

**OFFICERS  
AND  
DIRECTORS  
2007-2008**

**PRESIDENT**

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

**VICE PRESIDENT**

Jamshid Sadaghiyani, CISA, CPA  
PricewaterhouseCoopers LLP  
(313) 394-6567

**TREASURER**

John W. McCormick, CISA, CIA  
Accretive Solutions  
(248) 471-3075

**SECRETARY**

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

**DIRECTORS**

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

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

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  
Lason Systems, Inc.  
(248) 837-7375

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

Carrie Schrader, CISA, CBM, CFE  
KPMG LLP  
(313) 230-3222

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

Andrea M. Stromar, CISA

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

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

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

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



VOLUME 22, #4

REGION 2, CHAPTER 8

November 2007

*Monthly Meeting*

*Tuesday, December 11, 2007*

*Joint Meeting with IJA*

**Pre-Dinner Topic: "E-Discovery"**

Scott Baily, CISM, The Rehmann Group  
Chris Sobota, JD, MSIS, The Rehmann Group

**After-Dinner Topic: "End User Controls"**

Raj J. Patel, CISA, CISM, Plante Moran  
Joseph E. Oleksak, CISSP, Plante Moran

**Date:** Tuesday, December 11, 2007

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

**Location:** Vis Ta Tech on the Campus of Schoolcraft College  
(See map and directions on page 9)  
Vis Ta Tech is on the east side of Haggerty between 6 Mile and 7 Mile Roads  
18600 Haggerty Rd.  
Lavonia, MI 48152

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

**Please make reservations by 6:00 p.m. FRIDAY, December 7 at [isaca-det.org](http://isaca-det.org).**  
**Walk-ins and substitutions are welcome.**  
**Members and Non-Members will be charged an additional \$10 for reservations made after the deadline.**

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

## *Letter from the President*

Greetings ISACA Members,

Please note the date, time and location of the December meeting. This is our annual joint meeting with the IIA. It will be on Tuesday, December 11, with the pre-dinner presentation beginning at 4:30. The pre-dinner topic is E-Discovery with Scott Bailey and Chris Sabota of The Rehmann Group. The after dinner speaker is Raj Patel and Joseph E. Oleksak, Plante Moran speaking on the subject of End User Controls. (See the presentation description and speaker bios beginning on Page 3.)

For those of you that missed it, the November meeting with Ken Jaworski was awesome. Ken presented a tremendous amount of material on Data Privacy. Ken defined data privacy, and current legislation and the blending of data privacy and security. He explained the what and whys of a Privacy impact analysis and the need for a privacy risk analysis. Based on the positive response, we will probably try to plan a four hour meeting at least once a year.

HELP! We have had some negative comments about the badges (names misspelled, wrong credentials, names all caps, etc.). Yes, we are working on a solution, however, please note that the badges are printed from the registration information you enter when you register. So please ensure you enter your name, company, and credentials exactly the way you want them on your badge.

We also have a need for some help in the back office area. We need some clerical help in prepping the registered information for the registration table. We need someone to record and track attendance for CPE documentation. We would also like to have a Newsletter editor. Please let me know if you can help. We are working towards organizing tasks for which we seek help so that each can be accomplished in one to four hours per month.

Kamal Dave, co-founder of the itSMF Great Lakes Local Interest Group (GLLIG) has invited the our members to attend a December 4 meeting of the to meet and hear from Dave Cannon, co author of ITIL V3 Operations. Contact Kamal at [kamal.dave@hp.com](mailto:kamal.dave@hp.com) if your are interested in attending.

The CGEIT (Certified in the Governance of Enterprise IT) is now official. The CGEIT is for professionals working in the field of IT Governance. Grandfathering applications must be submitted by October 31, 2008. The requirements include eight (8) years of experience with IT governance contribution to an enterprise, with three (3) of these years performing tasks directly related to the CGEIT domains:

- (1) IT Governance Framework;
- (2) Strategic Alignment;
- (3) Value Delivery;
- (4) Risk Management;
- (5) Resource Management; and
- (6) Performance Measurement.

Applicants must submit a 200 – 500 word narrative of how they used the ITGI framework in supporting and improving the governance of an enterprise’s IT.

By the way, did anyone notice the article in *CIS Decisions* about the CIO that dropped ITIL for Microsoft Operations framework? Read the “Parting Shot” on the last page.

As always, if you have any questions, concerns, or suggestions, for the chapter, please contact me at [michael.forrest@jeffersonwells.com](mailto:michael.forrest@jeffersonwells.com) or call 248-371-7752. See you at the chapter meeting December 11.

Mike Forrest, CISA, ITIL  
President, ISACA Detroit Chapter

**PRE-DINNER INFORMATION****“E-Discovery”**

Electronically Stored Information Risk Assessment Is Critical In Light Of New E-Discovery And Database Breach Notification Laws

With over 90% of business communications being conducted by way of e-mail and other electronic means, it should be of no surprise that Electronically Stored Information (ESI) is frequently subpoenaed in litigation. Producing e-mail, text messages, databases, and instant messages in a timely manner can be much more difficult than paper documents. In December 2006, the Federal Rules of Civil Procedure were amended to specifically address ESI. Several states have adopted court rules addressing ESI and most other states are now in the process of amending court rules. In 2007, Michigan adopted a database breach notification law (MCL 445.72) and is currently in the process of amending the Michigan Court Rules to address ESI.

If you haven't received a notification requesting production of ESI, odds are that you will sometime in the near future. Even if your organization is not involved directly in a lawsuit, your organization could have to produce ESI records for another lawsuit as a third party. Could you produce the instant messages or e-mails between two employees from one year ago? How long is your organization retaining e-mail? How much time and money will it cost your IT department to pull backup tapes and restore records? Most organizations are not prepared to respond quickly to this type of ESI discovery request.

**Presenters:**

**Scott Bailey, CISM**  
**Managing Principal,**  
**Enterprise Risk Management**  
**The Rehmann Group**

Scott is Managing Principal of Enterprise Risk Management for The Rehmann Group, overseeing Internal Audit, IT Audit, SOX Consulting, Internal Control Consulting, Technology Risk Management and Security, Business Risk Consulting, e-Discovery and Digital Forensics.

Scott has over 24 years of experience in risk management, IT audit, information security, and forensic fields. He is nationally recognized for his expertise in information security and has consulted for Fortune 500 manufacturing companies, major financial institutions on internal controls, IT security, data encryption, strategic planning and policy development. He has assisted companies regarding compliance with Sarbanes-Oxley and Gramm-Leach-Bliley Acts and has conducted national seminars. Scott has also assisted companies with information technology strategic planning, stepping in as a temporary CIO when needed. In addition, Scott is a subject matter expert in digital forensics and e-Discovery, and has worked with corporations, law firms and law enforcement agencies on a variety of cases.

Previously, Scott worked as Director of Technology Risk Management for a global professional services firm, Data Processing Manager for a large financial institution and Software Architect for one of the Big Three automakers, where he developed enterprise software. Subsequent to this, as president of a private technology and software company, he provided expertise to the FBI, the U.S. Secret Service, law enforcement agencies, and public and private sector clients.

**Chris Sobota, JD, MSIS**  
**Information Technology Consultant**  
**The Rehmann Group**

Christopher is an Information Technology Consultant in Enterprise Risk Management for The Rehmann Group. He is located in the Troy office. Prior to joining the firm in 2007, Christopher worked as an attorney focusing on general civil and criminal legal matters and as a consultant focusing on information technology. Christopher has

### **DETROIT CHAPTER ISACA – YOUR ‘YEAR-ROUND’ PARTNER FOR PROFESSIONAL GROWTH**

extensive courtroom experience and an in-depth understanding of the complex interactions between law and information technology. Christopher advises clients in the areas of information technology and electronic commerce, with a focus on potential legal liability for high technology ventures. Christopher also consults on issues such as regulatory compliance, IT audit and IT security.

#### **After Dinner Information**

##### **End User Controls**

Often times, the weakest link in security (i.e. end user) is ignored. End users touch all three aspects of an information security program (policies, procedures, and mechanisms.) Additionally, the role of the end user has been greatly impacted by the evolution of technology (from the early introduction of computing to the Internet age.) This presentation discusses the role of end users in information security and its evolution. It will also touch on the end user effect from next generation of technology, virtual worlds.

##### **Presenters:**

**Raj J. Patel,**  
**Partner**  
**Technology Consulting and Solutions practice,**  
**Plante & Moran**

Raj has over 15 years of information technology security, control and audit experience in financial institutions, insurance, state & local government, and automotive industries. Mr. Patel's leads the Security Assurance and Consulting practice providing clients with IT internal audit, IT risk assessments, network security assessments / penetration studies, web application security assessments, Sarbanes-Oxley compliance, GLBA/HIPAA compliance, systems integration controls reviews, business continuity management, and eBusiness security.

Mr. Patel has also presented on security related topics in various white papers, newsletters, magazines and at various conferences. In March

**Page 4**

2007, Mr. Patel was awarded the “American Dreamer” award by Crain’s Detroit Business Magazine in recognition of his leadership in the business community in Michigan.

**Joe Oleksak,**  
**Manager**  
**Technology Consulting & Solutions Group,**  
**Plante & Moran**

Joe has over ten years of experience with IT security and audit. During his career, Mr. Oleksak has managed Information Technology (IT) security and audit work across several industries. Mr. Oleksak has extensive experience in business process and application security & control assessments, Network & Web Application Security Assessments, developing security policies / procedures / guidelines, and in performing regulatory security threat and risk assessments.

(Advertisement)



**"Innovative Executive Search & Staffing Solutions"**

---

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

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

*For a listing of current opportunities, testimonials, interview tips and other beneficial information, please visit us at [www.globalrecruiters.com](http://www.globalrecruiters.com)*

**Arthur Gluzman-Managing Partner**

arthur@globalrecruiters.com

248-489-1900 (ph)

248-390-5598 (cell)

# Year at a Glance

Saturday, December 08, 2007	CISA and CISM Exams
Thursday, December 06, 2007	6:00 p.m. - Deadline for on-line reservations for the December 11 meeting
Tuesday, December 11, 2007	Deadline for January Databyte submissions
Tuesday, December 11, 2007	Chapter Meeting - Joint meeting with IIA - Vis Ta Tech
Friday, January 05, 2007	6:00 p.m. - Deadline for on-line reservations for the January 10 meeting
Thursday, January 10, 2008	Deadline for February Databyte submissions
Thursday, January 10, 2008	Chapter Mtg - Joint with CFE – U of M – Dearborn Fairlane Center North
Friday, February 15, 2008	6:00 p.m. - Deadline for on-line reservations for the February 20 meeting
Wednesday, February 20, 2008	Deadline for March Databyte submissions
Wednesday, February 20, 2008	Chapter Meeting - University of Michigan-Dearborn Fairlane Center North
Friday, March 14, 2008	6:00 p.m. - Deadline for on-line reservations for the March 19 meeting
Wednesday, March 19, 2008	Deadline for April Databyte submissions
Wednesday, March 19, 2008	Chapter Meeting - University of Michigan-Dearborn Fairlane Center North
Wednesday, April 09, 2008	Final Deadline for registration for the June 14 CISA or CISM exams
Friday, April 11, 2008	6:00 p.m. - Deadline for on-line reservations for the April 16 meeting
Wednesday, April 16, 2008	Deadline for May Databyte submissions
Wednesday, April 16, 2008	Chapter Meeting - University of Michigan-Dearborn Fairlane Center North
Friday, May 16, 2008	6:00 p.m. - Deadline for on-line reservations for the May 21 meeting
Wednesday, May 21, 2008	Deadline for June Databyte submissions
Wednesday, May 21, 2008	Chapter Meeting & AGM – University of Michigan-Dearborn Fairlane Center North
Saturday, June 14, 2008	CISA and CISM Exams

(Advertisement)



## Information Technology Audit Senior

### Available for Contract Work

Need Additional Help? Contact me.

**(216) 459-9272**

Daniel J. Leo, CPA, CMA, CIA

Independent Contractor of IT Audit Services

-Will travel to your location(s)



#### Why Contract with me?:

- > SAVE \$\$ -Implement AS5 & Reduce Audit Costs
- > Meet Deadlines
- > Save Your Staff; I'll do the Traveling
- > Both IT and Internal Audit (Financial) Skills

#### Highest Quality Services:

- > Certified Quality – CPA, CMA, CIA
- > Successfully Passed the CISA exam
- > Experienced-17 yrs as Indep. Contractor
- > Excellent References -Satisfied Clients

## **New Detroit Chapter Members**

Stewart Charles Albert, III, ITIL	Muhammad K. Arqum, CISA, CISSP, PMP	Robert P. Bacigal, CISM, CISSP
Michael A. Blain	Lisbeth Evelyn Chavarria, PMP	Robert Hoffman
Raymond Hruska	Lauren C. Miller	Michael Parker
Loren Phillips	Natalie Ann Rostkowycz	Steven Todd Settle, CISA
Jon Smith	Julie Lynn Waggener	Mark W. White, CISM, CISSP

## **Certification News**

Congratulations to the following that have received their certification.

### **Recent ISACA Certifications**

#### **CISA Certifications**

Amit Agrawal, CISA	Muhammad K. Arqum, CISA, CISSP, PMP	William H. Ging, IV, CISA, MS
Magdalena A. Marriott, CISA, CPA	Lori McColl, CISA, BBA, MBA	Erik Pedersen, CISA
Peter J. Reuter, CISM, CISA, CISSP	Chandra S. Saripalli, CISA	James Simonis, CISA, CISSP

#### **CISM Certifications**

Timothy G. Baeten, CISM, CISSP	Sherry Lynn Desbrough, CISM, CISSP	Robert M. Doell, CISM, CISSP, CCSA
Daimon Erik Geopfert, CISM, CISSP	Peter J. Reuter, CISM, CISA, CISSP	Mark Wayne Whaite CISM, CISSP

Those that have received their certification and their managers will be invited as our guest to the April meeting where they will be recognized for their achievements.

### **NOVEMBER Drawing Winners**

Siobhan Jordan	Jeeve Joseph, CISA, CISSP	Dave McLachlan, CISA
	Mike Stolarczyk, CISA	

## Application Security Controls There Are No Silver Bullets

By Paul Rozek

Over the past decade, many companies adopted layered information security models. External-network Internet connectivity received most of the attention and funding, and robust firewall technologies were implemented to try to keep out the “bad guys.” This emphasis on technology actually resulted in a false sense of security in many companies as vulnerabilities and exploitations proliferated within business and technical software applications. Currently, it’s estimated that more than 90 percent of external attacks take advantage of misconfigured and poorly administered applications and systems.

According to Gartner Group’s, *U.S. IT Spending and Staffing Survey, 2005*, the top four areas of information technology (IT) spending were:

1. IT employees (salaries and benefits) – 30 percent
2. Hardware – 23 percent
3. Software – 18 percent
4. External service providers – 13 percent

With approximately 32 percent of internal staffing costs and 39 percent of external staffing costs spent on application development, maintenance, and support, it’s no wonder senior management worries about the security, integrity and availability of their applications and data.

### Leading industry practices

A key IT management control governing software acquisition and management is the application Systems Development Life Cycle (SDLC). A SDLC contains checkpoints to help ensure applications conform to standards and meet management’s business and technical expectations. Applications typically have four types of control requirements: 1) information security (controlling who can execute privileged functions and access transactions and/or data), 2) data input and validation, 3) processing/output accuracy and integrity, and 4) backup and recovery.

Within the following SDLC phases, the information security function should play a specific, vital role using these suggested actions:

**Request:** Identify and capture security requirements of the systems and business functions. Preliminary specifications should reveal if hardware, software, or external services are needed to fully implement the necessary security.

**Design:** Examine potential threats to the effective use of security features. The design of security controls (access to transactions, menus or data, or event or end-user activity logging) should be approved by all relevant IT and business area representatives, and, as applicable, endorsed by internal audit. Capture future testing criteria at this time.

**Development:** Thoroughly review software code relevant to security functionality and fully exercise and document security tests. Appropriate, automated tools should be used to scan software code for well-known security vulnerabilities – especially of Internet applications.

**Quality Assurance:** Perform full security system and business function security tests. Should changes impact a security feature, conduct regression tests to verify that unknown or unexpected changes have not occurred.

**Deployment:** Security issues should be high-priority and tracked and resolved on a timely basis. Regular application scans should be conducted, especially when the scanning software vendor changes, new vulnerabilities are discovered or significant application changes occur.

A common myth is that increasing security requirements and using security-testing tools and techniques within the SDLC dramatically increases development costs and extends deployment time-to-market. That may be true if the tools and techniques are used improperly or not at all. However, it’s more cost-effective to implement security controls and use security-testing processes early in the SDLC than trying to retrofit controls after the application’s development or deployment.

Unfortunately, professional hackers are usually one step ahead. The sooner companies detect, assess and remediate application security vulnerabilities, the less likely they are to fall victim to fraud. Once a hacker accesses sensitive data, the media and stakeholder ramifications can be devastating.

### **DETROIT CHAPTER ISACA – YOUR ‘YEAR-ROUND’ PARTNER FOR PROFESSIONAL GROWTH**

Not surprisingly, integrating information security into the SDLC may require a shift in the corporate culture. But Gartner predicts that by 2010, companies that properly integrate security into the SDLC process will experience an 80 percent decrease in critical vulnerabilities in either externally facing Internet applications or in publicly released software products.

The popularity of secure coding techniques continues to grow.

Information on common Web-based application vulnerabilities and techniques for reducing their risks is available on a variety of Internet Web sites. These risk-reducing techniques can be relevant whether a company develops its own Web applications or outsources development to a third party. Regardless, it's necessary to confirm that secure coding techniques and testing processes are consistently followed.

Independent, regularly scheduled scanning of Web-based applications, using sophisticated security vulnerability assessment software tools, is highly recommended. The challenge for smaller companies is that licensing fees for these tools can be prohibitive. In addition, many tool users are neither trained nor qualified to assess the potentially technical and complex findings. It's not surprising that these types of scans are often outsourced to professional security services firms.

#### **Control objectives**

Recent reports of industry compliance efforts revealed an alarming lack of basic security controls within application software. Companies should closely examine their business and technical applications. Many experts agree that, at a minimum, the following control objectives and their corresponding formal policies and procedures, should be consistently applied to all critical applications:

1. Securely authenticate users.
2. Maintain the effectiveness of application authentication and access mechanisms.
3. Ensure timely actions regarding requesting, establishing, issuing, suspending and closing application user accounts.
4. Periodically review and confirm user access rights.

5. Create application event logs, monitor relevant security activity, and identify security events and violations that should be reported to senior management.

6. Ensure appropriate segregation of duties surrounding requesting and granting access to application systems and data.

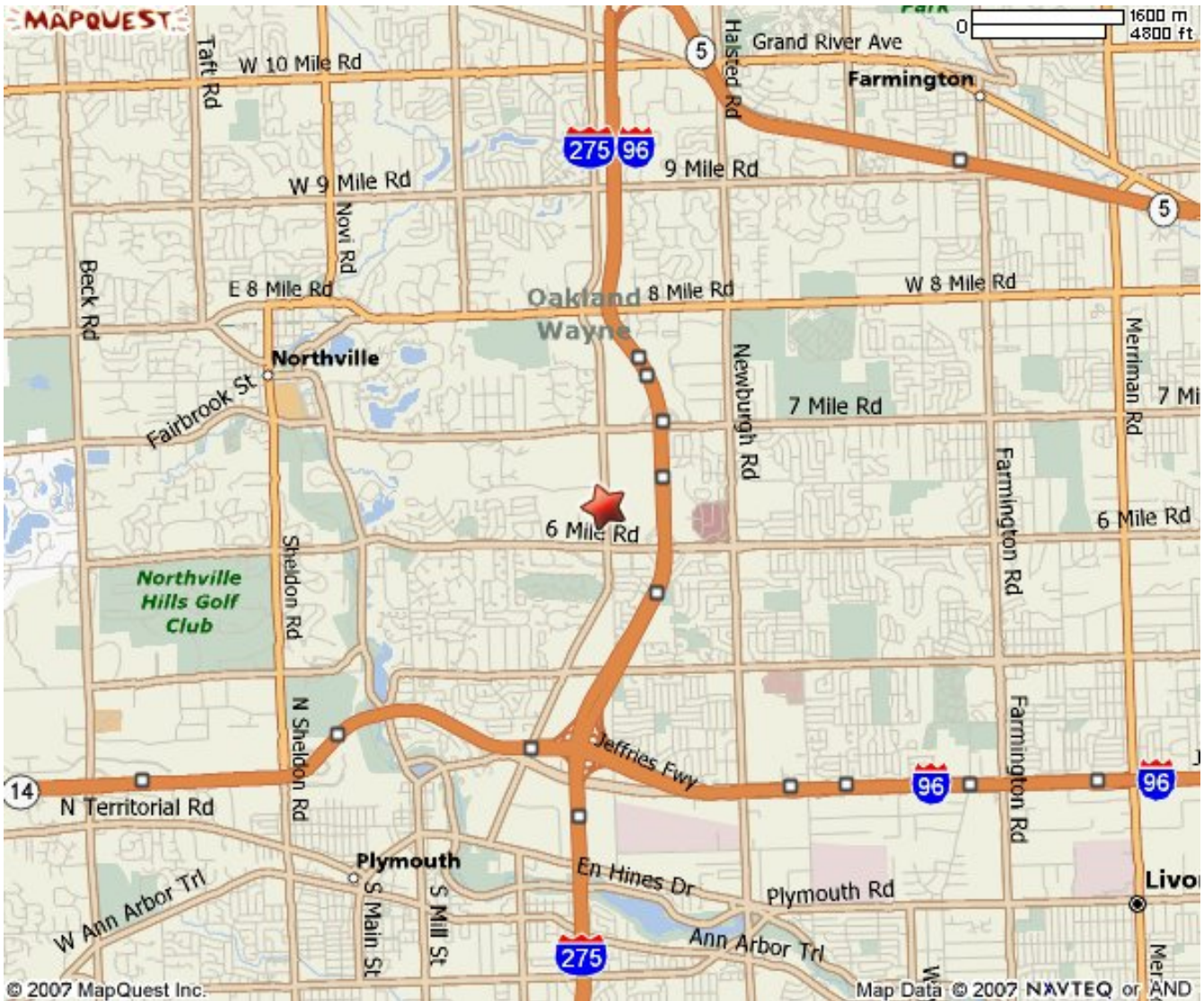
7. Ensure data is classified and secured based on its level of risk and the legal/regulatory privacy and confidentiality requirements.

These same security control objectives can be applied to the databases, servers and networks that support processing of such applications.

There are no silver bullets for effective application security controls. As long as people design, develop, test and deploy code, software errors and irregularities will exist. It's advisable for companies to implement and integrate effective security controls, testing and scanning tools, and related processes into their SDLC. Done properly, this should reduce overall application development costs, increase end-user satisfaction, improve segregation of duties over critical business functions, and enhance security controls that support audit and compliance requirements.

*Paul Rozek is Director of Technology Risk Management Services and Security Infrastructure Assessment Subject Matter Expert with Jefferson Wells. He can be reached in the Milwaukee office at 414-347-2345, or via e-mail at paul.rozek@jeffersonwells.com.*

**Vis Ta Tech  
Schoolcraft College  
18600 Haggerty Rd.  
(between 6 Mile and 7 Mile Roads)  
Livonia MI 48152**



*Month at a Glance*

Friday, December 7	6:00 p.m.	Advance Registration Closes
Tuesday, December 11, 2007	4:30 p.m.	<b>E-Discovery</b> Scott Bailey, CISM, The Rehmann Group Chris Sobota, JD, MSIS The Rehmann Group
	5:30	Dinner
	6:30	“End User Controls” Raj Patel, Plante Moran Joe Oleksak,

*Menu – November 14, 2007***DINNER BUFFET**

Roast Sirloin, au jus  
 Grilled portobello ravioli with Chardonnay butter sauce  
 Sautéed mushrooms with garlic butter  
 Parmesan Mashed Potatoes  
 Vegetable Tray with Herbed Dipping Sauce  
 Caesar Salad  
 Hearts of Palm, Cucumber and Mint Salad  
 Chocolate Éclair

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 early **prior to 6:00 p.m. Friday, December 7, 2007**. If you have made a reservation and cannot attend, please call Mike Forrest at (248) 226-1269. Your cooperation is greatly appreciated.

Advanced paid reservations not cancelled after the he cut off time (**6:00 p.m. Friday prior to the meeting**) and cannot be refunded.

Please note that the menu includes a vegetarian selection. If additional dietary needs are required, contact Mike Forrest

**DATA BYTE**

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