

**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, #3

REGION 2, CHAPTER 8

NOVEMBER, 2001

*Monthly Meeting*  
*Wednesday, November 14, 2001*

**Before Dinner Topic: Audit Issues of IT Outsourcing**  
**After Dinner Topic: Security in Oracle Applications**

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

**Date: Wednesday, November 14, 2001**

**Time: 4:30-5:00 Registration**  
**5:00-6:00 Before-Diner 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 4:00 PM, Friday November 9. You can make reservations online at [isaca-det.org](http://isaca-det.org). If you do not have access to the Internet, e-mail your reservation to Suzanne McCormick at [jsmccor65@aol.com](mailto:jsmccor65@aol.com) or call her at (248) 471-3075. Please identify it as an ISACA reservation and include your name, company, telephone number, and whether you are a member. If you need to fax your reservation, call ahead to ensure the fax line is activated and fax it to (248) 471-3075.**

*Visit our web site at: [isaca-det.org](http://isaca-det.org)*

## *Message from your President...*

Dear Members,

**I**t was another successful month for the Detroit Chapter of ISACA. Those who attended the October Dinner meeting were presented with some valuable information. The pre dinner presentation was on Internet Security by Tony Robinson, President of Pioneer Technology. The after dinner presentation was on the Privacy Risk Management Life Cycle and was presented by David Dunning, Senior Manager at KPMG, LLP. Both speakers possessed a great deal of experience and insight in their areas and did an excellent job of passing that along to us in their presentations.

Please note that our November meeting will be held on Wednesday, November 14. This is a departure from our normal practice of holding our meetings on the third Wednesday of each month. It was necessitated due to the Thanksgiving Holiday being the following Thursday. The meeting will still be held at Big Fish Seafood Bistro.

As we look ahead to our December and January meetings, please note that these will be joint meetings and will be held at other locations and on different nights. The December meeting will be held on Tuesday, December 11 and will be a joint meeting with IIA. The January 2002 meeting will be held on Thursday, January 10 and is a joint meeting with ACFE. Check future Databytes or our website at [www.isaca-det.org](http://www.isaca-det.org) for location and directions to these meeting places.

For those of you who are preparing the budgets for 2002, keep in mind that ISACA and IIA are once again planning on jointly sponsoring a Spring Conference. This is an opportunity to receive valuable training at a very reasonable cost in addition to avoiding the high cost of travel. In this time of tightening budgets and travel concerns we believe this is an excellent opportunity to provide value to our membership. More information on the Seminar will be coming over the next few months.

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 free to contact me or any other Board member. You can reach me through e-mail me at [aabruzzo@amerisure.com](mailto:aabruzzo@amerisure.com) or call me at (248) 426-7944. You can also contact us through the website at [www.isaca-det.org](http://www.isaca-det.org).

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

Art Abruzzo  
Chapter President

---

**G**eneral Motors will host a beta of the new ISC2 Certified Information System Security Professional (CISSP) review course at a GM facility in Pontiac Michigan from November 5 through 9. Because this course compresses the existing two week review into one, plan on long class days. The cost for attending this beta class is \$2500 which includes registration for the CISSP exam. The exam is scheduled to be administered Friday, November 30. While seating is limited, there are plenty of seats available as of 10/12.

Since this is a beta for the course, it will not be listed on the ISC2 schedule of courses nor will ISC2 register attendees. If you wish to attend please drop an email to [don.ledwith@gm.com](mailto:don.ledwith@gm.com) with a copy to [alan.drake@gm.com](mailto:alan.drake@gm.com). Please do not phone.

---

## CANAUDIT PERSPECTIVE NEWSLETTER

Volume 2, Number 2, November 2001

### Wireless LANs: The Hacker's Best Friend • By Chad Parks, Canaudit Inc.

Wireless networking and network security are like oil and water. Many companies have started implementing or considering the implementation of wireless LANs because of their ease of use, relatively low cost, and versatility, with little regard for security. If your company is among those seeking wireless-networking solutions, then there are some considerations that should be made.

The scenario: Your company has just started using wireless networking solutions before doing their homework. It's easy, it's fast, and most importantly, it's cheap. Time was an issue, and this had to be done yesterday. Audit didn't even know about it, and IT gave it to the "newbie" to take care of. Management has spent hundreds of thousands of dollars on intrusion detection and firewalls so the network must be safe. If an attempt is made to hack the network the IT staff will get all kinds of alerts and pages. In all the haste or because they wanted the extra speed that no encryption offers, the WEP was never turned on. Since everything is working fine, there is no need to go back and read those big bulky instruction books or cd-roms. IT can go back to putting out fires and getting Solitaire to work on the CEO's computer. A hacker has just heard about the new fad "war driving." It's easy, it's fast, and most importantly ? it's cheap. He drives by your company and picks up a signal. He flips a U-turn and is able to connect to your network and start hacking as if he were plugged into the network jack in the empty office down the hall. He can do this because your company isn't using WEP, and your DHCP server just gave him an IP address, domain name, and the IP address of the DNS, which he can now query to get a list of all the machines on the network. Let's start stealing information! Yes, it is that easy!

"Drive-by hacking" or "War-driving" is an exploding trend in the hacking community. All that is required to get started is a portable computer, a car, and a wireless LAN card. We have been conducting our own study of wireless networks in our local area of Southern California and those areas to which we travel on business in an attempt to see what the hype was all about (I have to say that I have become addicted to sniffing for wireless). We set up a portable computer with a wireless card and an antenna, and drove around the area at a normal speed, and discovered 459 wireless networks. Of the networks identified, only 24% were using the Wired Equivalent Privacy (WEP) that come with most, if not all, wireless hardware. WEP is a form of encryption that uses the RC4 algorithm. Wireless networking devices can use WEP to help protect the information being transmitted. Unfortunately, the default setting for most wireless network devices is, you guessed it, "NO WEP." If your company is not using WEP then anyone can sit in the parking lot of your building, jump on your network, and start probing the internal network as if they were sitting right next to you with a LAN cable plugged into your network. The really scary part about this is that you don't have to be a technical wizard to do this. There are even web sites that are listing wireless networks that people have discovered - your company could be one of them.

Your company may be vulnerable to a wireless attack even though wireless hasn't been implemented on the network. Access points are cheap and small and can be easily plugged into the network under test situations. A department or even another company building may have an access point for their area not realizing the exposure that they have created. There are tools that can be used to locate rogue access points and identify the SSID, MAC address of the device, the channel being used, the vendor name, and even if WEP is being used.

So the solution seems pretty easy, right? Just turn on WEP and everything is secure again. Not so fast! There are many lists of common and default WEP encryption keys posted on the Internet that are continually updated. If your company is using wireless networking you should make sure they are not using a vendor's key-generating program with an easy-to-guess pass-phrase. For example: the name of your company, the name of your wireless vendor, or the word "wireless," to name a few.

WEP crackers and 802.11 sniffers have also been developed running in both Windows and Unix. What does this mean to you? Even if you are using WEP, the chances of being hacked are still pretty high. AirSnort is a Linux based WEP cracker that passively grabs packets in mid-flight, and once it has enough packets (100 MB-1 GB), will crack the wireless encryption key in a few seconds. The process of collecting the required amount of useful packets, about 1 GB worth, can take some time on a wireless network that doesn't have much traffic. Remember though, an attacker only needs to leave a computer within range of your wireless network, unattended if they wish, until they get enough packets. Be assured that these programs will only become more efficient and faster as time goes on, greatly increasing the risk.

What can you do to secure a preexisting wireless network? Well, for the answer to this question, you have to sit down with the IT folks and brainstorm, use your networking imagination. Here are some ideas to help get those brain juices flowing.

1. Segment your wireless network from your wired network and use a VPN connection to access your wired network.
2. Use "end-to-end" encryption for wireless network traffic.
3. The use of directional antenna to minimize the signal from being sent out in every direction.
4. Don't use wireless networking solutions until the weaknesses have been remedied by the vendors; they are working on it as you read this article.

Consider the inherent security risks before implementing wireless. Are you and your company willing to allow an outsider to plug into your network and view your company's confidential files in the name of cost savings and ease of use? Do the benefits outweigh the major security risks? Can you effectively secure a wireless network using methods outside of WEP as discussed earlier? These are a couple of the questions that need to be answered before you and your organization implement wireless networking. If your company has already started using wireless networking, then you should make sure that, at a minimum, WEP is being used and that no unauthorized AP's are sitting on the network. A secondary form of "end-to-end" encryption should be researched and implemented immediately. Policies and procedures involving wireless networking should be developed, and employees need to be made aware of them. Securing your current wireless network should become a priority. If a hacker hasn't found your network yet, one surely will soon.

**The following audit program is provided for use for Canaudit clients. Should you have any questions, please call Chad, Paul, Chris, or Gordon at 805-583-3723.**

#### Wireless Audit Program Outline

##### 1. Design and Implementation

- A. Review the original configuration
  1. Identify the control over APs
  2. Detection of rogue wireless networks/APs
    - a. AP Map/Network Map (how much of the network is visible)
- B. Review the use of Encryption
  1. Level of encryption
    - a. Method of encryption (WEP, end-to-end encryption, SSH, SSL, IPsec)
  2. Security of encryption key (storage of hard copy)
  3. Encryption key change frequency
  4. RADIUS authentication

*Continued on page 4*

- C. Identify wireless integration to the wired network
  1. Segmentation, Firewall
  2. Use of VPN to separate WLAN & LAN
  3. Independent Networking
  4. Logical placement of hubs that integrate WLAN with LAN
  5. Logical placement of servers (can they be reached from WLAN)
2. **Change Management (are all areas covered?)**
  - A. Document change control mechanisms in the wireless environment
    - a. Determine if unauthorized changes have been made in the wireless environment
3. **Perform a range test to determine the effective transmission range with both a standard and an advanced antenna**
  - A. Determine the channel allocations
  - B. Identify adjacent WLAN overlap testing
4. **Document the principles and practices**
  - A. Written policies review
  - B. Vendor contract review
  - C. Employee security awareness regarding WLANS
  - D. Incident Response/Outages
5. **Wireless Network Penetration Test**
  - a. Perform a wireless penetration test
    - A. Identify the network segments that can be accessed
    - B. Determine if there are any controls to detect unauthorized connections to the network
    - C. Identify the level of encryption
6. **Server Authentication**
  - a. Determine the level of security of all servers that can be accessed from the wireless network
    - A. Review authentication controls on each of the servers
    - B. Determine if hacker tools such as CIS can be used on the servers and workstations.

---

**Handleman Company**, the leading supplier and merchandiser of music products for North America's leading retail chains and music labels is seeking a Senior Information Technology Auditor. The position entails independently conducting or supervising significant, broad scope and complex audits of information technology systems and procedures to assess the effectiveness of controls, accuracy of records, and efficiency of operations.

**ESSENTIAL DUTIES AND RESPONSIBILITIES** include the following. Other duties may be assigned.

- Examining systems and interviewing workers to ensure compliance with applicable laws and regulations.
- Participating in field audits of various business units, including analyzing policies and procedures relating to information systems, information security, operations functions, internal controls, and business processes.
- Conducting and documenting technical audits of mainframe, midrange, LAN/WAN and telecommunications systems.
- Participating on project initiatives and performing system development life cycle (SDLC)/conversion reviews to evaluate systems enhancements and development efforts.
- Analyzing data obtained for evidence of deficiencies in controls, duplication of effort, extravagance, fraud, or lack of compliance with laws, government regulations and management policies or procedures.
- Supervising, reviewing, approving the work of auditors, and preparing reports of findings and recommendations for management.
- Conducting special studies for management, such as those required to discover mechanics of detected fraud and to develop controls for fraud prevention.
- As necessary, participating on financial/operational related audit assignments.

### **QUALIFICATIONS:**

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily in a highly visible environment. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- Bachelor's degree in Information Technology, Accounting and/or Finance
- 3 - 5 years of proven public or internal informational systems auditing
- CPA, CISA or CIA is preferred
- Hardware/Operating system experience preferred: IBM mainframe/OS390, AS400, Unix, Sun Solaris, Windows NT and 2000, Novell, network infrastructure and desktop
- Software/Database experience preferred: Oracle database and ERP, Checkpoint firewall, ACL, ACF2, Bindview, supply chain software, EDI and MSAccess
- Financial/operational background is a plus in order to assess the impact of system implementations and changes
- Must be able to quickly assess risk within diverse company operations, establish audit review plans to efficiently and effectively evaluate the adequacy of related controls with minimal supervision
- Strong verbal and written communications and interpersonal skills are required
- Self-motivated with the ability to motivate others
- 25% Travel possible

Handleman Company offers a comprehensive benefits plan, including medical, dental, 401(K), pension, and merchandise discount on music products. We invite you to apply by sending your resume along with salary expectations to:

**HANDLEMAN COMPANY**

Human Resources/SIA • 500 Kirts Blvd. • Troy, MI 48084 • Fax: (248) 362-3656 • EOE

## Before-Dinner Presentation

### Audit Issues of IT Outsourcing

With the increasing role that third party providers are playing in an organization's IT environment, IS Auditors are faced with having to audit systems that are the responsibilities of other organizations. This presentation is designed to provide IS Auditors with an understanding of the risks associated with third party providers and suggested audit procedures that an IS Auditor could perform during an audit of systems that use third party providers.

Sander Wechsler is a Senior Manager with Ernst & Young, LLP in their Technology and Security Risk Services Practice. He is a current member of the ISACA Standards Board and past member of two AICPA Task Forces. He has spoken at the 1999 and 2001 North American CACS Conference, 1999 and 2000 International CACS Conference, 2000 AICPA, MIS, ISACA Business of eBusiness Conference, 1999 IIA General Audit Manager's Conference, 2000 MIS Conference, various IIA and ISACA chapter presentations, and 2001 MBA Internal Audit Conference.

## After-Dinner Presentation

### Security in Oracle Applications

Security is critical in all applications. Many vendors provide business solutions that require security and auditability. Jody Clayton will educate the audience at a high level on what security and auditing capabilities the Oracle e-Business Suite provides. During this presentation, topics such as LDAP, data encryption, roles, and Find Grain Security will be discussed in detail. At the end of the presentation, the audience should have a clear understanding of the capabilities delivered by the Oracle e-Business Suite as well as how Oracle achieves these high standards.

Jody Clayton obtained her Bachelors Degree from Central Michigan University, and MBA from Wayne State University. She has been a consultant at Oracle Corporation since November 1999. Her area of expertise is the technology that powers e-Business Suite. She was an Oracle DBA for four years prior to joining Oracle Corporation.

## Menu - November 14, 2001

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

- Entrée #1: London Broil
- Entrée #2: Raspberry Chicken
- Entrée #3: Broiled Salmon

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: New York Style Cheesecake
- 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.

## Drawing Winners

October 17 Monthly Meeting

Before Dinner

*Larry LaGrant*

*Joseph Ponnoly*

After Dinner

*Jim Joseph*

*Sharon Therrian*

## New members as of October 2001

Janet Kay Adkins

Nicholas J. Anson

Christopher Krapp

Charles Randall

Tina Redden, CISA

# *The Year At A Glance*

<b>Meeting Date</b>	<b>Before-Dinner Topic</b>	<b>After-Dinner Topic</b>
November 14, 2001 (Wed)	Audit Issues of IS Outsourcing	Oracle Application Security
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

**DATA BYTE**