

NEWSLETTER INFORMATION

Published nine times per year (September – June) by the Minnesota Information Professional Society. We welcome materials for publication (articles or news). Submit materials on disk or via E-mail to:

Earl C Joseph
365 Summit Avenue
St. Paul, MN 55102
Tel. (651) 290-2846
E-mail: ejoseph@waldenu.edu

NOTE

MEETING INFORMATION

MEETING PLACE:
Holiday Inn – Bloomington
35W at 94th

Phone (612) 884-8211 Meeting Times:

5:00 PM Social Hour
6:00 PM Dinner
6:45 PM Meeting & Program
8:00 PM Adjourn

For Reservation Call:

John Belich
by April 12th and choose:
Pan-Fried Walleye or
NY Strip Steak
Tel: (651) 634-1440
or e-mail:
john.belich@tech-pro.com
\$20 Members
\$25 for non-members

APRIL Dinner Meeting NOTICE

Tuesday April 16, 2002

Meeting of

Minnesota Information Professional
Society

Speakers Topic:

"Transforming the
Mature IT Organization:
Reenergizing and
Motivating People"

Speaker:

Dr. Bob Zawacki

Don't miss the April PreDinner Session on
"Networking for IT Professionals"
3:30 to 5:00 pm

MAY MEETING

Joint meeting at St. Louis Park's Doubletree
Hotel
with AITP on Thursday, May 2,
featuring a panel discussion on **Wireless IT
Opportunities**

President's Letter

Happy Spring to you and your family!
Please join us at our Tuesday, April 16th, dinner meeting at the Bloomington Holiday Inn.

I would like to welcome the newest MnIPS members that have joined our group recently, especially during the past month. We had a large group of 50+ people that attended our pre-dinner Networking seminar on March 19, with most of them staying for our regularly scheduled dinner & presentation that followed. Thanks to Jeanine Boss, Joe Perzel and Bill McTeer for hosting this event. MnIPS is a volunteer organization and we always welcome any help in our regular, ongoing committees or at a specific event, such as registering people at monthly dinner meetings (during 5-6pm) or staffing our booth at the Strictly eBusiness show on May 8-9. If you wish to link your personal web-site with our own www.mnips.org, contact Sylvia Wiebe at "swieb53@hotmail.com" or Bill McTeer at wmcteer@mcteersys.com.

Special thanks to MnIPS Secretary Bob Burkhardt for hosting the CyberCrime Fighting Forum on March 12 at Metro State University and its associated recognition dinner for our newsletter editor and IT pioneer Earl Joseph. The ECJ Scholarship drive began that night for IT student benefactors and is aptly named "Dollars for Scholars". If you wish to contribute finances or time to this worthy scholarship fund, contact Bob by e-mail at bob@acctts.com or telephone at (952) 888-1108

I look forward to hearing our April 16th speaker, Dr. Bob Zawacki, who will speak on "Transforming the Mature IT Organization: Reenergizing and Motivating People". Thanks to our March 19th presenter, Anita Cassidy, whose topic was "Planning for e-Business Success". Thanks also to our February 19th

speaker, Bruce Heulton, who talked about "Protecting Your Organization's e-Commerce Web Site". For a summary of Bruce's talk, please read the regular meeting review column in this newsletter.

If you are planning ahead, we will have a joint meeting at St. Louis Park's Doubletree Hotel with AITP on Thursday, May 2, featuring a panel discussion on Wireless IT opportunities. Our annual MnIPS Golf Outing at Anoka's Greenhaven Course will be on Monday, June 17th. I hope to see all of you at the April 16th meeting! --Dennis Cummings, President

19th ANNUAL STRICTLY eBusiness (May 8-9, 2002): RESOURCES FOR RESULTS

Business is moving faster. Competition is growing. Technology is Changing. With the largest regional technology event in the nation being in our own backyard, IT professionals and business owners can find the solutions crucial to the success and survival of every business at the 1,000 plus booth exposition. This year, expo management is pleased to announce partnerships with SANS, Novell's BrainShare on Tour and the TIA to offer conferences focused on security, networking, ebusiness and convergence...content relevant to every IT professional. Local groups involved with the exposition include MHTA, webgrrls, SOCAP, MnIPS, PMI, MTA, MCAI and many more. For additional information and FREE expo registration, please visit their WEB site www.strictlyebusiness.net or call 952.894.8007.

Oh, The Tangled Web(sites) That We Weave!

(February 2002 MnIPS meeting review, written by Dennis Cummings)

Mr. Bruce Heulton was the featured presenter at the Minnesota Information Professional Society's monthly dinner meeting held on February 19, 2002. He is an original MnIPS member and former Twin Cities Association of Computing Machinery (TCACM)

chapter chairman who now works with both technical and management issues at Extratelligence. Mr. Heaton has been researching and presenting on threats to e-Business sites and network infrastructure since 1995. He has presented on several topics at IEEE COMPSAC and Aerospace international conferences. He works with financial services, telecommunications and non-profit & governmental organizations to solve management, business and technological problems.

MnIPS' February newsletter gave an interesting preview of this "Protecting Your e-Commerce Website" session. The motto was "If you build it, they will come". Most commercial websites experience several potentially malicious probes every day. Everyone in e-Business (that's most of us in IT, in one way or another) needs to understand how to survive in the Internet jungle. This presentation described at least 15 different ways your site can be attacked and the general steps to protect it. It also covered how to keep your site doing business & avoid the costs of rebuilding it as well as what resources are reasonable and appropriate to guard your site.

Mr. Heaton started his presentation by focusing in on "Current Web Infections and Protections" based on a practitioner's perspective. He made a list of assumptions (to be worried about) and an "infectious agent" model. He covered the present threats, some incidents and possible action plans to handle potential problems. Mr. Heaton's assumptions for website owners' concern are that:

1. We live in a highly hostile "web world" with both individuals and groups actively seeking to impact the quality of any host site's computing environment.
2. Not everyone will have security as a primary concern or have strong support available.
3. Continuing evolution of the Internet

Mr. Heaton followed up by displaying his "Infection Model". A website is supposedly first exposed to an infectious agent and the host's environment is either immediately affected or is already set to eliminate/fight the intrusion. If the host environment is affected, then the host's staff must determine the "extent of damage" and develop tools to either cure the situation or treat the symptoms. Mr. Heaton focused shortly on how the host's personnel can handle a "connections" problem as an example.

1. Exposures can be treated after acquisition, prior to effects occurring (such as shutting down macros).

2. Dispersal of infection can occur prior to effects (e.g., mailing virus to group-lists).
3. Exposure to infectious agents results in active infection (e.g., unwanted file deletions).
4. An effect of infection can be dispersal of infectious agents (e.g., date-triggered problems later on).
5. Infections can result in damage or resource use.
6. Cure can address cleaning out an infection or treating symptoms.
7. Reinfection can result after treating only symptoms or after cure.
8. Reinfection or infection can occur as part of active infection.

Where are these "infectious agents" coming from? Mr. Heaton says that we can possibly have threats to and from the Internet (e.g., DNS attacks). We can also have attacks against local Networks (e.g., DoS). Further attacks may occur against local computing services (e.g., e-mail, web server, applications and even stealing service). Finally, attacks can surface against individual workstations (e.g., desktop/laptop, PDA, tele-computing). On the most famous examples of MS-Outlook attack are the "I Love You" or "Melissa" viruses, the latter named after Bill Gate's wife. This still occurs due to unpatched versions of Microsoft Outlook and may have different levels of individual site damage and dispersal. Various updates (from anti-virus sites) are not common enough to eradicate any infection on all systems.

Another infectious agent example is the "Code Red/Code Red II" worm, which occurred on July 19, 2001, and infected more than 250,000 systems in just 9 hours. It exploited the IIS index server flaw from its default installation and an estimated 1million systems suffered Code Red II worm problems. The NIMDA Dispersal (CIAC) virus, which is ADMIN spelled backwards, is another famous infection agent and had the following features:

1. Sent from client to client via email or open network shares.
2. Sent from web server to client via browsing of compromised web sites.
3. Sent from client to web server via active scanning for and exploitation of the "Microsoft IIS 4.0 / 5.0 directory traversal" vulnerability (VU #111677).
4. Sent from client to web server via scanning for the backdoors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms. The Internet is the preferred choice for some at-

tackers. Firstly, it is the ideal mechanism to disperse infectious agents such as Code Red. Secondly, it provides geographic independence of the attacker and those that are threatened (e.g., a PTT incident). Finally, it can expose infectious agents to a large group of unprotected areas like the NIMDA virus that became widespread within 12 hours of launch).

Mr. Heaton covered various filtering devices to eliminate or deter unauthorized attacks. They are the Screening Router, Proxy Server with dual-homed host, Dual-Homed Host, Screened Host and Screened Subnet. These "double-hosted firewall" designs can:

1. Protect against outside world in conjunction with router configurations.
2. Handle multiple network routings.
3. Provide highly configured barrier against intrusion.
4. Protect inside world with proxy services and filtering.
5. Provide services to inside world such as IP address translation.
6. Provide filtering opportunity for internal traffic.
7. Requires interlocking router and server configuration.
8. Frequent updating required.

What are the threats involved? There are local threats against both the network (e.g., LAN or PVN) and services (e.g., e-mail, webs, servers, telephones and applications). There can also be a "denial of service" (DoS), breach of security, or service stealing. In most cases, detection & identification are difficult and all threat management costs money. There are also individual threats as personal computing is becoming more pervasive (roaming on multiple machines, PDAs, wireless, and node computing) and can easily affect countless machines that may be connected to it. If you currently feel real secure, why should you even care about threats? Well, stolen identities nearing critical levels and anonymity is threatened causing eventual invasion into your business and/or personal life.

Mr. Heaton then described the features of the better-known infectious agents. The "I Love You" viruses rapidly infected systems worldwide across multiple OS (Microsoft-based scripting). The "Code Red/Code Red II" worms were limited to NT IIS web server attacks. They had an extremely high distribution of vulnerability meaning extremely high rates of dispersal and infection, especially on higher network bandwidth for any IP. The NIMDA virus had the worst characteristics of

Code Red and other prior infections. It had multiple vectors of dispersal and was an Intel-CPU based infection. Also of further concern is SNMP vulnerability which had a cross-vendor warning from the SANS Institute (CA-2002-03). Preliminary testing showed every piece of equipment is vulnerable, including servers, routers and switches.

Mr. Heaton then presented the "Top Ten" Emerging Threats to the industry from 1998 (with apologies to Dave Letterman) for our review and amusement. They were:

1. Cable modems (and other high-speed links) that enable Windows-specific vulnerabilities for large populations.
 2. AOL password-stealing via infected E-mails.
 3. MS Outlook/Exchange Script-based Vulnerabilities (server and client-based).
 4. Server agent based breaches (e.g., Lotus Notes, Exchange and SendMail).
 5. Wireless-exposed vulnerabilities (e.g., wireless data, CDPD and GSM data).
 6. Personal Appliance Replication on networks (e.g., Palm and Windows CE).
 7. Converging technologies (e.g., digital wiretapping, game consoles and set tops).
 8. Version-'itis' of software (e.g., Windows 2000 and NetScape).
 9. 'Free Software' from Linux, StarOffice and others.
 10. Instant-messaging breaches. What are today's "Top Ten" Emerging Threats to the industry?
- Mr. Heaton says that they are:
1. Continued threat to the installed base of systems means that 'dormant' viruses will be huge threats (e.g., CodeRed, Nimda and others).
 2. Emergent cell-networks will produce newer and even more widespread problems.
 3. Application-based attacks will emerge.
 4. Denial-of-Service (DoS) attacks will become the most common.
 5. Anonymous attacks by proxy machines will become normal.
 6. Info-war incidents will be the catalyst for major attacks.
 7. Infrastructure attacks will become known (e.g., electricity, gas, water and transportation). Governments will become major participants in countermeasures. Cost of Ownership levels will inhibit innovation.
 8. Attacks with social engineering will increase when combined with attacks on pri-

vacy and identity. Social engineering is when folks bypass system procedures to access critical data, such as employee impersonating on the telephone to get a company signon-ID from the operator. Asking questions of the social-engineer (e.g., SSN of the employee impersonated) will normally stop his/her attempt in an instant.

What then can a business do to help fight these attacks? Mr. Heaton suggests that they use:

A rapidly updated rule-based firewall automation service (e.g., ISS BlackICE or TrendMicro). An outsourced security-servicing process (like subscription and managed services). A network-active monitoring utility (such as Symantec). An agent-based behavior pattern recognition (example: Ad-Aware). A hardware-based authentication (possibly using SecureID). An 'over the shoulder' active agent (e.g., ZoneAlarm or TCP Wrappers). Role frameworks in task security management (e.g., PICS). Risk driven activity profiling (like "safewall" at work based on job task needs). Software-integrated personal authentication for applications (such as Passport).

Software-designed for better security (example: Secure Linux). What then can an individual do to thwart attacks? Mr. Heaton suggests the following:

If you have high-speed access, then use a double-bastion firewall and proxy. Access modems should use NAT. If you have a web site check it regularly to see it hasn't been hacked. Keep browsers current by using utilities like IEUpdate or SmartUpdate. Do multi-generation backup and archiving regularly. Use RAID for servers. Guard privacy. Never give out passwords or financial profiling. Minimize network protocols. (Turn off NetBEUI, IPX/SPX) Use WEP. Use active anti-virus software updated regularly. Use encryption locally and on protocol transport. Review audit trails and logs frequently. Observe Net-iquette. Avoid sites that violate it. Avoid the use of wireless networks.

Mr. Heaton finished his presentation by asking the old Alfred E. Newman (of MAD Magazine fame) question "What Me Worry?". I personally think of it as the old Al Franken (of Saturday Night Live fame) question "How does this affect me?". In either case, the advice was provided. Firstly, you do not have to pay attention because the problem will come to find you. Secondly, you don't have to change your state-of-practice since the start-

of-the-art will change faster than you do. Finally, you don't have to change your process because the rest of the world will change without you. Enough said. If you wish to learn more about Mr. Heaton or his work at Extratelligence, contact him by email at "bruce.heaton@extratelligence.com".

MnIPS hosts "Networking for IT Professionals"

A Two-part series

Already restructured, downsized, right-sized IT Professionals, as well as those concerned about their future, can learn how to improve their networking skills by attending the **Networking for IT Professionals seminar**. Hosted by the Minnesota Information Professional Society (MnIPS), this event will showcase IT staffing professionals and networking experts that will share their tips and techniques on how to network to find a job or to stay current with events and technology. **Featured topics include:** Welcome and Introduction

- Mn Workforce Center - Where to go for outside services & help
- Kurt Linberg, Capella U - Educational Opportunities and Hot IT Skills
- Christine Wisch, Kestrel Consulting – How to prepare for the interview
- Jennifer Tome, MorganStanley – Dealing with Financial issues from a lay-off
- Joe Perzel – Other Networking Opportunities in the Twin Cities
- Group Panel Q & A

When: Tuesday, April 16th Networking Seminar, 3:30 to 5:00 pm

Contacts: Jeanine Boss 952-432-2959, email jeanineboss@aol.com
Joe Perzel 952-340-1110, email jperzel@enrgi.com

Cost: **No cost for the Networking seminar** and Networking part of meeting.

Reservations for the seminar are highly preferred, but not required. To make your Seminar and Dinner meeting reservations, email your name and contact information to info@mnips.org.

If you've ever lost your job, you know about the stress that comes with it. This meeting is intended to ease some of that stress during their transition while helping people make valuable career contacts.

MnIPS Officers 2002

President

Dennis Cummings (W) 651-205-2632

Vice President

Gerry Lindner (W) 651-292-9304

Past President & Treasurer

Joe Perzel (W) 612-340-1110

Programs

Kurt Linberg (W) 612-252-4335

Marketing

Joe Reilly (W) 612-513-5951

Secretary

Bob Burkhart (W) 952-888-1108

Arrangements

John Belich (W) 651-634-1440

Newsletter Editor

Earl C. Joseph (W) 651-290-2846

Education

Haziel Matias (W) 612-627-2171

Summer Golf Outing

Jeff Hemauer (W) 651-766-1387

Audit & Bylaws

Dave Farmer (W) 651-637-2568

Special Projects

Bill McTeer (W) 612-333-4115

Data Base

Tom Walters (W) 952-995-4066

MnIPS Newsletter

P.O. Box 201243

Bloomington, MN 55420-1243

Address Service Requested

DINNER MEETING

Tuesday, April 16, 2002 – 5-8PM

TOPIC

**“Transforming the Mature IT
Organization”**

NOTE: Meeting Location

Holiday Inn Bloomington
35W & 94th (1201 W. 94th St.)

