

ISACA Hudson Valley

February 2004 Newsletter

In this issue:

- [President's Message](#)
- [Member Articles](#)
- [Membership](#)
- [CISA and CISM News](#)
- [ISACA International News](#)

President's Message

So... where's the March place to be? You guessed it, the TCTC at the Holiday Inn Turf! *The Conference That Counts 2004* is just around the corner and chances are, the brochure is sitting on your desk, just waiting for you. This year's conference will be held on March 15 - 17, 2004.

As a member of the Program Committee, I'm happy to say that we've lined up a great slate of presenters for you to choose from. As always, the TCTC is a great opportunity to earn up to 21 quality CPEs. Plus, this year we've made it even easier for you to select your sessions. Online registrations

<http://www.aganycap.org/education/events/tctc/tctc.htm> are now being accepted, so don't wait too long. The only problem now is trying to choose.

On another topic, I'd like to draw your attention to the article entitled "Securing Home Computing" written by Wes More. A while back, I asked our members to consider writing articles to share with their colleagues. This is Wes' second article and in it he explains some steps to take to secure home computers from becoming a threat to business and the Internet. If you would like to submit your own article, please send it to our editor, Mark Ren at mren@osc.state.ny.us.

Are you interested in being a Chapter leader?

It won't be long before we're putting together a new slate of candidates for the Board so if you're interested in stepping forward, and guiding our Chapter into the new membership year, please let me know.

Chapter President

Securing Home Computing

By Wes More

Many companies today rely on the Internet to do business, market their products and use email. Accordingly, it's critical the Internet remain available everyday to ensure business activities can be carried out. However, there are risks such as viruses and hackers that can jeopardize the availability of the Internet and the computers used to access the Internet.

Businesses have recognized these risks and have implemented controls such as virus protection software and firewalls.

Many also use Intrusion Detection Systems and perform a software management function to update software when security weaknesses in the software are identified. Businesses have taken aggressive steps to ensure their systems stay free from viruses and other problems.

While businesses have taken these steps, home computers don't always receive the same attention leaving home systems exposed to problems.

As a result, home computers are one of today's biggest threats to business and the Internet.

Most home computers do have virus protection and some even have personal firewalls. However, these tools need to be monitored by the owner of the system to ensure virus protection software is kept up to date and personal firewalls have been set up properly. Most anti-virus software vendors will, for a fee, keep their product up to date automatically. This service is necessary as new viruses are created every day. Any virus protection not kept up to date will not

provide computers with the maximum protection.

Some software companies provide a personal firewall free for non-commercial use. Additionally, many companies sell personal firewall products. The personal firewall acts as a combination firewall and intrusion detection system. It can be set to log and alert the user for unusual activity and can block activity on designated ports in either direction.

Sometimes home computer software is sold with undiscovered security weaknesses known as vulnerabilities. Once discovered, software vendors fix these weaknesses by providing software patches or fixes. Home computer users need to monitor the websites of software vendors to determine when vulnerabilities are discovered and when fixes are made available. The home computer software needs to be updated with these fixes.

Home users can protect their systems and the Internet by employing these tools and keeping them up to date. Rigorously employing virus protection and personal firewalls and updating software with the latest fixes can keep the home computers from being a threat to business and the Internet.

This article has been designed to provide a basic understanding of securing the home computer. I would welcome any questions and comments you may have regarding secure home computing at wmore_12066@yahoo.com. In future articles, I will attempt to address the issues raised.

From the Desk of Membership

by Lisa LeBlanc, CISA

I would like to give a warm welcome to the newest members of the Hudson Valley Chapter.

§ Scott M. Spencer, CISM is an Information Assurance Consultant at General Dynamics Networks Systems at Headquarters US European Command Joint Analysis Center, Molesworth, United Kingdom. Scott chose to join the Hudson Valley Chapter because he hopes to live in our area when he returns to the U.S.

§ John A. Pacini, CISA, CPA, CGFM from Slingerlands also joined our chapter recently.

Welcome!

CISA and CISM[®]

Our chapter is considering holding another CISA review course this year if we have enough members who are interested. This course has proven valuable in past years to chapter members who sat for the CISA exam. Please contact our CISA Coordinator, Bill O'Toole (wmotoole@gw.dec.state.ny.us or 402-9147) to let him know if you are interested in our chapter holding a CISA review course this year.

2004 CISA and CISM Exam Dates:

Early registration deadline: February 4, 2004

Final registration deadline: March 31, 2004

Exams given worldwide on: June 12, 2004

Register now: www.isaca.org/examreg

Study materials for the [CISA](#) and [CISM](#) are available at ISACA's bookstore online.

ISACA International News

Procedures for Information Systems Auditing

The specialized nature of information system (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS audit. One of the goals of ISACA is to advance globally applicable [Standards](#) to

meet this need.

To help assist IS auditing practitioners meet these Standards, ISACA's Standard's Board has developed "Procedures for Information Systems Auditing" to provide examples of the steps IS auditors might take during an audit engagement. These [Procedures](#) provide helpful guidance related to specific IS topics that auditors typically encounter during audits. ISACA's Standard's Board is continually updating these Procedures, so ISACA members are encouraged to regularly reference ISACA's web site.

Audit Programs

Check out the ISACA website for new [audit programs](#). They can be found in the following areas:

- . AS 400 OS
 - . Business continuity Planning
 - . Cellular Management Billing
 - . Change Control
 - . E-Commerce
 - . Networking
 - . Outsourcing
 - . Software Licensing
 - . Systems Development Life Cycle
 - . Telephone Management
 - . UNIX OS
-