

**OFFICERS AND DIRECTORS 2002-2003**

**PRESIDENT**

Carrie Schrader, CISA, CBM  
Handleman Company  
248-362-4400 ext. 358

**VICE PRESIDENT**

Mike Stolarczyk, CISA  
Jefferson Wells International  
248-350-3006

**TREASURER**

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

**SECRETARY**

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

**DIRECTORS**

Salman Aziz  
The Detroit Medical Center  
313-966-5155

Ed Barszcz, CIA, CFE  
Blue Cross/Blue Shield of MI  
313-225-9076

Gerald Baumgart, CISA  
Comerica  
248-371-7060

Patti Earl-Cole, CISA, CIA  
Blue Cross/Blue Shield of MI  
313-225-8577

John Hoppesch, CISA  
Kmart Corporation  
248-614-9975

Brenda Karl, CISA  
Jefferson Wells International  
248-350-3006

Michael Mullens, CISA, CIA  
General Motors  
cell 586-382-1543

Brandy Pfeiffer, CPA  
Federal-Mogul Corp  
248-354-2602

John Quaine II, CISA, CPA, CIA  
Blue Cross/Blue Shield of MI  
313-225-7663

Cyndi Shelton, CISA  
General Motors  
734-604-1797 cell

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

Sander Wechsler, CISA, CPA  
cell 313-492-6071

Karine Wegrzynowicz, CISA  
Ford Motor Company  
313-337-5796

**PAST PRESIDENTS**

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



*Information Systems  
Audit and Control  
Association*

***DATABYTE***

NEWSLETTER OF THE DETROIT AREA CHAPTER

VOLUME 17, #2

REGION 2, CHAPTER 8

OCTOBER, 2002

*Monthly Meeting*  
*Wednesday, October 16, 2002*

**Pre-Dinner Topic: "Audit/Control of an Oracle Database."**

**After-Dinner Topic: "Audit/Control of your Telecommunications Infrastructure."**

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

**Date: Wednesday, October 16, 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 will be taken by John Hoppesch. If possible, please make reservations by 4:00 pm Friday, October 11th, 2002. You can make your reservation online at [isaca-det.org](http://isaca-det.org) or e-mail your reservation to John Hoppesch at [jhoppesch@yahoo.com](mailto:jhoppesch@yahoo.com). If you do not have access to the Internet, call John Hoppesch at 248-614-9975 or fax your reservation to him at 248-614-0701. Please include your name, company, telephone number, and whether you are a Member, Non-member, Student or Retiree. Walk-ins are welcome, but the food selection may be limited.**

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

# Letter from the President

Dear Members,

I hope that everyone enjoyed the September dinner meeting. I would like to thank Mr. Zager from Plante & Moran LLP for the educational pre-dinner presentation on "Securing Your Wireless Network" and Special Agent Rytman from the Federal Bureau of Investigations for the informative after-dinner presentation on "A Perspective on Network Security and Cyber Crime/Terrorism Since 9/11." We are in the process of making arrangements with both speakers to obtain a portion or entire presentation to post to the chapter's website. Going forward we will continue to make these presentation available, wherever possible, on our website. Please watch the website at [www.isaca-det.org](http://www.isaca-det.org) for these new additions.

This month we have to exciting topics for our dinner meeting, "Audit and Control or Oracle Databases" and "Telemanagement Reporting: Gaining Efficiencies and Increasing Security." I hope to see all of you at the meeting. As a reminder, you can register through our website by selecting "Register for Next Meeting" from the home page.

As promised in the first issue, I would like to take a moment to give you some background on one of our committees. This month I would like to focus on the Programs Committee. The chairperson for this committee is your past-president, Art Abruzzo. He and several board members have worked to prepare an educational and informative program year. The committee is responsible for:

- Developing a program plan by 1) reviewing the prior years membership survey of requested topics, 2) reviewing significant industry issues, and 3) meeting with other organization leaders to obtain input on interesting topics for joint organizational meetings.
- Networking with companies to obtain high quality speakers to fulfill the program plan.
- Identifying potential educational materials that can be given to the membership such as books, certificates, etc.
- Working with the facilities committee to ensure all speakers needs are met.

If you would like to become involved with the programs committee, either now or in the future, I encourage you to contact Art or myself for further information.

As always, the board is here to serve the membership, if you have any suggestions on how to improve any of the programs that we offer or to provide a new program, please contact Mike Stolarczyk, myself, or any of the board members listed on the front page of this newsletter. We would be happy to help and look forward to hearing from you.

Carrie Schrader  
Chapter President

## Audit/Control of an Oracle Database:

Jamshid Sadaghiyani

In today's business environment, data is the most valuable asset for organizations. Over the last few years, the amount of data stored in databases has grown exponentially. The accessibility of this data has greatly increased the productivity of organizations as well as the security risks that they face. The security of the database is one of the most important, yet least talked about, issues that organizations face in implementing a database system.

The presentation explains how security works in an Oracle database management system and outlines Oracle security and integrity features; such as profiles, roles, procedures, constraints and triggers. It also discusses the Oracle auditing facilities.

Jamshid Sadaghiyani is a CISA and CPA. He holds a BS degree in Accounting, an MBA and is currently pursuing an MS in Computer Science. He is a Principal Information Systems Auditor for Blue Cross Blue Shield of Michigan and has more than 12 years experience in Information Systems, Financial and Operational audits.



# AVOTUS

## Information Systems Audit and Control Association

Marc Layne

Marc Layne is an Account Executive with Avotus Corporation. Prior to working with Avotus, Marc spent eight years with Verizon Wireless in several Sales and Sales Management capacities including Director of Business Sales in Michigan. Marc also spent a year with Nextel as Manager of the Corporate Account Sales Team in Detroit. Marc has a B.A. in Marketing from Michigan State University and an M.B.A. from Wayne State University.

Avotus Corporation is a world-class enterprise software company. The company is the global leader in its space, and has a premier client base that includes 42% of the Fortune 100 and 28% of the Global 500. Avotus solutions help reduce costs, provide better service to customers, enhance employee productivity and reduce security risks.

Telemanagement Reporting:  
Gaining Efficiencies and Increasing Security

- \* Call Accounting including: cost allocation, bill reconciliation, and reporting
- \* Corporate Directory-LDAP compliancy
- \* Alarms
- \* Security
- \* Traffic Management
- \* Internet and E-Mail Accountability

## CHECKMATE!

By Chad Parks, Canaudit Inc.

Information security is much like a game of cyber chess with enormous potential consequences for the loser. These consequences include jail time and heavy fines for the hacker while businesses face the theft of confidential information and embarrassment with the potential for multimillion-dollar losses in damages. In addition, there is the cost of security officers and cyber forensics specialists, such as Canaudit, to investigate the incident. Hackers always seem to be several moves ahead of IT Security in the big game of cyber chess, resulting with hackers, more or less, controlling the board. Every time a new vulnerability is identified, hackers exploit it, and IT finds a way to secure it. Then hackers find two more new vulnerabilities, and so on. Occasionally, a hacker may get caught behind enemy lines, and for a short time the roles are reversed. The hacker then unwillingly and unknowingly becomes the prey, and the IT security group hunts them and attempts to collect the required evidence to prosecute. The problem is that this doesn't happen enough, and by this time, the damage is usually already done. The risks and consequences of losing are much greater for the business than for the hacker. Reactive security alone is not going to win the big game of cyber chess. However, the right combination of reactive and preemptive security will greatly improve our odds.

So, why does the IT security group assume the role of the underdog? Because IT security and audit have too many hurdles to jump before a security enhancement can be implemented to correct known vulnerabilities. Each hurdle equates to more time for the hacker to plan his next move. We all know these time-consuming hurdles very well. They include waiting for the vendor to release a patch, testing the patch in the test lab, audit review, management approval, and, eventually, the transfer into production. Meanwhile, hackers perfect the exploitation; writing code so that less technical "script kiddies" can exploit the vulnerability and possibly create a worm that will do all the work for them on a global scale. They also start modifying the exploit in anticipation of the vendor patches. The hackers are always several steps ahead. If we continue to make use of strictly reactive information security, we are providing hackers with the ability to manipulate the next move of IT security as a whole.

From the moment a new security hole is identified and posted on the Internet, it is a matter of minutes before hackers from all over the world begin exploiting it. On the other hand, it can take weeks or sometimes months from the time a new vulnerability is identified for the vendor to patch it, and even longer before the patch is actually implemented in the production environment. A recent article written by Bob Sullivan, msnbc.com, discusses a test that was conducted where Dan Clements of cardcops.com posted fake credit card numbers on the Internet. Within 15 minutes, 74 credit card thieves from 31 countries had viewed the credit card numbers. By the end of the week, over 1,600 credit card thieves from 75 countries had viewed the numbers (the full article by Bob Sullivan can be read here at:

<http://www.msnbc.com/news/739128.asp?0dm=C227T#BODY>). New Internet security vulnerabilities travel just as quickly or, perhaps, even quicker than credit card numbers. When it takes only minutes for a new security vulnerability to spread across the world, whereas it usually takes months before a patch is finally installed, it is no wonder that the hackers are almost always several steps ahead of us. It doesn't take rocket science to figure that one out.

During the time it takes to implement a new security patch into the production environment, a good hacker may have created several backdoors into your system and possibly installed a rootkit making it next to impossible to detect him or her. This can be a relatively simple process, as you can see from the excerpt below:

- A hacker hears about a new buffer overflow vulnerability that someone else has posted on the Internet, along with the some code to help other, less sophisticated hackers exploit this new vulnerability.
- A buffer overflow, very simply put, allows an attacker to execute a command on a target system by feeding the system, or buffer, more information than it was designed to handle. When this happens, the information that is in excess of what can be handled spills over and ends up being processed resulting in the ability for an attacker to execute arbitrary commands on the target system.
- The hacker then runs this new buffer overflow vulnerability against your web server giving him the ability to run a command.
- The hacker then runs a "GET" command using FTP or TFTP at the end of his buffer overflow, which will transfer a small backdoor onto the target system from his or her remote system or perhaps a mirror site that has been set up earlier.
- The hacker then must execute the back door, so he launches the buffer overflow again. This time he forwards a command that will launch the back door that he has just transferred.
- Next, the hacker will connect to your server using the back door that he just pushed over and will execute and attempt to do several things:
  - Create another backdoor
  - Attempt to escalate his privileges
  - Harvest some information
  - Map out the systems on the Internal network or DMZ
  - Hide his trail by manipulating logs and access dates
- At this point, the hacker may decide to fix the original buffer overflow vulnerability that got him on the web server so that other hackers cannot attempt to steal his glory. Keep in mind that the hacker still has a newly created backdoor on to the system.

- This is where we separate truly evil hackers from a hacker who is just out to have some fun. At this point, a truly evil hacker will install a rootkit on the target web server. Once the hacker has installed a rootkit, he truly owns the web server.

- A rootkit can allow the hacker to take over system programs and replace them with modified system programs that hide and lie about everything involving the attack; including logs, processes that are running, creation dates, and even who is currently logged on. If you have a rootkit running on your system, it would be very difficult to detect, as the system appears to be running as it should. The hacker could control even the anti-virus software by providing you with false reports or not even reporting viruses at all.

## CHECKMATE!

You may think, “oh well, that’s okay, because I have a firewall protecting my web server”. That is great; you are on the right track; BUT your firewall doesn’t stop port 80 http. This is the port that your web site requires in order to function properly on the Internet. Countless buffer overflows can be run by simply inputting a malformed URL at the end of your website address or by taking advantage of some poorly written HTML code.

Some firewalls offer signature checking to prevent this type of buffer overflow attack. This is where the firewall examines the data packets being sent to the server for known attacks. The firewall compares the information within the data packet to a database of known attack signatures to see if they match. As more attacks are identified, more signatures are created and uploaded to the firewall, much like anti-virus software is updated with new virus definitions. Unfortunately, hackers have found a way around these types of firewalls. They have tools that will break up data packets or fragment the packets. They also have tools that will tear apart code and reassemble it so that its signature or appearance is completely different but will function exactly the same. In fact, a new tool was released April 24, 2002 called Fragroute that will automatically modify packets that an attacker is sending. The impact of this is that a hacker could have a buffer overflow written 100 different ways or more, making it impossible for a firewall or IDS (Intrusion Detection System) to detect. This is commonly known as a polymorphic buffer overflow and is very difficult to protect against.

So, how do you protect your systems and servers from such attacks if every time you take a new security measure, the hackers develop a new counter measure, just like in the game of Chess? Firewalls and IDS are great, but you can also eliminate one of the hacker’s number one advantages, the advantage of time. When a new security patch is released, it should be implemented as soon as possible. It is up to you and your company to determine how fast “as soon as possible” is. When determining this, remember what I mentioned earlier in this article about how quickly information spreads. It may only take minutes for a hacker to compromise your systems. Obviously, it will take more than minutes to test a new security patch, but a determined effort should be made to test the patch as quickly and as accurately as possible. Don’t put security

patches on the back burner, or your company may end up on the receiving end of a Checkmate!

With that said, there are 10 new security vulnerabilities that you should be aware of if you are using Microsoft IIS 4.0, 5.0 or 5.1. Don’t feel left out if your not using IIS; there are probably some out there for your web server too. If not, there will be soon! Microsoft has been notified of these vulnerabilities and has identified them in MS020-018, dated April 10, 2002. They developed a patch that should be installed immediately. Click the URL below for the information required to fix these vulnerabilities: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-018.asp>

The hackers know all about them and are using them right now. It’s your move...

The opinions in this article are mine alone. I invite your comments. Please email me at [Chad@canaudit.com](mailto:Chad@canaudit.com). I will read your comments and respond to them, usually within 24 hours.

---

**Congratulations to the following ISACA members for successfully passing the CISA exam this past June. The CISA certification is widely recognized and very prestigious. This is an achievement to be proud of!!**

Janet Adkins	William Johnson	Donna Shuart
Kathleen Allour	Michael Juchno	Clayton Snyder
Diane Baker	Lisa Keller	Diana Sobczak
Kimberley Coyner	Neil Lindholm	Andrew Tanner
Lorraine Davis	Theresa Mazur	John Vadalabene
Scott De Mea	Erin McNitt	James Watson
William Gregg	Rachelle Miller	Philip Yanick
Christopher Hickson	Kenneth Murray	
Stephen Irvine	Randy Oliver	

**Congratulations to the following non-members awarded CEP Memberships, who also passed:**

Shannon Herbst	Amine Houari
Rajesh Nayak	Sukanya Rangarajan
Linda Scibilia	Michael Stokes

\* Please note \* This list EXCLUDES individuals that requested their exam results NOT be released and/or who have not paid exam related fees.

## *Career Opportunities*

*Handleman Company, the leading supplier and merchandiser of music products for North America's leading retail chains and music labels is seeking a Senior Internal Auditor.* The position entails independently conducting audits of 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 financial/operational audits of various business units, including analyzing policies and procedures relating to operations functions, internal controls, and business processes.
- Responsible for preparing benefit plan financial statements for review by management and independent accountants.
- Participates in consulting projects to give guidance and provide review on operational and financial controls. 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.
- 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.

**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 Accounting and/or Finance
- 3 - 5 years of proven public or internal auditing experience
- CPA or CIA is preferred
- 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 product. We invite you to apply by sending your resume along with salary expectations to:

**HANDLEMAN COMPANY**

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

*CISM, the Certified Information Security Manager* is ISACA's new certification and is specifically geared toward experienced information security professionals. CISM is business-oriented and focused on information risk management while addressing management, design and technical security issues at the conceptual level. It is for the individual who must maintain a view of the "big picture" by managing, designing, overseeing and assessing an enterprise's information security. The Detroit Chapter ISACA board will bring you more information as it becomes available; however, you may access the ISACA International website at [www.isaca.org/cert1.htm](http://www.isaca.org/cert1.htm) for the information that is currently available.

**ISACA announces the 2003 Certified Information Systems Auditor Examination on June 14th 2003.**

The only globally recognized certification program for information systems audit, control and security professionals announces it's next examination. For the 22nd consecutive year ISACA will administer the Certified Information Systems Auditor (CISA) Examination. The 2003 CISA Examination will be conducted on Saturday, June 14, 2003, and will be offered at more than 180 international test centers in 58 countries. The exam composed of 200 multiple choice questions, will be held in one four-hour session. The 2003 CISA Examination will be offered in ten languages.

The exam covers the following process and content areas: 1) The IS Audit Process; 2) Management, Planning and Organization of IS; 3) Technical Infrastructure and Operational Practices; 4) Protection of Information Assets; 5) Disaster Recovery and Business Continuity; 6) Business Application System Development, Acquisition, Implementation and Maintenance; 7) Business Process Evaluation and Risk Management.

This international certification program grants the title of Certified Information Systems Auditor (CISA) to candidates who achieve a passing score on the examination and demonstrate five or more years experience in the information systems auditing, security, or control professions.

The CISA designation is widely recognized as a professional standard of excellence. More than 23,000 specialists in Information Systems Auditing Security and Control have earned the designation worldwide.

A Candidates Guide to the CISA Examination, the 2003 CISA Review Technical Information Manual, the 2003 CISA Review Questions, Answers and Explanations Manual, the CISA Review Questions, Answers and Explanations 2003 Supplement and the CISA Review Questions, Answers and Explanations CD\_ROM are available from ISACA to help candidates prepare for the exam. Detailed information can be obtained from ISACA by phone at 1.847.253.1545, Certification Department, by fax at 1.847.253.1443, or by e-mail at [certification@isaca.org](mailto:certification@isaca.org).

The Detroit Chapter will once again offer a CISA Examination Review Course. Please watch future issues of the Databyte and website, [www.isaca-det.org](http://www.isaca-det.org) for further details.

## The Year At A Glance

October 16, 2002	Audit/Control of an Oracle Database	Audit/Control of your Telecommunications Infrastructure
November 20, 2002	Auditing Servers	Auditing Servers cont.
December 11, 2002 (IIA)	Computer Incident Response Team	To be determined
January 9, 2003 (CFE)	No presentation	To be determined
February 19, 2003	CISA Roundtable	Virus Protection
March 19, 2003	To be determined	To be determined
April 16, 2003	Risk Analysis/Audit Planning	Single Sign-on Solution
May 21, 2003	Auditing Windows 2000	E-Business System Development

The 4th Annual Spring Conference dates for 2003 have been set. They are March 24, 25 and 26, 2003.  
(Co-sponsored by the Detroit Chapter of the IIA and Detroit Area Chapter of ISACA)

### Menu - October 16, 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 Beef Stir-Fry  
Entree #2 Raspberry Chicken  
Entree #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: Key Lime Pie
- 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 John Hoppesch at (248) 614-9975. Your cooperation is greatly appreciated.

### Monthly Drawing Winners!!

Steve Erwin - Borders Group, Inc.  
John Williams - Echelon Technologies  
John Duke - BCBSM  
John McCormick - DMC

# DATA BYTE

DETROIT AREA CHAPTER  
P.O. BOX 4297  
TROY, MICHIGAN 48069-4297

Information Systems  
Audit and Control  
Association

