



The Disk Patch



Volume 20 Issue No. 1

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

December, 2001

Message From The President

Roger Yost,
2001-2002 ISACA Winnipeg Chapter President



Welcome to the Winnipeg ISACA Chapter newsletter. We strive to be 'the little chapter that could' in bringing world class training to our members and the Winnipeg IT community. This year we are offering a mix of luncheon and multi-day sessions with topics that were suggested in our annual member survey. New this year is our **free members event**, held on December 6 where members will have a chance to network with other members and learn more about what the chapter has done and is planning to do.

Inside This Issue:

2001/2002 Board of Directors	2
From the Editor's Desk	3
Spotlight On "Information Security Strategies for Successful Protection"	4
Bits & Bytes. All the news that's fit to print	6
Fear and Loathing in the Audit	8
ISACA Membership Value	9



*Information Systems
Audit and Control
Association*

Information Systems Audit and Control Association Board of Directors 2001-2002

<u>Position</u>	<u>Name</u>	<u>Voice</u>	<u>Fax</u>	<u>Email</u>
President	Roger Yost	945-3277	948-3277	ryost@gov.mb.ca
Past President	Gord Glesmann	945-3790	945-2169	gglesmann@pao.mb.ca
1st Vice President/Program Chair	Lawrence Elkow	474-8430		cyberjet@icenter.net
Secretary	Mike Rogers	474-6691	474-7638	rogers@Ms.Umanitoba.ca
Treasurer	Fred Horbaty	926-2411	944-1020	Fred.j.horbaty@ca.pwcglobal.com
Asst Treasurer	Barry Saunders	945-4106	945-2169	bsaunders@pao.mb.ca
Newsletter Editor	Jeff Thomas	957-2291	957-0808	jwthomas@kpmg.ca
Webmaster/Program Fax	Michael Li	947-6912		mike@ingen.mb.ca
Director Marketing	Jeff Murray	933-0264	956-0138	jeff.murray@ca.eyi.com
Director Research	Dan Swanson	956-8625	942-1880	dan.swanson@investorsgroup.com
Director – Membership & CISA	Les Hansen	946-7918	946-8478	les.hansen@gwl.ca
Director – Program	Stewart Bidinosti	986-4214	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	Barry Safiniuk	275-4394		bsafiniuk@cangene.com
Director – Program	Alan Gellatly	926-2400	944-1020	alan.m.gellatly@pwcglobal.com
Director – Program	Patrick McCarthy	956-8188		pat.mccarthy@investorsgroup.com
Director – Program	Bryan Mansky	986-4136	986-4134	bmansky@city.winnipeg.mb.ca
Event Registrar	Cheryl Devaney	945-4130	948-3021	Cdevaney@fin.gov.mb.ca

ISACA International Internet Addresses

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

E-Mail:

membership@isaca.org

certification@isaca.org

conference@isaca.org

education@isaca.org

publication@isaca.org

research@isaca.org

exec@isaca.org

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:

The 2001/2002 program year at the Winnipeg ISACA chapter is off to a huge start. You can check out our web page at <http://www.isaca-wpg.org> for all program details and gobs of other really useful stuff.

Whatever you do, don't forget about the **FREE LUNCH** for ISACA members on December 6 with Jon Singleton. Jon's got a lot of stuff happening what with the school board fiasco and opposition allegations of meddling so I am sure he will be a very interesting speaker. Actually, Jon is supposed to be talking about IT Governance, an area that has been getting a lot of attention lately and on which Mr. Singleton is well qualified.

Starting January we have lined up 8.5 days of really excellent training on top of breakfasts and lunches. In depth training includes Systems Assurance, Auditing Business Continuity Plans, Windows 2000 Hacking, CISA Review and Project Management for IT.

Also on our web page you will find an announcement congratulating this year's successful **CISA** exam writers. Congratulations to

Mr. Dave T. Abesamis
Mr. Wade J. Bo-Maguire, CA
Ms. Nicole L. Brown, CIA
Mr. Jon A. Lamb, CGA, CIA
Mr. Patrick J. McCarthy, CAP
Ms. Kerri S. Pelland, CA
Ms. Signy E. Shaw, CA
Mr. Richard G. Winchester

The Bits & Bytes section of this issue of DiskPatch has some great news about K-Net, ISACA's global knowledge resource. Check out the news and then check out K-Net at <http://www.isaca.org/gir/girMenu.cfm>

In the last newsletter I presented an opportunity for you to earn some money, just by sending me an email. And then, when the newsletter came out, my email address changed. So for those of you who responded and figured you got shortchanged, here it is again.

Here's a challenge to all Disk Patch readers:

Imagine that I flip a coin (a loonie) and make a bet with Roger Yost. For each coin toss that comes up heads I will give Roger a dollar and for each coin toss that comes up tails Roger will give me a dollar. Simultaneously I make a bet with Mike Rogers on the same coin toss so that Mike gives me a dollar when it comes up heads and I give Mike a dollar when it comes up tails. Finally, Roger and Mike and I agree we will only toss the coin five times.

What does this coin toss example illustrate about risk and control?

I have a loonie for the first five people who send me an answer at the email address shown below (Disk Patch reviewers excluded). All the answers will be included in the next issue of Disk Patch. Who knows, maybe Donn B. Parker will send me an email (see page 4).

Thanks to everyone who contributed information for the Disk Patch. Like most good things, it is a team effort!

Jeff Thomas, CA, CIA, CISA, CMC



Write to Disk Patch at:

Jeff Thomas
c/o KPMG LLP
Information Risk Management
One Lombard Place
Suite 2000
Winnipeg, Manitoba R3B 0X3

email: jwthomas@kpmg.ca
facsimile: (204) 957-0808

Or call...
telephone: (204) 957-2291



Spotlight On



Executive Security Briefing: Information Security Strategies for Successful Protection

Donn Parker got up in front of the audience at the Institute of Internal Auditor's opening day Security Conference and told us all we were doing security wrong. Donn went on to say that the common current day information security objectives and benefits were backwards, that the information security jargon we use is wrong, and our security foundation and framework is faulty. Donn is a contrarian and he knows it.

A retired emeritus senior consultant at AtomicTangerine, Donn B. Parker, CISSP, has spent 30 years in the computer field engaged in research, writing, consulting, and lecturing world-wide on computer crime and information security. He has performed more than 250 security reviews, appeared on 60 Minutes and 20/20, and been featured in People, Fortune, Time, Newsweek and other magazines. His sixth and most recent book is "Fighting Computer Crime, a New Framework for Protecting Information". Donn spends his time interviewing, analyzing and understanding the enemy.

The objective of information security is not reduction of risks or losses, Donn tells us. Rather, the objectives are (1) least protection to achieve due diligence, and (2) achievement of organizational objectives. The benefits of a security program then become the possible reduction of risk and losses and avoidance of negligence.

Focusing on due diligence as the objective, rather than risk reduction, is necessary, Donn argues, because the sources of risk are unknown and constantly changing. When thinking about security we should start with the enemy. They are the reason we need security. When people talk about attacks, following the technical details, and examining vulnerabilities, they are missing the enemy. Unknown, unpredictable and irrational enemies having unknown changing goals, targets and timing are attacking our greatest unknown vulnerabilities.

This adds up to a lot of uncertainty as to where the next attack is coming from. Security professionals are left trying to defend against all possible attacks while the attacker can focus on the one vulnerability we don't yet know about. In this context, due diligence, taking whatever steps are reasonably available, becomes the goal, rather than getting caught up in chasing the unknown.

Donn corrected our security jargon. For example, when we talk about Integrity of data we may think this means the information is correct. Integrity means only that the information is in good condition. Clearly, having a common understanding of the terms we use everyday in discussing information security is critical to achieving our objectives. Donn spent some time explaining that there is no such thing as a security audit, and that work related to examination of security control objectives and activities should properly be called security review (*audit practitioners know that SysTrust is an actual audit, performed by Certified Public Accountants in the U.S. and by Chartered Accountants in Canada, that specifically addresses security control objectives and activities*).

The new Framework of Information Security that Donn describes replaces the current and faulty

(Continued on page 5)

(Continued from page 4)

foundation and framework model. The current framework describes information security as:

the preservation of information **qualities** from unintended **actions** by risk assessment selection of **specific controls** to achieve the reduction of risk of loss to an acceptable level.

Where: **qualities** are confidentiality, integrity, availability, nonrepudiation, and authenticity of people
actions are destruction, disclosure, use, and modification
specific controls are prevention, detection, recovery, and awareness

The New Framework is described as:

Information security meets the owners' needs to preserve **qualities** of information from accidental and intentional acts of abusers and misusers and forces that would cause **bad things** by applications of **various** safeguards and practices that are selected by due diligence and special needs to achieve **objectives**

Where: **qualities** are availability, utility, integrity, authenticity, confidentiality, and possession
bad things are destruction or copying, interference with use, use of false data, modification or replacement, misrepresentation or repudiation, misuse or failure to use, finding or taking, disclosure or observation, endangerment
various includes avoidance and deterrence, prevention and detection, mitigation and investigation, transference, sanctions and rewards, recovery and correction, motivation and education.
objectives are avoidance of negligence, an orderly and protected society, conformance to laws and regulations, ethical conduct, successful commerce, and privacy

This new framework is certainly more comprehensive and maintains Donn's focus on due diligence as the primary objective of information security activities.

The keys to achieving due diligence

- ◆ Perform security reviews and benchmarking
- ◆ Do what others do under similar circumstances or document reasons for deviations
- ◆ Use sources of standards of due diligence and generally accepted good practices

Donn recognizes that one of the difficulties in preserving a secure environment is engaging employees to ensure their commitment to security. Or, as Mr. Parker says, Motivate Motivate Motivate! We need to find ways to make security a part of job performance, not in conflict with it. Security motivation must therefore be ahead of security awareness.

The Top Four Recommendations

- ◆ Update your policies, standards, and training using the new framework.
- ◆ Replace risk-based security with due diligence
- ◆ Strive for prudent security in your organization, not the maximum that people will tolerate
- ◆ Motivate good security with rewards, penalties, and inclusion in job performance evaluations.

Written by Jeff Thomas, CA, CISA, CIA, CMC
Senior Manager, Information Risk Management
KPMG

This article is the first in a series based on presentations delivered at the IIA Security Conference in Winnipeg, October 16 to 19, 2001. The articles are intended to summarize the key thoughts of the presenter and should not be considered an alternative to conference attendance. While an attempt has been made to capture the significant elements of the presentation the reader should be aware that errors and omissions may exist and the content is highly summarized. This article was based on notes taken during the presentation as well as handouts available to conference attendees.

Bits & Bytes

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

0100110100110001011010010011101011101001101101101001001011010001100110110001101011

CISA Mentor Program

ISACA International encourages all CISAs to become mentors for prospective CISA candidates.

According to member and CISA survey information, the best promoters of the CISA exam are those who have become CISAs or are strong supporters of the program through their continued promotion of the program to their staff, colleagues and peers.

A CISA mentor is encouraged to:

- Speak with at least one non-CISA about taking the exam in 2002
- See ISACA's web site for more details. A downloadable copy of the *Bulletin of Information* can be obtained from the ISACA web site at www.isaca.org/exam1.htm
- Follow up from time to time with the individual to see how he/she is doing

CISA Tops Certification-related Bonus List

In a recent survey by the Foote Partners, the CISA designation was determined to provide professionals with the highest salary bonus among the 39 technical skills certification programs examined in the survey, according to an article in the August 2001 issue of *Information Security* magazine. A press release regarding this survey is available at www.isaca.org/prcisacert.htm.

Journal Update

The *Information Systems Control Journal* is seeking articles for volume 2 2002, to be issued in March 2002. The deadline is 2 January 2001, and the theme is **Information Integrity**. The *Journal* is particularly interested in articles on risk, vulnerabilities, best practices in risk and best practices in attaining information integrity. For more details, e-mail jblader@isaca.org

K-NET Services

K-NET, a global knowledge network for IT governance, control and assurance, has recently added a feature to allow searching of its knowledge database.

With 12 subject areas, more than 90 topic areas and

more than 1,400 references, this feature provides quick results when searching by words or phrases throughout the database.

This Internet-based compendium of knowledge is updated weekly to include articles, books and web sites that have been peer-reviewed by members of the association. References are expected to more than double over the next twelve months. As the number of references increases, the search engine will become even more valuable.

In addition to the search feature, K-NET offers a personalized service that enables members to remain current on topic areas most important to them. With notification (push) technology, K-NET automatically e-mails members on a weekly basis about new database references within their specified areas of interest. Members can activate this personalized service and register to receive updates on specified topics of interest simply by visiting www.isaca.org/gir/gir_tuf.htm. They are certain to find this personalized service of great value.

K-NET Volunteers Can Earn CPE Credits

Volunteer to assist in the continued development of K-NET.

By submitting potential K-NET web site references or volunteering to review and evaluate web sites for possible inclusion in K-NET, members truly can make a difference. Your input will help ensure that K-NET is the professional resource fellow ISACA members will turn to for answers to their professional questions.

Additionally, members who volunteer and participate as reviewers of potential K-NET web site references can earn up to 10 CE credits.

This is a great opportunity to make a contribution to the profession. Members may obtain additional information on becoming a K-NET volunteer at www.isaca.org/knetvol.cfm.

To access K-NET, visit www.isaca.org/knet.

(Continued on page 7)

(Continued from page 6)

Research News

COBIT

To further strengthen COBIT's benefits, ISACA has added 16 new case studies to the eight already featured on its web site. These case studies provide practical applications of COBIT in a multitude of different business and industry environments.

To provide convenient browsing, a chart with brief outlines of all 24 case studies, as well as a link to the full text of the study, can be accessed at www.isaca.org/ct_case.htm. Please utilize this resource.

Preparations have already begun for development of COBIT 4th Edition. A benchmark survey to enhance the maturity models is being conducted. Additionally, a special version of COBIT for small to medium-sized enterprises is envisioned.

Creating the Privacy-compliant Organization

The ISACF Research Board is developing a management guide to address the complex issues of privacy. The guide will include sample policies, a 10-step methodology, work plans, questionnaires and templates to guide the organization through the process of meeting legislative, regulatory and marketplace expectations of and demands for personal information privacy. Look for availability in December 2001.

Security and Risk Management in ERP Project

ERP systems are now pervasive globally in medium to large enterprises and in the public sector. There has been a need for a series of definitive audit guides, including details on testing techniques within specific ERP products and their execution, for these products for some time. This technical reference guide series will cover application security and technical infrastructure considerations for the three largest ERPs. The purpose of this research is to document current best practices in ERP risk and control, identify future trends in ERP risk and control issues, and design a practical how-to guide. Some sections of the guides, which cover the introduction to ERP and strategic risk management in an ERP environment and directions in ERP audit, will be common to all three guides. The remaining sections dealing with ERP product-specific characteristics and auditing techniques will be unique to each of the respective technical reference guides.

The first in this series will be SAP, which is one of the leading developers of enterprise applications worldwide. Its primary ERP product is SAP R/3. The SAP portion of the project is targeted for completion in the fourth quarter of 2001. The remaining two guides in the series will focus on

Oracle and PeopleSoft.

Wireless Communication Project

Because wireless communications transcend traditional and regulatory boundaries, they pose significant technical challenges, as well as greater challenges in the areas of control, security and audit. Wireless users expect the same features they enjoy on their home network when they roam onto foreign networks and expect to use their communications devices wherever they travel. This project will provide both a technical and functional assessment and will be written from a business and risk management perspective. The project is targeted for completion in first quarter 2002.

Enterprise Information Integrity Project

In an increasingly dynamic global environment, IT organizations must address complex solutions and operating environments to provide assurance of the dependability and trustworthiness of information across the enterprise. The purpose of this project is to define the key elements of enterprise information integrity, as well as benefits criteria associated with them, and to present a framework and process for management. The Centre for IS Assurance is expected to conduct this project for ISACF.

Oracle Database Project

Work has begun on an update to *Security and Controls in an Oracle Environment*, a part of the ISACA Monograph Series. The revised edition will include the issues that have changed in subsequent Oracle environments, resulting in the addition or removal of topics from the book, and a recommended plan for addressing the changes. Project completion is expected in the second quarter 2002.

IT Control Practices

A prototype is being used by the ITCP Committee to develop IT Control Practices for COBIT control objectives. Chapters are assisting the committee in developing these practices. Please contact research@isaca.org, to participate in this project and be linked to the global research efforts of ISACF.

Managing Access to Platforms Project

"Turning up" and "turning down" access privileges are not quite as simple as flicking a switch. Provisioning encompasses much more than assigning user passwords. It requires companies to determine roles based on predefined business policies and standards, and then assign the appropriate roles to the appropriate users. The objective of this research is to present to senior management, CIOs, COOs and CISOs the concept of resource provisioning management solutions in the current business arena and why companies should move toward establishing a single authoritative system for tracking and granting access to resources within the organization. Project completion is expected in the second quarter 2002.

Fear and Loathing in the Audit

YOU are being audited.

What do you feel when you hear that statement? Some possibilities are excitement, anticipation or elation and the most common one could be dread. Usually this is because you fear some outside individual will be identifying deficiencies that you were not aware of.

ISACA has published COBIT, a set of control objectives that are used by some organisations for auditing systems. I contend that we can reduce the 'dread' factor of auditing if we can introduce COBIT to the application development process and encourage use of the control objectives in COBIT while systems are being developed. This differs from the frequent practice of introducing COBIT to the auditee during an audit.

COBIT may contain control objectives that are not applicable to a particular organisation, due to reasons such as their operating environment. The organisation can document why they have not chosen to follow those control objectives and have that information ready for an audit.

Information system auditing is not about laying blame. It is about recognizing good work and identifying ways that we can do things better. Fear and dread are the auditor's enemy. When a client fears the audit, they will be less willing to internalize and adopt any resulting recommendations.

By putting COBIT into the hands of systems

developers and managers early in the development process, we have a better chance that they will understand and incorporate the COBIT objectives into their systems. And when we perform the audit, they will be familiar with what we are looking for and less fearful of the process.

As auditors, we have a responsibility not only to identify opportunities for improvement, but to do so in such a way that we encourage the implementation of practices best suited to the particular situation. Communicating our expectations (COBIT) early in the development process is key to our success and the success of system developers and managers.



This commentary was prepared by Roger Yost, Winnipeg ISACA Chapter President and Jeff Thomas, Winnipeg ISACA Chapter Newsletter Editor.

**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



“Why should I belong?”

“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