

OFFICERS AND DIRECTORS 2001-2002

PRESIDENT

Art Abruzzo, CISA, CDP, CSP
Amerisure
(248) 426-7944

VICE PRESIDENT

Carrie Schrader, CISA
Handleman Company
(248) 362-4400, Ext. 358

TREASURER

John McCormick, CISA, CIA
The Detroit Medical Center
(313) 966-5104

SECRETARY

James Cramer, CISA
The Detroit Medical Center
(313) 966-5170

DIRECTORS

Ed Barszcz, CIA, CFE
Facilities Chairperson
Blue Cross/Blue Shield of MI
(313) 225-9076

Karen Cordes, CIA, CISA
Consumers Energy
(517) 788-0439

Patti Earl-Cole, CISA, CIA
Student Relations Chairperson
Blue Cross/Blue Shield of MI
(313) 225-8577

William G. Garvey, CISA
Delphi Automotive
(248) 267-5723

Brenda L. Karl, CISA
Job Bank Chairperson
Jefferson Wells International
(248) 350-3006

Ray Kaslik, CISA, CIA, CFE, CMA
Seminar Chairperson
AAA Michigan
(810) 727-1962

Don Ledwith, CISA, CCP, CQA
Membership Chairperson
General Motors Corporation
(810) 492-1092

Michael Mullens, CISA, CIA
Cyndi Shelton, CISA
General Motors Corporation
(313) 665-0000, Ext. 44056

Mike Stolarczyk, CISA
Jefferson Wells International
(248) 350-3006 ext. 1319

David F. Thompson, CISA
CISA Chairperson
Blue Cross/Blue Shield of MI
(313) 225-6384

Michael Tomasek, CISA, CIA
(810) 805-8191
Sander Wechsler, CPA, CISA
Ernst & Young, LLP
(313) 628-8024

Brent W. Wylie, CIA, CISA, CFE
Internet / Newsletter Chairperson
Blue Cross/Blue Shield of MI
(313) 225-0527

PAST PRESIDENTS

Todd McGowan, CPA, CISA
Deloitte & Touche, LLP
(313) 396-3407

Marci Klain, CPA, CISA, CIA
General Motors Corporation
313-665-0000, Ext. 44072



*Information Systems
Audit and Control
Association*

DATABYTE

NEWSLETTER OF THE DETROIT AREA CHAPTER

VOLUME 16, #8

REGION 2, CHAPTER 8

APRIL, 2002

Monthly Meeting

Wednesday, April 17, 2002

Pre-Dinner Topic: "Wireless Security Presentation: Managing Your Wireless Risk"

After-Dinner Topic: "Protection from Hidden Threats"

**Location: Big Fish Seafood Bistro
1111 W. 14 mile, Madison Heights
Corner of 14 mile/ Stephenson Hwy.
248/585/5933**

Date: Wednesday, April 17, 2002

**Time: 4:30-5:00 Registration/Networking
5:00-6:00 Before-Dinner Presentation
6:00-7:00 Dinner
7:00-8:00 After-Dinner Presentation**

**Cost: \$30.00 Members
\$35.00 Others
\$20.00 Students and Retirees**

Reservations---Make your reservation by 4:00PM Friday, April 12th. You can make your reservation online at isaca-det.org. If you do not have access to the Internet, e-mail your reservation to Art Abruzzo at aabruzzo@amerisure.com or call him at (248) 426-7944. Please include your name, company, telephone number, and whether you are a member.

Visit our web site at: isaca-det.org

Message from your President...

Dear Members,

The year is quickly slipping by as April marks our next to last meeting. The March pre-dinner presentation was a roundtable on the CISA exam, headed by Dave Thompson. Dave's presentation dealt with a little of the history of the exam as well as talking about the benefits of taking the exam and included some tips on how to successfully pass. Prospective candidates came away from the presentation ready to take on this new challenge. Dave has done an outstanding job the past few years, heading up the CISA committee. Our review course held over a two month period has been extremely successful in preparing exam takers to successfully pass the exam. If you are interested in taking the CISA exam and have not yet signed up for our FREE course, please contact Dave for more information.

Our after-dinner presentation was on Digital Signatures and was presented by Ed van Essen, a Senior Manager with Deloitte & Touche LLP. Ed made an outstanding effort just to speak to our group as he was in route from Minneapolis to Cleveland. Ed has spoken to our group a few times in the past and, as always, did an outstanding job presenting his subject material.

I would like to thank both Dave and Ed for their efforts to enlighten us with their presentations.

By the time you receive this Newsletter we will have concluded our joint conference with the IIA. Registration numbers at this time indicate the potential for the most successful conference to date. I believe there will be over 150 attendees for each of the 3 days of the conference. Our partnership with the IIA in co-sponsoring this event has provided outstanding benefits to our organization. This is a partnership that I hope continues for some time. A great deal of hard work has gone into the planning and execution of this Conference and I would like to thank all of those individuals for their efforts. I will report back next month on the success of this event.

I would once again like to stress to you, our members, that we (the Board) are here to serve the membership. If you do not believe we are adequately doing that or have a suggestion you think will help us do it better, please feel to contact me or any other Board member. You can reach me through e-mail me at aabruzzo@amerisure.com or call me at (248) 426-7944. You can also contact us through the website at www.isaca-det.org.

I look forward to seeing all of you at the March dinner meeting.

Art Abruzzo
Chapter President

Pre-Dinner Topic:
Wireless Security Presentation:
Managing Your Wireless Risk
Speaker: *Louis Devaney*

Advances in high-speed wireless data communications, along with the widespread availability of low-cost laptops, PDAs, cell phones, and pagers have ushered in a new era of wireless connectivity. Network access is now easily accomplished in previously impossible environments, free from the restraints of physical wire connections.

Unfortunately, this new freedom and growth brings with it a new array of risks and challenges for information security managers. In this presentation, Mr. Devaney will discuss the risks associated with common wireless computing environments, and how to reduce these risks through the application of management strategies and technical controls.

Louis Devaney is a CISSP certified Senior Consultant working in the Detroit office of Espiria (www.espiria.com), a leading developer of comprehensive security programs. With over 10 years experience in the security field, Mr. Devaney has played a key role in the development of security programs and performed assessments or training for multiple Fortune 500 corporations and the U.S. Military. His significant accomplishments include acting as the initial security architect for a key automotive exchange, and authoring security software implemented on classified systems throughout the U.S. Air Force.

After-Dinner Topic:
Protection from Hidden Threats
Speaker: *James C. Shaeffer*

A pest is malicious code found on a PC or a computer network. Pests include software such as Trojans, spyware, remote administration tools, hacker tool kits and more. All pests share common characteristics: Most people impacted by pests don't know anything about them, did not invite them in, do not know they are present, and do not want them in their systems. That is the heart of the problem. With thousands of files in today's computers, no one could be expected to know what every single one does. And, without a master detector to help find pests, they can live and thrive in your system.

Pests have become rampant. Pests can do anything software can do. This can include:

- Turning on your computer's microphone, capturing the sounds in the room, and transmitting them across the Internet.
- Collecting your e-mail address and other contact information.
- Gradually corrupting files on your hard drive.
- Initiating a remotely controlled attack against a third party.

(continued on page 5)

CANAUDIT PERSPECTIVE NEWSLETTER

Volume 3 Number 3 March 2002

THE NEED TO SECURE THE WEB PRESENCE

By Chris Schroeder
Manager, Technical Audits, Canaudit, Inc.

When creating a new web site, your organization makes a significant investment in designing and building the web site. They enlist the help of “experts” who research the pros and cons of hosting your own web server. After spending thousands of dollars, the company finally has a web site they are proud to unveil to the world. Once the web site goes live, *Headline News* reports that a credit card company was hacked and that thousands of credit card numbers were stolen. Your company management says that you don’t have anything to worry about, as the company doesn’t have anything the hackers want on the web site. Have you heard this when doing your audits or security reviews?

Your System Administrators are usually top-notch people with good skill sets. They tell you that you have a secure web site. After all, we had some of the best consultants help us build it and “we have a firewall.” Then one day a customer calls to complain about the pornography on your web site. When you review the web site, you discover that many of the pictures on your web site have been replaced with pornographic photos. If you had a firewall, built and managed by experts, how did this happen?

Stated simply, your company’s web site was the victim of a hacker. There are many similar events happening every day. The knowledge level of the hackers is increasing, as is the number of hackers is increasing. Hackers share exploits as soon as they are discovered and usually before vendors can develop and test a patch. Web administrators must take additional precautions to ensure that the web site is properly protected. While this may seem unnecessary when planning and building the web site, the extra security will pay off in the long run.

Often management thinks that security is not required as there isn’t anything of value on the site. This does not mean that you can’t be a victim, it just means that you may be a different type of victim. Instead of stealing customer credit cards, hackers post pornography or “paint up” your site. If this is reported by the press, there is an immediate public relations issue that can be very costly to correct. The P.R. nightmare can even have an effect on the share price as shareholders sell the stock. Also, customer confidence may be affected.

Your system administrators may be brilliant; however, they often do not have the time required to keep up to date on the latest exploits and required patches. Nor do they have the staff to regularly perform a security test on the web site. Through the course of our audits, we have determined that system administrators are often overworked and understaffed. They know that security is not at the peak level, but management puts their priorities in other areas. We have heard all of the excuses. “We don’t have the funds,” “we are not at risk,” and “you auditor’s are paranoid.” The fact is: you do have the funds, you are at risk, and we auditors are not paranoid, we’re just cautious.

If a hacker successfully targets your company’s website, there will be damage. The amount of damage depends on the type and severity of the attack. A denial of service attack (DoS) may disrupt your site for a while; however, it usually does not do any permanent damage. The theft or alteration of customer information, such as customer names and social security numbers, can be very serious. Changing the posted interest rates by half a point overnight can be very serious if your organization is a bank that accepts overnight deposits from other financial institutions. Each night, these organizations search for the best overnight rate for their funds. If you are half a point higher than anyone else, you may be flooded with more money than you can invest. As a result, a simple change in interest rates could cause large overnight losses.

(continued on page 4)

(continued from page 3)

Aside from a P.R. nightmare, your stock may very well drop. Once your customers find out that your network is unsecured, they will not use it. If their confidence in your site security is destroyed, your customers may even band together and launch a class action suit. If management chooses not to fund security, then the company is at significant risk. To get the funding, it is necessary to build a business case for investing in web security.

Here is an example that management will understand. Let's say the CEO owns 1,000,000 shares of company stock that is currently trading at \$50 per share. A hacker penetrates the company website and USA Today runs a front-page story about the incident. The next day, your stock drops five points. (Our research shows that affected stock prices drop approximately 10% to 15% when this happens. It normally bounces back up after a while; however, if a short seller had prior knowledge of the attack, then there could be SEC issues as well). The CEO is now out of \$5,000,000, and the shareholders may have an even greater loss. The CEO now has the embarrassing task of explaining to the shareholders that the company's security was ineffective and the actions that will be taken to improve security in the future. By spending \$50,000 upfront to secure the web presence, this problem could have been avoided.

During some of our classes, we offer the participants a free examination of their web site. Usually the participants are amazed at what we find. Some common examples are staff and customer accounts and passwords, as well as poorly secured databases or other customer information that we "harvest." No site is completely safe. The best practice is to protect your site so that is not a target. One of the ways you can do this is to perform a penetration test on your own site. Once the vulnerabilities have been identified, they can then be resolved. The site should then be retested on a regular basis to ensure that it remains secure.

One of the most common flaws we discover during our penetration tests is that port 139 (NetBios) is open to the Internet. From this port, we obtain a list of all of the shares; every account name on this system; the days since the last password change; how many times the accounts have been used; and whether the account is a regular user, guest or an Administrator account. All of this can be done without your system administrators knowing we are doing it, even if you have intrusion detection software!

Thirty percent of the time, we find an Administrator account with no password. We then map a drive to this I.P. Address and logon as Administrator. Once we have Administrative rights, we take the password file from the registry and crack all the passwords. Using the passwords we cracked, we log onto other systems and steal those passwords. These passwords or other control weaknesses may give us control over the routers and firewalls. With just a little bit of luck, we will gain access to the company's internal network. Gaining access to the internal servers should be easy as we have already cracked some of the required passwords. The Domino Effect then takes over and your entire network crumbles, giving us or worse, real hackers, the keys to the corporate kingdom.

Another port that we frequently find open is port 21 (FTP). Quite often, anonymous login is allowed with read and write permissions. Hackers love this, as they can use your disks to store their porn and software (Warez). They can also upload a Trojan or virus, place a back door on your machines, or use your machines in a coordinated distributed denial of service attack against another organization. These actions could result in a significant legal liability, as well as disgrace the good name of the company.

Echo and Chargen are services that we also frequently find active during our Internet reviews. There are exploits that combine these two ports to create a DoS that will knock your system offline in about three seconds. These ports are normally not used and could easily be deactivated. There are many other ports that are as vulnerable as those mentioned; I've just mentioned a few of the most common faults we find when we do our audits and security reviews.

To mitigate these threats, your organization's web site must be tested on a regular surprise basis. If your organization does not have a penetration team, then you should either build and train one, or contract with a professional firm to perform these tests. The Canaudit Penetration Team (a.k.a. The Strike Force) can test your sites on a monthly or quarterly basis. Our team uses the same tools and exploits that the hackers do. We run our tests slowly over an extended period of time so that we stay below your intrusion detection software.

(continued on page 5)

(continued from page 4)

We document your extranet or web presence. Then we identify the exposures and provide solutions to eliminate or reduce the risk. We can also train your security staff to perform this testing.

(Ultimate Network Penetration Class Registration Info <http://www.canaudit.com/Ultimate/ultimate_menu.htm>).

It is also very important that your organization establish a preemptive security team. The members of this team should research new exploits, identify vulnerabilities in your network, and correct them before hackers can use them to take control of your website or deface it. In addition, there should be strong computer incident procedures to detect, document, and resolve computer incidents in real time. Your computer incident response procedure should identify the different levels of alerts and the steps that should be used to follow up on them.

You need people that you trust on this team. They will have the keys to your kingdom. You don't need the best people in the security field. Rather, you need people that are willing and able to learn and will be diligent in performing their tasks. You will also need a manager who can talk to the "C" people i.e. CIO, CEO, CFO, CAE. This person must know how to translate the technical jargon into business language that management can understand. To be effective, this security team should be independent of the IT department and report to a senior executive.

Now is the time to be proactive, and not reactive. Get a team of qualified people together and attempt to penetrate your own network. You will be surprised at what you find and the amount of work that is required to ensure that your web site is properly protected. Canaudit is offering a series of courses in the next few months to provide you will the skills needed to protect your organization. These are:

April 1 – 4

Registration Info <http://www.canaudit.com/pd_weeks/simi-april-1-4_registration.htm>

Control & Security of Wireless Networks <<http://www.canaudit.com/Seminars/tis16.htm>>

Control & Security of PeopleSoft <<http://www.canaudit.com/Seminars/tis14.htm>>

April 29 – May 2

Registration Info <http://www.canaudit.com/pd_weeks/simi-april-29-2_registration.htm>

Control & Security of Oracle <<http://www.canaudit.com/Seminars/tis9.htm>>

Control & Security of UNIX <<http://www.canaudit.com/Seminars/tis8.htm>>

Control & Security of Telecommunications <<http://www.canaudit.com/Seminars/tis17.htm>>

Control & Security of Windows 2000 <<http://www.canaudit.com/Seminars/tis2.htm>>

CONTACT THE AUTHOR

As always, I am interested in your feedback. Please email your comments to chris@canaudit.com. I will respond to each comment, usually within 24 to 48 hours. By working together, I believe that we can make the Internet a safer place for customers, while we protect your corporate assets.

Chris Schroeder
Manager, Technical Audits and Security Services
Canaudit Inc.

After-Dinner Topic:

(continued from page 4)

There are some applications that everyone would judge to be a pest, such as a program that interferes with mouse motion. But other programs might be helpful to one user yet harmful to another. Consider the "password recovery tool" that can help you when you forget a password. Such a tool is fine when you use it to solve your own problem but not so fine when someone else aims it at files or a system you have tried to protect. One recent example of a pest is the "LoveLetter.vbs," which e-mailed itself to entire address books and was a nuisance for many businesses worldwide.

James C. Shaeffer incorporated James C. Shaeffer & Associates in 1991 in Michigan. It is a leading distributor of PC and LAN Security Software. Jim has actively and successfully marketed PC and LAN Security Products to Fortune 1000 and smaller companies across North America. He has provide technical assistance to many companies in the areas relating to software auditing, computer security and anti-virus protection.

The Year At A Glance

Meeting Date

May 15, 2002 (Wed)

Pre-Dinner Topic

CRM

After-Dinner Topic

Single Signon

Menu - April 17, 2002

When making your reservation, please indicate which entree you prefer. Attendees not specifying a choice will be served entree #2.

The following entrees will be served:

Entree #1 New York Strip

Entree #2 Raspberry Chicken

Entree #3 Broiled Salmon

Vegetarian plate is available for those on special diets.



All meals include:

- Specialty Bread
- Rice or Potato of the Day
- Tossed Salad with Raspberry Dressing
- Fresh Seasonal Vegetable
- Dessert: White Swirl Chocolate Mousse
- Coffee or Tea
- Cash Bar Available

The Chapter must provide the number of reservations by the Monday before the meeting. To ensure that we can accommodate those who wish to attend and the restaurant can provide the best service possible, please make your reservations early. If you have made a reservation and cannot attend, please call in a cancellation. Your cooperation is greatly appreciated.

Monthly Drawing Winners!!

Chris Hickson

Mike Forrest

Michael Tomasek

Andrea Stromar

DATA BYTE

Information Systems
Audit and Control
Association
DETROIT AREA CHAPTER
P.O. BOX 4297
TROY, MICHIGAN 48099-4297

