

OFFICERS AND DIRECTORS

1999-2000

PRESIDENT

Marci Klain, CPA, CISA
General Motors Corporation
(313) 665-3753

VICE PRESIDENT

Todd McGowan, CPA, CISA
Deloitte & Touche, LLP
(313) 396-3407

INTERIM TREASURER

Marci Robinson, CPA, CISA

SECRETARY

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

DIRECTORS:

Ed Barszcz, CIA, CFE
Facilities Chairperson
Blue Cross/Blue Shield of MI
(313) 225-9076

Sharon Brennan, CPA, CISA
Job Bank Chairperson
University of Michigan
(734) 647-7504

Karen Cordes, CIA, CISA
Newsletter Chairperson
Consumers Energy
(517) 788-0439

Jerry Jarvis, CISA, CIA, CFSA
Program Chairperson
GM Audit Services
(313) 665-3615

Ray Kaslik, CISA, CIA, CFE, CMA
Seminar Chairperson
MCN Energy Group, Inc.
(313) 256-5155

Don Ledwith, CISA, CCP, CQA
Internet Chairperson
Kmart
(248) 643-2428

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

Mike Reading, CISA
St. John Health System
(810) 753-1166

Charles Rodolico, CISA
General Motors Corporation
(800) 327-6770, Ext. 58479

Carrie Schrader, CISA
Membership Chairperson
The Detroit Medical Center
(313) 966-5178

Danielle Snyder, CIA, CISA
Student Relations Chairperson
General Motors Audit Services
(313) 665-3755

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

Mike Tomasek, CISA
BDO Seudnabm LLP
(248) 244-6558

Brent W. Wylie, CIA, CISA, CFE
Federal-Mogul Corp.
(248) 354-9407

PAST PRESIDENTS:

Linda Alderman, CISA
Audit Force
(248) 350-3006, Ext. 150

Dave Shears, CISA, CISSP
Federal Mogul
(248) 354-7825



*Information Systems
Audit and Control
Association*

DATABYTE

NEWSLETTER OF THE DETROIT AREA CHAPTER

VOLUME 14, #5

REGION 2, CHAPTER 8

JANUARY, 2000

MONTHLY DINNER MEETING

January 19, 2000

Pre-Dinner Presentation:—Intrusion Detection Systems

After-Dinner Presentation:—Understanding Internet Security Risks

Location: Troy Marriott.
200 W. Big Beaver Road in Troy
Take I-75 to Big Beaver Road East.
The Marriott is on the left (North) side just east of I-75.

Date: Wednesday, January 19, 2000

Time: 4:30-5:00 Registration
5:00-6:00 Pre-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—E-mail your reservation to Sharon Brennan at sharonlb@umich.edu or fax your reservation to (734) 647-7501 by 4:00 PM, Friday, January 14th. Please include your name, company, telephone number, and whether you are a member. If you do not have access to e-mail or a fax machine, call Sharon at (734) 647-7504. Please indicate your meal choice. The default is entree #2.

Visit our web site at: isaca-det.adaptive.net

Message from your President...

Dear Members,

Welcome back! I hope everyone had a wonderful holiday season and is refreshed and ready for the new year ahead of us. Does anyone have any interesting or funny Y2K New Year's stories? Please share them with us when you visit our web site at <http://isacadet.adaptive.net> or send them to PO box 4297, Troy Michigan 48099.

Although this is a new calendar year, the ISACA board members are continuing to work hard to bring you exciting and informative presentations at each dinner meeting. Our next meeting is a joint meeting with the Association of Information Technology Professionals (AITP.) Don't miss this chance to meet others in the IT profession. Please note that the meeting will be held on Wednesday, January 19, at the **Troy Marriott**.

Along with the new year comes new changes. The *IS Audit & Control Journal* is now called the *Information Systems Control Journal*. This change acknowledges the fact that information technology controls are not just the concern of auditors. More and more, managers and other professionals are concerned with, and even taking ownership of, IT related controls. This also reflects the fact that even though some of you may move on to non-audit related opportunities, ISACA may still provide you with beneficial information and tools. Remember, you do not have to have 'audit' in your title to participate in ISACA.

Don't forget to mark your calendars for the Spring Conference which will be held on **March 22-24, 2000**. Please refer to page 6 of this newsletter for further information. We will also continue to update our web site with further details as they become available. Please visit our web site or contact Ray Kaslik at (313) 256-5155 with any questions.

Your President, Marci Robinson

Advertise in your DataByte Newsletter...

If you are interested in advertising in the DataByte, please contact Karen Cordes for all the details.

She can be reached at:

Consumers Energy Company

1945 Parnall Road

Jackson, MI 49201

Telephone: (517) 788-0439

E-mail: khcordes@cmsenergy.com

Menu - January 19, 2000

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

Entree #1: *Roast New York Sirloin—sliced and served with Cabernet Sauce and Tobacco Onions*

Entree #2: *Chicken Sonoma—served with a Chardonnay & Citrus Beurre Blanc*

A vegetarian pasta plate is available by special request.

All entrees include:

- Rainbow Salad
- Rolls and butter
- Rice or potato of the day
- Italian Spumoni Ice Cream Cake
- Coffee, tea, milk, or soft drinks



The Chapter must provide the number of reservations and menu selections to the restaurant by 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 reservation early. Your cooperation is greatly appreciated.

After-Dinner Speaker - Dan Erwin

D.G. (Dan) Erwin, CISSP The Dow Chemical Company

Dan Erwin has 30+ years experience at Dow Chemical in Midland. He is a member of Dow's Information Security Strategy and Planning function, providing risk assessment and information security consulting for management and project teams. Dan has held both technical and management positions during his career at Dow. He has Management and Professional certification in both Business Management and Information Security and is an active member of a number of Information Security organizations.

Dan has been involved in Dow's Security Program since the early 80's, developing many of the process models that Dow used to establish their effective computer security program, including a risk assessment process that is quickly becoming an industry standard. Dow Chemical won the Computer Security Institute's Information Security Program of the Year Award for 1999).

After-Dinner Presentation by Dan Erwin

Understanding the Risk

Are you confused by all the reports and statistics that are being recounted in the press and management trade journals? Do you wish someone would do a session that would review the studies that many of these reports are based on and summarize the major risk/threat to your information systems, in a clear, easy to understand presentation? If so, this is it.

This presentation will clearly demonstrate where your valuable time, money and effort should be spent in order to achieve the maximum payback based on risk. The emphasis of this session is evaluating risk and establishing proactive processes to mitigate that risk. If you have ever worried that you are working on the wrong things, this presentation is for you.

Pre-Dinner Speaker Biography

Dan Wiechec

Dan has over 13 years of industry and public accounting experience and is currently the Security Practice Leader for the Great Lakes Market Circle. During his career, Dan has managed security assessment and architecture projects in addition to evaluating system intrusions that occurred at various organizations. Dan graduated with a BS from the University of Maryland and an MAS from the Johns Hopkins University. Dan is also a past president of the Detroit Area Chapter of ISACA.

Pre-Dinner Presentation

Intrusion Detection

Intrusion detection systems

What are they? Why should companies use them? How do they work? What should companies do to prepare for using intrusion detection systems? In the pre-dinner presentation we will answer these questions to help you better understand what intrusion detection systems are, why they are being used and the benefits that can be derived from using these systems. Throughout our discussion we will focus on the business case for implementing an intrusion detection system within your organization. Additionally, we will demonstrate how intrusion detection systems work.

Taking the mystery out of...Public Key

This is one in a series of management mini-briefings on Information Protection (IP) technology and techniques. These briefings are designed to be short, easy to read and structured to provide an understanding of the basic nature, purpose, major components, distinctions and business benefits of the topic. In this series, we try to simplify but not oversimplify IP subjects that are complex, often misunderstood and frequently the objects of conflicting opinions. This document won't make you an expert but we hope it adds to your working knowledge.

What is it?

"Public Key" (aka asymmetric key) refers to a novel form of cryptography in which the key has two parts. The two parts of the key, known collectively as a "key pair," are mathematically related in such a way that what is encrypted with one part can only be decrypted with the other. This marvelous property works in both directions, i.e., either part, A or B, can be used to encrypt and the other part to decrypt. What is encrypted with A can only be decrypted with B and what is encrypted with B can only be decrypted with A. Similarly, anything that can be decrypted with B must have been encrypted with A and vice versa.

In practice, one part of the key, called d (for decrypting), or the "private" key, is kept secret but the other part, e, the "public" key, is published for all the world to see and use. Again, in practice, the key is published on a public server. If you want to send someone a secret message, you simply look up their public key and use it to encrypt the message. They use their secret key to decrypt it. This use to hide the meaning of a message from all but the intended recipient is called a digital envelope and is the traditional use of cryptography.

But remember what we said earlier, "what is decrypted with A could have only been encrypted with B?" Well, this property is useful. If the holder of the secret key uses it to encrypt a message, then anyone, using the public key, can read it but only the holder could have created it. This novel application, called a digital signature, enables the receiver, not only to know with a high degree of confidence who originated the message but also to demonstrate it to a third party. Not only can he demonstrate that the message originated with the sender but also that it has not been altered since it was sent.

Public key cryptography relies for its security on mathematical problems that are easy to compute in one direction and extremely difficult to do in the other direction. For example, RSA cryptography, the de facto standard, relies on the fact that multiplication is easier to do than factoring. Finding the product of two large prime numbers is relatively easy while finding those two numbers from the product (factoring) is computationally infeasible. The bigger the numbers, the harder the problem.

Because Public Key cryptography is slow when compared to more traditional, symmetric key, cryptography, it is used almost exclusively for managing keys for this faster cryptography. The resulting "hybrid" cryptography gives us the speed of conventional cryptography while preserving the convenience of public key.

What is its Business Benefit?

A hurdle to the application of encryption to business applications has been the safe and efficient management of the necessary number of encryption keys. "Public Key" cryptography (PKC) solves this problem.

Business uses Public Key cryptography (PKC) to provide for the control of information. By combining the two abstractions of digital envelope and digital signature, we are able to simulate the behavior of all controls over bits and bytes that we have been able to exercise over information on paper. We can have digital credentials, checkbooks, cash, and wallets. We can have digital transactions, contracts, wills, and testaments.

- Confidentiality - While business can hide messages and files using conventional cryptography, PKC offers the additional benefit that it can do so without the costly and risky step of prior exchange of a secret key. It can perform file encryption without the recipient's passphrase.
- Integrity - PKC can be used to ensure that a message had actually originated from where it appears to and that it had not been modified in transit.
- Non-repudiation - While both parties to conventional cryptography can be confident that a message encrypted under the secret key originates with the other, PKC offers the unique and additional benefit that they can demonstrate it to a third party.
- Forgery resistance - PKC can also be used to produce data objects that can be recognized as original but are infeasible to counterfeit. This capability can be used to produce credentials like credit cards and licenses that are more difficult to counterfeit and that can be recognized at a distance.

Continued on page 5

Continued from page 4

How is it Used?

Ideally, the use of PKC is automated, integrated into the application, and hidden from the user. For example, the originator of an e-mail message might have his message signed, so that it could be recognized as authentic by the recipient, and sealed, in a logical envelope that could only be opened by the intended recipient, automatically and without any special action on his part. When the message was opened by the recipient, he could have confidence that it originated with the sender, had not been modified since sent, and could not have been read by anyone else in transit.

The e-mail application at both ends would find the proper keys and encrypt and decrypt as necessary. If it did not already have beneficial use of the necessary private keys, it would prompt the users for the necessary key name and pass-phrase. If it did not already have access to the necessary public keys, it would simply go to a server and look them up. The users might see an icon that told them that the message was secure and they could look at the information about the keys if they wished. However, as long as the application did not recognize any problems, the icon might be sufficient.

Private keys are always stored encrypted under conventional cipher. The key for this cipher is obtained by compressing a pass-phrase to the length of the key used by the cipher. Thus, beneficial use of the private key requires that one have both a copy of it in its encrypted form and knowledge of the pass-phrase. The pass-phrase should never be written down or stored. It may also be useful to store the cryptogram of the private key in a safe place such as in a secure file system or on removable storage like a diskette or PCMCIA card.

Where is it Used?

Like other forms of cryptography, Public Key cryptography is used in hostile environments and sensitive applications. These include environments like the Internet and applications like electronic commerce. It is particularly well adapted for use in very large open user populations, where keeping keys secret while sharing them is difficult. Since it requires a minimum of prearrangement, it is useful in applications like e-mail where we may not know in advance with whom we may wish to correspond. As we mentioned earlier, PKC is used to manage keys in conventional cryptography. It is used to resist forgery in such credentials as employee badges and credit cards while permitting them to be recognized with confidence at a distance.

PKC is used in almost all serious business software that is intended for use in a modern distributed computing environment. For example, it is used for the security of Lotus Notes and many e-mail packages. It is used in the Netscape and Microsoft Internet servers and browsers. It is used in file system encryption utilities such as RSA Secure and Norton Your Eyes Only. It is used in electronic commerce and digital cash applications such as Cybercoin and Digicash. While it might not be obvious to you, if you have used any of these applications, you have used PKC.

Other Things Worth Knowing

Strength - Like other forms of cryptography, the strength of PKC is variable (with the size of the key) and may be as strong as we need it to be. It will rarely be the weak link in the security chain.

Certificates - While public keys are not sensitive to disclosure, one must be sure that one is using the right key for the intended recipient. The best way to know that a key is the right one for a particular user is to receive it from their own hand but this will rarely be practical. In practice, one will usually receive the key over a network along with a certificate signed by an authority that you already trust and whose public key you already have. Since this will usually be automatic, you need not worry about it.

Reprinted from Todd McGowan with permission of Deloitte & Touche LLP.

Welcome New Members...

Johnathan Landsman
John Lopez

IIA/ISACA SPRING CONFERENCE 2000

The ISACA Programs Committee has been working together with representatives from the Detroit Chapter IIA to offer our memberships a high quality low cost training opportunity. The Matrix below presents the topics and dates for the sessions. A variety of session lengths from 1 day to 3 days will be available depending upon the topic.

Similar to the ISACA Great Lakes Audit Conferences presented in the past, the venue will be the Lyon Meadows Conference Center at 53200 Grand River Ave. in New Hudson, MI. That's just west of Novi. Costs are being finalized and will be published in a brochure that will be mailed in early January.

The cornerstone of the conference, from an IT Audit perspective, is the 3 day Audit, Control, and Security of Electronic Commerce seminar. It is being presented by MIS Training Institute and is one of their most popular seminars. MIS normally charges \$1,195 for this seminar if you attend it at one of their out of town locations. We will be pricing it at \$500 for members. Less than half price with no travel costs! This unique offering will alert you to the critical risks in electronic commerce environments and provide you with proven controls and procedures for minimizing them. Class exercises will lead you through a step-by-step approach for identifying the new business and security risks unleashed by EC technologies. As an added bonus, attendees will receive a diskette with sample EDI and EC audit review programs.

Please mark your calendar or make an entry in your Palm Pilot for March 22 - 24 and plan to attend the joint IIA/ISACA Spring Conference 2000. For additional information, or to reserve a space for the E Commerce seminar, please contact the ISACA Program chairman Ray Kaslik. His E Mail address is RAY.KASLIK@MCNENERGY.COM, his phone is 313-256-5155. Look for additional information on the ISACA Detroit Chapter website soon.

PROGRAM MATRIX

Keynote Speaker: Ms. Jackie Wagner, General Auditor, General Motors Corporation, 30 minutes 3/22, Auditorium

Tracks	Day 1 - 3/22 Wed	Day 2 - 3/23 Thurs	Day 3 - 3/24 Fri
Computer Assisted Audit Techniques (CAAT)	CAAT Concepts	ACL Basics	ACL Basics
Technical	Audit, Control, and Security of Electronic Commerce	Audit, Control, and Security of Electronic Commerce	Audit, Control, and Security of Electronic Commerce
Technical	Remote Access	Network Security Scanning Tools	Operating System Security Concepts & Issues
Communication Skills	Consulting Excellence	Negotiating Skills	Presentation Skills
Business Process Risks & Controls Assessments	Risk Assessment	Process Flow Analysis	IT Auditing Basics
Management Briefings & Key Topics of Interest	CFIA Roundtable ----- Audit Committee Roundtable	Value Added Auditing, Customer Satisfaction, Benchmarking, IA Best Practices Roundtable	Using the Internet ----- The Internet and Audit Research

History of our Chapter

This year, the 1999-2000 year, is the 25th anniversary of the Detroit Chapter of ISACA. We want to recognize our longevity and the dedication of all the people that have participated over the last 25 years to make us a successful professional organization. Historic information will be included in our newsletters so that you can share in the appreciation of the background of this chapter.

The Detroit Area Chapter of the Electronic Data Processing Auditors Association (EDPAA) was founded in 1974 by a handful of dedicated auditing professionals seeking to expand into the world of EDP auditing. After attending an EDPAA National Conference in Chicago during the summer of 1974, Seymour Ribiat and Ed Barszcz of Blue Cross and Blue Shield of Michigan decided to organize a local chapter. The original members wanted an organization that focused on EDP auditing and controls. Therefore, the eighth chapter of the EDPAA was born in Detroit on September 10, 1974. The EDPAA was renamed to ISACA in 1994.

The following were the founding officers and directors. They were professionals from the following industries: banking, savings and loan companies, insurance, universities and computer companies.

President: E. Read Peirce
Vice-President: Ailway Cowger
Secretary: Seymour Ribiat
Treasurer: Malcome Miline
Directors: Edward Barszcz, Kathleen Hertz, Yale Gealer, Phil Fisher, Bob Moenart, John Merrick

The chapter has grown from the original 18 members to 321 as we begin the year 2000. The most important benefits our members enjoy are the friendships and cooperation, which results from being an active participant in monthly meetings. We hope you will participate actively in your chapter.

Assistant Director/Internal Audit Central Michigan University

This internal audit position performs information system audits of University departments and activities and may assist in operational, financial and compliance audits. Minimum qualifications include a Bachelor's degree in accounting, information systems or related field; two years of increasingly responsible auditing or information systems experience; ability to organize and document work effectively; familiarity and experience with information system auditing or information systems; ability to communicate effectively and project a positive image; experience with word processing and spreadsheet software. Desired qualifications include certification as a CPA, CIA, or CISA; familiarity with higher education or fund accounting and SAP. Send cover letter, resume, and the names, addresses and phone numbers of three professional references to: Human Resources/Staff, Rowe 109, Mt. Pleasant, MI 48859. Review of applications will continue until the position is filled. CMU provides flexible benefits, an excellent retirement program with tax deferred investment options, tuition waiver for employee and family, and competitive salaries in an environment committed to excellence and customer service. CMU, an AA/EO institution, is strongly and actively committed to increasing diversity within its community (see www.cmich.edu/aeo.html).

The Year At A Glance

Meeting Date	Pre-Dinner Topic	Post Dinner Topic
January 19, 2000 (Wed) <i>Joint meeting with AITP (Troy Marriott)</i>	Intrusion Detection Systems	Understanding Internet Security Risks
February 16, 2000 (Wed)	Post Y2K Concerns	CISA Roundtable
March 15, 2000 (Wed)	Implementing CobIT	Controlling the Desktop
March 2000—CISA Review Course begins		
April 19, 2000 (Wed)	Auditing SAP Applications	Auditing PeopleSoft Applications
May 17, 2000 (Wed)	Software License Administration	Risk Modeling
June 20, 2000 (Sat)—CISA Exam		

DATA BYTE

