstate the number of actual titles B&N carries, because they include several editions and formats of the same book (and they also include books better categorized as Internet company securities, in the Business and Finance area).

Amazon.com (also available in Britain, Canada, Germany, and Japan) is *the* giant online bookseller. It offers well over a million titles and, like B&N, includes reader reviews, "People who bought this book also bought" lists, and additional information from the book itself. In addition, Amazon includes customer-favorites lists in a side bar menu. Frequently Amazon includes excerpts, table of contents, and index pages from a selected book. While it discounts many titles and offers used copies for even less, B&N tends to do better on price, especially for B&N registered members. Amazon's search function is more sophisticated than B&N's; a search on "subject: (computer or network or information) and security and not (stocks or investment)" returned over 3,300 items. Results are listed in "featured item" order; they can be sorted by title, price, publication date, average review rating, best selling – but not by author or publisher. (However, even this search will not exclude multiple editions and formats of the same title.) Amazon also offers subscriptions to 200 magazines on IT subjects. (A word of warning: double check their subscription rates against the magazine publisher's rates; they may not be the best rates available.)

I would recommend Border's Books as well, but their online presence is served by Amazon.com. I often go to Border's to look at books I may want to buy, then order from the Web. (I don't find online reviews as helpful as handling a book.) I also get a better sense of what's available by perusing the computers and programming section directly than I do browsing online. Another reason for actually going to Border's is their changing inventory of cheap books, especially superceded editions. Most of the companies and agencies I deal with are two to four years behind leading technology, so many "out-of-date" books are still perfectly relevant.

A dedicated online computer bookstore is Computer Books Online. It includes over 300 titles categorized as "Security."[189] The webmasters are currently upgrading the site to add more "bells and whistles" such as a member area, an improved "Used Books" site, and expanded customer services. Search results show only the book titles, but full information is provided at the link for each book. I like CBO, because it is visually clean and well-organized; however, since the layout is not typical to most websites (publishing and price information is presented in a side bar on the Details page), it may take some getting used to. (On the other hand, the new, improved website may join the ranks of the common.)

---

[189] http://www.computerbooksonline.com/securityindex.htm, "Computer Security Book Index," Computer Books Online, 2003, Last Modified: November 05, 2003.

Reiter's, a Washington, DC book store, specializes in business, computers, engineering, law, medicine, and the sciences. While their offerings do not cover as broad a range as Amazon, Barnes & Noble, and the like, their focus tends to be on authoritative editions and on college-level textbooks.[190]

Bookpool Discount Technical Books[191] offers business and technical books at 20% to 40% discounts from over 30 publishers, including heavy-weights Artech House, Cambridge University Press, MIT Press, and Springer-Verlag. Bookpool's offerings run the gamut from popular get-the-job-done guides through certification guides to intensely technical academic subjects (for example, *Learning and Soft Computing: with Support Vector Machines, Neural Networks, and Fuzzy Logic Models (Complex Adaptive Systems)*[192]).

Amazon, B&N, Border's, Reiters, and Bookpool are examples of the variety of booksellers available online. Others include Blackwell's of Oxford, England[193] (and Blackwell's U.S. site[194]) and Powell's of Portland, Oregon.[195] There are thousands of websites selling computer books.

Hundreds of websites promise to find the lowest price for a given book, by searching the databases of a couple to several dozen (online) bookstores. All Bookstores.Com[196] includes a selection of general interest, textbook, technical/professional, off-price, and rare/used book dealers in the U.S., Canada, and Britain. Books can be searched by title, author, keyword, or ISBN number; browsing by subject or author is also available. Other low-price sites are AAABookSearch (U.S. and Canada),[197] Half Price Computer Books (U.S. and Canada),[198] and 123PriceCheck! (United Kingdom).[199]

Safari Books Online[200] is a partnership between Pearson Education, Inc., and O'Reilly and Associates; it maintains several hundred books in electronic format. It is a subscription service ($10 to $30 a month, depending on how "large" a personal library one wishes to borrow), but two features may make the fee worth it: the books you "rent" are completely searchable, and the selection includes more than a dozen major publishers (although not *all* the books by a publisher – at least, not yet). The Pearson imprints include Java/Sun, Adobe, Que, Sams,

---

[190] http://www.reiters.com/index.cgi?f=t&sid=251&ses=2944271&h=t10, "Reiter's Online Store: Computers," Reiter's.
[191] http://www.bookpool.com, Bookpool Discount Technical Books, Bookpool LLC, 2003.
[192] http://www.bookpool.com/.x/p8nwy4omer/sm/0262112558, Learning and Soft Computing: with Support Vector Machines, Neural Networks, and Fuzzy Logic Models (Complex Adaptive Systems), V. Kecman, MIT Press, 2001.
[193] http://www.blackwells.com, Blackwell's Online Bookstore," Blackwell's Online Bookshop, 2003. To reach some 700 items on Computer Security, go down to the "Browse Subject Area" section and follow the links "Computers/Security/View the Books."
[194] http://bookshop.blackwell.com/bobus/scripts/welcome.jsp, "Blackwell's Online Bookshop [(US site]'" Blackwell's Online Bookshop, 2003. To reach some 700 items on Computer Security, select "Computing" in the "Go to:" drop down menu on the "Welcome" page and follow the links "Security/View the Books."
[195] http://www.powells.com/subsection/NetworkingComputerSecurity.html, Powell's Books – Networking-Computer Security, Powells.com, 2003.
[196] http://www.allbookstores.com, "Compare prices on new, used, and out of print books and textbooks," Allbookstores.com, 2003.
[197] http://www.aaabooksearch.com/subjectcomp.aspx, "Browse by Subject – Computers," AAABookSearch.com, Oceanview Technologies, Inc, 2003.
[198] http://www.halfpricecomputerbooks.com, "Half Price Computer Books," Half Price Computer Books.
[199] http://www.123pricecheck.com, "123PriceCheck.com," WebConcepts, 2003.
[200] http://secure.safaribooksonline.com, "Default Safari Online," Safari Tech Books Online, 2002.

Addison-Wesley, Cisco, and Macromedia Press; the easiest access to all Pearson IT titles is through its InformIT Bookstore portal.[201] Both InformIT and O'Reilly have links to Safari.

Some twenty major companies publish books on information technology subjects. While authors have a direct impact on a book's style, ease of use, etc., I find that certain publishers are more dependable than others in producing books I want to use. For example, I haven't found a New Riders book yet that I like, but SAMS books are very "readable" to me. I avoid Microsoft (MS) Press books for general reference, but depend on them for MS certification materials. MS-independent publishers are more likely to keep their material "real" and less apt to toe the party line. Amazon, B&N, and Bookpool list most of them; all of them have their own websites.

The one indispensible publisher is O'Reilly and Associates.[202] Its "About Us" explains why. They have been important participants in developing open-system information technologies, pioneers of the (public) world wide Web, and die-hard champions of "tell it like it is" manuals. Although they spring from open-source development and manuals (Linux, UNIX, and their many attendant pieces), they also cover Microsoft operating systems (NT and later) and the Mac X OS. They have paid attention to security issues from the early days of the Web. In addition to the two dozen or so books explicitly on security topics,[203] O'Reilly books integrate security advice as a natural dimension of information technology. My number one O'Reilly book is *Practical UNIX and Internet Security*. I also rely on the *In a Nutshell*, *Pocket Reference*, and *Pocket Guide* series for Linux and Windows. In addition to books, O'Reilly has packaged some of its related titles into several CD-based libraries.[204] Contents are accessible through a standard Web browser and a master index integrates topics from all the books on the CD. O'Reilly also sponsors conferences on developing technologies, offers eight online publications, and includes news items and commentary at their website. In addition to the distinctive "critters" on the covers of its books, O'Reilly color-codes the spines; general security titles are usually yellow.

Microsoft has added a Security link at its home page, although, as of December 2003, it appears to be a site still in development.[205] The real meat of Microsoft security is at Microsoft TechNet.[206] Additional "Security Resources" are available at Microsoft's brand-new "Microsoft Learning Center" (brought online in December 2003); these include training courses, exam guides, and books.[207] Of particular interest might be the *Microsoft Encyclopedia of Security*, written by Mitch Tulloch, which does not dwell only on MS products.[208]

---

[201] http://www.informit.com/book_store/index.asp, "InformIT.com: Book Store," Pearson Education, Inc., 2003.
[202] http://www.oreilly.com, "www.oreilly.com -- Welcome to O'Reilly & Associates," O'Reilly & Associates, 2003.
[203] http://security.oreilly.com, "Welcome to the O'Reilly Security Center," O'Reilly & Associates, 2003.
[204] http://cdbookshelves.oreilly.com, "O'Reilly CD Bookshelf Series," O'Reilly & Associates, 2003.
[205] http://www.microsoft.com/learning/centers/security.asp, "Microsoft Security," Microsoft Corporation, 2003.
[206] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp , "Security," Microsoft Corporation, 2003.
[207] http://www.microsoft.com/learning/centers/security.asp, "Security Resources," Microsoft Corporation, 2003.
[208] http://www.microsoft.com/MSPress/books/6429.asp, Microsoft Encyclopedia of Security, Mitch Tulloch, Microsoft Press, 2003.

Information system security is about the systems, as well as the means of attacking or protecting them. The information in user manuals and context-sensitive help can be too awkward to get at or entirely lacking. So a necessary part of an ISSP's library includes a number of how-to books for the systems they protect. These will range from the simplistic (such as the *… for Dummies* and *Idiot's Guide to …*) to encyclopedic (the *… Bible* series by John Wiley and Associates or *… Unleashed* series by Sams Publishing). The Sams *Teach Yourself…* series are basic tutorials which break up the material into concise chapters, each designed to be mastered within a few minutes/ an hour/ a day (depending on the title: *In 10 Minutes*, *In 24 Hours* or *In 21 Days*). They are not meant to be all-inclusive, but they're good for a quick-and-dirty – for example, when one is assigned an emergency project outside one's usual expertise. The books on a particular ISSP's shelf typically cover the operating systems and major applications for which that ISSP is responsible, with or without mention of security (although publishers are now adding security material to their how-to books – as well as publishing whole books entirely about security). Another type of how-to books are the graphical, step-by-step guides. These illustrate every step with screen shots from the program being covered. Like the *Dummies* and *Idiots* books, they are quite basic and tend to cover applications suitable for a home computing system. On the other hand, they make a great reference for all but the most pestiferous end user.

Then there are the certification study guides, thousands of titles covering nearly every certification exam out there (even for SANS GIAC Security Essentials![209]). Study guides can serve two purposes. Besides the obvious one of exam preparation, they can provide a structured means to learning a new subject, one not quite so elementary as the *Dummies* and *Idiots* guides, nor so detailed as the *Bible* and *Unleashed* compendiums. However, some extra thought is required in selecting useful study guides; the *Exam Cram* series by Pearson[210] is too focused on exam material to be a good day-to-day resource. Que Publishing, on the other hand, another Pearson company, specializes in all levels of "tutorial reference products," from the simplest to the most in depth.[211]

Conclusion

I had intended to follow Taylor's paper and simply update his resources and add some new ones. I find that I have gone off in a completely different direction than he did. It illustrates how "personal" a personal ISSP knowledge base can be. Where Taylor listed some 50 "white hat" and "black hat" websites, I see "government," "standards," and "security" portals and forums. While Taylor was able to rely on only one Web resource for books, I depend on half-a-dozen or more.

Appendix B lists nearly 200 Web pages on IS and IT topics; this is perhaps 25% of the webpages I actually looked at in the course of writing this article; I have not looked at even one percent of the websites potentially useful to an ISSP.(Had I simply presented

---

209 http://search.barnesandnoble.com/booksearch/isbnInquiry.asp?userid=2UQABVAETZ&endeca=1&isbn=0789727749&itm=1778, SANS GIAC Certification: Security Essentials Toolkit (GSEC), Eric Cole, Matthew Newfield, John M. Millican, Pearson Education, 2002.

210 http://www.informit.com/examcram2, "InforIT.com: Exam Cram 2," Pearson Education, Inc., 2003.

211 http://www.quepublishing.com/about, "About Que," Que Publishing, 2003.

only my current list of resources, it would have been all Microsoft and Novell and exceedingly light on UNIX/Linux.)

It is not feasible to look at a hundred or more websites every single day. You have to choose a limited number of the resources most valuable to you. Give three or four alert services and newsletters a trial period – perhap a month or so – to decide whether their information is useful enough to keep getting them. Consider how much time you really have available to read; if you subscribe to too many automatic emails, you are likely to miss truly important information, because you may not be able to "see" it amongst everything else coming to your Inbox (even if you use filters to file most of your email into more manageable folders).

I suggest that you bookmark SANS, InfoSysSec, and WhatIs?Com. Become familiar with what they offer and branch out from them as duties, interests, and career guide you.The SANS Reading Room keeps hundreds of IS articles and white papers on file; every one of them includes references to useful websites. InfoSysSec is particularly useful for discovering new resources. WhatIs?Com is a continuously updated lexicon of IT concepts, technology, terms, and slang.

In addition, three books in particular provide appendices of valuable security resources, (although, being in books, some references have become obsolete). O'Reilly and Associates' *Practical UNIX and Internet Security* lists security periodicals[212] (of which many now have websites), electronic resources,[213] and organizations.[214] The book was published in 1996; you will likely find that resources still in business are very valuable, by virtue of their longevity. The *SANS Security Essentials with CISSP CBK*, Version 2.1, includes a 17-page appendix of URLs, organized by chapter;[215] this list provides references for dozens of security-related software tools, as well as addresses to organizations, Usenet groups, mailing lists, standards, and other resources. (A closely related book, published by Que, is *SANS GIAC Certification: Security Essentials Toolkit* by Cole, Newfield, Millican, and Northcutt; it not only has security/hacking tools, but provides hands-on exercises which guide the reader in their use.[216]) Another outstanding source, especially for tools, is Eric Cole's recent book, *Hackers Beware*.[217]

The important thing is to think about what you already know, figure out what you need to know, and decide when you need to know it. Out of that matrix, you can collect the resources that serve you best. You must also develop a habit of pruning out Internet resources that are no longer as useful as they once were, either because they are no longer relevant, or because you have found better resources.

[212] Garfinkel and Spafford, pp. 889-891, (in Appendix D).
[213] Ibid., "Appendix E", pp. 893-907.
[214] Ibid., "Appendix F", pp.909-923.
[215] Cole, Fossen, Northcutt, and Pomeranz, "Appendix H", pp. A162-A178.
[216] Cole, Newfield, Millican, and Northcutt, *SANS GIAC Certification: Security Essentials Toolkit*, Que Press, 2002.
[217] Cole, "Appendix A", pp. 731-748.

Appendix A

Internet Tools

A Web browser is the "vehicle" that navigates the Web; it is the application interface between the user and the universe of data on the Web. The choice of a Web browser depends only somewhat on the operating system in use. Microsoft Windows users are not inescapably locked into Internet Explorer (IE), nor must they pay for an alternative. (Internet Explorer is required for Microsoft Updates and for some Websites; however, it does not need to be the default browser to support these special situations. On the other hand, using IE even ocassionally means keeping patches for it up-to-date.) Windows, UNIX/Linux and Mac users can choose among several free Web browsers, Netscape[218] and Mozilla[219] the most popular among them. Netscape and Mozilla share a common development; now owned by AOL, Netscape tends to lag Mozilla in capability; it also sells a fuller featured version. Mozilla is supported by the open source community, so it is always free. It also offers a version (Firebird) that is pure browser (stripped of email, IRC and other "enhancements") making it a faster tool; Camino is Mozilla's Mac Web browser. Opera[220] is available for current Windows systems, Mac, Linux, FreeBDS, Solaris and OS/2. Some versions are free; some cost a nominal $40 or so. It can even be used on hand-helds; versions are available for Web-capable cell phones and PDAs. Lynx is a text-based open-source browser available for Windows, DOS, VMS, OS/2, Mac and various flavors of UNIX.[221] Because it is text-based, it does not load graphics, which makes it very fast; but because it is text-based, the user may not see everything on the page. If the html code supporting the page is not written entirely to standard, Lynx may be unable to "translate" properly the fancier elements into text descriptions. It is keyboard-driven, which makes it fast; but it is keyboard-driven, which makes it awkward for GUI slaves.[222] (In the wake of the Americans with Disabilities Act, Lynx supplies a viable accomodation for people with visual or neurological difficulties; it provides the text that text-to-voice and Braille readers need and it eliminates flashing lights, running banners and other distracting animation.) America Online (AOL) uses its own browser technolgy, regardless of operating system; other ISPs (for example, Earthlink, cable internet providers, DSL providers) often layer their own skin over Netscape or IE. Users (including AOL members) are not locked into these customized versions for Web browsing, but they may be necessary to access special features added by the ISP. Linux users can keep the browser that comes packaged with their particular distribution (Red Hat, SuSe, Debian, etc.) or select a browser from the several available for open systems (Mozilla, Opera, Netscape, KDE's Konqueror, Chimera and others). A more complete list of links to Web browsers can be

---

[218] http://www.netscape.com, "Netscape.com," Netscape, 2003.
[219] http://www.mozilla.org, "mozilla – home of the mozilla, firebird, and camino web browsers," The Mozilla Organization, 2003.
[220] http://www.opera.com, "Opera Internet Browser," Opera Software ASA.
[221] http://lynx.isc.org/current, "Lynx current distribution directory," Internet Software Consortium.
[222] http://www.subir.com/lynx/what.html, ""What is Lynx, and why would I want to use it?," Subir Grewal (See http://www.subir.com, "Subir Grewal", Last Updated 1 March 2003.)

found at Yahoo!'s Browsers Web Software Directory.[223] Selection criteria include speed, privacy security, control of advertising, "parental controls," ease of use and additional features. Another note: a few Websites insist they are accessible only to IE or Netscape; I do not include any in this article.

A search engine is a Web service that finds and lists Web pages that contain a user's list of keywords. Search engines use a variety of search technologies and offer a wide array of additional features. One may use two or three routinely, depending on the information sought and the nature of the search. Google, Yahoo!, Hotbot, AOL and MSN Search are all currently popular choices for a primary search engine. AskJeeves is unique in permitting "natural language" queries, rather than requiring keywords (although it responds equally well to keywords or Boolean constructions). All "general function" search engines (such as the ones just mentioned) have advanced search functions that can handle Boolean logic and restrict results by time, language, and/or placement of keywords in a Web page. LexisNexis, the authoritative law research service, provides a selection of popular search engines with an explanation how each works.[224] While SearchEngineWatch.Com[225] focuses on "search engine marketing," it also provides useful information for search engine end users. A selection of "Major Search Engines and Directories"[226] covers "search" technology used (crawler vs. directory), history and relative merits; it also provides links to each search engine it discusses. There is a list of "search engines of search engines," a kind of portal to search engine directories, at the Guides to Search Engines page[227]. For people who prefer to search in a language other than English, or who want to conduct searches based on geographical criteria, Search Engine Colossus claims to list search engines and directories from over 200 countries and territories around the world.[228] Beaucoup, a portal of specialty search engines and directories, lists over 2,000 search resources by category.[229] The site attempts to include all such sources of "free" informaton (that is, sites that do not require fee-based membership), although some of the resources listed on the target sites may *not* be free. Sources are categorized and include a brief description, usually taken verbatim from the resource's Homepage or "About" page. Taylor referred to Cyward Internet Education for an article explaining search engine

---

[223] http://dir.yahoo.com/Computers_and_Internet/Software/Internet/World_Wide_Web/Browsers, "Yahoo! Directory Web Software > Browsers," Yahoo! Inc., 2003.

[224] http://www.lexisone.com/legalresearch/legalguide/internet_search_engines/directories_and_search_engines.htm, "Directories and Search Engines," Lexis/Nexis, 2003.

[225] http://searchenginewatch.com, "Search Engine Watch: Tips About Internet Search Engines & Search Engine Submission," Jupitermedia, Inc. 2003.

[226] http://searchenginewatch.com/links/article.php/2156221, "Major Search Engines and Directories," Jupitermedia, Inc. 2003.

[227] http://www.searchenginewatch.com/links/article.php/2156161, "Guides to Search Engines," Jupitermedia, Inc. 2003.

[228] http://www.searchenginecolossus.com, "Find search engines across the world with Search Engine Colossus," Bryan A. Strome, 2003.

[229] http://www.beaucoup.com, "Beaucoup! 2,000+ Search Engines Indices and Directories," T.Madden, 2001.

technology, but the article has been removed. Still, Cyward presents an extensive selection of search engines, sorted by type, size and specialty.[230]

As the result of, on the one hand, the wholesale invasion by spammers and on the other hand, the proliferation of discussion groups hosted by websites, Usenet has become a forum of last resort. It requires a fairly significant investment in time, selecting the appropriate groups, reading enough posts to become familiar with their participants and to evaluate the general worth of their discussions, reading the faqs to learn what questions to avoid – essentially, to become familiar with the neighborhood – before it can become a useful resource. Staying current with even a few newsgroups can become tedious. Spammers found it a very rich field, both to sow spam messages into and reap email addresses out of it; user-based anti-spam technology has not advanced far enough to filter out all undesirable Usenet posts. Moderated groups are generally free of spam, flamers and irrelevant posts, but they are very, very few in the vast ocean of groups. A handful of dotcom companies maintain newsgroup servers, which provide the 30,000-or-so most popular groups, but they charge a subscription fee for (meaningful) access. Part of this is the result of Usenet depending on a different protocol – NNTP, network news transport protocol – and servers than the Web. Navigating native Usenet in its enormity requires a newsreader, generally available for a small price and generally awkward to use (compared to the relative ease of navigating the Web); Cnet offers a selection at its Download.com page.[231] Some major Web browsers (and Microsoft Outlook) include NNTP clients, usually as a part of the e-mail client, which require separate configuration. There are a few Web-based "gateways" to Usenet. Currently, Google maintains extensive Usenet archives (as far back as 1981) and provides a Web-based newsreader as part of its search engine,[232] which integrates both the archives and current postings. Google attempts to block access to illegal/obscene newsgroups and filter spam out, but does not police Usenet, nor censor posted content. Yahoo! provides several links to Usenet resources[233] and its own version of a Usenet.[234] Other Usenet gateways are available, but the timeliness of the posts depends on how frequently the search engine behind the gateway indexes the groups; a group updated only twice a year is pretty useless, regardless of the importance of its subject.

I think of IRC as instant-gratification Usenet: a collection of realtime chatrooms, also organized (somewhat) by topic. IRC's biggest difference from Usenet is its material is ephemeral. Usenet posts are retained for varying lengths of time and can be searched (and many groups are archived); IRC conversations are not. It requires an instant messaging application, like the AIM application bundled with America Online software and other Web browsers. Taylor lists a few chatrooms and offers suggestions for finding

---

[230] http://www.cyward.com/speciali.htm, "Specialized Directories & Search Engines Compiled by Cyward," Nancy Picchi, 2002.
[231] http://download.com.com/3150-2164-0.html?tag=dir, "Newsreaders – Download.com – Free dowmloads, shareware, and more," CNET Networks, Inc., 2003.
[232] http://groups.google.com, "Google Groups," Google, Inc., 2003.
[233] http://dir.yahoo.com/Computers_and_Internet/Internet/Chats_and_Forums/Usenet, "Yahoo! Directory Internet > Usenet," Yahoo! Inc. 2003.
[234] http://help.yahoo.com/help/us/groups, "Yahoo! Groups – Groups," Yahoo! Inc. 2003.

"secret" hacker groups. I am ignorant here and leave it for interested readers to see his article.[235] Like Usenet, the chatrooms can become a time sink, and the information given to you is only as good as the credibility of the person talking to you.

[235] http://www.sans.org/rr/papers/index.php?id=519, "Keep Current with Little Time," p.3, Robert Taylor and The SANS Institute, 2001.

APPENDIX B/ REFERENCES

(ISC)^2. "(ISC)2." https://www.isc2.org/cgi/content.cgi?category=3. (29 December 2003).

101 Communications. "The E-Gov Institute." http://www.e-gov.com. (29 December 2003).

101communications LLC. "101communications LLC: Enabling Technology Professionals to Succeed." http://www.101com.com. (29 December 2003).

*2600: The Hacker Quarterly. "*2600: The Hacker Quarterly." http://www.2600.com. 2600 Enterprises, Inc. (29 December 2003).

AAABookSearch. com. "Browse by Subject – Computers." http://www.aaabooksearch.com/subjectcomp.aspx. Oceanview Technologies, Inc. (29 December 2003).

Allbookstores.com. "Compare prices on new, used, and out of print books and textbooks." http://www.allbookstores.com. (29 December 2003).

Amazon.com. "Power Search" page. http://www.amazon.com/exec/obidos/ats-query-page/ref=b_bh_l_a_2/104-6644241-2991900#powersearch. 2003. (29 December 2003).

APNIC Pty. Ltd. "List of ISO 3166 codes and corresponding RIRs." http://www.apnic.net/info/reference/lookup_codes_text.html. Last modified 19 November 2003. (29 December 2003).

ARIN. "Some Codes from ISO 3166." ftp://ftp.arin.net/netinfo/iso3166-countrycodes. (29 December 2003).

ASIS International. "ASIS International: Home Page." http://www.asisonline.org. (29 December 2003).

AusCERT. "AusCERT – Australia's National Computer Emergency Response Team." http://national.auscert.org.au. (29 December 2003).

Bartleby.com. "Reference: Dictionary, Encyclopedia, Thesauri, Usage, Quotations, and more." http://www.bartleby.com/reference. (29 December 2003).

Black Hat, Inc. "bhmediakit.pdf." http://www.blackhat.com/images/bh-about/bhmediakit.pdf. (29 December 2003).

Black Hat, Inc. "Black Hat Briefings Training and Consulting Security home page." http://www.blackhat.com/main.html. (29 December 2003).

Blackwell's Online Bookshop. "Blackwell's Online Bookshop [(US site]." http://bookshop.blackwell.com/bobus/scripts/welcome.jsp. (29 December 2003).

Blackwell's Online Bookshop. "Blackwell's Online Bookstore." http://www.blackwells.com. (29 December 2003).

Bookpool LLC. "Bookpool Discount Technical Books." http://www.bookpool.com. (29 December 2003).

Boswell, James. *The Life of Samuel Johnson*. Borzoi/Alfred A Knopf. New York, 1992.

Box Network team. "New Order – the computer & networking security portal." http://www.neworder.box.sk. (29 December 2003).

Carnegie-Mellon Software Engineering Institute. "CERT Coordination Center Alerts." http://www.cert.org/nav/alerts.html#summaries. Last modified: 17 December 2003. (29 December 2003).

Center for Internet Security. "Center for Internet Security – Standards." http://www.cisecurity.org. (29 December 2003).

CERIAS and Purdue University. "CERIAS – Electronic Law\Dedicated Sites." http://www.cerias.purdue.edu/tools_and_resources/hotlist/details.php?id=57. last updated 27 September 2003. (29 December 2003).

Check Point Software technologies, LTD. "Corporate Fact Sheet." http://www.checkpoint.com/corporate/corporate.html. (29 December 2003).

CIO Insight. "CIO Insight." http://www.cioinsight.com. Ziff Davis Media. (29 December 2003).

CIO. "@CIO.com – CIO Magazine and more online." http://www.cio.com. CXO Media Inc. (29 December 2003).

Cisco Systems, Inc. "Career Certifications and Paths – Cisco Systems." http://cisco.com/en/US/learning/le3/learning_career_certifications_and_learning_paths_home.html. (29 December 2003).

CMP United Business Media. "CMP." http://www.cmp.com. CMP Media, LLC. (29 December 2003).

CNET Networks, Inc. "CNET.com." http://www.cnet.com. CNET Networks, Inc. (29 December 2003).

CNET Networks, Inc. "Newsreaders – Download.com – Free dowmloads, shareware, and more." http://download.com.com/3150-2164-0.html?tag=dir. (29 December 2003).

CNET Networks, Inc. "TechRepublic – Real World. Real Time. Real IT." TechPublic. http://www.techrepublic.com. (29 December 2003).

Cole, Eric, Jason Fossen, Stephen Northcutt, and Hal Pomeranz. *SANS Security Essentials with CISSP CBK, Version 2.1*. SANS Press. United States. 2003.

Cole, Eric, Matthew Newfield and John M. Millican. *SANS GIAC Certification: Security Essentials Toolkit (GSEC)*. http://search.barnesandnoble.com/booksearch/isbnInquiry.asp?userid=2UQABVAETZ&endeca=1&isbn=0789727749&itm=1778. Pearson Education. (29 December 2003).

Cole, Eric. *Hackers Beware*. New Riders Publishing. Indianapolis, IN. 2002.

Computer Books Online. "Computer Security Book Index." http://www.computerbooksonline.com/securityindex.htm. Last Modified: 05 November 2003. (29 December 2003).

Computer Books Online. "Site Map." http://www.computerbooksonline.com/toc1.htm. Last Modified: 15 November 2003. (29 December 2003).

Computer Incident Advisory Capability. "U.S. DOE-CIAC: Federal and Security Information Sites." http://www.ciac.org/ciac/related_sites.html. U.S. Department of Energy. (29 December 2003).

Computer Security Institute. "Computer Security Institute." http://www.gocsi.com/events. (29 December 2003).

Computers and Security. "Computers and Security." http://www.elsevier.nl/inca/publications/store/4/0/5/8/7/7. Elsevier Advanced Technology. 2003. Last updated 23 December 2003. (29 December 2003).

Computerworld Inc. "Computerworld." http://www.computerworld.com. 2003. (29 December 2003).

Computing Technology Industry Association, Inc. "CompTIA Linux+ Certification." http://comptia.com/certification/linux/default.asp. (29 December 2003).

Computing Technology Industry Association, Inc. "CompTIA Security+ Certification." http://comptia.com/certification/security/default.asp. (29 December 2003).

Creative Element. "Annoyances.org." http://www.annoyances.org. (29 December 2003).

Creative Element. "Welcome to Creative Element." http://www.creativelement.com. (29 December 2003).

CSO. "CSO Magazine for Chief Security Officers and senior security executives." http://csoonline.com. CXO Media Inc. (29 December 2003).

Dark Tangent. "other Conventions & Events." http://www.defcon.org/html/links/other-conventions.html. last updated on: 7 November 2003. (29 December 2003).

Dorfest, Rael. "Why the Hacks Series." http://hacks.oreilly.com/pub/a/oreilly/hacks/whyhacks.html. O'Reilly and Associates. October 2003. (29 December 2003).

ECT News Network. "Linux News: Security." http://www.linuxinsider.com/perl/section/security. ECT News Network. 2003. (29 December 2003).

e-gov Digest. "e-gov Digest." http://www.e-gov.com/egov_digest. 101 Communications. (29 December 2003).

Electronic Freedom Foundation. "EFF: About." http://www.eff.org/about. Last updated 22 December 2003. (29 December 2003).

Electronic Freedom Foundation. "EFF: Homepage." http://www.eff.org. Last updated 22 December 2003. (29 December 2003).

Elsevier. "Compsec Online." http://www.compseconline.com. (29 December 2003).

EnterpriseITplanet.com's AntiOnline. "AntiOnline – Computer Security." http://antionline.com. Jupitermedia Corporation. (29 December 2003).

*eWEEK Enterprise News and Reviews. "*eWEEK.com." http://www.eweek.com. Ziff Davis Media. 2003. (29 December 2003).

*Federal Computer Weekly. "*FCW.com Home." http://www.fcw.com. FCW Media Group. (29 December 2003).

FreeBSD Project. "FreeBSD Security Information." www.freebsd.org/security. Last modified: 14 November 2003. (29 December 2003).

Guardian Digital. "Linux Security – The Community's Center for Security." http://www.linuxsecurity.org. Guardian Digital, Inc. 2002. (29 December 2003).

Garfinkel, Simson and Gene Spafford. *Practical UNIX and Internet Security,2nd Edition*. O'Reilly & Associates, Inc. Sebastopol, CA. 1996.

Google, Inc. "Google Groups." http://groups.google.com. (29 December 2003).

Government Computer News. "Government Computer News (GCN) home." http://www.gcn.com. Post-Newsweek Media, Inc. (29 December 2003).

Grewal, Subir. "What is Lynx, and why would I want to use it?" http://www.subir.com/lynx/what.html. Last updated 1 March 2003. (29 December 2003).

Guardian Digital, Inc. "Linux Security – The Community's Center for Security." http://www.linuxsecurity.org. (29 December 2003).

Guardian Digital, Inc. "LinuxSecurity –Newsletter." http://www.linuxsecurity.com/general/newsletter.html. (29 December 2003).

Half Price Computer Books. "Half Price Computer Books." http://www.halfpricecomputerbooks.com. (29 December 2003).

Hewlett-PackardCompany. "HP Certified Professional Certification Program." http://h10017.www1.hp.com/certification/about_the_program.html. (29 December 2003).

Hill Associates. "Hill Associates – RSA Live E-Learn Events." http://www.hill.com/partners/rsa. (29 December 2003).

IDG, Inc. "CXO Media, Inc. Resources for Management." http://www.cxo.com. (29 December 2003).

InfiniSource, Inc. “InfiniSource – The Internet’s Premier Resource Center.” http://www.infinisource.com. (29 December 2003).

Infoplease. “Information Please.” http://www.infoplease.com. Pearson Education. (29 December 2003).

Information Analysis Infrastructure Protection. “National Infrastructure Protection Center (NIPC) – Incident Report.” http://www.nipc.gov/incident/incident.htm. U.S. Department of Homeland Security. (29 December 2003).

Information Assurance Directorate. “The NSA/CSS Infosec Page.” http://www.nsa.gov/isso/index.html. National Security Agency. Revised 3 June2003. (29 December 2003).

Information Assurance Support Environment. “IASE Public Home Page.” http://iase.disa.mil/index2.html. Defense Information Systems Agency, U.S. Department of Defense. Revised 15 December 2003. (29 December 2003).

*Information Security. “*Information Security Magazine.” http://infosecuritymag.techtarget.com. TechTarget IT Media. (29 December 2003).

InformIT. “InformIT – Your Online Guide to Tech Reference.” http://www.informit.com. Pearson Education. (29 December 2003).

InfoSysSec Security Portal. “Advertising that targets the real IT security professionals.” http://www.infosyssec.com/infosyssec/advertise.htm. (29 December 2003).

InfoSysSec. “Hacking and Hackers -- Computer Security Programs Downloading Search Engines Portal News.” http://www.infosyssec.com. 2002. (29 December 2003).

*InfoWorld. “*InfoWorld Homepage.” http://www.infoworld.com. InfoWorld Media Group. 2003. (29 December 2003).

InfoWorld. “InfoWorld Special Report: Linux under siege: Tracking the course of SCO’s lawsuit.” http://www.infoworld.com/reports/SRscosuit.html. IDG News Service. (29 December 2003).

Institute of Electrical and Electronics Engineers, Inc. “Cipher: The Newsletter of the IEEE Computer Society Technical Committee on Security and Privacy.” http://www.ieee-security.org/cipher.html. (29 December 2003).

Internet Security Systems. “X-Force Research.” http://xforce.iss.net. (29 December 2003).

Internet Software Consortium. “Lynx current distribution directory.” http://lynx.isc.org/current. (29 December 2003).

Internet Software Marketing Ltd. “Anti-virus.” http://www.windowsecurity.com/software/Anti_Virus. Internet Software Marketing Ltd. 2003. (29 December 2003).

Internet Software Marketing Ltd. “Microsoft Windows security site: intrusion detection, anti-virus, firewalls, and more!” WindowSecurity.com. http://www.windowsecurity.com. (29 December 2003).

Jupitermedia Corporation. “About Jupitermedia.” http://www.internet.com/corporate/about.html. (29 December 2003).

Jupitermedia Corporation. “Webopedia: Online Dictionary for Computer and Internet Terms.” http://www.webopedia.com. (29 December 2003).

Jupitermedia Corporation. “www.Wi-FiPlanet.com.” http://wi-fiplanet.webopedia.com. (29 December 2003).

Jupitermedia, Inc. “Guides to Search Engines.” http://www.searchenginewatch.com/links/article.php/2156161. (29 December 2003).

Jupitermedia, Inc. “Major Search Engines and Directories.” http://searchenginewatch.com/links/article.php/2156221. (29 December 2003).

Kasperky Lab.(Site written in Cyrilic). http://www.avp.ru/products.html. (29 December 2003).

Kecman, Vojislav. *Learning and Soft Computing: with Support Vector Machines, Neural Networks, and Fuzzy Logic Models (Complex Adaptive Systems)*. http://www.bookpool.com/.x/p8nwy4omer/sm/0262112558. MIT Press, Cambridge, MA, 2001. (29 December 2003).

Lawrence Livermore National Laboratory/U.S. DOE. "CIAC Bulletins." http://ciac.llnl.gov/cgi-bin/index/bulletins. Lawrence Livermore National Laboratory/U.S. Department of Energy. (29 December 2003).

Lawrence Livermore National Laboratory/U.S. DOE. "CIAC C-Notes." http://www.ciac.org/cgi-bin/cnotes. Lawrence Livermore National Laboratory/U.S. Department of Energy. (29 December 2003).

Lawrence Livermore National Laboratory/U.S. DOE. "DOE Computer Security Resources." http://doe-is.llnl.gov/DOESecurityResources.html. Lawrence Livermore National Laboratory/ U.S. Department of Energy.Last modified 22-Feb-2002. (29 December 2003).

Lawrence Livermore National Laboratory/U.S. DOE. "U.S. DOE-CIAC – Windows NT Information." http://www.ciac.org/ciacNT/index.html. Lawrence Livermore National Laboratory/U.S. Department of Energy. (29 December 2003).

Lawrence Livermore National Laboratory/U.S. DOE. "U.S. DOE-CIAC: CSTC (Cyber Solutions Tool Center)." http://www.ciac.org/cstc/CSTCHome.html. Lawrence Livermore National Laboratory/U.S. Department of Energy. (29 December 2003).

Lexis/Nexis. "Directories and Search Engines." http://www.lexisone.com/legalresearch/legalguide/internet_search_engines/directories_and_search_engines.htm. (29 December 2003).

LexisNexis. "About Lexis/Nexis." http://www.lexisnexis.com/about. (29 December 2003).

LexisNexis. "Computer Center." http://www.lexisone.com/legalresearch/legalguide/computer_center/computers_center_index.htm. (29 December 2003).

LexisNexis. "Computer Security." http://www.lexisone.com/legalresearch/legalguide/computer_center/computers_antivirus_security_introduction.htm. (29 December 2003).

LexisNexis. "Cyberspace & Internet Law." http://www.lexisone.com/legalresearch/legalguide/practice_areas/cyberspace_internet_law.htm#7. (29 December 2003).

LexisNexis. "lexisONE." http://www.lexisone.com. (29 December 2003).

Mac Publishing, LLC. "Macworld: About Us." http://www.macworld.com/info/aboutus. (29 December 2003).

Macworld. "Macworld: The Mac Product Experts." http://www.macworld.com. Mac Publishing, LLC. (29 December 2003).

Madden, T. "Beaucoup! 2,000+ Search Engines Indices and Directories." http://www.beaucoup.com. (29 December 2003).

McCurley, Kevin. "DigiCrime, Inc." . http://www.digicrime.com/dc.html. DigiCrime. (29 December 2003).

McCurley, Kevin. "Kevin McCurley." http://www.swcp.com/~mccurley. (29 December 2003).

Merriam-Webster Dictionary. "Merriam-Webster Online." http://www.m-w.com. (29 December 2003).

Microsoft Corporation. "Community Newsgroups." http://support.microsoft.com/newsgroups. (29 December 2003).

Microsoft Corporation. "Downloads and Updates." http://support.microsoft.com/default.aspx?scid=fh;EN-US;DOWNLOADOVER. (29 December 2003).

Microsoft Corporation. “Microsoft Certifications.” http://www.microsoft.com/traincert/mcp/default.asp. (29 December 2003).

Microsoft Corporation. “Microsoft Help and Support.” http://support.microsoft.com/default.aspx. (29 December 2003).

Microsoft Corporation. “Microsoft Product Communities: Find a Community for a Microsoft Product or Technology.” http://www.microsoft.com/communities/products/default.mspx?qssnb=1. (29 December 2003).

Microsoft Corporation. “Security Resources.” http://www.microsoft.com/learning/centers/security.asp. (29 December 2003).

Microsoft Corporation. “Security.” http://www.microsoft.com/Security. (29 December 2003).

Microsoft Corporation. “Security.” http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp. (29 December 2003).

MIS Training Institute. “About MIS Training Institute.” http://www.misti.com/northamerica.asp?page=4&subpage=2&region=1&disp=about. (29 December 2003).

MIS Training Institute. “Audit and Information Security Training [Europe].” http://www.mistieurope.com/MIS/about.asp. (29 December 2003).

MIS Training Institute. “MIS Conferences (Infosecurity).” http://www.misti.com/northamerica.asp?page=1&disp=conf&region=1&subpage=2. (29 December 2003).

MIS Training Institute. “Welcome to MIS Asia.” http://www.misti.com/asia.asp. (29 December 2003).

MIS Training Institute. “What’s Up in Infosecurity.” http://www.misti.com/northamerica.asp?page=1&subpage=0&region=1. (29 December 2003).

Mozilla Organization. “mozilla – home of the mozilla, firebird, and camino web browsers.” http://www.mozilla.org. (29 December 2003).

National Center for Supercomputing Applications. “NCSA: History.” http://www.ncsa.uiuc.edu/AboutUs/Overview/Historythe1990s.html. University of Illinois at Urbana-Champaign. 2003. Last updated 23 December 2003. (29 December 2003).

National Institute of Standards and Technology. “CCEVS WebPage.” http://niap.nist.gov/cc-scheme/GuidanceDocs.html. National Information Assurance Partnership, National Institute of Standards and Technology, U.S. Department of Commerce. Last updated 27 December 2003. (29 December 2003).

National Institute of Standards and Technology “C S R C – Guidance / Publications / Library.” http://www.csrc.nist.gov/publications. Computer Security Resource Center. National Institute of Standards and Technology, U.S. Department of Commerce. Last updated: 13 December 2002. (29 December 2003).

National Institute of Standards and Technology. “NIST Computer Security Division 893 and CSRC Home Page.” http://csrc.nist.gov. Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce. (29 December 2003).

National Institute of Standards and Technology. “NIST Vulnerability and Threat Portal.” http://icat.nist.gov/vt_portal.cfm. National Institute of Standards and Technology, U.S. Department of Commerce. (29 December 2003).

National Security Telecommunications and Information Systems Security Committee. “nstissam_compusec_1-99.pdf.” http://www.nstissc.gov/Assets/pdf/nstissam_compusec_1-99.pdf. National Information Assurance Partnership, National Institute of Standards and Technology, U.S. Department of Commerce. (29 December 2003).

NDU – IRMC. "NDU – IRM College." http://www.ndu.edu/irmc. Information Resource Management College, National Defense University. (29 December 2003).

Netscape. "Netscape.com." http://www.netscape.com. (29 December 2003).

*Network Computing. "*Technology Guide: Security." http://www.nwc.com/core/core7.jhtml. CMP Media, LLC. (29 December 2003).

*Network Magazine. "*Network Magazine – Technology Architecture for the 21st Century." http://www.networkmagazine.com. CMP Media, LLC. (29 December 2003).

*NetworkWorldFusion. "*Network World Fusion." http://www.nwfusion.com/index.html. Network World, Inc. 2003. (29 December 2003).

Newsfeeds.com. "Welcome to Newsfeeds.com." http://www.newsfeeds.com. (29 December 2003).

Nkrumah Kwame (1909-1972, first leader of post-colonial Ghana). As attributed by William C. Robinson, "Community Analysis." http://web.utk.edu/~wrobinso/560_lec_commun-analysis.html. University of Tennessee, Knoxville. 2003. (29 December 2003).

Northcutt, Stephen and Lara Corcoran. "Global Information Assurance Certification, Objectives and Curriculum," version 6. http://www.giac.org/GIAC_Cert_Brief.pdf. SANS Institute. August 2003. (29 December 2003).

Novell press release. "Novell: Novell Announces Agreement to Acquire Leading Enterprise Linux Technology Company SuSE Linux." http://www.novell.com/news/press/archive/2003/11/pr03069.html. Novell. 4 November 2003. (29 December 2003).

O'Reilly & Associates. "About O'Reilly & Associates." http://www.oreilly.com/oreilly/about.html. (29 December 2003).

O'Reilly & Associates. "Welcome to the O'Reilly Security Center." http://security.oreilly.com. (29 December 2003).

O'Reilly & Associates. "www.oreilly.com -- Welcome to O'Reilly & Associates." http://www.oreilly.com. (29 December 2003).

Open Source Development Network. "Geocrawler.com – Security—Mailing List Archives." http://geocrawler.com/lists/3/Security. (29 December 2003).

Opera Software ASA. "Opera Internet Browser." http://www.opera.com. (29 December 2003).

*PC World. "*PCWorld." http://www.pcworld.com. IDG, Inc. 2003. (29 December 2003).

Pearson Education, Inc. "InformIT.com: Book Store." http://www.informit.com/book_store/index.asp. (29 December 2003).

Penton Media, Inc. "Windows & .Net Magazine Network." http://www.winnetmag.com. (29 December 2003).

Picchi, Nancy. "Specialized Directories & Search Engines Compiled by Cyward." http://www.cyward.com/speciali.htm. (29 December 2003).

Powells.com. "Powell's Books – Networking-Computer Security." http://www.powells.com/subsection/NetworkingComputerSecurity.html. (29 December 2003).

Pratchett, Terry. *Soul Music* in *Death Trilogy*. Victor Gollancz. London. (29 December 2003).

Que Publishing. "About Que." http://www.quepublishing.com/about. (29 December 2003).

Raymond, Eric, ed. "Jargon 4.2 node: Jargon File 4.2.0 dated Jan 31, 2000." http://www.science.uva.nl/~mes/jargon. Faculteit der Natuurwetenschappen, Wiskunde en Informatica de Universiteit van Amsterdam. (29 December 2003).

Red Hat, Inc. “redhat.com – Red Hat Enterprise Linux Migration Center.” http://www.redhat.com/solutions/migration/rhl. (29 December 2003).

Red Hat, Inc. “redhat.com – Red Hat Linux Training, Certification, RHCT, RHCE.” http://www.redhat.com/training. (29 December 2003).

Reiter’s Scientific Books. “Reiter’s Online Store: Computers.” http://www.reiters.com/index.cgi?f=t&sid=251&ses=2944271&h=t10. (29 December 2003).

RIPE NCC. “RIPE NCC Local Internet Registries: Country Index.” http://www.ripe.net/ripencc/mem-services/general/indices/index.html. (29 December 2003).

RSA Security Inc. “RSA Security – Identity and Access Management e-Security.” http://www.rsasecurity.com. 2003. (29 December 2003).

Safari Tech Books Online. “Default Safari Online.” http://secure.safaribooksonline.com. (29 December 2003).

SANS Institute. “Internet Storm Center.” http://isc.sans.org. (29 December 2003).

SANS Institute. “S.C.O.R.E. – Security Consensus Operational Readiness Evaluation.” http://www.sans.org/score. (29 December 2003).

SANS Institute. “SANS InfoSec Reading Room.” http://www.sans.org/rr. (29 December 2003).

SANS Institute. “SANS Institute – Computer Security Newsletters.” http://www.sans.org/newsletters. (29 December 2003).

SANS Institute. “SANS Institute – Security Policy Project.” http://www.sans.org/resources/policies. (29 December 2003).

SANS Institute. “SANS Institute –Computer Security Education and information Security Training.” http://www.sans.org. (29 December 2003).

SANS Institute. “SANS Institute: Security Projects.” http://www.sans.org/projects. (29 December 2003).

SANS Institute. “SANS Online Training.” http://www.sans.org/onlinetraining. (29 December 2003).

SC Informationsecurity News. “Information Security News.” http://www.infosecnews.com. West Coast Publishing. (29 December 2003).

SC Magazine. “Secure Computing Magazine – West Coast Publishing.” http://www.westcoast.com/cgi-bin/redirect.pl. West Coast Publishing. (29 December 2003).

S-Cure. “Trusted Introducer / CSIRT Teams.” http://www.ti.terena.nl/teams/index.html. Amersfoort, NL. 2003. Last updated 03 June 2003. (29 December 2003).

SearchEngineWatch.Com. “Search Engine Submission Tips.” http://www.searchenginewatch.com/webmasters/index.php. (29 December 2003).

Security Advisor. “Security Advisor – securityadvisor.info.” http://securityadvisor.info. Advisor Media. (29 December 2003).

Security Focus. “SecurityFocus BugTraq Mailing List.” http://securityfocus.com/archive/1. 2003. (29 December 2003).

Security Focus. “SecurityFocus Newsletters.” http://securityfocus.com/newsletters. (29 December 2003).

Security Management. “Security Management Online.” http://www.securitymanagement.com. (29 December 2003).

Security Pipeline. “Security Pipeline.” http://informationweek.securitypipeline.com. CMP Media, LLC. (29 December 2003).

SecurityNewsPortal.com. “Security News Portal,…Page Two.” http://www.snpx.com/pagetwo.html. (29 December 2003).

Silicon Graphics, Inc. “SGI – Services & Support: Security Home Page.” www.sgi.com/support/security. (29 December 2003).

Software in the Public Interest, Inc. “Debian GNU/Linux – Security information.” www.debian.org/security. Last Modified: 22 Dec 2003. (29 December 2003).

Strome, Bryan A. “Find search engines across the world with Search Engine Colossus.” http://www.searchenginecolossus.com. (29 December 2003).

Sun Microsystems, Inc. “Security and the Java Platform.” http://java.sun.com/security. (29 December 2003).

Sun Microsystems, Inc. “Sun training and certification programs.” http://training.sun.com/US/certification. (29 December 2003).

Sun Microsystems, Inc. “SunSolve Home.” http://sunsolve.sun.com/pub-cgi/show.pl?target=home. (29 December 2003).

Sunbelt Media Services. “W2Knews.” http://www.w2knews.com/about-us.cfm. (29 December 2003).

*Sys Admin Magazine. “*Sys Admin Magazine.” http://sysadminmag.com. CMP Media, LLC. (29 December 2003).

Taylor, Robert. “Keep Current with Little Time.” http://www.sans.org/rr/catindex.php?cat_id=48. SANS Institute. 2001. (29 December 2003. Note: I originally found this in the SANS Reading Room, under “Getting Started/InfoSec” topic; although it has since disappeared from the webpage, I was able to access it by the given URL.).

TechTarget. “About TechTarget.” http://www.techtarget.com/html/ab_index.htm. (29 December 2003).

TechTarget. “SearchEnterpriseLinux.com.” http://searchenterpriselinux.techtarget.com. (29 December 2003).

TechTarget. “SearchSecurity.com.” http://searchsecurity.techtarget.com. (29 December 2003).

TechTarget. “SearchTechTarget – Welcome.” http://searchtechtarget.techtarget.com. (29 December 2003).

TechTarget. “SearchWin2000.com.” http://searchwin2000.techtarget.com. (29 December 2003).

TechTarget. “WhatIs.Com.” http://whatis.techtarget.com. (29 December 2003).

TechWeb. “TechWeb: The Business Technology Network.” http://www.techweb.com. CMP Media, LLC. (29 December 2003).

Techworld. “Techworld.com.” http://www.techworld.com. IDG. (29 December 2003).

TERENA. “TERENA -- About TERENA.” http://www.terena.nl/about. Last modified 14 November 2002. (29 December 2003).

The SANS Institute. “SANS Institute – Computer Education and Information Security Training.” http://sans.org. (29 December 2003).

Tulloch, Mitch. *Microsoft Encyclopedia of Security*. http://www.microsoft.com/MSPress/books/6429.asp. Microsoft Press. 2003. (29 December 2003).

U.S. Department of Agriculture. “Graduate School, USDA.” http://grad.usda.gov/index.html. (29 December 2003).

U.S. Department of Defense. “DoD-CERT Online.” http://www.cert.mil. (29 December 2003).

U.S. Department of Homeland Security. “Federal Computer Incident Response Center.” http://www.fedcirc.gov. (29 December 2003).

U.S. Department of Homeland Security. “Sitemap.” http://www.fedcirc.gov/generalInfo/siteMap.html. (29 December 2003).

U.S. Department of Homeland Security. "US-CERT: Working whith US-CERT." http://www.uscert.gov/workwithus. last updated 13 December 2003. (29 December 2003).

USENIX/SAGE. "USENIX – Events Calendar." http://www.usenix.org/events. Last changed: 18 December 2003. (29 December 2003).

VA Software, Inc. "VA Software: OSDN." http://www.vasoftware.com/osdn.php. (29 December 2003).

VNU Business Publications Ltd. "PC Magazine Online." http://www.pcmag.co.uk. (29 December 2003).

VNU Business Publications Ltd. "VNU Subscriptions." http://www.vnusubs.co.uk. (29 December 2003).

VNU Business Publications Ltd. "vnunet.com Homepage." http://www.vnunet.com. (29 December 2003).

VNU Business Publications Ltd. "vnunet.com Security." http://www.vnunet.com/News/Security. (29 December 2003).

VNU Business Publications Ltd. "vnunet.com SME Business Innovation Centre." http://business.vnunet.com. (29 December 2003).

WebConcepts. "123PriceCheck.com." http://www.123pricecheck.com. (29 December 2003).

Windows-Help.NET. "Windows-Help.NET." http://www.windows-help.net/index.shtml. (29 December 2003).

Wired magazine. "Wired News." http://www.wired.com. Condé Nast. (29 December 2003).

Yahoo! Inc. "Yahoo! Directory Internet > Usenet." http://dir.yahoo.com/Computers_and_Internet/Internet/Chats_and_Forums/Usenet. (29 December 2003).

Yahoo! Inc. "Yahoo! Directory Web Software > Browsers." http://dir.yahoo.com/Computers_and_Internet/Software/Internet/World_Wide_Web/Browsers. (29 December 2003).

Yahoo! Inc. "Yahoo! Groups – Groups." http://help.yahoo.com/help/us/groups. (29 December 2003).

ZDNet. "Information resources for IT professionals – ZDNet." http://www.zdnet.com. CNET Network, Inc. (29 December 2003).

Ziff Davis Media Inc. *PC Magazine*. http://www.pcmag.com. (29 December 2003).