

**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
(810) 727-1962

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

Michael Mullins, CISA, CIA
Cindrich, Mahalak & Co, PC
(810) 296-1155

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

Mike Stolarczyk, CISA
Jefferson Wells International
(810) 350-3006, Ext. 194

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

Michael Tomasek, CISA, CIA
Program Chairperson
Experio Solutions
(248) 244-6558

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, #2

REGION 2, CHAPTER 8

OCTOBER, 2001

Monthly Meeting
Wednesday, October 17, 2001

Before Dinner Topic: Internet Security

After Dinner Topic: Privacy

Location: Big Fish Seafood Bistro
1111 14 Mile Road
Madison Heights, Michigan

Date: Wednesday, October 17, 2001

Time: 4:30-5:00 Registration
5:00-6:00 Pre-Diner Presentation

Dinner: 6:00-7:00
7:00-8:00 After-Dinner Presentation

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

Reservations—Make your reservation by 4:00 PM, Friday, October 12th. You can do online reservation at isaca-det.org. If you do not have access to the Internet, e-mail your reservation to Carrie Schrader at c.schrader@handleman.com or fax it to (248) 362-6409. Please include your name, company, telephone number, and whether you are a member. If you do not have access to the Internet, e-mail or a fax machine, call Carrie Schrader at (248) 362-4400, Ext. 358.

Visit our web site at: isaca-det.org

Message from your President...

Dear Members,

The year is off to another excellent start. Those of you who attended our September meeting were treated to two fine presentations. The pre-dinner topic was called Managing Data Security in an End-user Computing Environment and was presented by Charlotte Partridge of Experio Solutions. Our after-dinner presentation was put on by Deborah Wiley-Crossen of KPMG and dealt with the Health Insurance Portability and Accountability Act (HIPAA). Thank you Charlotte and Deborah for two enlightening presentations.

The Program Committee, chaired by Michael Tomasek, is always looking for additional presentation topics or people who would be willing to speak at one of our Dinner meetings. Please contact Michael with any of this information.

Congratulations to all those who sat for the last CISA exam and passed!!!! This is an achievement to be proud of. The CISA certification is widely recognized and very prestigious. For all of you who are considering taking the exam in the future, our chapter offers a free review course to members to help you prepare. More information will be available in the coming months. If you have any questions, feel free to contact our CISA Chairperson, Dave Thompson.

On a more somber note, I am sure we are all saddened and still feeling some effects of the horrible attacks that befell some of our fellow human beings on September 11. The Detroit Chapter of ISACA would like to extend our deepest sympathy to the victims and their families. In light of this tragedy, the Board has voted to donate \$1000.00 to the Salvation Army Relief fund.

If you want more information about our organization or have any suggestions you believe will make our chapter better, you can e-mail me at aabruzzo@amerisure.com or call me at (248) 426-7944. You can also contact us through the website at isaca-det.org.

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

Art Abruzzo
Chapter President



GLOBAL RECRUITERS IS A FULL SERVICE FINANCIAL EXECUTIVE PERSONNEL FIRM REPRESENTING WORLD CLASS LOCAL, NATIONAL AND INTERNATIONAL FORTUNE 100, TIER I AND II, BIG THREE, BIG 5, REGIONAL AND LOCAL CPA FIRMS, HIGH-TECH, VENTURE CAPITAL AND VARIOUS OTHER ORGANIZATIONS IN SEARCH OF TOP NOTCH TALENT WITH THE FOLLOWING DESIGNATIONS.



CPA, CIA, CISA, CFSA, CMA AND/OR MST .

IF YOU HAVE A BA/MBA/MST-ACCOUNTING/FINANCE W/ 1-10 YEARS PUBLIC ACCOUNTING AND/OR INDUSTRY EXP., EXCELLENT ANALYTICAL, COMMUNICATION AND PC SKILLS AND LOOKING FOR A CHANGE, THE TIME IS NOW!!

CALL, FAX OR E-MAIL RESUMES TO:

GLOBAL RECRUITERS

ARTHUR G.

27650 FARMINGTON RD #206

F. HILLS, MI 48334

PH: 248.489.1900 – FAX: 248.489.9008

E-MAIL: SIRCHFIRM@AOL.COM

INTERNET: WWW.GLOBALRECRUITERS.COM

2001 Copyright Canaudit, Inc. • All Rights Reserved
Securing the Internet for 2002

CANAUDIT PERSPECTIVE NEWSLETTER
Volume 2: Number 1; September 2001

Securing the Internet for 2002

By Gordon Smith, President, Canaudit Inc.

As we complete more of our Internet penetration and network audits, there seems to be a very disturbing trend. Many organizations have serious Internet issues that need to be addressed. The purpose of this article is to enable you to understand the key risks of an organization's web presence and mitigate those risks. We have presented the issues in an orderly manner, encompassing from initial design to security testing.

Cataloging Your Organizations Internet Sites

Many organizations are not aware of their full Internet presence. They are often aware of their main web site, and sometimes they might even be aware of their full Extranet exposure. However, many of them have "Rogue" Internet connections set up by small groups or large departments within the organization! In several of our recent Internet penetration audits, we penetrated the client's network by identifying and exploiting a poorly controlled rogue site that connected to the internal network. These sites bypass normal IT development, management and security procedures. As a result, the required controls are not in place, and hackers can simply slide into the network.

Once we have penetrated a network using a rogue site, IT management is often upset because they did not even know the site existed. Yet management holds them responsible for Internet security. This is why it is so important that your organization's Internet presence be mapped and catalogued. This can be done by the IT security group or by an outside source such as Canaudit. In fact, cataloging the client's complete Internet presence is the first thing we do when commencing an Internet or Internet penetration audit. You can bet that hackers have already probed your rogue sites for weaknesses in your Internet presence.

Design and Configuration

For many organizations, the Internet presence started out much like the California Gold Rush. Everyone lined up; someone counted to three; and, viola, your company was on the Internet. "Let's just get it up, we'll control it later." "We have to be on the 'net' because our competitors are already there." "We have a firewall." We've heard these and similar phases many times, as I'm sure you have. Despite best intentions, some organizations never revisit their Internet design and configuration. Not only does this lead to poor controls over the Internet presence, but it can also lead to Internet sites that do not have the required functionality to attract and retain your customer base.

Many of the sites we have reviewed are primarily "brochure" sites. These sites provide information about products and services. This is great for clients who simply want to browse an electronic catalog. Unfortunately, it does not capture marketing information about your Internet visitors. Nor does it enable your organization to contact customers, permit customers to order product, or enable your company to push critical information such as price changes and other sales data out to them.

From a security standpoint, poor design and configuration results in very poor security. In most cases, security consists of a firewall. Unfortunately, firewalls can be bypassed through rogue connections mentioned above, or by poorly configured routers, servers and trading partner connections. Internet design and configuration should include the initial design of the Internet sites and the controls required to control those sites. The actual controls are implemented either through firewall, server and application controls and/or the installation of security software.

Internet design and configuration is not something to be reviewed only once. It is an ongoing task that needs to be performed semi-annually. This will ensure that the Internet connections continue to meet the needs of your organization and your customers.

The Extranet

Many organizations are moving applications out onto the Extranet. As a result, the critical control points must also migrate to the Extranet. Our audits have identified that many organizations have a poorly controlled Extranet environment. Critical customer information, as well as business transactions, can be accessed, copied or even altered by hackers and electronic espionage consultants. These "consultants" data mine the Internet for information that can be sold to criminals and competitors. Effective Extranet security encompasses Internet, server, network, database and application security. Most Extranets have not been subjected to a full security review or audit. One of the priorities for this year should be to complete these reviews so that controls can be enhanced and funding allocated for ongoing Extranet security in 2002.

Many organizations have outsourced their Extranet to an ISP or an ASP. This does not mean that security and control will be any better, nor does outsourcing the Extranet relieve your organization of the responsibility to protect your client's data. We are currently very concerned that several of the major ISPs may have serious cash flow issues, as the dot-coms turn into dot-busts. If your ISP fails, what happens to your Extranet and your ability to process Internet transactions? Additional information on Extranets is available in our course Control and Security of the Extranet.

Continued on page 4

Continued from page 3

Firewalls

Firewalls are a great control; however, our audits show that firewalls can be bypassed. Also, if your organization fails to install the required upgrades and patches, then firewall controls may be breached. Another issue is intruder detection and response. We have noticed that many organizations let the firewall block attempts. In many cases, the firewall logs are not reviewed. Hackers can quietly probe the site, document vulnerabilities and, hopefully with success (from their standpoint), execute and exploit the site. If the firewall blocks their IP address, a hacker will just use another account to continue their attack. Only an automated alert, combined with formalized intrusion detection and response procedures, can ensure that a sustained attack is detected and properly investigated. Additional information is available in our seminar Control and Security of Firewalls and Intrusion Detection.

Virtual Private Networks

VPNs are often marketed as a safe alternative to other connectivity technologies. While this can be true if properly installed and secured, some VPNs have been used by hackers to penetrate corporate networks. In February of 2001, many organizations were successfully penetrated from Eastern Europe using their own VPN connections. Not only were their controls defeated, but these companies had to foot the bill! Some of these companies discovered they were had only once they saw the VPN provider invoice. This could have been discovered much earlier using a query against the VPN data. An effective means of monitoring VPN connections would be to simply have the VPN provider supply a file on a daily or weekly basis with information about your user sessions. This includes account number, origination point, date and time of login, date and time of logout, session duration packets transmitted and packets received. Put this data into a database or spreadsheet and sort it by looking for very long sessions and impossible combinations (logging in from Seattle at 1 pm, then New York at 1:05 pm). Also look for concurrent logins (two or more logins with the same account at the same time). This will enable you to discover compromised or shared accounts. The last simple test is to look for large data volumes from a particular account. This may be a hacker who is downloading your data or uploading his or her data to your servers.

Content Management and Security

Many organizations lack controls over web site content. We regularly find site content that has been altered by hackers. Since no one is reviewing the site on a regular basis, these altered pages will only be noticed by your customers! Some changes are made because of poorly controlled CGI code. Other changes are made by exploiting the site software. IIS, as everyone knows, is particularly vulnerable. Every organization should have a formal review process before content is placed on the web, regular reviews to ensure that the content has not changed, and effective security to protect your site and site content.

Management Control and Oversight

We have found that management often delegates web content, management and oversight to low-level staff. This not only demonstrates that management is not interested in the Internet presence, but that a significant part of an organization's customer contact and web content is implemented by project leaders and analysts, not marketing people. Management must take an active role in managing web sites and content. They must determine what information is public and ensure that the information is presented in an acceptable format that will not expose the organization to legal issues. In addition, non-public content and customer information must be protected. Management must also ensure that the Internet presence is secured and that intrusion detection is in place. A senior executive should head the computer incident response team to ensure that incidents are properly reported to executive management and that there are no cover ups.

As you can see, there are many issues relating to Internet security. This article highlights only a few of them. We highly recommend that every organization's Internet presence be audited or subjected to a security review at least once a quarter. You can perform this review yourself or you can hire someone to do it for you. Canaudit provides a full range of seminars to prepare you for such a review, or we can do the Internet penetration audit for you. Seminars that provide such training will be offered at our upcoming Professional Development Week in Minneapolis and at our Ultimate Network Penetration Class in Simi Valley, CA, which you can register for at our web site at www.canaudit.com or by phone at (805) 583-3723.

The Canaudit web site also contains many free software tools that can assist you in your reviews. If you require additional information on our seminars, Internet and Extranet audits, as well as Internet penetration testing, please contact Gordon@canaudit.com, Chris@canaudit.com or Paul@canaudit.com.

Newsletter Delivery

As we announced in the last issue, we will be changing our primary method of DataByte delivery to an online format. Over the next few weeks, we will be contacting all members and non-members who receive the DataByte to confirm email addresses. Although electronic delivery will be the default format beginning in December, everyone will have the opportunity to request that a paper copy be delivered. You can view our current newsletter online at isaca-det.org

Pre-Dinner speaker

Internet Security

The Internet is used by almost everybody from work or home. Tony Robinson will discuss Internet intrusion detection (internal and external), as well as the steps that can be taken to protect systems. These steps include monitoring, system backups, biometrics and other access security options.

Tony Robinson is President of Pioneer Technology, a Michigan Corporation. Pioneer Technology has been in business since 1983, providing technology solutions in automotive, engineering, computer systems, networks, and (since 1995) e-Security. Tony holds a Masters in Computer Science with over 20 years background experience in high technology Research and Development and technology management in Control systems, Military systems development, Biometrics, embedded chip technology, systems and network integration, as well as complete e-Security solutions.

After Dinner speaker

Understanding the Privacy Risk Management Life Cycle

Companies are going to far greater lengths to protect their data by establishing sophisticated systems and processes to mitigate the ever-present risks associated with information systems. David Dunning will provide an understanding of the life cycle of privacy risk management and how to identify and manage privacy-related information risks. He will discuss the Strategy and Risk Identification, Development and Implementation, and Monitoring and Control phases.

David Dunning is a Senior Manager in the Information Risk Management Practice at KPMG, LLP. He has presented a variety of security topics at national and regional conferences and workshops.

We are pleased to inform you that records were once again surpassed for the 2001 CISA examination. A total of 8,210 candidates sat for the exam with an overall pass rate of 50 percent.

Congratulations to the following ISACA members for successfully passing the CISA exam this past June.

Daniel Bargy, Keith Bateman, Kimberly Buck, Cassandra Carson, Michael Forrest, Phil Gibbs, Thomas Hart, Rich Hibner, Kathryn Kavolinas, Johnathan Landsman, Laura Laukonis, Trish Monteleon, Jeff Monville, Debbie Nykiel, Jim Petruska, Michael Powaser, Sheila Purol, Jamshid Sadaghiyani, David Schankin, Michael Sharlow, Deborah Smith, Ted Tifrea, Ronald Wagner, Joseph Wang, Christine Wisneski, Yu Zhu.

Congratulations to the following non-members awarded CEP Memberships.

Steven Erwin, Brian Gawne, Julie Grant, Carl Lambert, Ronald Murphy, Joseph Ponnoly, Jeff Recor, Dorothy Smith, Jeremy Zager.

Menu - October 17, 2001

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

Entrée #1: Top Sirloin (NOTE: Only registrations by October 12.)

Entrée #2: Chicken Cordon Bleu

Entrée #3: Broiled Whitefish

A 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: Hot fudge cream puff
- Coffee or tea
- Cash bar available

The Chapter must provide the number of reservations and menu selections to the restaurant 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.



New Members for September 2001

Steven Erwin, CPA, CIA

Brian Gawne, CISSP

Julie Grant

Carl Lambert

Jennifer Major

Ronald Murphy

Joseph Ponnoly, CISSP

Patrick Powers, CISA, CISSP, CA

Jeff Recor, CA, CISSP

Dorothy Smith, CPA

Jeremy Zager

John Batek, CPA

Neha Patel, CISA

Raffle Winners

September 19, 2001 Chapter Meeting

Before Dinner

Dave Hebel

Jeff Fisher

After Dinner

Brent Wylie

Valerie Ziemke

The Year At A Glance

Meeting Date	Pre-Dinner Topic	After-Dinner Topic
October 17, 2001 (Wed)	Internet Security	Privacy
November 14, 2001 (Wed)	Oracle	Audit Issues of IS Outsourcing
December 11, 2001 (Tue) <i>Joint meeting with IIA</i>	Firewalls	Network Penetration
January 10, 2002 (Thu)	Joint meeting with ACFE	Cybercrime
February 20, 2002 (Wed)	Government Impact on Disaster Recovery	Network Contingency Plans
March 20, 2002 (Wed)	CISA Roundtable	E signature
April 17, 2002 (Wed)	Wireless Security	Internet Virus
May 15, 2002 (Wed)	CRM	Single Signon



*Information Systems
Audit and Control
Association*

DETROIT AREA CHAPTER
P.O. BOX 4297
TROY, MICHIGAN 48099-4297

DATABYTE