

Control Bits & Audit Bytes

Western Michigan *INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION* Newsletter

FEBRUARY 2002 NEWSLETTER

OFFICERS

PRESIDENT

Leslie Dalzell, CPA
Steelcase, Inc. CH-3E-18
P.O. Box 1967
Grand Rapids, MI 49501-1967
616 / 246-4764
FAX: 616 / 248-7550
ldalzell@steelcase.com

VICE PRESIDENT

Terry Brown, CISA
Meijer, Inc.
2929 Walker N.W.
Grand Rapids, Michigan 49544
(616) 735-7934
terry.brown@meijer.com

SECRETARY

Jamie Depuydt, CISA
Steelcase, Inc. CH-3E-18
P.O. Box 1967
Grand Rapids, MI 49501-1967
616 / 248-7426
FAX: 616 / 248-7550
jdepuydt@steelcase.com

TREASURER

Pam Bradford, CISA
National City, K-A16-C7
One National City Pkwy
Kalamazoo, MI 49009-8002
616 / 376-7523
FAX: 616 / 376-4408
pam.bradford@nationalcity.com

BOARD OF DIRECTORS

CISA COORDINATOR

Michael Sekoni, CISA
Accident Fund of Michigan
P.O. Box 40790
Lansing, MI 48901-7998
517 / 342-4200 ext. 721
FAX: 517 / 342-4299
michaels@accidentfund.com

NEWSLETTER EDITOR

Leslie Dalzell, CPA
Steelcase, Inc. CH-3E-18
P.O. Box 1967
Grand Rapids, MI 49501-1967
616 / 246-4764
FAX: 616 / 248-7550
ldalzell@steelcase.com

PAST PRESIDENT

Rick Cummings, CISA
Jackson National Life Insurance Co.
5901 Executive Drive S52
Lansing, MI 48911-5389
517 / 367-4301
FAX: 517 / 394-1795
rick.cummings@jnli.com

WEB MASTER

John Blair, CISA
Foremost Insurance
5600 Beech Tree Lane
Caledonia, MI 49316-9482
Location Code: 1260
616 / 956-3568
FAX: 616 / 956-4450
john.blair@foremost.com

February 20th Dinner Meeting Holiday Inn -West 7501 W. Saginaw Hwy, Lansing

ACL Toolkits

The main emphasis will be providing an example of a CAAT toolkit that can be built using ACL software.

PROFESSIONAL BIOGRAPHY OF LESLIE DALZELL

Leslie Dalzell joined Steelcase, Inc, in July 2000, as an Information Systems Internal Auditor. Previously, she worked at Rehmann Robson, PC, for three years where she was a Senior Auditor in their Audit and Assurance department. Prior to that, she held the position of Staff Auditor for Beene Garter, LLP. Leslie began her career as an IT Audit Intern with the Michigan Office of the Auditor General.

Leslie earned her Bachelors degree from Central Michigan University with a major in Accounting and a minor in Management Information Systems. She has also obtained her CPA license and is awaiting her CISA certification.

Please make your reservation and meal selection (see below) by February 15th!

Call Jamie Depuydt and make your reservation today!! **(616) 248-7426**
OR e-mail Jamie at jdepuydt@steelcase.com

Costs - \$27 Non Members / \$24 Members

Dinner menu:
1 - Turkey or Chicken
2 - Beef
Salad
Dessert

5:00-5:30 Social Hour / Registration
5:30-6:30 Presentation
6:30-7:30 Dinner

As seen in the media . . .

A very UN–scientific approach to gathering meaningful information from the “giga-tons” of electronic and printed material that intrudes into our lives . . . and is occasionally actually worthwhile! Here are some of the latest “discoveries” . . .



MICROSOFT GETS SERIOUS ABOUT SECURITY

★★★★

If you've seen practically any computer media in the last month or so, you've probably already seen the hype being generated by an announcement from Microsoft that they want to focus on better security in their products. Many of you have scoffed or dismissed it as media hype. Interestingly enough, this editor had the opportunity to sit in on “beef session” between my own company’s senior IT managers and two Microsoft reps, one direct from Redmond(!), the middle of January. During the discussions, the Redmond-based rep made the statement that it hadn't been widely announced as of yet (obviously, he hadn't read any of the major computer ‘rags’ in awhile), but during the month of February, 2002, all Microsoft development staff was stopping work on all projects, and they had been “ordered” to attend security training. As per standard MS-fare, there was no elaboration behind the statement, even after some vivid coaxing by my IT managers and yours truly. The only additional comment on the subject was that every Microsoft developer was going to have some “serious training” in security, and that Microsoft’s goal to incorporate better security within *all* of its apps.

Exactly how effective this training will be, and whether we will actually see some truly “security–conscious” product forthcoming from the people at Redmond are questions yet to be determined. It is somewhat gratifying to see first–hand, however, a major vendor finally realizing the need for proper controls in the products they develop. If nothing else, the lip service was welcome news. Now, about the verification process . . .

THE METER IS RUNNING . . .

★★★★

CIO, Vol. 15, No. 7, January 15, 2002, pp. 52–62

The price to ride with Microsoft looks to have hit a major roadblock. The *Software Licensing 6.0* and *Software Assurance* program has hit a major brick wall in the form of CIO's who are saying “NO!” to what they see as a slow ride to nowhere at an ever increasing fare. The program, which took effect on October 1, 2001, was Microsoft's plan to simplify software licensing management for both itself and its customers by making software a service rather than a commodity. Problem is, it would also raise the license fees for aging Windows and Office products without providing improvements in either. Interestingly, once IT heads started understanding MS's strategy, a new word sprang into their vendor correspondence vocabulary; “NO!” A *CIO* poll of 122 IT executives revealed only 15% of respondents were planning to enroll. But the details get even better. Make a copy of your IT head's issue and read on!

<http://www.cio.com>

STRAIGHT–THROUGH TRADE PROCESSING: ON YOUR MARK . . .

★★★

Computerworld, Vol. 36, No. 4, Jan 21, 2002

For those of you with “degrading memories”, Congress passed a measure whereby financial transactions are supposed to be cleared and settled within 24 hours. The measure, called “straight-through processing”, or “STP/T+1”, was postponed by 2 years following the September 11th tragedy. But a recent poll found that fewer than 10% of financial firms effected by the ruling have taken any steps at all in addressing the upcoming issue. The biggest problem: a lack of standardization in products, technology, and operating platforms. A poll of 113 brokerages attending the Securities Industry Association's STP/T+1 conference found 41% were still evaluating how to move to STP/T+1, 10% hadn't even started the evaluation, 3% had begun evaluation, and 13% had

started modifying their back-office systems and business rules.

<http://www.computerworld.com>

THEY'RE STILL GETTING IN . . .

★★★

"News To Use From Infowar.Com", Jan 25, 2002

Infowar.Com has this innate ability to hit the nail on the head, so when their URL pops upon my e-mail list, you know where I'm headed first! A couple of their more interesting articles from the latest "issue":

- DESTA – Destabilization, Terrorism, & Disinformation, Volume X, No. 1, January 2002 — A Northern Newsletter of Threat Analysis — looking at European threats
http://www.infowar.com/class_3/02/class3_012402a_j.shtml
 - U.S. & Canadian Bank Database Breaches — a December 2001 Evans Data Corp study revealed that 12% of online corporate databases suffered security breaches in 2001, and 27% of banking and financial services databases were breached. 18% of medical/health care and telecomm industries were breached.
http://www.infowar.com/survey/02/survey_012202a_j.shtml
-

“RETHINKING SECURITY – Seven Steps to Tighten Network Security”

★★★

Novell Connection, January 2002, pp. 6–21

There's nothing like getting your info straight from the source. Alan Mark, Novell's Chief Security Strategist, has penned a nice article highlighting seven steps you can take to tighten up your Novell network security. True, it's biased towards Novell utilities and extras, but it also lists some tips, alternatives, and URL references to help you address some common security problems. It is also a useful article when planning the review of security on your Novell network.

<http://www.ncmag.com>

MDOT DOES GOOD (?)

★★

CIO, Vol. 15, No. 8, February 1, 2002, “*Paving Over Paperwork*”, pp. 82-86

It is a welcome surprise to open up a major industry publication and find out that someone from your home town has been cited for doing something good. Michigan Department of Transportation CIO, C. Douglass Couto, is listed as one of the recipients of *CIO* magazines' Tenth Annual Enterprise Value Awards. The MDOT CIO's claim to fame is the implementation of an automated system for collection of road construction inspection data, which has helped the department keep a handle on \$1.5 billion annual road and bridge construction budget, cut staff from 5,000 down to 3,000, and get more projects completed on time, too. Couto's secret: a value methodology based on the Balanced Scorecard. This methodology helps him prioritize his investments and ensures that high-value projects stay on track. Read more about it at:

<http://www.cio.com>

“IT DIFFICULTIES HELP TAKE KMART DOWN”

★

Computerworld, Vol 36, No. 5, January 28, 2002

This ones going to be on the back of most CIO's minds for awhile: Long-standing IT woes play a contributing role in business problems that led Kmart Corp. to seek bankruptcy protection. For former dot-comers', this is old news, but for a retail giant to make this claim is something out of a financial analyst's worst nightmare! Imagine the new CIO having to face a \$195 million write-off for fixing failed supply-chain systems? Daunting task, to say the least. The ink ain't dry on this one yet, so stay tuned . . .

<http://www.computerworld.com>

Looking for some security training? Look west! RSA Security Inc. presents RSA Conference 2002 February 18 - 22, McEnery Convention Center, San Jose CA.

http://www.rsaconference.net/docs/RSA02_Brochure.pdf

Looking for a good source for info on hackers, crackers and data thieves? Try InfoWar.Com. Want to get first-hand info? Check out InfowarCon – 2002, scheduled for Sept 3–6, 2002, in Washington D.C.

<http://www.infowar.com>

The “STAR” guide:	★★★★ = Too good not to pass on!	★★ = Good stuff — it helps
	★★★ = Better than expected!	★ = Worth noting

[Cntl][Alt][
Del]

Taking a hint from “Men in Black”, it’s somewhat surprising what truthful tidbits can be obtained from the “gossip columns” of the IT world (and other “questionable” sources). Here’s some of the latest “fluff” . . .

- ☹ 2001 was known as the year of the e-mail worm. Media analysts are now saying that 2002 will be known as the year of the buffer bug. Why? Because (1) buffer bugs are more effective than e-mail worms, (2) they’re easier to create, (3) they’ve been around for a *very* long time, and (4) most programmers don’t realize that this type of attack is easy to prevent! Windows XP, AOL’s Instant Messenger, Sun Solaris are all suffering from buffer overflow attacks which could have been prevented had the developer limited how much data the buffer takes in. Supposedly, it’s as simple as that. This one will bear watching, folks!
- ☹ With all the fall-out from the **Enron** scandal, did anyone notice that Enron’s Information Security group outsourced themselves into a separate company? While the head of the former Info Security group said it had nothing to do with the company’s financial woes, one has to wonder exactly what promulgated this type of move.
..
- ☹ Under our “Things That Make You Go, “HmMMMMmm” department, the head network engineer for a major southeast Michigan business was overheard griping that the main reason his company was converting servers to Windows .Net from Novell was not because of the advantages of the Microsoft system, but because he can’t find sufficient *human resources* to support NetWare. All the resumes coming in the door have MS-type certifications up the wazoo, but not a single NetWare shingle. Sign of things to come???
- ☹ Seems Novell is getting a bit touchy about all the negative hype Microsoft is spewing forth with its push of its new .Net product line. Novell announced the launch of a new web site, “www.whytheylie.com”, calling the web site an “unapologetic, direct, bold, focused ‘truth assault’ campaign” that combats Microsoft claims.



<p>If you have an article you would like to share with the Western Michigan Chapter members, please submit it to Leslie Dalzell at ldalzell@steelcase.com. Thanks!</p>

Coming Attractions...

March's Meeting: March 20th Michael Sekoni, CISA presenting on "Resumption Planning/Business Continuity Plan" Location to be Holiday Inn -West on Saginaw Highway.

April's Meeting: April 17-18 Peter Osterio Seminar on "Risk Base Integrated Auditing & How to Build Computer Models for Continuous Monitoring". Kalamazoo location to be determined.

Updates regarding the upcoming meeting schedule can be found on the Chapter Website at www.iserv.net/~wmisaca/.

Control Bits and Audit Bytes is a publication of the Western Michigan Chapter of the *Information Systems Audit and Control Association (ISACA)*. The purpose of this publication is to disseminate useful and timely information on automated systems control and security issues to Chapter members and selected practitioners of computer systems audit and security. Articles, submissions, and advertisements are the responsibility of the submitter, and do not reflect the opinions, beliefs, or practices of the Western Michigan Chapter.

Materials submitted for publication in ***Control Bits and Audit Bytes*** must be received by the Newsletter Editor no later than the submission deadline published in the newsletter. If no submission deadline is published, the default deadline is approximately three weeks prior to the next scheduled meeting of the Western Michigan Chapter of the *Information Systems Audit and Control Association*.



*Information Systems
Audit and Control
Association*