San Francisco ISACA Chapter
Luncheon Presentation

Internet Resources for IS Auditors & Security Professionals

David Fong, **CPA, CISA**

December 15, 1998

Agenda/Objective

- Brief Overview Of The Internet
- Tips For Getting Connected
- Practical Approaches To Utilizing Internet Technologies
- Impact of Intranets On The Audit
- Where Do I Start?
  - Finding The Information You Need
  - Overview of Useful Sites & Resources

Brief Overview of the Internet

The “Net”

“The Internet, often called simply "the Net," is a worldwide system of computer networks and, in a larger sense, the people using it.” -- whatis?com™

History of the Internet

The Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 implemented ARPAnet, the predecessor to the current Internet.

The intent was to construct a fault-tolerant network that would continue to function even if a large portion of it were destroyed.

Today’s Internet

“The Internet is now a public, cooperative, and self-sustaining facility accessible to tens of millions of people worldwide. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol).”--

whatis?com™

Internet Timeline

1962 - Paul Baran, an engineer at the Rand Corporation, finds a way for messages to move through a network of Defense Department computers even if one communication line is destroyed.

1968 - The Department of Defense commissions the Advanced Research Projects Agency to build ARPAnet

1986 - ARPAnet becomes part of the NFSNET, sponsored by the National Science Foundation.

1989 - The European computer science laboratory called CERN proposes the World Wide Web(WWW). WWW officially released by CERN in 1991.

1993 - Mosaic is released by the University of Illinois. First widely distributed graphical browser for the Internet.

1997 - Estimated 16.1 million computers are connected to the Internet.

The “Other” -nets

- Intranets
  - STRUCTURE
    - internal Company network comprised of interlinked LANs and also use leased-lines in WANs
  - PURPOSE
    - used to share internal information to its employees
  - EXAMPLE
    - HR Manual, Phone Directories, SP&P Manuals, Travel Planner

The “Other” -nets

- Extranet
  - STRUCTURE
    - private network using Internet protocol and public telecommunication system
  - PURPOSE
    - used to securely share information with suppliers, vendors, business partners…
  - EXAMPLE
    - EDI with business partners, such as suppliers, using a tool like Netscape ECExpert

The “Other” -nets

- Virtual Private Network (VPN)
  - STRUCTURE
    - a private data network that makes used of the public telecommunication infrastructure
    - security and privacy maintained through the use of tunneling protocols and security procedures

Tips for Getting Connected

Internet Service Providers

- Internet Service Providers (ISPs) provide:
  - individuals and businesses connectivity to the "Net"
  - facilities for email and web site hosting
  - EXAMPLES:
    - AT&T Worldnet, IBM Global Network, MCI, AOL, Compuserv, and etc.

Connectivity Provider

- Connectivity Providers
  - Telecommunication companies
  - Cable providers
- Sample Speeds

Phone lines	33.6Kbps/56Kbps
ISDN	128Kbps
ADSL	1.544Mbps - 8Mbps
Cable	1-2Mbps
T1s	1.544Mbps
T3s	44.736Mbps

Browsers

- Browsers provide users a means to read, see and hear graphical content on web sites using the “Hyper-Text Transfer Protocol (HTTP)” language
  - EXAMPLES:
    - Netscape Navigator
    - Microsoft Internet Explorer

Popular Plug-ins

- Software programs that extend the capability of the browser to delivery internet web page content. Examples:
    - Real Video/Audio
        - Provides live and on-demand real-time streaming content
    - AdobeAcrobat
        - Provides ability to view formatted documents

Practical Approaches to Utilizing Internet Technologies

Internet Services

- Email
- Newsgroups
- Research
- Company/Product Information
- Downloads

Email

- PROs
  - useful for sending files/attachments
  - relatively easy-to-use
  - software independent (SMTP)
  - access to content requires user id and passwords

- CONs
  - cannot ensure received by recipient
  - spread viruses
  - content may be subject to unauthorized disclosure or modification
  - difficult to authenticate sender

Newsgroups

- PROs
  - information is organized in a hierarchical structure
  - access to individuals with interest in the subject matter
  - search tools are available (i.e., DejaNews)

- CONs
  - communication may be read by inappropriate individuals
  - postings may deemed to be “official”
  - not always “friendly”; “flaming”

Research

- PROs
  - vast amount of information available
  - most of the information is free
  - numerous sources of information can be searched without leaving your office
- CONs
  - information may not be easily accessible
  - search results tends to be voluminous
  - information may be outdated
  - no one really responsible for its content and reliability

Product/Company Information

- PROs
  - free!
  - retrieve information quickly
  - on-line product manuals/sales literature
  - good overview

- CONs
  - information provided may lead to further questions
  - sometimes a lot of “glitz” with little content

Downloads

- PROs
  - current up-to-date product drivers
  - access to freeware, shareware, software
  - anti-virus data file updates
  - audit programs
  - forms

- CONs
  - downloads may contain viruses
  - time-consuming
  - “licensing” issues

Impact of Intranets On The Audit

Intranet as a “Resource”

- Current Events and New Products/Services
- Company Policy & Procedure Manuals
- Electronic Forms
- Telephone Directories
- Organization Charts
- FAQs

Intranet as a “Repository”

- Used to capture audit information
- Audit applications
- Used to share information with other users on the intranet
- No need to distribute specialized applications to end-users

Intranet as an “Open Door”

- Sensitive and confidential information may not be adequately protected
- Critical web-based applications may not have the same robustness or redundancy of mainframe programs
- Weak security over intranet applications could lead to compromise of applications and data

Where Do I Start?

Finding Information Quickly

- Using Search Engines/ Directories

  searches are performed on keyword(s) from a single database of web-pages owned by the search tool.

  - http://www.yahoo.com
  - http://www.infoseek.com
  - http://www.excite.com
  - http://www.lycos.com
  - http://www.webcrawler.com
  - http://www.altavista.digital.com
  - http://www.hotbot.com
  - http://www.dejanews.com

Finding Information Quickly

- Meta-Search Engines

  Meta-Search Engines transmit search request simultaneously to numerous search engines.   Results containing matching sites from all of the search engines queried are then displayed.

  - http://www.dogpile.com
  - http://www.infind.com/
  - http://www.metacrawler.com/
  - http://www.mamma.com/
  - http://www.metafind.com/

Overview of Useful Sites & Resources

- Security Information
- Audit Tools
- Communication Forums
- Technical Resources

Security Information

- Vendor-maintained
  - http://www.microsoft.com/security
  - http://sunsolve.sun.com/
  - http://java.sun.com/security/
  - http://www.ers.ibm.com/tech-info/index.html

Security Information

(continued...)

- General
  - http://www.ntbugtraq.com/
  - http://www.iss.net/vd/library.html
  - http://www.cs.purdue.edu/coast/
  - http://www.nsi.org/compsec.html
  - http://www.cert.org/
  - http://www.telstra.com.au/info/security.html
  - http://www.first.org

Audit Tools

- Audit Programs
  - http://www.auditnet.org/
  - http://www.aetna.com/audit/ST-WPLNS.HTM
- Resources
  - http://www.isaca.org/
  - http://www.itaudit.org
  - http://www.aicpa.org
  - http://www.sfisaca.org/
  - http://www.whatis.com

Communication Forums

- Two major components:
  - Mailing lists
  - Newsgroups
- Good starting point to answers to questions
- But…should not be blindly relied upon. Information should be considered and carefully evaluated against your own situation.
  - Some contributors are truly knowledgeable, while others are not. Contributors may:
    - be experts
    - have good intentions
    - be malicious

Mailing Lists

- Allows people with “common” interest to receive and share information via email.
    - bugtraq-request@fc.net
    - advisory-request@cert.org
- Finding a mailing list
  - Use “Publicly Accessible Mailing” Lists
    - http://www.NeoSoft.com/internet/paml

Mailing Lists (continued...)

- How to subscribe:
  - listserv & listproc
    - SUBSCRIBE [listname] your_first_name your_last_name
  - majordomo
    - SUBSCRIBE [listname] your_email_address
- How to unsubscribe:
    - listserv & listproc
      - unsubscribe [listname]
    - majordomo
      - unsubscribe [listname] [email_address]

Newsgroups

- An electronic discussion bulletin board used to discuss a specific subject.
  - comp.* (computer-related)
    - comp.security.unix / comp.security.firewalls
    - comp.virus
    - comp.admin.policy
  - sci.* (science-related)
    - sci.crypt
    - sci.crypt.research

Software Resources

NOTE: Prior to installing/executing any software, the code should be carefully reviewed and tested prior to use on any production or mission critical machines. This reduces the risk of any malicious code that may have been embedded into the software.

- Computer Oracle and Password System (COPS)
  - ftp://coast.cs.purdue.edu/pub/tools/unix/cops
- Internet Security Scanner(ISS)
  - ftp://coast.cs.purdue.edu/pub/tools/unix/iss
- SATAN
  - ftp://coast.cs.purdue.edu/pub/tools/unix/satan.tar.z
- Tripwire
  - ftp://coast.cs.purdue.edu/pub/COAST/Tripwire

Questions