

❖ Consultants in Minnesota ❖

September 2001

President's Message

By Randy Hayman

Greetings All!

Even though we had no monthly meeting last month, there was plenty of activity within our chapter. The Board of Directors carried on lengthy electronic discussions about our chapter and had time to meet during the month of August. We came up with a number of initiatives which we would like assistance implementing. More on these initiatives further down in the column.

In the event you do not know who your Board of Directors is, take a look to the left of this column. According to our By-Laws, the President, Vice-President, Treasurer, Secretary, and the previous Chapter President make up the Board of Directors. You can find the contact information for all but the previous Chapter President in each Newsletter. Our previous Chapter President is Larry Bremer.

The reason our Chapter has been in existence for 20 years is due to the great contributions of many of its members. For instance, Joan Barnes sponsored the August special presentation on Geographic Information Systems (GIS). Suzanne Fliege of PlanSight gave a remarkable presentation on GIS, its current use, local applications, and the astounding value of adding spatial elements to data and being able to present that as graphics.

Thank you Joan and Suzanne!

Other examples of great contributions are our newsletter editor, Magne Hatlevik. I'd be willing to bet Magne hasn't heard a resounding Thank You! for his efforts. Well, Magne, Thank You! keep up the great work. There are many many more examples of unselfish contributions to our organization, however, each of us needs to make a conscious effort to do something for our organization each quarter - four times per year. If you read our last newsletter, you know that we have lost enormous contributions which one of our Chapter founders had been providing. The remaining members of our chapter must now fill that void. Yes, that

means you, too.

Next month, please join us at the Wyndham Garden Hotel for Ray Giske's sponsored presentation on Web Marketing. Bruce Stash will be speaking and this is sure to be another great offering.

In October, we will be having a presentation on the Benefits of ICCA. This is one meeting you shouldn't miss.

For November, we need a sponsor to step forward with a topic and somebody they can coerce into speaking at our meeting. Contact Amy McKenna, Vice President, with your ideas (or she may just call you and have you already volunteered).

Back to the initiatives the Board of Directors has outlined for our Chapter. After a three year hiatus, we have moved forward with our own web site. Jack Rose and Jerry Stiff have graciously volunteered to help make this a reality. We are trying to get our web site up within the next couple of months. To do this, we need content ideas and input from each of you. This is not Jack's, or Jerry's, or even my, web site, it is our Chapter's web site. Join us in making it so.

Other initiatives we are moving forward with are informal notes from each of you on what benefits you get out of ICCA, so we can use that as marketing material. Remember, when I became president, I wanted to grow membership and gain name recognition for our chapter? Well, these efforts are for just that purpose.

We are also looking to amend our By-Laws, to better conform to the current state of our non-profit organization. One example of a pending amendment, is to change the month that our elected officers take office - to coincide with the month that the National Officers take office.

Lastly, I would like to deeply thank each and every one of you who has done something special for our organization recently. Bill Buending, for allowing himself to be appointed interim secretary until, and *only* until the next elections (there is absolutely no chance that Bill will even consider being nominated, so we need another chapter member to step forward). Bill McTeer, for his warm and heartfelt presentation in recognition of our late Ben Moyle and his contributions to ICCA, personally and professionally.

Thank you very much, to all of you whom I mentioned or not - you know who you are, for the wonderful contributions you have bestowed upon our chapter. Without you, there would be no need for us to be in existence.

Officers:

President: Randy Hayman

Voice (651) 261-9939

Fax (651) 456-9426

email: haymanr@pureice.com

CO-VicePresident: Amy McKenna

Voice (651) 702-5036

email: amymckenna@aol.com

CO-VicePresident: Charles Brotzler

Voice (952) 440-6673

Fax (952) 440-6673

email: stellarsol@icca.org

Treasurer: Norm Nelson

Voice (612) 399-0107

email: norm.nelson@icca.org

Secretary: William A. Buending

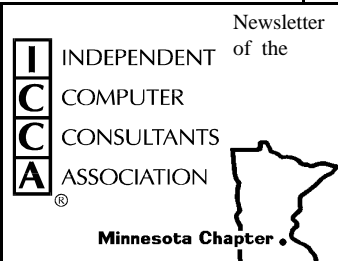
Voice (952) 931-9754

email: wbassoc@buending.com

Editor: Magne A. Hatlevik

Voice (651) 264-1608

email: magne@magpcs.com



(Continued from page 1)

That's the view from here. Let me know your thoughts by sending me email at haymanr@pureice.com.

Computer Security, what does it really mean to me and my systems?

An Overview, Part I of many to come.
By Randy Hayman

With the very recent Code Red security threat, did you know what and where your vulnerabilities were? Did you know that a patch for the Microsoft Internet Information Server (IIS) exists to keep the Code Red Worm from affecting it? Did you also know that you can download a free assessment and removal tool from Symantec so you can check your own systems? Go to www.symantec.com/avcenter/venc/data/codered.worm.html for details.

Did you know that Cisco 600 series DSL routers locked up when scanned by the Code Red worm? Qwest's website has the patch you need if you use Qwest's DSL service with a Cisco 600 series DSL router.

I hope to open your eyes to some security issues you may be facing and may not know it.

What does it mean to be secure?

Think for a moment, about the way security was handled in the days of yore when castles were walled villages needing protection. First, the location, often on a hill, or cliff with access only from certain areas. If the castle was on a cliff, attacks were likely to only come from the areas not protected by the steep cliff access. The castles had very high exterior walls surrounded by a moat with a single drawbridge for access to the interior. This set of physical barriers denied access to many many attackers. Access to the castle was watched by sentrys. Often these castles had a short earthen, or rock wall, about three feet tall about 200 or 300 yards out in the cleared meadow surrounding the castle. By clearing the surrounding forest, the sentrys had an advance warning system - they could see attackers coming. The short wall out in the meadow was to slow down advancing attackers, and inhibit large wheeled vehicles.

In short, these castles were protected by half a dozen or more individual items. The general rule of thumb in security today is that if you do not have the breath and depth of ten items protecting you, you are not secure enough. Practically speaking, like security for your home or vehicle, you

just need to be more secure than your neighbor to repel the majority of attacks. Unfortunately, as far as security is concerned, in the world of the Internet, we are all neighbors.

Am I, and my business secure?

It has been said that security is like Y2K without the deadline. This means that your success with security is measured by what doesn't happen, and it is a continuous effort.

To be secure enough, you need to ask yourself: "For my situation, what computing environment architecture pieces can I lose without affecting me, my business, my family, or our communication." Can you do without any of the data on any of your systems? Are any of your systems shared systems used by other family members? What if I had a hardware failure of any piece of my computing architecture? How much time or money can I afford to spend recovering from any of the above contingencies? And, what if I couldn't recover the data on my system(s) at any cost?

To be secure enough, you need to have answers to the above questions, and put in place various security items to mitigate the risks associated with them.

Some of the security items you can put in place are as follows: Use a secure operating system - one that enforces password access, unlike many versions of Windows. Use passwords for accessing your systems and use the secure screen lock feature. Pick good passwords, and change all default passwords. Do not use password remembering features of any of your software. A backup and recovery plan, that is adhered to and has been tested. Lock up your backup media if you have any sensitive data on them. Regularly store an archive of your data offsite. Disk partition configuration - isolation of different types of data. File system security Access Control Lists (ACLs). Disable your modem from answering calls. Run Network Address Translation (NAT). Run your machines off of an Uninterruptable Power Supply (UPS), which also conditions the A/C power. A contingency plan in the event one of your computing architecture pieces isn't available. A personal firewall on each of your machines. A network firewall protecting your LAN. The use of non-routable IP numbers for your LAN. Virus Checking software on all of your machines, as available. Turning off any unnecessary services your system has running. Turning off file and print sharing. Maintaining current patch levels of all of

your operating systems and software on all of your systems. This is the single most effective item that you can do to secure your systems. Not sharing your business computer with other family members use of the Internet. Running an Intrusion Detection System (IDS). Not opening email or attachments from those you do not know, and anything suspect. Not running known insecure software. Not staying connected to the Internet, unless you are actively doing something online. Not running Wireless Access Protocol (WAP) 802.11b in an area where the perimeter of the WAP goes beyond an area you can control access to. Physically limit access to your systems. Knowing your system - what services should be running, and why. Knowing your system - maintaining an inventory of software, licenses, and versions on your machines. Knowing your system - configuration of your machine(s) hardware in them. knowing your system - create a network topology drawing for your LAN.

What are your vulnerabilities and risks?

If you, or your family members access the Internet, at the very least, you need to be running a personal firewall on your machines. Two very good ones that I have used for Windows machines are Zone Alarm (www.zonelabs.com) which is free for personal and non-profit users, and Sygate personal firewall (www.sygate.com), again free for personal use. If you are concerned about privacy, and you should be, these little gems called personal firewalls also warn you (and by default block) when something in your system wants to send something to the Internet. For those of us using Linux, use ipchains or iptables on your machine to limit unwanted access attempts.

On any machine accessing the Internet, you need to be running a current version of a virus detection utility. For Windows machines, I have McAfee VirusScan and just recently got a floppy disk from a friend which had the Stoned.Unint virus on it - this virus from ten years ago would have rendered my system unbootable, by munging the Master Boot Record (MBR) had I even opened the floppy with windows explorer prior to running a virus check on it. This 30 second scan saved me many hours of time recovering from the virus.

Do you know what all your family accesses and downloads from the Internet? I do not, but I do monitor what my 10 year old son does on the Internet. I have also isolated my risks by educating my family and partitioning the vulnerabilities they can get

(Continued from page 2)
into.

Black Hats (nefarious crackers, and virus writers) have more time and drive to access your systems than we think we have to protect our systems. The time it takes to secure your systems is minimal. Securing your systems is mandatory unless you have more time and money to replace what you will lose one day. How do you put a value on your intellectual property stored on your system(s)?

In my situation, I run multiple systems on a LAN, and use a very old 486-DX2 (90MHz, 3GB HDD, 16MB RAM) machine, which I rebuilt for under \$50, running Linux as my network firewall - it has been protecting my LAN without a reboot since I got DSL well over a year ago. I have all access services (sendmail, telnet, ftp, rsh, rlogin, finger, date, etc...) turned off on this machine, and I use non-routable IPs on my LAN. To date, this old machine has logged but not allowed any successful attempts to access my machines. I know exactly which IPs try what intrusions to my LAN, not that I can do anything about most of them, but I can tell how active the Black Hats and their products are. I also have a second old machine configured identically to the firewall, on a shelf in the event I detect an intrusion. On each of my Windows machines, I run Zone Alarm in high-security mode, configured for my needs. I also run automated backups each night on all of my machines, and keep well over a month of backups.

I have my disks partitioned into multiple partitions where the operating system, and only the operating system is in a single partition, my applications which can be re-installed from CD in another partition, and any data I have created in yet another partition. This way, I can cut one or more CDs of just my data partition and I have a quick and easy archival method. Of the downloads that I have installed, I save the downloaded files into a separate directory, and I do cut a CD of that periodically so I can recover any software easily.

I do not run Microsoft Outlook, or IIS since they are two very well known insecure applications with constant patches. Just to maintain the patch levels of these applications adds more time to my security efforts, time I don't have to spend if I use other more secure software. I do not run Windows 95, 98, or ME - they are not secure enough for me. I have voted with my dollars to get off of and stay off of as much Microsoft software that I can, since, for

many years, they have been so crass about security.

I use network Print Servers to share my printers between my systems, so I do not need to use file and print sharing. I also have a separate system that my son uses (which he helped me build for well under \$500), and his system is isolated from my other systems.

Can you tell that I spent many years as a lead UNIX systems administrator for a very large heterogeneous environment? We never lost one bit of data, nor did we have a successful breach of security during my tenure there either.

We all have choices to make about how secure we wish to be. There are costs associated with security, none of which are excessive if you consider the cost of losing what you've worked so hard for.

To close, let me share an experience a close friend had recently. He was going to change the configuration of one of his Windows machines, but since it was a small change, he decided against backing up his machine. He also hadn't backup up that machine for over six months. In the process of making that one small change, his system became unbootable and unusable. He was then faced with deadlines in addition to rebuilding that machine completely, from scratch, during which he lost any and all of the personal data he had on that machine younger than six months old.

We all make choices, let's start making smarter choices with regards to security. Become proactive, not reactive - it actually saves time and money!

ICCA Disclaimer notice.

"Discussion of any legal issues in any article that appears in this publication is presented as educational material only. The Independent Computer Consultants Association does not and cannot take responsibility for any statements made within this publication as to the meaning or effect of any federal or state law, statute, regulation or ordinance and any opinions expressed in this publication as to such meaning or effect are the opinions of the authors and are not the opinions of the Independent Computer consultants Association, Inc. Any actions or legal steps taken should be thoroughly reviewed with your personal attorney or tax consultant as laws vary from state to state and also because the facts or your situation may not support application of any rule, statement, or suggestion that may be printed in this publication."



Meeting Reservations: Members may phone your reservation to Joan Barnes at 651-257-2570, by 3:00 PM, Friday September 14, 2001. Non-members should mail this form to: ICCA Minnesota, c/o Norm Nelson, 2200 E 22nd St. Minneapolis, MN 55404-3165

Name: _____ Company: _____
 Address: _____ City: _____
 State: _____ Phone: () _____

Menu Selection: Chicken Dijonaise, London Broil
 Beef Stroganoff

Members \$25 Non-members \$28 x _____ = _____
 Late Charge \$2 x _____ = _____
 Enclosed is a check for: _____



Next Meeting

Tuesday, September 18, 2001

Successfully Selling Website Design Projects

Wyndham Garden Hotel

4460 W 78th St. Circle
952-831-3131

Social Hour at 5:30PM
Dinner at 6:30PM

For reservations call
Joan Barnes @ 651-257-2570

FUTURE MEETINGS

Wed Oct 17 Italian Market Deli by Lido
Thurs Nov 22 Wyndham Garden Hotel

Successfully Selling Website Design Projects

Bruce D. Stasch is the Director of Sales and a partner at Apex Marketing Group, a web development and graphic design firm based in Hopkins, Minnesota. Apex provides both standard web design and development services as well as advanced applications like Flash animation, ASP, DHTML programming and SQLserver database development. Apex has recently designed websites for 3M, Personix, Atomic Props, and Lowe's Home Centers and works with both a local and national client base.

Mr. Stasch will be presenting to ICCA members a talk on "Successfully Selling Website Design Projects". He will explain how selling web interface design is different than selling programming and database development to a client. He will also show how partnering with a web design firm can lead to winning more development projects.

Permission is granted to all ICCA publications to quote and reprint any material appearing in Consultants in Minnesota, except where protected by individual copyright, provided credit is given to the author and Consultants in Minnesota



7632 Sherwood Road
Woodbury, MN 55125

Stamp

First Class Mail

