Global Information Assurance Certification Paper

So Many Security Articles, So Little Time….

By Laura J. Nielsen

Overview

In September, 2001, Robert Taylor did a wonderful paper called "Keep Current With Little Time."[1] Written just a week after the 9-11 attacks, he outlined a plan to help an individual with little time to keep current on security issues. Since then, there has been an explosion of available security information, making it even more imperative that, as security professional, you make a wise investment of your valuable time to stay current and focused in this ever changing environment. This paper shows you how to develop a personal plan to stay current with security information, updating and adding to the information in Robert Taylor's paper, and introduces productivity tools that will allow you to more easily collect, organize, and disseminate security information.

Scope

This paper is for someone who is already well versed in computer security. It is not intended to get you "up to speed" but rather to "keep you in the game." I have intentionally excluded training companies and university programs from this paper. Security training is a topic substantial enough to warrant its own paper. Suffice to say, if you feel compelled to attend any training course, examine the credentials of the person teaching it before you pay a cent. You may be surprised to find that you have more experience than the trainer as many "security trainers" were doing something else a short time ago. For that reason, and based on my own personal experience as a SANS student, I highly recommend that you check out the training provided through SANS at http://www.sans.org . SANS classes are excellent and are offered in many locations.

Planning

There are four basic elements to planning your Personal Security Information Plan. They are Rank, Accuracy, Timing, Speed and Sharing or RATSS. Each element will help your define your specific security information needs.

Rank

Before you determine **how** to get it, you need to determine **what type** of information is most necessary to you and **how fast** you need to receive it.

According to the International Information Systems Security Consortium (ISC^2), the Common Body of Knowledge, or CBK, is "a compilation and distillation of all security information collected internationally of relevance to Information Security [IS] professionals."[2] There are 10 different security areas or "domains" in the CBK:

- Access Control and Methodology
- Applications and Systems Development Security

- Business Continuity Planning and Disaster Recovery Planning
- Cryptography
- Law, Investigation and Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Networking Security

Each domain contains numerous subjects and each has a plethora of information written about it. In 2002 CERT had a total of 82,094 computer virus incidents reported[3]… and computer viruses is just ONE topic in ONE of the 10 domains. You get the picture. It's impossible to keep up with ALL of the information in ALL of the domains, so how do you decide just what specific topics should have your highest personal priority? As a security professional, this will probably be determined by your specific job function.

Obviously, the breadth and depth of your interest in any one subject is different if you're a security administrator for a small business or the Chief Information Security Officer (CISO) of a large Federal Agency. In most cases, a security administrator for a small company needs to know something about everything in security at a "deep" level, such as how to configure clients and servers, keep them up to date with the latest patches, etc. A CISO has to know security from a managerial view, such as how the security meshes with the enterprise infrastructure, if resources and processes are in place to support legal and business case requirements and the like. So focus on those topics that are of most importance to you.

Accuracy

Be sure to carefully consider the source of your security information. Take every bit of information with a grain of salt and make certain that your source is worthy of your time and trust. Deception is a major part of cyber crime and we are already seeing bogus "security updates" from "Microsoft" [4] and others. Also, when looking at polls, look for particulars on the number and types of people who participated. Know what the track record is of someone who purports to be a "security expert" before blindly following his/her advice or sending it on. The reason for gaining this knowledge is to be a savvy and educated proponent for yourself and your organization. Otherwise you could actually become a hindrance or even an unwitting participant in a social engineering attack on your own organization.

Time

Be realistic with yourself about the amount of time you have available for "keeping up" given the current level of demands in both your professional and private lives. Thinking you'll have several hours a day to leisurely peruse information probably wouldn't fit with the demanding IT security professional, regardless of your job description and

especially if you want to have any kind of personal life. On the other hand, it's amazing how much time you can glean during such mundane "tasks" as waiting for a meeting to start or while sitting and installing software. By judiciously using email capabilities or a Personal Digital Assistant (PDA), your empty time can become positive and enjoyable, rather than boring and frustrating.

Speed

Consider how swiftly you need information on a specific topic. For instance, it's likely that you'll want information on a new virus immediately so that you can begin taking action to mitigate it, while information on new training course can probably hold off until it's convenient for you to look at it. The urgency and speed with which you must use the information will determine the best methods for acquiring it.

Sharing

Once you have this information and you have verified its accuracy, who else must receive it and is it your responsibility to pass it on? If so, what specific information should you pass on? Will it reveal a vulnerability in your organization to others? When must it be sent and to whom? What happens if such information is obtained by a third party as a result of your actions, whether by their intent or not? These questions must be answered before considering if, when, and how to disseminate any information you obtain.

Security awareness is one type of information. Users should be constantly reminded of strong password criteria, i.e., not leaving their passwords taped to their monitor, never to give out their password to anyone, etc. That can be done in an almost methodical way. Then there are critical emergencies. For the average security administrator, this could be passing on information about a fast moving new virus so that users don't open a malicious email. For a CISO, it could be handling an anthrax or bomb threat.

Information sharing must also be based on specific criteria to different audiences. Some security information will go to all users. Other information may be for system administrators only.

By applying the RATSS methodology, you can make the most of your limited time and available security information resources and those of the people who rely on you. Emergency situations in particular call for fast and accurate communication, and planning for events like those has to happen before they occur.

Collecting Information

Whenever possible you want to make use of the talents of others to gather and prioritize security information. If it's possible, have a person who reports to you monitor and disseminate security related information. For those of us who don't have the benefit of such help, security related services are the next best thing. These can take the form of

Security advisories, newsletters and forums, security-related and vendor websites, conferences, magazines, and books. Because electronic means are much faster than printed, they are listed first here.

Security Web Directories

Security Web Directories are an immense portal to internet security information. Google, Yahoo and Tile.net are examples of sites that offer web search and newsgroup services.

Google (http://www.Google.com): Figure 1 shows the results of my Google search on "Computer Security".[5] Notice that there are 27 different categories under "computer security" with 644 different sites for products and tools alone!

Yahoo (http://www.yahoo.com) Figure 2 shows the results of my Yahoo search on "Computer Security". It has 22 different subcategories.

Tile.net (http://www.Tile.net): Tile.net has a much simpler interface than Google and Yahoo, as Figure 3 shows, but it requires a higher level of existing knowledge. In addition to supporting searches of lists and newsgroups, Tile.net also allows you to search FTP sites and computer product vendors.

Incident Response Centers

Incident Response Centers give fast and reliable information concerning vulnerabilities. Time is of the essence when a new computer virus is discovered, The complexity of exploits continues to grow, so the time to backward engineer and fix them is taking longer and longer. That's why your knowing what's "out there" immediately, even if a fix is not yet available, is crucial. For some the option of turning off a server is preferable to rebuilding it later.

Australian Computer Emergency Response Team (AUSCERT):
http://www.auscert.org.au/
emailauscert@auscert.org.au or call +6 1 7 3365 4417

CERT(sm) Coordination Center: http://www.cert.org/
email cert@cert.org or call +1 412 268-7090
Computer Incident Advisory Capability (CIAC): http://ciac.llnl.gov
email ciac@llnl.gov or call +1 925 422-8193

Defense Information Systems Agency Center for Automated System Security Incident Support Team (ASSIST, for DoD sites): http://www.assist.mil/
email cert@cert.mil or call +1 800 357-4231

Federal Bureau of Investigation (FBI) - National Infrastructure Protection Center (NIPC)
http://www.fbi.gov/nipc/index.htm or email nipc@fbi.gov
Nearest FBI Field Offices can be found at: http://www.fbi.gov/contact/fo/fo.htm

Federal Computer Incident Response Capability (FedCIRC): http://www.fedcirc.gov/
email fedcirc@fedcirc.gov or call +1 888 282-0870

Forum of Incident Response and Security Teams (FIRST): http://www.first.org/
email first-sec.first.org

German Research Network CERT (DFN-CERT): Http://www.cert.dfn.de/eng/dfncert
Email dfncert@cert.dfn.de

Internet Storm Center: http://isc.incidents.org
isc@incidents.org

NASA Incident Response Center (NASIRC): http://www-nasirc.nasa.gov/incidents.html
email nasirc@masirc.nasa.gov or call +1 800 762-7472

A full list of European CERTS can be found at:
http://www.cert.dfn.de/eng/csir/europe/certs.html

Bulletins and Archives

Bugtraq Full Disclosure List: listserv@securityfocus.com
CERT Advisories: Cert-advisory-request@cert.org
CIAC Advisories (ciac bulletin): majordomo@rumpole.llnl.gov
COAST Security Archive: Coast-request@cs.purdue.edu
Firewalls Digest: majordomo@lists.gnac.net
Firewall Wizards (firewall-wizards): majordomo@nfr.net
FreeSD Security Issues: majordomo@freesd.org
Intrusion Detection Systems (ids): majordomo@uow.edu.au
Linux Security Issues: Linux-security-request@RedHat.com
Legal Aspects of Computer Crime (lacc): majordomo@suburbia.net
NT Bugtraq : listserv@listserv.ntbugtraq.com
The RISKS Forum (risks): Risks-requests@csl.sri.com
WWW Security (ww-security-new): majordomo@nsmx.rutgers.edu
The Virus Lists (virus-l & virus): LISTSERV@lehigh.edu
Security list FAQ located at: http://xforce.iss.net/maillists/otherlists.php3
Stronghold Webserver Site: http://stronghold.redhat.com/

Newsletters

Government Executive, GovExec.com, subscribe: http://www.govexec.com/email
CISCO, subscribe: http://www.cisco.com/offer/subscribe
CISCO TAC, subscribe:
http://www.cisco.com/tac/newsflash/0303_tac_web_sem_seg3.html
Security Wire Digest, subscribe: http://infosecuritymag.bellevue.com
TechTarget "The Most Targeted IT Media" (http://www.techtarget.com)
SANS NewsBites, subscribe: http://www.sans.org/sansnews/
Cipher Newsletter: http://www.ieee-security.org/cipher.html
A Newsletter of the IEEE Committee on Security & Privacy provides a wide range of information of current news in the field.
Computer Incident Advisory Capability (CIAC) Notes: http://ciac.llnl.gov/cgi-bin/cnotes features information about computer security threats for Macs, PCs, Unix systems as well as other systems.
Internet Security Newsletter : http://www.securecomputing.com/index.cfm?skey=415
A quarterly newsletter that addresses various relevant network security issues, including security threats, recent computer security-related news stories, and editorials and recommendations from certified staff of network security professionals.
Internet Security Review: http://www.isr.net/
Committed to bringing daily updates on breakings news and industry developments on the topic of network/Internet security issues.

Microsoft TechNet Newsletter:
http://register.microsoft.com/regsys/ValueProp.asp?FU=http%3A%2F%2Fregister%2Emicrosoft%2Ecom%2Fregsys%2Fregsys%2Easp%3Fwizid%253D5823%2526lcid%253D1033&LCID=1033&WizID=5823&sl=0

Secure News: http://www.isecure.com/newslet.htm
A newsletter for Data and System Security from Innovative Security Products features information on current events.

SecurityTracker.com: http://securitytracker.com/
Reporting on computer vulnerabilities.

Newsgroups

Newsgroups and other forums are a great place for collecting and sharing information with others. Newsgroups are most often peer interest groups. Some of the information is very useful, some not, some accurate, some incorrect, and often times thought provoking. Figures 4 and 5 show what groups are available through Google and Yahoo, respectively. If you're unfamiliar with the workings of a newsgroup or need instructions on how to join one, there is a short but excellent discussion in the book, "Using

Microsoft Outlook, Special Edition"[6] or go to the online article, "Exploring Usenet Groups." [7] To access a newsgroup you can either:

- Use Outlook Express or Outlook XP, 2002, etc. to access your newsgroups through your Internet Service Provider (ISP). You will need to input the name of the news server (the name of which is usually available on the ISP web site) and select the groups that you wish to join. Individual messages will be sent to your newsreader folder, one subfolder for each of the lists you join. You can sort and do searches by text on these messages just like any other Outlook email, or

- Access the groups you wish to participate in using a web directory service like Google. Go to the directory service home page, select the groups tab, and search for the available groups by subject. Figure 6 shows the Google Comp. Security.Firewalls Group. Notice that there are many discussions or "threads" running simultaneously.

A note of caution: You can never know for certain who is monitoring these groups and what their intention is. Never disclose anything sensitive about yourself or your organization. When posting, ask yourself, "How would I feel if this was printed on the front page of "USA Today"?

The following are USENET security related newsgroups found using Tile.net:

alt.comp.virus
alt.comp.virus.pro-virus : pro-computer virus discussion and information
alt.comp.virus.source.code: The source code to various virii.
alt.disasters.planning
alt.hackers
alt.security : Security issues on computer systems.
alt.security.alarms : Discussion of Home/Business/Vehicle security alarms
alt.security.espionage : Espionage, intelligence, and tradecraft.
alt.security.index : Pointers to good stuff in alt.security. (Moderated)
alt.security.keydist
alt.security.neighborhood
alt.security.pgp : The Pretty Good Privacy package.
alt.security.ripem
alt.security.terrorism : Terrorism -- the bomb, the bullet, and the blade
alt.security.terrorism.atlanta : The Bomb the rocked Olympics '96
alt.security.terrorism.flight800: TWA Flight 800 over Long Island.
alt.security.tscm
comp.lang.java.security : Java security
comp.os.ms-windows.nt.admin.security
comp.os.netware.security : Netware security
comp.protocols.kerberos : Kerberos protocols
comp.risks : computer risks
comp.security.announce : Announcements from the CERT about security. (Moderated)

comp.security.firewalls : Anything pertaining to network firewall security.
comp.security.gss-api : Generic Security Service Application Program Interface.
comp.security.misc: Security issues of computers and networks.
comp.security.pgp.discuss : PGP and its implications
comp.security.pgp.resources : PGP related resources, information and more.
comp.security.pgp.announce : New PGP versions, utils and such. (Moderated)
comp.security.pgp.tech : Use of PGP, bug reports and help
comp.security.ssh ; SSH secure remote login and tunneling tools.
comp.security.unix: : Discussion of Unix security.
info.firewalls-digest: Firewall security
misc.security: miscellaneous Security
sci.crypt: cryptography, cryptanalysis, and related issues
sci.crypt.research: cryptography, cryptanalysis, and related issues

Magazines

Many magazines have both printed and on-line versions. With some magazines the on-line versions tend to be more dynamic, while others limit their on-line versions to archived copies only.

Security Related Magazines

Wired News, San Francisco, CA http://www.wired.com

2600:The Hacker Quarterly, Middle Island, NY: http://www.2600.com
Federal Computer Week, "Your Government IT Resource", http://www.fcw.com
CNET Networks, Inc., San Francisco, CA http://www.zdnet.com
Computerworld, Framingham, Ma http://www.computerworld.com
Cipher Magazine, IEEE Computer Society, Washington, DC: http://www.ieee-security.org/cipher.html
Computers & Security, Elsevier Int'l, RSO New York, NY, http://www.elsevier.nl/inca/publications/store/4/0/5/8/7/7/
Information Security World, http://www.isec-worldwide.com/
Information Security Magazine, Trusecure Corp., Norwood, Mass. http://www.infosecuritymag.com/
Infosecurity News, http://www.infosecnews.com/
Access, National Center for Supercomputing Applications (NCSA), University of Illinois, Champaign-Urbana, http://access.ncsa.uiuc.edu/
SC Magazine, (UK Ed.) http://www.westcoast.com/
Security Focus, Symantec Corporate Offices, Cupertino, CA http://www.securityfocus.com/
Security Management, ASIS International,http://www.securitymanagement.com/
Security Sales & Integration, Torrance, CA, http://www.securitysales.com/main.cfm

Computer Magazines

CIO Insight -- http://www.cioinsight.com/
CIO Magazine - <http://www.cio.com
CSO Magazine - <http://www.cso.com
Computer Technology Review -- http://www.wwpi.com/home_ctr.asp
ComputerWorld -- http://www.computerworld.com/
Federal Times -- http://federaltimes.com
Fortune -- http://www.fortune.com/fortune/home_channel/
Government Executive - <http://www.govexec.com
Government Computer News -- <http://www.gcn.com
Federal ComputerWeek -- <http://www.fcw.com/
The Federal Paper (Past issues ONLY online) -- http://www.fedpaper.com/
Information Security -- http://www.infosecuritymag.com/
Information Week -- http://www.informationweek.com
InfoWorld Magazine – http://www.infoworld.com
Network Magazine -- http://www.networkmagazine.com/
Network World -- http://www.nwfusion.com
Oracle Magazine -- http://otn.oracle.com/oramag/oracle/content.html
PC Magazine - http://www.pcmag.com/

Security Conference Links

These sites are a clearinghouse of information on security conferences sponsored by many different vendors:

The University of California, San Diego http://www.cs.ucsd.edu/users/mihir/confs.html
Operation: Security, http://www.operationsecurity.com/resource_db.php?viewCat=21

Security Conference Sponsors

Black Hat Briefings, Seattle WA, http://www.blackhat.com/
Computer Security Institute, San Francisco, CA , http://www.gocsi.com/
RSA Security, Bedford, MA , http://www.rsasecurity.com/
Systems Administration, Networking and Security Organization (SANS)
http: www.sans.org
White Hat Security, Santa Clara, CA, http://www.whitehatsec.com/

Vendor Sites

This is a good place to look for security patches and drivers:

Berkeley Software Design: http://www.bsdi.com/services/support
Cisco Systems, Inc: http://www.cisco.com/warp/public/707/sec_incident_response.shtml
Compaq Corporation: http://www.compaq.com
The FreeSD Project: http://www.freesd.org/security
Hewlett Packard http://us-support.external.hp.com
IBM: http://www-1.ibm.com/services/continuity/recover1.nsf/home
Linux (Caldera): http://www.calderasystems.com/support/security
Linux (Debian): http://www.debion.org/security
Linux (Red Hat): http://www.redhat.com/cgi-bin/support
Microsoft Corporation: http://www.microsoft.com/security/
Novell: http://www.support.novell.com
The Open BSD Project: http://www.openbsd.org/security.html
Santa Cruz Operation: http://www.sco.com/support/ftplists/index.html
Silicon Graphics, Inc.: http://www.sgi.com/support/Patch_intro.html
Sun Microsystems, Inc.: http://sunsolve.sun.com/pub-cgi/secBulletin.pl

Technical Web Sites

These contain information on a myriad of security and in some cases, non-security related information. Some require that you register your email address so that they can bombard you with sales information, but all are free.

SearchWin2000.com White Paper Library:
http://searchwin2000.com/whitepapers?Offer=wp2knetiq2

Mitre Corp., Common Vulnerabilities and Exposures:
http://cve.org

Internet Security Systems: X-Force™ Threat Analysis Service
http://xforce.iss.net

The Vulnerabilities Project Computer Security Lab, Computer Science Dept., UC - Davis
http://seclab.cs.ucdavis.edu/projects/vulnerabilities/#database

General Publications

While not specifically security related, these sites often contain security information and recent technological developments.

Washington Post Technology Pages, http://technews.com

Time Magazine -- http://www.time.com/time/business/

General Security Websites

These are excellent sites.

http://www.sans.org/giac.html
http://cerias.purdue.edu/coast
http://java.sun.com/security
http://www.telstra.com.au/info/security.html
http://www.ntbugtraq.com
http://www.nsi.org/compsec.html
http://www.boran.com/securityhttp://www.securityportal.com
http://www.tno.nl/instit/fel/intern/wkinfsec.html
http://l0pht.com
ftp://ftp.porcupine.org/pub/security/index.html
http://www.packetstorm.security.com

Professional Associations

Professional associations can be a good place for relevant information. However, it depends solely on the individual organization.

International Systems Security Consortium, Inc. (ISC^2) http://www.isc2.org
Current Certified Systems Security Professionals can also join the CISSP group forum.

Information Systems Security Association (ISSA) http://www.issa.org/

Government Sites

Government sites tend to play to their strengths, namely federal policy and procedures. These are just a few of them and this list will continue to grow as more agencies get into the "security business."

GSA, Office of Electronic Government and Technology http://www.itpolicy.gsa.gov
Naval Surface Warfare Center - Dahlgren http://www.nswc.navy.mil/ISSEC
National Institutes of Health, Computer Information Technology
http://www.cit.nih.gov/security.html
National Institute of Standards and Technology http://cs-www.ncsl.nist.gov
Computer Security Institute http://www.gocsi.com/

Books

Books are my last option of choice because, by the time the book has been written, edited, printed and distributed, the information is greatly delayed. Even with the new Print on Demand technology, where the information is moved electronically at points in the distribution process, it still takes weeks or months by the time the completed manuscript in your hand.

That said, there are some excellent security books available. One of the problems is that there are so many to choose from and, at $50 (U.S.) or more each, the cost of buying more than a few of them can be a hardship for the average person. Also, knowing what book to buy, making the wise investment in time and money, requires that you do a little home work first. For that reason, I've included a section that follows on Security Book Reviewers. Read what other folks have to say about a book before investing in it. Look it up on Amazon.com and see what chapters they may have for your review. Better yet, see if it's available from your public or work library. Just remember that the hot book you're buying now won't be worth the paper it's printed on in a short time as an updated version or another hot book hits the shelves.

Security Book Reviewers

When deciding who can make a recommendation that's right for YOU, ask yourself, "What does this person know about security that s/he can actually evaluate a book?" and "What can this person gain by recommending this book?" Anyone can write a review – good or bad – about a book, but is their opinion worth anything to you? The following is a list of security book reviewers:

LabMice.net: http://www.labmice.net/BookReviews/books_w2ksecurity.htm
Description: "The "LabMice" are a group of a dozen or so consultants, Administrators, Hackers, and other hardcore NT nuts I've had the pleasure of working with in the past several years. Most are MCSE's. All of them are simply the best and brightest people I've worked with at some of America's largest companies. (Including General Electric, BP/Amoco, Goodyear, IBM, HP, and Microsoft). Since its original inception in 1999, the LabMice community has grown to include technology professionals from around the world." From http://www.labmice.net/about.htm

About.com: http://netsecurity.about.com/cs/bookreviews/
Description: My name is Tony Bradley. I have been working with computers for over 20 years. I hope that I can provide some value for you and help you learn what you need to know about computer security. From: http://netsecurity.about.com/mbiopage.htm

Computer World Security Bookshelf:
http://www.computerworld.com/departments/management/bookreviews?from=bsm

Security Geeks: http://securitygeeks.shmoo.com/index.php?topic=BookReviews
SecurityGeeks is an effort to foster communication between security professionals on a regional basis.

Anton Chuvakin, Ph.D, GCIA: http://www.chuvakin.org/newbooks.html
An instructor for SANS, his complete resume is on his website.

USC Office of Information Assurance & Center for Information Assurance Studies: http://www.usc.edu/org/infosec/resources/books.html

Windows IT Library: http://www.windowsitlibrary.com/BookReviews/

International Association of Home Safety and Security Professionals, Inc. (Physical Security) http://www.iahssp.org/books.html

Online Book Stores

The following are links to technical book distributors. When available, their security book section has been linked.

Amazon.Com (now partnered with Borders Books): http://www.amazon.com

Barnes & Noble Technical Books: http://www.bn.com

BookPool: http://www.bookpool.com/.x/7hbw3anyb8/ho

eCampus:
http://www.ecampus.com/cat_searchresult.asp?cat1=Computers&cat2=Security&cat3=&cat4=

InformIt: http://www.informit.com/

O'Reilly Security Books: http://security.oreilly.com/

Organizing Information

Sorting Email

Email can be sorted by a number of parameters in Outlook including date received, sender, subject, priority, etc. You can also search emails by a string within the messages themselves. This is particularly useful when you have to find an email that you may have read sometime previously. To sort your emails, simply click on the label

of the field that you wish to sort by and Viola! Your inbox is sorted. You can also sort email within personal folders the same way.

Personal Folders

Although sorting your emails is very useful, if you get massive amounts of email you may wish to forward your incoming emails to specific folders. This way you can tell immediately if you've received new mail from a particular sender. Also, if you're high enough on the corporate food chain to have an executive assistant, you can allow that person access to some or all of your folders allowing you whatever privacy you may wish.

First, create a separate folder for each of the emails categories. It can be a subfolder under your Inbox or anywhere that you have permissions to create a new personal folder such as a local hard drive or remote server. Instructions for how to do this are available free on the web from Microsoft[8] or there are a number of publications available that can help you such as Outlook Step-By-Step, also from Microsoft[9] You may choose to have a separate folder for SANS alerts, or one for TechRepublic articles, etc., or group emails from several sources by topic -- virtually any combination that's good for you can be designed into your email personal folder structure. One person I know has emails from her boss sent to a separate folder. I have list mail sent directly to a folder for each list. Make certain that you have plenty of storage space as Outlook (.pst) files can quickly grow. With the volume of email that I receive, I have my email folders going to different .pst files so that no one file gets too unwieldy.

On very large email lists, which may receive hundreds of posts a day, I will often do a sort within that list folder. Let's face it, some people post stuff that doesn't interest me while others do, or there may be a thread that I want to follow. I want to spend my time and effort judiciously, and by using both the email forwarding and sort properties in Outlook, I can glean the useful information I want much faster.

Downloading to a Personal Digital Assistant (PDA)

You'd be amazed at how much time you have available when you look busy, but you're not. Perhaps it's riding the metro to and from work, or waiting for a meeting to start. You can make times like those really count by using a PDA, such as a Palm Pilot, to read and respond to your email alerts and newsletters. You may decide to respond to or forward a message that can just as easily be uploaded to your email and sent once you access your PC. Again, you want to make the most of your time. It's far more interesting to read a security bulletin than stare off into space or glance at your watch, waiting for that meeting to start. Simply follow the directions that came with your PDA to download your email or you can find freeware for downloading email at www.tucows.com/.[10]

Disseminating Information

Create your own personal distribution list

This can be very time consuming to set up and maintain, particularly if you need to create a large distribution list, as you are responsible for adding and deleting recipients as necessary. Instructions for creating a personal distribution list are available from many online resources.[11] A better alternative is to create an Exchange Public Folder.

Exchange Public Folders

Public Folders allow whomever you want to access a folder available through Outlook By applying Microsoft security privileges to each folder, you can easily control access to it. I use public folders to share interesting security related articles, documents, PowerPoint slide presentations, and even have list mail sent directly to them. For example, I have one folder that I use to share general security information with everyone in the enterprise and others to share confidential information with only those for whom it is OK. Public folders are a major topic of discussion, but suffice to say that you should carefully plan and design them for maximum use. Information on how to plan and build Public Folders using Exchange is free from Microsoft on their web site.[12]

You can also have list mail sent directly to public folders and I have found this to be very useful. Establish the public folder. Then, subscribe to the desired list using the Public Folder's SMTP address as the recipient's email address. There are several advantages of setting up list mail this way: 1) should you have several people needing/wanting access to this list mail, you simply have to make sure they have access to the public folder, 2) enabling/disabling user access to the public folder is much easier than having them added/deleted from a list you do not administer, 3) it can greatly reduce the amount of incoming email traffic, and 4) it allows you to archive the list mail in one single place.

A note of caution: some lists have restrictions on forwarding list messages to others. Make certain that you are not compromising security or ethics when using public folders for list mail.

Text Messaging Pagers

Text messaging pagers are a double edged sword. They have potential to be valuable tools for sending emails back and forth, but this capability can also be harassment if not limited to priority messages only. When using text messaging, remember that every word is transmitted, including the subject line and all headers. Make certain that folks who will be sending you messages know to keep the message length to a minimum and, if possible, when asking a question make is so that it can easily be answered with one of the standard replies for which there is a template: "Yes", "No", and "OK".

These devices are best used for high priority alerts rather than for regular lengthy messages like newsletters. Several antivirus programs, such as Computer Associate's InnoculateIT, and net monitoring programs allow you to have alerts sent to pagers. This may or may not be appropriate depending on your responsibilities within the organization. Only authorized personnel should have access to the text messaging distribution lists to prevent a social engineering attack.

BlackBerrys

Blackberry mobile devices offer wireless, encrypted access to email, schedules and other data using Microsoft Exchange or Lotus Dominoes. Not only do they offer "real time" accessibility to your email, they can be used to contact large numbers of recipients using a distribution list. Every member of the U.S. Congress has a BlackBerry and that was the means by which they were notified to evacuate the Capitol building during the Anthrax attack in October 2001. Care should be taken with all wireless devices to ensure that they remain secure.

Private Newsgroups

One way for you to enjoy the benefits of a newsgroup without compromising security is to host your own newsgroup. This will allow you to control who has access to the group what and from where they can post. It also has an additional advantage over a Public folder because unlike a public folder, which is static and must be refreshed to stay in "synch", a newsgroup -- or list serve as it's called – automatically emails the messages to each recipient much as a distribution list does. However, there's the cost of equipment and of course the administration of the group to contend with. One privately owned security list of which I was a member had a major "glitch" over a weekend with many, many copies of each and every post being sent to the members. The administrator was unavailable and the list went haywire for almost three days. When people returned to work the following Monday, there were a couple of thousand messages in their inbox – if it hadn't already crashed! Many list members either opted to unsub from the list or were forced to by their none-too-happy mail administrators and it was a major embarrassment for the sponsoring organization and the users. For more information on how to set up an Exchange Server as a List Server[13], go to http://www.exchangeadmin.com/Articles/Print.cfm?ArticleID=5184 .

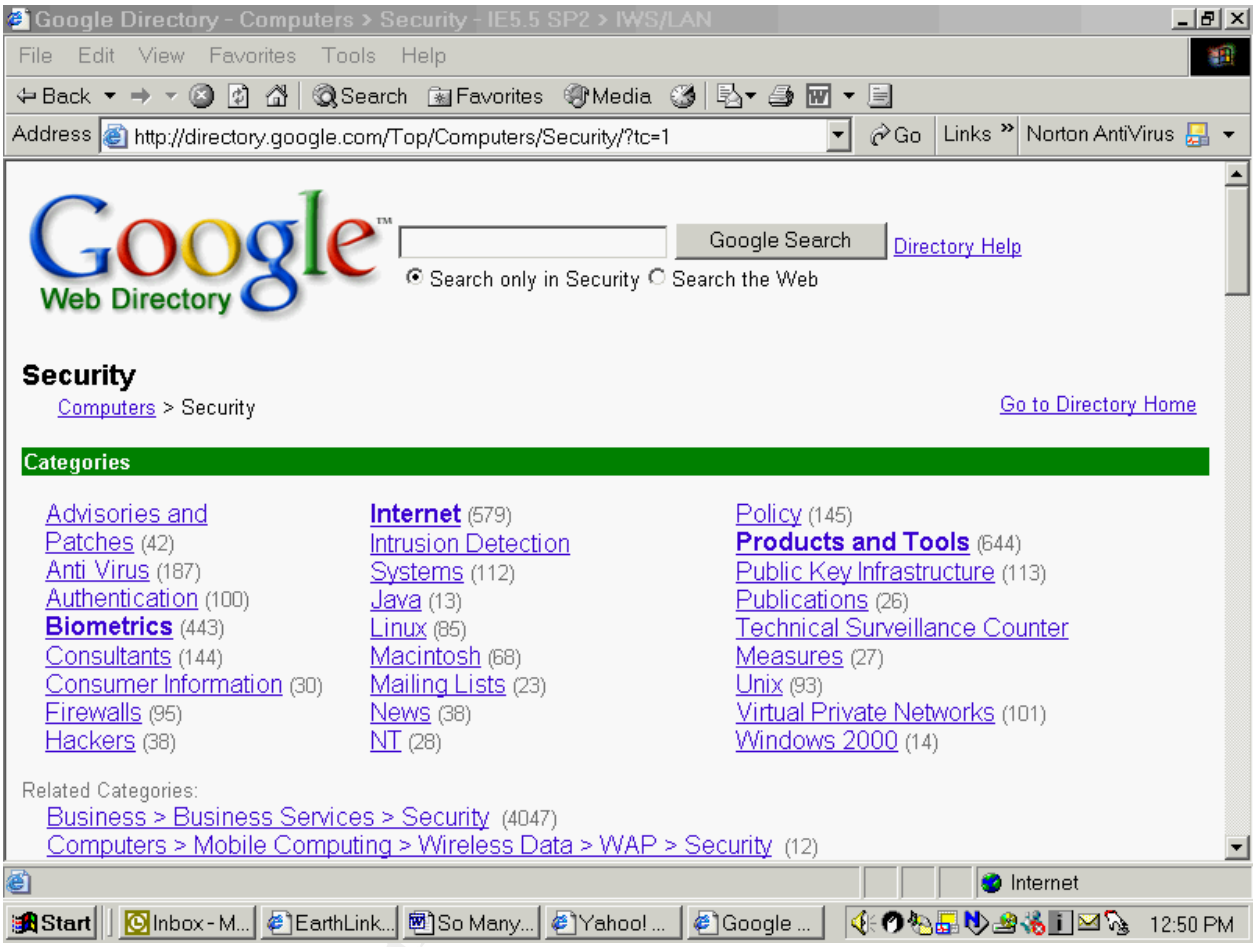
If security is not a major issue, i.e., the content will not be sensitive, an easier way of hosting your own group is to enlist the aid of providers like Yahoogroups or Smartgroups. These list services offer free list servers. You establish and moderate the group as you see fit. The "free" part of this is that your group members will be routinely bombarded with ads. However, having been both a list owner and member of several such groups, the downside is small compared to the benefits of these for nonsensitive information sharing.

Summary

As a security professional, it's imperative that you keep abreast of the information available. Due to the volume and complexity of all the security related material available, this could be an overwhelming task. By applying the RATTS (Rank, Accuracy, Time, Speed, and Sharing) methodology to this information, you can collect what's valuable to you, organize it in a meaningful way, and know how and to whom to disseminate that information. The useful tools that I have described in this paper will help you accomplish those tasks.

Figure 1

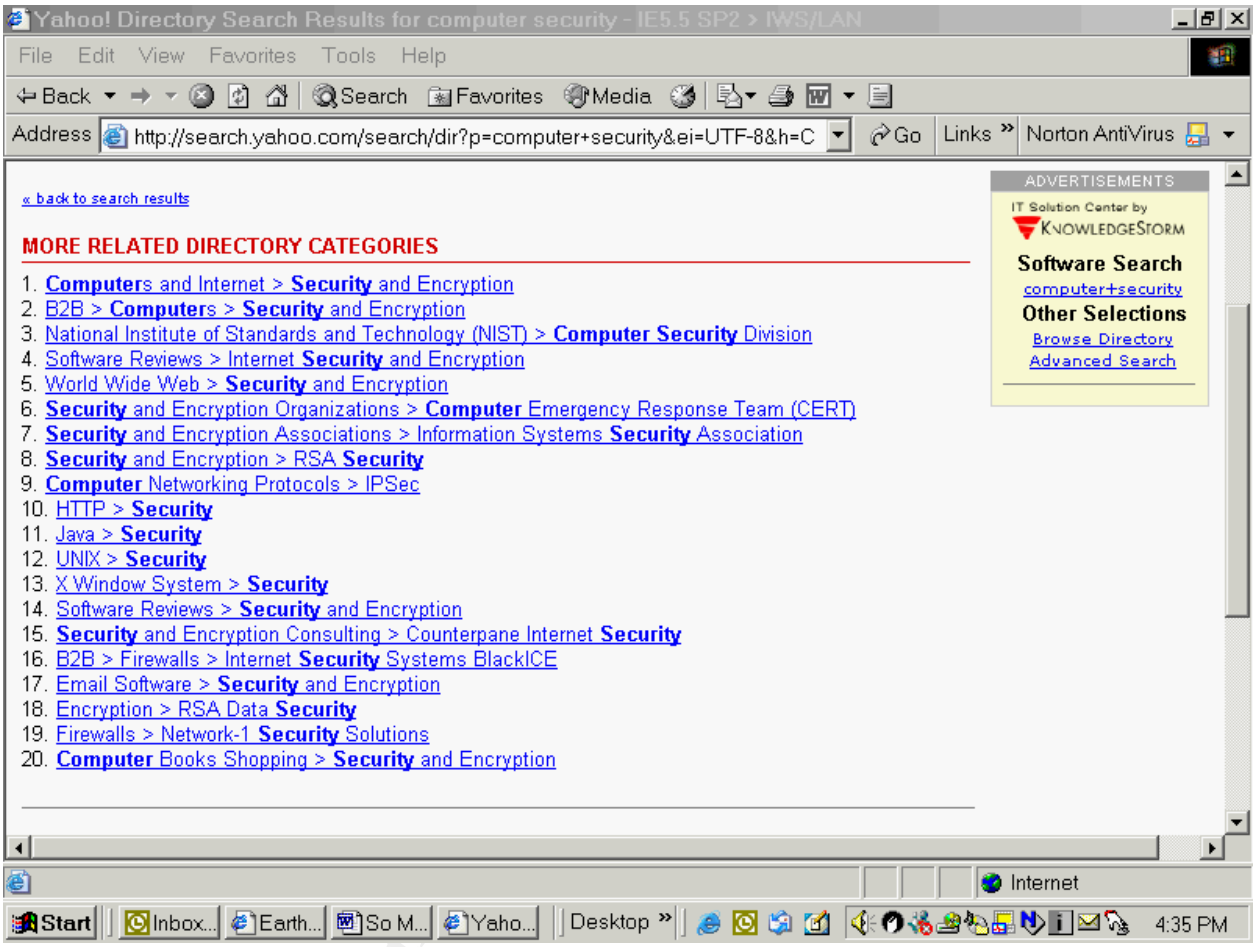
Google Computer Security Web Search



From: http://directory.google.com/Top/Computers/Security/?tc=1

Figure 2

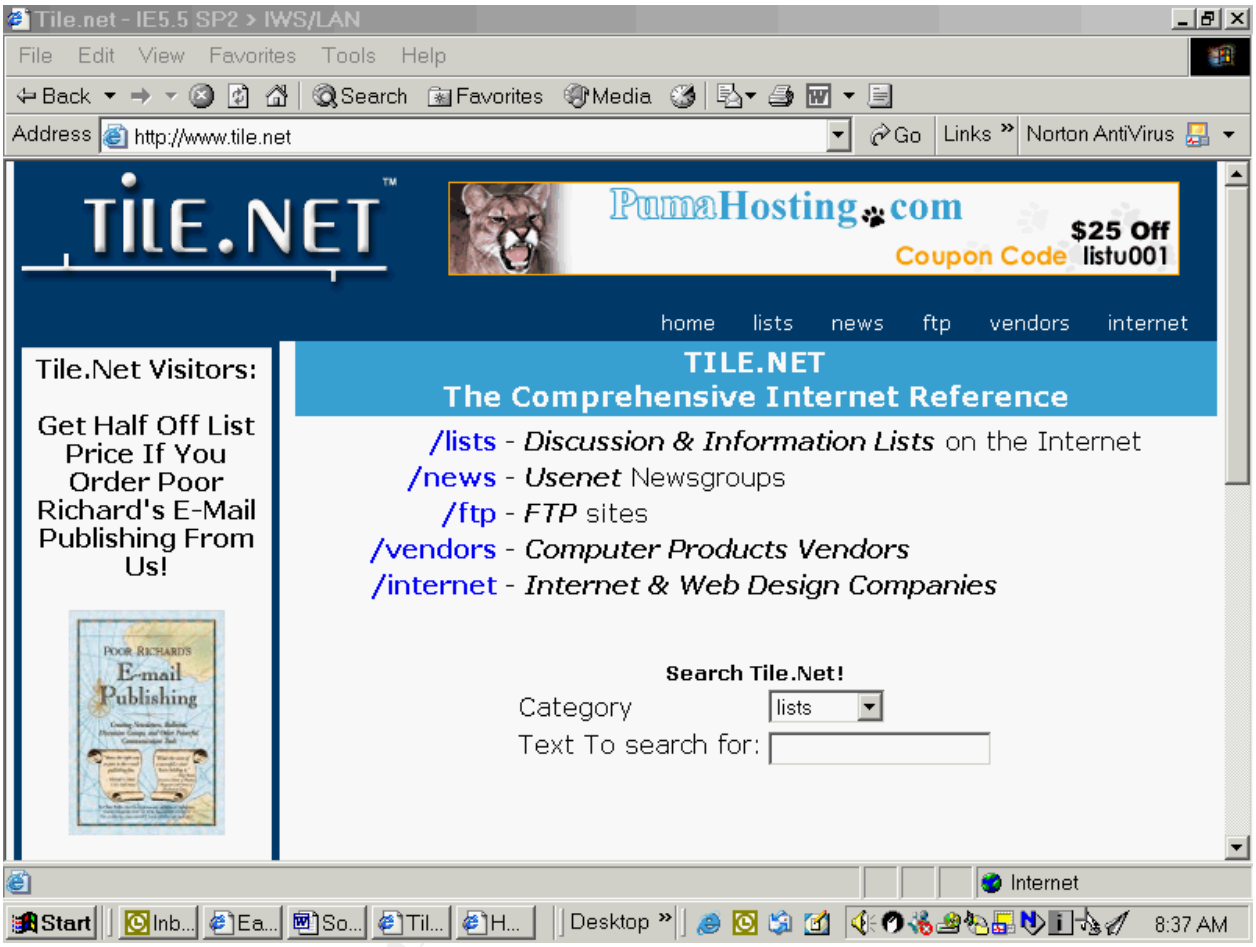
Yahoo Computer Security Web Search



URL: http://search.yahoo.com/search/dir?p=computer+security&ei=UTF-8&h=C

Figure 3

Tile.net Main Page



URL: http://www.tile.net

Figure 4

Yahoogroups Security Newsgroups

View Security Groups

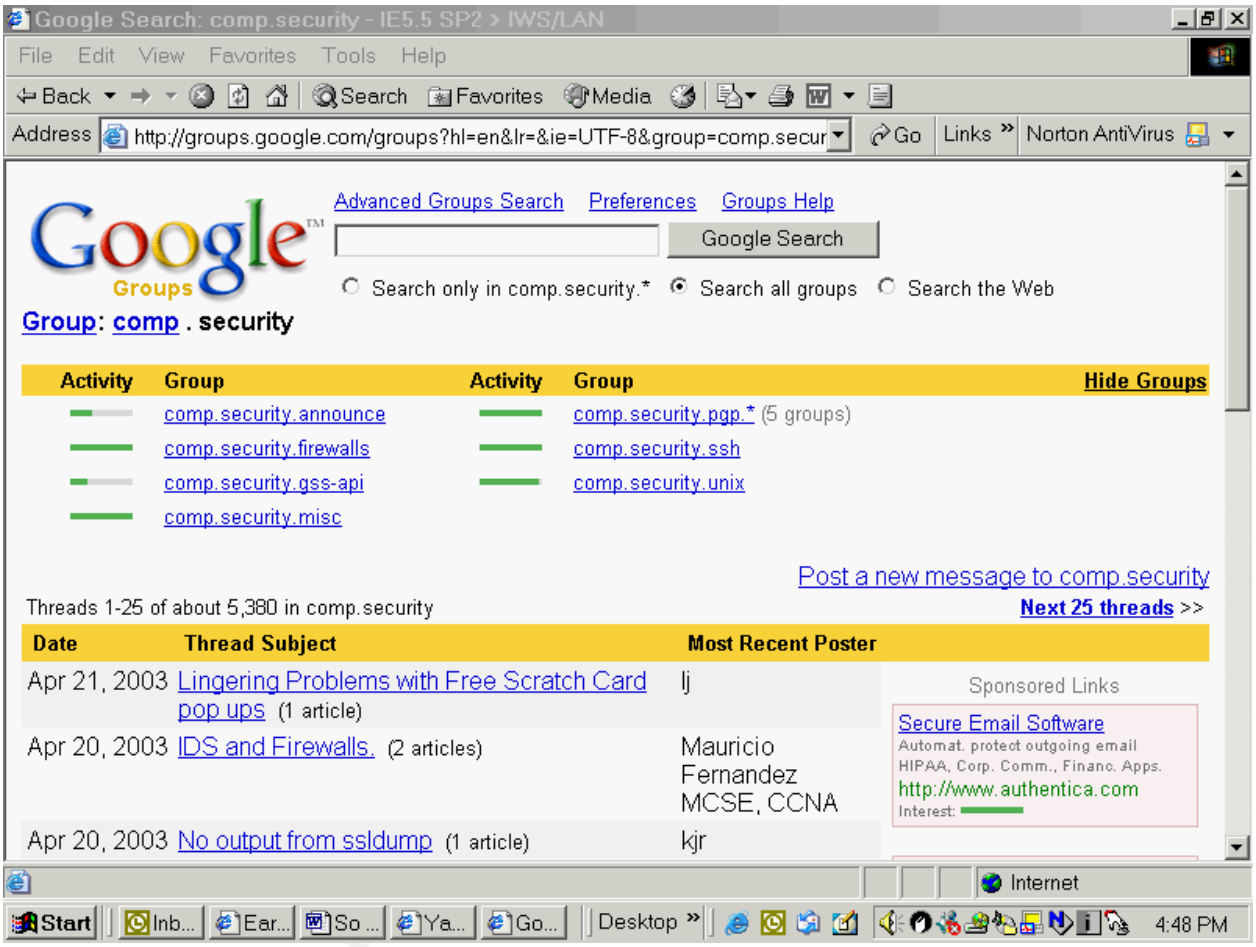
- **Security Groups** *(1146)* <>

Browse for more specialized Groups

- **Cryptography** *(98)*
- **Hardware** *(63)*
- **Networking** *(560)*
- **Viruses** *(163)*

Figure 5

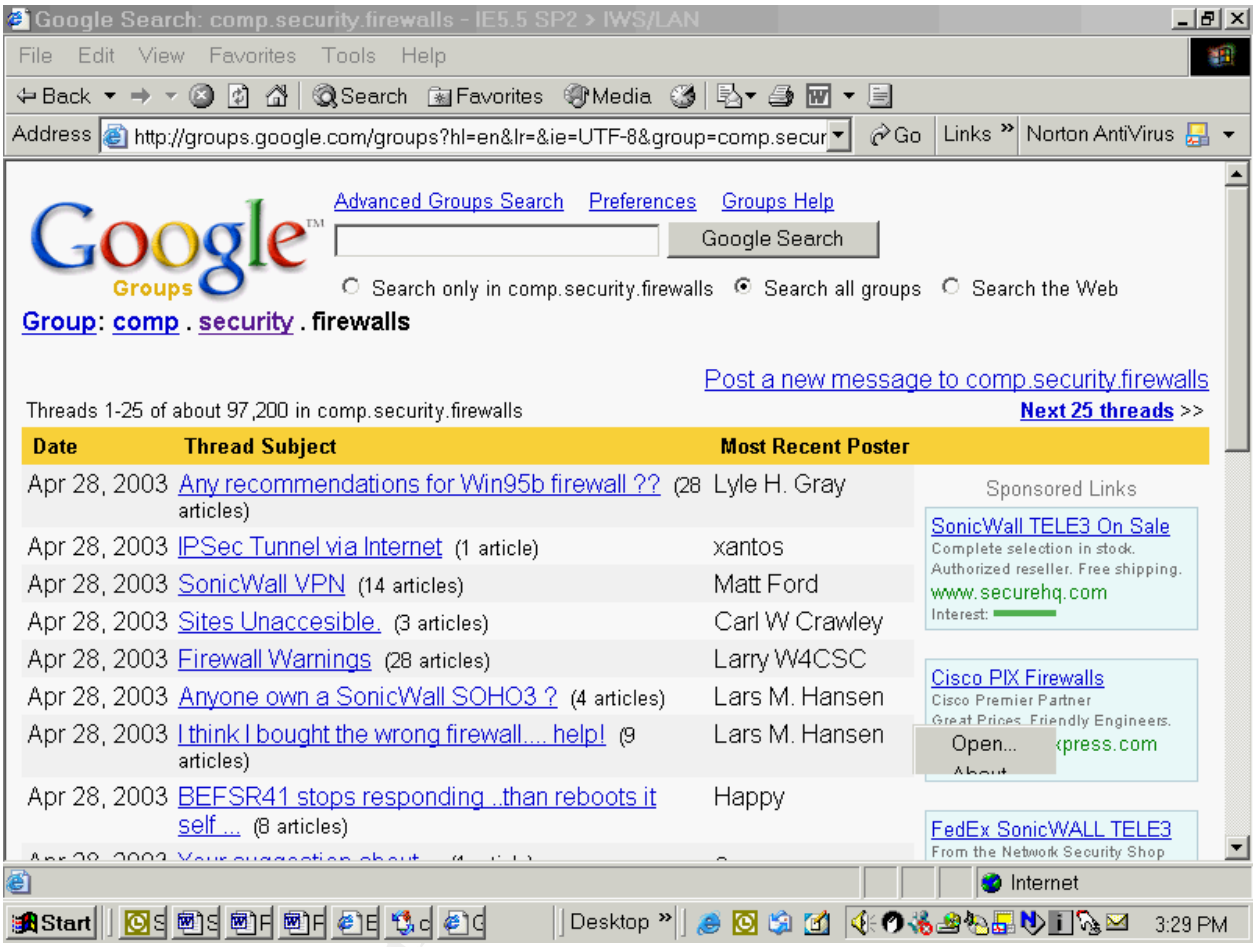
Google Computer Security Newsgroups



URL: http://groups.google.com/groups?hl=en&lr=&ie=UTF-8&group=comp.security

Figure 6

Google Computer Security Firewalls Newsgroups



URL: http://groups.google.com/groups?hl=en&lr=&ie=UTF-8&group=comp.security.firewalls

Bibliography

[1]Taylor, Robert. "Keep Current With Little Time." URL: http://www.sans.org/rr/securitybasics/current.php (19 September 2001)

[2]International Information Systems Security Consortium (ISC2) URL: http://www.isc2.org/cgi-bin/content.cgi?category=8 (22 April 2003)

[3]CERT/CC Statistics, 1988-2003. URL: http://www.cert.org/stats/cert_stats.html (4 February 2003)

[4]"Information on Bogus Microsoft Security Bulletin." Microsoft Technet. URL: http://www.microsoft.com/technet/security/news/bogus.asp?frame=true (14 April 2003)

[5]Google Search. URL: http://directory.google.com/Top/Computers/Security/?tc=1

[6]Padwick, Gordon. Using Microsoft Outlook 2002, Special Edition. Indianapolis, IN: Que, 2002. ISBN: 0-7897-2514-2

[7][Webnovice.com] Ebner, Joe. "Exploring Usenet groups." URL: http://www.webnovice.com/newsgrps.htm (20 April 2002)

[8]"HOW TO: Create Personal Folders in Exchange 2000 Server". Microsoft Knowledge Base Article #315060. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315060&sd=tech (26 October 2002)

[9]Crupi, Kristen et al. Microsoft Outlook Version 2002 Step by Step. Microsoft Press: Book and CD edition, July 2001. ISBN: 0735612986

[10]Tucows Software Library. URL: http://www.tucows.com

[11]For example: "How To Create a Personal Distribution List" University of South Florida, College of Business. URL: http://www.coba.usf.edu/services/computing/facsupport/outlook/distlist.htm (23 April 2003)

[12] "HOW TO: Create a New Public Folder Tree and Store in Exchange 2000 Server." Microsoft TechNet Article #255077. URL: Http://support.microsoft.com/default.aspx?scid=kb;en-us;Q255077&sd=tech (27 October 2002)

[13][exchangeadmin.com] Redmond, Tony. "Using Exchange Server as a List Server." URL: http://www.exchangeadmin.com/Articles/Print.cfm?ArticleID=5184 (22 April 2003)

Website Sources

Computer Security Expert Assist Team (CSEAT), "Computer Security Plans References for Agency Review". URL: http://csrc.nist.gov/cseat/cseat_computer_security_plans_ref_ar.html (31 March 03)

[Netsurfer Focus] "Security Focus: Computer and Network Security." URL: http://www.netsurf.com/nsf/v01/01/resource/newsgrp.html (26 April 1995)

"SANS Network Security Roadmap to Security Tools & Services – 2001." 4th Edition. URL: http://www.sans.org (Winter 2001)

"SANS Network Security Roadmap to Security Tools & Services – 2003." 8th Edition. URL: http://www.sans.org (Winter 2003)

"Security related resources / information from other organizations / sources." DFNCERT. URL: http://www.cert.dfn.de/eng/resource/ (13 September 2002)