



The Disk Patch

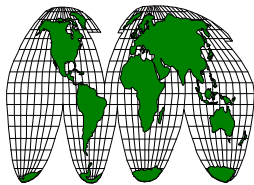


Volume 18 Issue No. 1

*Newsletter of the Winnipeg Chapter of the
Information Systems Audit and Control Association*

December, 2000

Message From The President



As president of the Winnipeg Chapter, I am looking forward to continuing our commitment to providing a high caliber of current events. Over the past couple of years, we have focussed on providing increased specialized and hands on training to meet the demanding requirements of the IT profession. I look forward to working with a very experienced and dedicated board that has taken on more and more challenges each year.

Our web site is an excellent source of information. We have a number of informative pages as well as links to various other information sources.

Gord Glesmann
President, Winnipeg Chapter

Inside This Issue:

2000/2001 Board of Directors	2
From the Editor's Desk	3
Spotlight On "The Need for a Balanced Security Posture"	4
Your Board	5
Bits & Bytes	7
2000/2001 Program	8



**Information Systems Audit and Control Association
Board of Directors
2000-2001**

<u>Position</u>	<u>Name</u>	<u>Voice</u>	<u>Fax</u>	<u>Email</u>
President	Gord Glesmann	945-3790	945-2169	gglesmann@pao.mb.ca
Vice President/ Program Chair	Roger Yost	945-3277	948-3860	ryost@gov.mb.ca
Assistant Program Chair	Alan Gellatly	926-2400	944-1020	alan.m.gellatly@ca.pwcglobal.com
Treasurer	Fred Horbaty	926-2411	944-1020	Fred.j.horbaty@ca.pwcglobal.com
Assistant Treasurer	Barry Saunders	945-4106	945-2169	bsaunders@pao.mb.ca
Secretary	Mike Rogers	474-6691	474-7638	rogers@ms.umanitoba.ca
Director - Newsletter	Jeff Thomas	944-3639	947-9390	jefthomas@deloitte.ca
Director - Membership & CISA	Les Hansen	946-7918	946-8478	les.hansen@gwl.ca
Director - Marketing				
Director - Program	Stewart Bidinosti	986-8274	986-4134	sbidinos@city.winnipeg.mb.ca
Director - Program	Mike Rogers	474-6691	474-7638	rogers@ms.umanitoba.ca
Director - Program	John Graeb	632-2194	633-6489	jgraeb@rrc.mb.ca
Director - Program	Jeff Murray	933-0264	956-0138	jeff.murray@ca.eyi.com
Director - Program	Lawrence Elkow	474-8430		cyberjet@icenter.net
Director - Program	Jeff Butler	667-5535	663-0308	jbutler@wilsonautoelectric.com
Director - Program	Pat McCarthy	956-8188		pat.mccarthy@investorsgroup.com
Director - Program Email	Ken Fitzpatrick	949-3648	727-7761	kfitzpatrick@westmangroup.com
Director - Research & Library	Dan Swanson	956-8625	942-1880	dan.swanson@investorsgroup.com
Director - Security	Dave Abesamis	956-8782	942-1880	ABESAD1@investorsgroup.com
Event Registrar	Cheryl Devaney	945-4130	948-3021	Cdevaney@fin.gov.mb.ca
Past President	Barry Safiniuk	933-0230	956-0138	barry.safiniuk@ca.eyi.com
Webmaster/Program Fax	Michael Li	947-6912		mike@ingen.mb.ca

If you have any comments, questions or ideas about the chapter activities, publications, seminars, membership, C.I.S.A. designation, library books or would like other information about the ISACA, please contact one of the above persons.

From the Editor's Desk:

ISACA plays a number of significant roles in the world of IS audit including certification, standard setting, research, authoritative publications, and professional networking opportunities. From a local chapter perspective, one of the best things about ISACA is the opportunity for truly outstanding learning and growth.

Learning Opportunities

In past years I have looked forward to attending large conferences in warm cities and getting in a good solid week of learning and networking. I have enjoyed an evening chat with many of you while reviewing the day's happenings.

This year I am going to try something different. I am going to attend as many of the local learning events as I can. The reason for this is threefold:

- I want to support and encourage the high quality of training activities that we have been bringing to table these past years.
- I want to send a message to people across the country and within Winnipeg that we are hosting world class learning and growth events right here in Winnipeg.
- I want to spend more time in sessions with people that I will be working with on a daily basis.

I will still go to International ISACA events, but it won't be the focus of my learning. First and foremost, I want to make sure that I help to keep local learning opportunities strong and effective.

Already this year we saw an excellent **Hands on Unix Security program** with Randy Marchany of Virginia Tech and heard Jan Wolynski of IBM talk about E-Commerce Security. I wonder how many IS auditors in Winnipeg are **not** interested in E-Commerce Security?

What is coming up that's really interesting?

On December 13 we'll go for lunch with Marc Rogers, CISSP. Marc is working on his Ph.D. in Psychology, focusing on the behaviour of criminals who use the Internet and computer systems to commit their crimes. Marc has extensive computer security experience so I expect he will have some interesting

things to say.

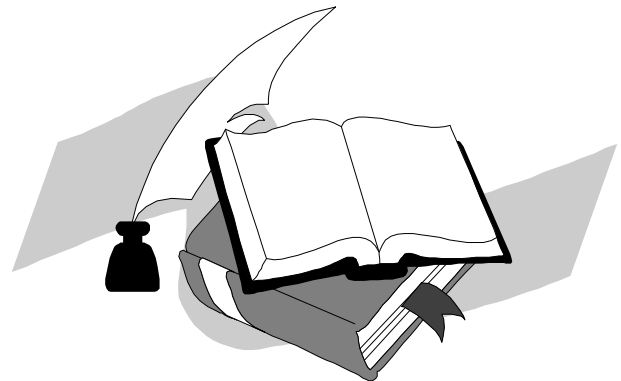
The new year starts three days of training January 16, 17 and 18. **Fraud Detection and Investigation** for two days and a day of **Fraud Awareness for Managers**. This is a joint presentation with the CFE and IIA presented by Courtney Thompson of Courtney Thompson & Associates in Dallas Texas.

February 7 (mark it down!) brings a day of **SAP Audit** training with Graham Larson from Deloitte & Touche. Stewart Bidinosti is organizing this one so be sure to give Stewart a call and thank him.

If you don't need SAP training, maybe 2 days of **Oracle Security Audit and Control Issues** are more to the point. Betty Dorsey, MIS Institute, will be in town March 1 and 2 to present this program.

That's all I'm going to tell you about for this issue of Disk Patch. The rest of the good news will have to wait until the next issue. Thanks to everyone who contributed information for the Disk Patch. Like most good things, it is a team effort!

**Jeff Thomas, CA, CISA, CMC
Newsletter**



Write to Disk Patch at:

Jeff Thomas, CA, CISA, CMC
c/o Deloitte & Touche LLP
Enterprise Risk Services
360 Main Street, Suite 2300
Winnipeg, Manitoba R3C 3Z3

email: jeffthomas@deloitte.ca
facsimile: (204) 947-9390

Or call...
telephone: (204) 944-3639



Spotlight On



The Need for a Balanced Security Posture

Almost daily the media reports cases of the evil "hacker" attacking some system or network. Information security surveys are being conducted, and concluding that information security is important to businesses (not a very amazing finding I may add). Information security companies are popping up at an unprecedented rate, with adds depicting some young male counter-culture stereo-type, who will no doubt "own" your systems unless you hire the company or buy the product. The unfortunate side effect of all this is that business, organizations, governments, and users, start to focus information security almost exclusively on the outside threat. But, what about the threat that is already on the inside? What about the disgruntled employee, or mole, or agent working for the competitor, or simply the professional criminal?

The dangerous or criminal insider is as big a threat, if not bigger, than the "boogeyman" outside attacker. There is a plethora of documented insider attacks against businesses, governments, etc. The CSI/FBI 1998 Computer Crime Survey indicated that the average outside attack cost companies \$56,000.00, while the average insider attack cost companies \$2.7 Million. The CSI/FBI 1999 Computer Security Survey indicated that 55% of the reported attacks were from insiders. The more recent CSI/FBI 2000 Computer Crime Survey stated that 71% of the respondents had been the victim of internal attacks. The Director of the FBI, Louis J. Freeh, in a recent statement before the US Senate, stated that the disgruntled insider was the principal source of computer crimes.

Academics are starting to turn their attention to insiders as well. Recent studies have begun to look at the characteristics, and motivations of the criminal insiders. There has been some recent preliminary work at developing a sort of taxonomy of the insider. These studies suggest that the most common insider is the disgruntled employee who feels slighted and plays out a revenge scenario against the organization. Other categories of insiders include, Explorers, Good Samaritans, Hackers, Golden Parachuters, Machiavellians, Exceptions, Proprietors, Avengers, Career Thieves, and Moles.

Despite the anecdotal, and documented evidence that internal attacks are a risk, most organizations, when developing their information security posture, ignore the insider. I have seen more than one organization whose information security environment could best be described as a "wagon wheel". This being the kids treat with the hard crusty exterior and the soft mushy inside. Organizations spend tens of thousands of dollars on external firewalls, Intrusion Detection Systems, VPNs, and developing a DMZ, but almost nothing on the inside apart from maybe host based anti-virus. It is imperative that we, as an industry, start promoting and educating our customers toward a more balanced approach to information security. Organizations need to pay as much attention to their inside security, as they do to their outside perimeters. What sense is there in fortifying the hen-house if the fox is already inside. This unbalanced posture gives us a false sense of security. If we are only as secure as the weakest link in the chain, then as it stands today, we may be in serious trouble. We may be ignoring the criminal insider, but they are not ignoring us.

Marc Rogers, Ph.D. (Candidate), CISSP

- 1 The Survey did indicate that internal attacks had dropped to 38%, but that theft of proprietary information and internal internet abuse had risen.
- 2 Shaw, E., Post, J., & Ruby, K. (1999). Inside the mind of the insider. Available: <http://www.securitymanagement.com/library>
- 3 Interested readers are directed to the reference above for more details.

Fred Horbaty, CA, Treasurer

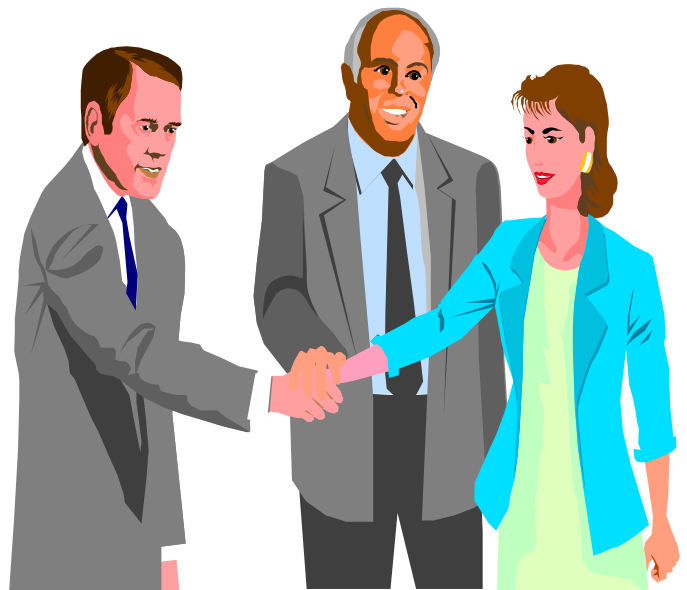
Fred is a Manager, Global Risk Management Solutions, with PricewaterhouseCoopers LLP in Winnipeg. Fred specializes in providing computer assurance services including financial audit support, information system risk assessments and section 5900 reporting. Fred joined ISACA in 1999 and is currently pursuing his CISA designation. Fred attained his Chartered Accountant designation in 1999.

Barry Safiniuk, CISA, Past President

Barry is a Consulting Manager with Ernst & Young's eSecurity Solutions Practice. Barry is an ex-programmer by trade and currently specializes in IS and IT Auditing, Information Security advisory services, Project Management and the occasional Section 5900. 2000-2001 will be Barry's eighth year with ISACA. He received his B.Sc Honors degree (Computer Science major) in 1979 and his CISA designation in 1996. Outside of work Barry likes to spend his time camping with his wife and two children and playing sports.

Patrick McCarthy, Program Director

Pat is the Information Security Leader for Great-West Life, London Life and Investors Group. Pat is responsible for directing effective information security planning and implementation for Great West Life, London Life and Investors Group. The Information Security Leader serves as the owner of all Information Security Systems (ISS) policies, procedures, and practices, oversees all ISS processes, and serves as the focal point for all ISS issues and concerns. Prior to Pat's recent appointment, he worked for Great-West Life as the Associate Manager(IT) in the Internal Audit department.



**Your Winnipeg Chapter
Board Members**

Jeff Thomas, CA, CISA, CMC, Newsletter

Jeff is a Senior Manager, Enterprise Risk Services, with Deloitte & Touche in Winnipeg. Jeff specializes in providing information systems assurance services including financial audit support, WebTrust, SysTrust and Section 5900 reporting. Jeff joined ISACA in 1995 and attained his CISA in 1997. Jeff is also a Chartered Accountant (1994) and Certified Management Consultant (1999). In typical Winnipegger fashion, Jeff likes to spend summer weekends at the lake with his wife and three children.

Bits & Bytes

All the news that's fit to print. From ISACA International, members, and anywhere else we can find it.

010011010011000101101001001110101110100110110110100100101101000110011

CISA Exam Results

Congratulations are due to these very talented individuals who passed the CISA exam in June:

- Ms. Lauren DeVlieger, CGA
- Mr. Kevin Henry, CISSP
- Mr. Gerry Koreman, CGA
- Mr. Raymond Lau
- Mr. Frederick Hobarty, CA
- Mr. David Sachvie, CA

The next step towards achieving the CISA designation is completion of the work requirements. For more information on the CISA designation and how it can benefit you call Les Hansen, Director, Membership & CISA, 946-7918.

Auditing Continuing Education Hours

It might seem odd if the Information Systems Audit & Control Association didn't audit members' continuing education (CE) hours. So as to avoid any such perception, ISACA is auditing the 1999 CE hours of selected members. If you have been selected for audit remember that the deadline for complying with the request for information is December 31, 2000. Failure to comply will result in revocation of the CISA designation.

Now where did I put my 1999 CE documentation?

New IT Security Credentialing Program

ISACA's Board of Directors recently approved advancement on an IT security credentialing program. To this end, the Board has instructed a recently appointed Credentialing Task Force to research the IT security certification market and compare/contrast the common body of knowledge of existing

programs to the CISA job analysis.

Based on this research, the task force will present the Board with its recommendations on how to proceed, which may include working with others and/or offering the credential as a CISA specialty.

2001 ISACA Educational Opportunities

North America CACS 2001

April 29 to May 4, 2001

Lake Buena Vista, Florida, USA

You will not want to miss the 31st annual conference, held at the world-famous Disney's Contemporary Resort in Lake Buena Vista, Florida. Conference presentations will include:

- The Virtual Audit Department
 - Core Competencies
 - E-Business
 - Fraud and Forensics
 - CIO Perspective on Audit Issues
- and much more.

Info Exchange, highlighting the latest products and services, will also be showcased. A very special evening event is also being planned. ISACA members who register before January 31, 2001 will receive US \$100 off the US \$1,295 conference registration fee.

Members can access the ISACA web site www.isaca.org/conf1.htm for timely information.

International Conference 2001

June 10 to 13, 2001

Paris, France

Now is the time to plan to attend the International Conference 2001! A thought-provoking and insightful conference, this event will be sure to educate, motivate and inspire you. Join colleagues and peers from around the world in the City of Lights, Paris.

Conference presentations will include:

- IT Governance
- E-business
- IT Audit Strategies
- Information Security Management Systems
- UNIX
- LINUX
- Windows 2000

An exhibition showcasing the latest and best IT products and services, coupled with a special evening event, ensure a conference to remember.

ISACA members who register before March 12, 2001 will receive US \$100 off the US \$1,295 conference registration fee. Check www.isaca.org/cof1.htm for updates.

Not to mention bagettes, red wine, the Arc de Triomphe, the Louvre

Continue your education with ISACA by visiting our Internet Resource Centre

<http://www.isaca-wpg.org/>



Discount on COBIT® (Control Objectives for Information and related Technology) 2nd Edition © (includes Executive Summary, Framework, Control Objectives, Audit Guidelines, Implementation Tool Set and fully searchable CD-ROM). Discounts on CISA® Examination fee and materials. Discounts on leading-edge technical and managerial conferences and workshops. Discounts on co-sponsored events. Subscription to the bi-monthly Information Systems Control Journal, which features articles on current and future practices and technology, and *Global Communiqué*, a member publication. Access to the latest IT research and to ISACA Bookstore publications. Leadership and networking opportunities through participation on ISACA boards/committees that are making a positive impact on the IT profession.

Answering the Membership Value Question

“What's in it for me?”

become better at your job as a result of access to leading-edge research

increase your value to your employer by expanding your warehouse of skills

pay less for publications of value to you

expand your network of business contacts

International ISACA web site:

<http://www.isaca.org/>

earn global credentials in the IS audit profession with CISA accreditation

prepare yourself for management responsibility

leadership opportunities through participation on ISACA boards and committees

IT Balanced Scorecard

Did you notice that Winnipeg's own Ronald Saull (*MBA, CSP, Senior Vice President and Chief Information Officer of the Information Services division of Great-West Life, London Life and Investors Group*) had an article in Volume 2, 2000 Information Systems Control Journal?

Ron's article includes a discussion of the trend for consolidation and the consequent impact on IT operations.

Ron is the past chairman of the ISACF Research Board and is currently active as a member of the Research Board, the International Board of Trustees and the IT Governance Task Force. He was recently appointed to the COBIT Steering Committee which is engaged in the development of COBIT 3rd Edition, which includes the addition of the Management Guidelines.

2000/2001 Program & Events

The *Information Systems Audit and Control Association (ISACA)* is devoted to the development and support of professionals involved in the audit and control of computer-based systems. The 2000-2001 professional development program covers management issues and control practices facing professionals involved with information technology (IT) and audit.

Date	Topic	Speaker	Event Director(s)	Advance Registration Deadline
September 20, 2000 Luncheon	E-Commerce Security	Jan Wolynski	Mike Rogers 474-6691	
November 30 & December 1, 2000 2 day event	Hands on Unix Security (Hands on lab at U of M Downtown with individual computers)	Randy Marchany, Virginia Tech	Dave Abesamis 956-8782	
December 13, 2000 Wednesday Luncheon	Information Security - A Balanced Approach	Marc Rogers	Pat McCarthy 956-8188	
January 16, 17 & 18, 2001 Tuesday, Wednesday & Thursday 3 day event	Fraud Detection & Investigation (2 days) Fraud Awareness for Managers (1 day) (Joint session with CFE & IIA)	Courtney Thompson Courtney Thompson & Associates, Dallas Texas	Mike Rogers 474-6691 Brian Brown (IIA) 944-5660 George Anderson (CFE) 954-4444	January 12, 2001
February 7, 2001 Wednesday 1 day event	SAP Audit (Joint session with CGA & IIA)	Graham Larson, Deloitte & Touche	Stewart Bidinosti 986-8274	
March 1 & 2, 2001 Thursday & Friday 2 day event	Oracle Security Audit and Control Issues	Betty Dorsey, MIS Training Institute	John Graeb 632-2194 Lawrence Elkow 474-8430	
April 9, 10 & 11, 2001 Monday, Tuesday, & Wednesday 3 day event	Intermediate IT Audit and Security	Stuart B. Holoman, MIS Training Institute	Jeff Murray 933-0264	
May 17, 2001 Thursday Luncheon	Enabling Security, Integrity, and Trust for Your E-business Initiatives	Robert Reimer, PricewaterhouseCoopers	Alan Gellatly 926-2400	