

**OFFICERS  
AND  
DIRECTORS  
2008-2009**

**PRESIDENT**

Jamshid Sadaghiyani, CISA, CPA  
Delphi Corporation  
248.813.3258

**VICE PRESIDENT**

Susan A. Yamin, CPA  
Comerica, Inc.  
(313) 222-7730

**TREASURER**

Richard A. Morris  
Comerica Bank  
248-371-4505

**SECRETARY**

Douglas S. Wahr, CISA, CISSP  
The Auto Club Group  
(313) 436-7277

**DIRECTORS**

Edward R. Barszcz, CIA, CFE  
Consultant  
(313) 278-3915

Henry Danowski, CGEIT, CISA, CISM,  
CISSP  
Jefferson Wells  
(313) 399-2662

Michael A. Forrest, CISA  
Jefferson Wells  
(248) 226-1269

Brandy A. Hanna, CISA, CPA  
Federal-Mogul Corporation  
(248) 354-2602

Michele Haroon, CPA, CISA  
Accretive Solutions  
248-643-9480

M. Siobhan Jordan, CISA  
Lafarge North America Inc.  
(248) 447-2621

Brenda L. Karl, CISA  
Accretive Solutions  
(248) 633-2347

Nikhil Kothari, CISA, CPA, CA  
Blue Cross Blue Shield of MI  
(313) 225-8685

Donald K. Ledwith, CISA, CISSP  
HOV Services, Inc.  
(248) 837-7375

D. Robert Okopny, Phd, CIA, CFE  
Eastern Michigan University  
(734) 487-0246

Carrie Schrader, CISA, CBM, CFE  
GMAC Financial Services  
(313) 656-67621

Charles A. Silva, CISA  
General Motors Corporation  
(313) 665-3738

Jason A. Thompson  
KPMG LLP  
(313) 230-3371

James M. Watson, CISSP, CISA, CIA  
Ford Motor Company  
(313) 594-0609

Manish Zaveri, CISA, CPA  
Delphi Automotive  
(248) 813-6820



**Detroit Chapter**

VOLUME 23, #3

REGION 4, CHAPTER 8

November 2008

*Monthly Meeting*

*Wednesday, November 19 2008*

**Pre-Dinner Topic: Auditing IT Governance from the Banking Perspective**

Owen Rockentine  
Comerica

**After-Dinner Topic: Cyber Crime and Cyber Threats in the Information Age**  
FBI

**Date:** Wednesday, November 19, 2008

**Time:** 4:30 – 5:00 Registration & Networking  
5:00 – 6:00 Pre – Dinner Presentation  
6:00 – 7:00 Dinner  
7:00 – 8:00 after Dinner Presentation

**Location:** University of Michigan – Dearborn Fairlane Center North  
(See map and directions on page 7)  
19000 Hubbard  
Dearborn MI 48126  
(248) 356-5602

**Cost:** **Advance Registration:**  
\$25.00 Members  
\$35.00 Non-Members  
\$10.00 Students and Retirees

**Make reservation at [www.isaca-det.com](http://www.isaca-det.com).**

**Advance registration ends at midnight Saturday, November 15.**

**Members & Non-Members making reservations after the reservation deadline will be charged an additional \$10.**

**Walk-ins, excluding Students and Retirees are subject to the late charge.**

### *A Word from the President*

Dear Members:

I hope everyone enjoyed two excellent presentations that Mr. Mike Cherry from GM and Ms. Terri Coppens from Control Solutions presented at our October dinner meeting. Both presentations were very informative and elicited some very interesting dialog around the tables. I hope you'll join us for our next meeting. We'll have two distinguished speakers, Owen Rockentine from Comerica and a Special Agent from the FBI. They'll discuss IT Governance and cyber crimes. I am sure you'll enjoy both presentations.

As I mentioned on my last month message, in addition to our regular monthly meeting, we'll offer a two days COBIT Foundation course in November. The course will be an interactive, classroom-based learning experience and will explain the elements and supporting materials of the COBIT framework in a logical and example-driven approach. The course has been well received by our members and more than 60 members have signed up for the course so far.

I also wanted to remind all of you that the 2009 Member-Get-A-Member (MGAM) Campaign is underway and will continue through 29 April 2009. I think this a great opportunity for all of us to share the benefits of ISACA membership with our colleagues, while also earning a chance to win one of the following prizes.

- **GRAND PRIZE (US\$ 1,000)**—For the member who recruits the most full-dues\* paying new members;
- **SECOND PRIZE (US\$ 500)**—For the member who recruits the second highest number of full-dues\* paying new members,
- **RANDOM DRAWING (US\$ 500)** — One randomly selected winner will be chosen. Each member will receive one entry in the drawing for each full-dues\* paying new member recruited.

Please feel free to contact Megan Moritz (at [mgam@isaca.org](mailto:mgam@isaca.org)) if you have any questions or concerns.

Also, we are into November and time is running out for those of you who still want to be grand fathered as a CGEIT. As indicated in the ISACA's International

recent email, you have until December 31, 2008 to take advantage of the CGEIT window for grand fathering. More than 1000 individuals have applied for this one-time opportunity so far. If you are interested, please visit [www.isaca.org](http://www.isaca.org).

Again, as I mentioned on my previous messages, we are constantly looking for feedback on how to improve our processes, and bringing value to our Chapter members. If you have any questions, concerns, or suggestions, please contact myself, or any of the Board members listed on the front page of this newsletter. I look forward to hearing from you.

Best regards,  
Jamshid Sadaghiyani

### Chapter News:

#### Grandfather Application Deadline Extension

Demand for CGEIT (Certified in the Governance of Enterprise IT) has been impressive. During 2008 ISACA has certified more than 1,000 CGEITs! Due to overwhelming response, the application deadline for certification under the grandfathering provision has been extended to 31 December 2008.

CGEIT certification is available to a wide range of IT governance related professionals. If you perform any of the activities below, you may be eligible for certification:

- \* Audit/Assurance -- Advise on industry accepted practices and frameworks to improve IT Governance
- \* IT Management -- Manage the enterprise architecture, including infrastructure and applications
- \* Project Management -- Manage IT-enabled investment portfolios through their useful asset life cycle
- \* Consultancy -- Develop IT and IS strategic plans and control frameworks
- \* Information Security -- Integrate information security into enterprise IT governance
- \* Risk Management -- Oversee the development and consistent application of the risk management framework
- \* Executive Management -- Oversee the development and maintenance of the IT strategic plan

For more information on grandfathering requirements or to obtain an application, please visit [www.isaca.org/cgeitapp](http://www.isaca.org/cgeitapp). Act today before the grandfathering opportunity expires!

Should you find that you do not meet the grandfathering work experience requirements, consider the CGEIT

exam. Achieving certification by passing the CGEIT examination and submitting an application for approval requires fewer years of work experience than under the grandfathering provision. The next exam offering is June 2009 and corresponding updates will be posted in December at [www.isaca.org/cgeit](http://www.isaca.org/cgeit).

If you have any questions, please send e-mail to ISACA's Certification Department at [certification@isaca.org](mailto:certification@isaca.org).

### **November Meeting Location.**

The meeting will be held in the Quad E Room, North Building. It is the first room to the right in the first aisle past the receptionist desk.

### **New Administrator**

Many thanks to our new chapter administrator, GERALYN JARMOLUK. She assembled the Newsletter this month and will be taking over as editor. Mike Forrest will still be a contact and will be responsible for membership but will take a much less active role in the newsletter. This will be very good news to the many of you that have spotted my many errors. Welcome GERALYN.

### **Cvent Registration Software**

Finally, this month we are switching over to our new registration software, Cvent. We, the board, think you will like its many features. Eventually (as we become familiar with it) the Newsletter will be sent out via Cvent. Also, once your general information is entered, Cvent securely stores that data so that the next time you register for a meeting, your data is all filled in ready for you to accept or change. Those of you that signed up for the Cobit class used Cvent. AND many thanks for the time and sacrifice of Brandy Hanna to get Cvent working. Thanks Brandy!

## **PRE-DINNER INFORMATION**

### **Pre Dinner Subject:**

#### **“Auditing IT Governance from the Banking Perspective”**

The presentation summary was not available at time of publication. It will be posted on the web site when available.

### **The Speaker:**

#### **Owen Rockentine. CISA**

Owen is a Vice President and IT Audit Manager in the Comerica Service Company Audit Team. Owen originally joined Comerica in 1982. He has held various positions within Internal Audit from Audit Programmer to IT Auditor. Owen joined Comerica Mortgage in 1997 as their Technology Manager where he was responsible for day to day processing, a help desk and systems development. In 1998, he joined Comerica's IS department as Vice President in the newly formed desktop area. Owen enjoyed a short sabbatical from 1998 until 2000 when he joined AAA as their IT Audit Manager. Owen returned to Comerica in his current position in 2001.

Owen is a CISA and is active in the Detroit chapters of ISACA and the IIA. He is also on the Academic Advisory board of Oakland University. In his spare time, he enjoys spending time with his wife and three daughters. He also enjoys golfing and anything outdoors.

Owen holds a Bachelor of Science degree in Computer Science from Oakland University.

## **AFTER DINNER INFORMATION**

### **“Cyber Crime and Cyber Threats in the Information Age”**

A special agent from the FBI will cover the following topics:

- Cybercrime trends and traits
- State sponsored hacking
- Cyber Terrorism

### **The Speaker:**

We are pleased to have a Special Agent from the Federal Bureau of Investigations in Detroit to speak on the above topic. The gentleman has 5 years of experience with the FBI working on cyber crime investigations. Prior to joining the FBI, he has worked in the IT field.

## Year at a Glance

<u>Date</u>		<u>Topic</u>	<u>Speaker</u>	<u>Company</u>
<b>September 17th</b>				
	Pre Dinner	SQL Injection Vulnerability	Steven Fox	General Motors
	After Dinner	Records Management and eDiscovery	Daniel Quealy	E&Y
<b>October 15th</b>				
	Pre Dinner	Vulnerability Assessments	Mike Cherry	General Motors
	After Dinner	Automated Internal Audit Environments	Terri Coppens	Control Solutions
<b>November 6th &amp; 7th</b>				
		Cobit Training		
<b>November 19th</b>				
	Pre Dinner	Auditing IT Governance from the Banking Perspective	Owen Rockentine	Comerica
	After Dinner	Cyber Crime and Cyber Threats in the Information Age	Special Agent	FBI
<b>December 9th</b>				
(Joint Meeting	Pre Dinner	XBRL		KPMG
with IIA)	After Dinner	Mobile Commuting	Bill Fryberger	Deloitte
<b>January 21st</b>				
(Joint Meeting	Pre Dinner	Road map to Prevention and Detection	Bill Hardin	Protiviti
with ACFE)	After Dinner			
<b>February 18th</b>				
	Pre Dinner	IFRS - Financial Perspective	Laura Buckley	KPMG
	After Dinner	IFRS – IT Perspective	Todd Markus	Accreative Solutions
<b>March 18th</b>				
	Pre Dinner	Is Your Organization Confidential Data For Sale Online?	Kathy Ossian	Miller Canfield
	After Dinner	Business Continuity Management	Daniel Berger	Jefferson Wells
<b>April 15th</b>				
	Pre Dinner	MFGPro/QAD	Deepti Talwar	E&Y
	After Dinner	IT Outsourcing	Jackie Slaga	PwC
<b>May 20th</b>				
	Pre Dinner	JDE	Jacqueline Walker and Lauren Nalu	Deloitte
	After Dinner	Wireless Hacking		Rehmann Group

## **The Detroit Chapter of ISACA**

### **CISA & CISM EXAM REVIEW CLASSES**

The Detroit Chapter of ISACA is pleased to announce it's semi-annual CISA and CISM review classes. The classes will be held simultaneously at the Blue Cross Blue Shield of Michigan Southfield Campus. The review class consists of 6 sessions (5 Tuesday evenings and one all day Saturday).

The fee for the entire review is \$100 per person

**Registration** is via the web site [www.isaca-det.org](http://www.isaca-det.org) under the event CISA Exam Review Class or CISM Exam

**Where:** **Blue Cross Blue Shield of Michigan, Southfield Campus**

Directions will be provided upon registration

<b>When:</b>	<b>Tuesday, October 28</b>	<b>6:00 p.m. to 9:00 p.m.</b>
	<b>Saturday, November 1</b>	<b>8:00 a.m. to 5:00 p.m.</b>
	<b>Tuesday, November 11</b>	<b>6:00 p.m. to 9:00 p.m.</b>
	<b>Tuesday, November 18</b>	<b>6:00 p.m. to 9:00 p.m.</b>
	<b>Tuesday, November 25</b>	<b>6:00 p.m. to 9:00 p.m.</b>
	<b>Tuesday, December 2</b>	<b>6:00 p.m. to 9:00 p.m.</b>

NOTE: chapters may not be covered in sequence; a schedule of subjects covered and dates covered will be published in early October. Verification of registration will be sent within a week of registration.

A box lunch and beverage will be provided for each session.

(Advertisement)



**GLOBAL  
CONSULTING**

"Innovative Executive Search & Staffing Solutions"

***Elevating the careers of ISACA members since 1998***

### **Current Opportunities**

**IT Audit Manager** - up to \$120K, up to 35% travel, international automotive company  
**IT/SoX Compliance Senior** - up to \$90K, limited travel, non automotive Mfg. organization  
**SAP Senior Security Analyst** - up to \$95K, ZERO travel, non-automotive mfg. organization  
**IT Audit Staff/Senior Professional** - up to \$85K, up to ZERO to 40% travel, various organizations including public accounting with regional and national CPA/Consulting firms

**National opportunities also available**

*Please call for a confidential career consultation  
and evaluation of your resume*

**[www.globalrecruiters.com](http://www.globalrecruiters.com)**

**Arthur Gluzman - Managing Partner**

arthur@globalrecruiters.com

248-489-1900 (ph)

248-390-5598 (cell)

# Canaudit Perspective

October 2008  
Volume 9, Issue 2

**DATA MINING: HOW HACKERS STEAL SENSITIVE ELECTRONIC INFORMATION**



Since my very successful presentation on data mining personal information at a recent conference, I have had several people contact me to convert the presentation into an article. This edition of the Canaudit Perspective presents the main items in the presentation in written form. Obviously the live, hands-on demonstrations cannot be

presented here, but the techniques can certainly be explained. At the conference, we offered a significant discount for performing a Canaudit IT Security Baseline or a Network Penetration Test. At the end of this article, I will provide details of the significant discount off our normal price for a basic 360-Degree IT Security Baseline. Now onto the article:

There are six main objectives of this article that coincide with the six processes the hackers use to gain access to and copy sensitive electronic information. These are as follows:

- How do hackers gain access to the network?
- How do hackers avoid detection, even if there is an Intrusion Detection System or Intrusion Prevention System implemented?
- How do hackers identify or catalog the machines in the environment?
- How do hackers identify and target sensitive data?
- How do hackers compromise databases and take sensitive data?
- How do they implement a firewall breach so they can return at will from the Internet?

**GAINING ACCESS TO THE NETWORK**

Most organizations have public areas. As many of you know from my classes, breaching physical security is relatively easy. A few days of observation usually give me the ability to exploit flaws in the organization. Often times I just walk in, find an empty desk, conference room, or office and plug in. If I am asked any questions, I just say that I am an auditor. In every case where I have used this technique, I have been left alone to work. At each location, I have been able to identify a workspace, set up a computer, and start working on defeating the network security. Physical security is very difficult to implement in many organizations, as often parts of a facility, district, or regional office are open to the public. It is up to the employees to be aware of unusual activity and report it. Awareness training and a well established hotline for security events are a must.

Another access point is poorly secured wireless networks. During many of our audits we have sat in the parking lot and gained access to the wireless network and the internal network. Unencrypted and poorly secured wireless is still an issue at some organizations. Certain industries, such as hospitals, are worse than other industries and organizations as some have not identified wireless as a risk and have not taken the necessary steps to secure it.

While the internal network at an organization may be secured, it is often possible for an insider to set up an unauthorized wireless network. The equipment can be purchased from Best Buy for \$40, plugged into the network, and be used by anyone within broadcast range. It is critical that regular wireless sweeps be conducted to identify rogue and poorly secured wireless networks.

Hackers may also be able to compromise the Virtual Private Network (VPN) that may connect both external and internal users to the network. This results primarily from poorly secured network devices, the use of default accounts and passwords, and the failure to use two-factor authentication (RSA SecurID or other mechanisms). If the VPN is “hacked” from the Internet, the hackers may have a high-speed

connection to the internal network. Poor controls over webmail may provide hackers the leverage to gain access through the VPN. It is best to provide SecurID tokens or other two-factor authentication to secure the webmail application. Once these devices have been purchased for use on webmail or for external connection through the VPN to the internal network, why not go one step further? Use the tokens for access to the internal network where possible.

We have some clients who have successfully implemented two-factor authentication. There are always concerns that tokens will impede the ability of users to log in, particularly in an emergency. By selecting the correct methodologies and working with staff, these hurdles can and have been overcome.

The last major entry point is poorly secured trading partners that connect to the network. Often these partners have networks that connect to other organizations. This makes understanding all of the access points to the network very difficult indeed. This risk could be compounded if the trading partner does not meet or exceed your organization’s security standard. If the partners’ network is compromised by hackers, then it may be possible for the hackers to view and possibly migrate their attack your network. Compounding this risk, trading partners often connect to many other trading partners. A hacker can take advantage of a poorly secured trading partner network and may be able to compromise several organizations networks from the same breached partner network. Some of our clients have mitigated this risk by requiring partners to meet the minimum standard before connecting to the organization’s network. If they cannot meet or exceed the standard, they cannot connect their network to the network. Instead they come in with a secure Virtual Private Network connection, with very little or no access to the internal network.

#### HOW HACKERS AVOID DETECTION

For many organizations, an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) is considered a luxury that the organization cannot afford. As a result, they have no ability to detect a hacking attack during the early stages, isolate the activity, and investigate the incident. Without an IDS, the scale is dramatically tipped toward the hacker. Without an IDS or IPS, there is very little defense against even a novice hacker attack. Experienced hackers will be able to gain access to the network, identify personal information and trade secrets, and capture a copy of it within one to three hours. In an unprotected network, our teams often have complete administrative access to the Active Directory and the Windows domains within an hour.

**Canaudit, Inc.**  
AUDITS • SEMINARS • CONSULTING

© 2008 1376 Erringer Rd, Simi Valley, CA 93065 • PH: (805) 583-3723 • FAX: (805) 582-2676 • [www.canaudit.com](http://www.canaudit.com)

If a network does have an IDS, a knowledgeable hacker has several techniques they can use to avoid detection. The first is to avoid broad network scanning. Most IDS’s pick up multi-port scanning as a serious threat. To avoid scanning, a hacker can use the “net view” command from a command prompt. This command, when directed against a domain, provides the hacker with a list of all of the machines connected to the domain. Using this list, they do not have to scan the network. Instead, they can launch a low-level attack against these machines, identify the poorly secured machines, and gain administrative right to those machines. We teach auditors and security staff to use the same tools at our IT Audit and Security Boot Camp. The best way to secure the network is to test it with the same tools that the bad guys use and then implement the required security.

Hackers defeat an IPS by masquerading as devices that are normally excluded from IPS monitoring. These include printers, video conferencing devices, and Voice over IP (VoIP) systems. These types of systems are excluded as they normally create a large volume of false positives or alarms. These false alarms result in investigations that divert security staff from directing their efforts to real attacks. Our philosophy is to properly configure the IPS so that the false alarms are minimized. Management needs to recognize that this will take a significant manual effort by the security folks, so it must be staffed and funded properly.

Clearly, a properly configured IPS or IDS is an essential component in a security package. They work in conjunction with other controls to ensure the early detection and investigation of hacking attempts.

#### CATALOGING THE ENVIRONMENT, IDENTIFYING TARGETS

There are many ways to document or catalog the network. In our normal network audits, we use tools that work quickly, but are easily detectable. Hackers, on the other hand, want to remain undetected as long as possible. Once they have connected to the network, there are several approaches they can use to avoid detection. The first is to use a simple scanner such as Solar Winds IP Browser. Most IDS’s are configured to ignore simple network management protocol (SNMP) scans as many network management tools use this service. Using Solar Winds, many of the devices in the network can be identified. Naming conventions for machines may reveal the nature of the information on the machine. A machine with a name of Psoft most likely hosts the PeopleSoft application. Other names we often see are Lawson, McKesson, and Cerner. Once the machines are identified, it is a simple matter to determine if known exploits have been patched.

In some organizations, patches are often not applied due to concerns about the impact on the application. As a result, we can normally get onto these unpatched systems and harvest sensitive files. One of the easiest files to harvest is the database backup file. Whether the database is Oracle, DB2, or Sybase, the backup files are generally world readable. This means that anyone who can get onto the system can capture a copy of the backup. It is a simple matter for the hacker to import the backup into a database on one of their own systems. They now have a fully accessible copy of all of the data in the database.

There are two lessons here. The first is to ensure that all machines are properly patched. If there is some uncertainty that a critical application will run after the patch is implemented, then take an image of the machine and load it onto a test server. Then apply the patch, and run full testing of the application. If it continues to perform well, then the patch will likely not cause any harm. Take another image of the production system, and then apply the patches to production during a low-volume period, such as over night. If the machine fails, restore from the image and resume normal operations. Machines that absolutely cannot be patched should be isolated behind an internal firewall so that hackers cannot access them. If you cannot remediate an issue, then isolate it on a protected network segment.

The second lesson is that backups should not be world readable. Modify the backup procedure so that any time a backup is created, the file permissions on the backup file restrict access to only a few people. These people would be the ones who would restore an application after a process interruption or failure.

Another way to quickly find databases is to use a scanner such as SuperScan and set it to only scan for specific ports. The Oracle listener port is TCP port 1521. By setting the scanner to only locate the listener, the attacker can minimize the likelihood of being detected, while quickly identifying the Oracle databases. Our audits reveal that most Oracle databases have default accounts and passwords that can give an attacker database administrator-type access. Once they are able to get onto the database, they can extract additional passwords from the UserData table and crack them with Cain or another free Oracle password cracker. With database Administrator (DBA) access it is easy to extract the

PHI or customer financial data from the databases. Many of our clients are now using Microsoft SQL (MS/SQL) database applications. Again using SuperScan or a similar scanner, scan for TCP port 1433. MS/SQL databases that are poorly secured are simple to compromise. Simplistic passwords on DBA empowered accounts, such as ‘sa’ with a password or ‘sa’ or ‘admin’ with a password of ‘admin’, give the attacker DBA-type access in a few minutes. Once they have DBA access, they can use a simple query to take sensitive data. They can also gain local system access to the server which may lead to the compromise of the entire Active Directory and the domains within it.

The quickest way to data mine confidential information is to go directly to the databases. Hackers do not bother scanning the entire network. Instead, they identify the machines hosting databases, directly connect to the databases, and take the data.

### BUILDING AN INFORMATION SUPERHIGHWAY THROUGH YOUR FIREWALL

Once a hacker gains access to the internal network, they like to be able to come back at will. The best way to do this is to place a copy of LogMeIn software (free from [www.logmein.com](http://www.logmein.com)) on a windows machine within the network. Once this software is installed, a hacker can pass through the firewall and gain high speed access to the internal network. I have written about this in several of my articles and demonstrated it in several of my classes. I will not pontificate any further on these inside-out, outside-in exploits. Just remember that software such as LogMeIn, GoToMyPC and RemotelyAnywhere can create openings in the firewall that can be compromised by hackers.

### CONCLUSION

Most organizations in general are a target for data miners due to the lack of a properly configured Intrusion Detection System, failure to apply patches, and the use of simplistic passwords. Once in, a hacker can easily glean personal information and confidential business data. A full IT Security Baseline is required to identify flaws for remediation. Periodic baseline checkup need to be performed to measure and quantify improvements to create metrics that senior executives can understand and evaluate. Follow-up baseline scans can also identify additional risks since the first baseline was performed.

---

*The opinions expressed in this article are mine and mine alone. I look forward to receiving your comments and questions. You can email me at [Gordon@canaudit.com](mailto:Gordon@canaudit.com) If you would like to receive articles like this in the future directly, please optin to our distribution list on the Canaudit website*



**University of Michigan – Dearborn  
Fairlane Center North  
19000 Hubbard  
Dearborn MI 48126**

**From the West**

Take I-94 East to Southfield (M-39) and exit North. Follow Southfield (North) to the Michigan Ave. (U.S. 12) exit. Stay on the Southfield Service Drive to Hubbard Drive and turn left. Follow Hubbard Drive and turn right into the Southern entrance of the UMDearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building

**From the East**

Take I-94 West to Southfield (M-39) and exit North. Follow Southfield (North) to the Michigan Ave. (U.S. 12) exit. Stay on the Southfield Service Drive to Hubbard Drive and turn left. Follow Hubbard Drive and turn right into the Southern entrance of the UMDearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building

**From the South**

Take Southfield (M-39) North to the Michigan Avenue exit. Stay on the Southfield Service Drive to Hubbard Drive and turn left. Follow Hubbard Drive and turn right into the Southern entrance of the UM-Dearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building

**From the North**

Take Southfield (M-39) South to the Ford Road exit. Stay on the Ford Road Service Drive to Hubbard Drive and turn right. Follow Hubbard Drive and turn right into the Southern entrance of the UM-Dearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building

*Menu – November 19, 2008*



**Dinner Buffet:**

Michigan Salad: Greens with Dried Cherries, Walnuts.

Pasta Salad

Roast Round of Beef with Gravy and Mushrooms.

Baked Salmon

Boneless Park Place Chicken with sauce

Green Beans Almondine

Garlic Mashed Potatoes and Gravy

**DESERT:** Pumpkin and Apple Pies

**VEGETARIAN PLATE AVAILABLE ONLY BY PRE-REGISTRATION .**

All dinners include Rolls/Butter, Relish Tray and Coffee/Soda-pop

**OPEN BAR:** Beer and Wine. Two alcoholic drink limit. No other liquor available.

**NO ADDITIONAL ALCOHOLIC DRINK TICKETS CAN BE SOLD.**

**UNLIMITED COFFEE AND SODA/POP**

The Chapter must provide the number of reservations by 8:00 a.m. Monday before the meeting. To ensure that we can accommodate those who wish to attend and the facility can provide the best service possible, please make your reservations **prior to midnight Saturday, November 15, 2008**. If you have made a reservation and cannot attend, please email Geralyn Jarmoluk at [GeralynJarmoluk@aol.com](mailto:GeralynJarmoluk@aol.com) **prior** to the above noted deadline for refunds. Your cooperation is greatly appreciated.

**We are very sorry, but reservations not cancelled prior to the above noted deadline (midnight. Saturday prior to the meeting) cannot be refunded as we are committed to the caterer for the meals ordered.**

**DATABYTE**



*Mike Forrest, Editor*  
*P.O. Box 1317*  
*Troy, MI 48099-1317*