

# Control Bits & Audit Bytes

Western Michigan *INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION* Newsletter

## NOVEMBER 2001 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

## November 28th Dinner Meeting

*Duba's Restaurant*

*420 E Beltline NE, GR*

## Software Licensing

The unauthorized or illegal copying of proprietary software products is punishable by fines and/or imprisonment. A nationwide city-by-city crackdown on software licensing compliance began earlier this year. It targeted suspected organizations and companies, fining them up to several hundred thousand dollars for installing unlicensed copies of software programs on their computers. You can help your organization ensure compliance and avoid costly penalties with a few simple steps that will establish and maintain an ongoing software license management program.

### *PROFESSIONAL BIOGRAPHY OF DAVID FLYNN*

David Flynn has over 10 years experience in audit, information technology and project management. His background crosses several industries including banking, manufacturing and utilities. Dave joined Jefferson Wells International in 1996 as a Director of Information Technology and is currently the Managing Director for the Detroit office.

Please make your reservation and meal selection (see below) by November 22nd!

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

### **Costs - \$27 Non Members / \$25 Members**

Lunch menu:  
1 - Chicken  
2 - Beef  
3 - Vegetarian  
Salad  
Dessert

**11:30-12:00 Social Hour /  
Registration  
12:00-1:00 Lunch  
1:00-2:00 Presentation**

## As seen in the media . . .

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



Since the tragic events of September 11<sup>th</sup>, there have been a plethora of activities on the “security front-lines” — some good, some which raise more questions than they answer. Here’s some of the latest . . .

---

### “LAWS? WE DON’T NEED NO STINKIN’ LAWS!”

★★★★

*InformationWeek Behind the Lines* — Oct. 8, 2001

Paraphrasing Alfonso Bedoya's famous line from "The Treasure Of The Sierra Madre", Federal Trade Commission chairman Timothy Muris delivered that message at the Privacy 2001 conference in Cleveland the first week of October. It was his first major address on privacy enforcement under the FTC of the new administration. "Acres of trees died to produce a blizzard of barely comprehensible privacy notices," said Muris, referring to the most recent privacy statute, the Gramm-Leach-Bliley Act, which forced financial firms to disclose their privacy policies to consumers. "This is a statute that only lawyers could love — until they found out it applied to them." Instead of pushing new legislation, the FTC will increase the resources it uses to enforce current privacy regulations by 50%. This includes an increase in the number of "full-time equivalent" FTC employees working on privacy matters from 36 to 60 and significant investment in data-mining software to track spam and cross-reference privacy complaints. Muris' anti-legislation stance is one that rings true with some businesses. Kirk Herath, chief privacy officer for insurer Nationwide, speaking at the conference the day before, said the country doesn't need more privacy legislation. "We need less legislation and less-confusing laws," Herath said.

<http://www.informationweek.com>

<http://www.computerworld.com>

---

### OPPORTUNITY FROM THE ASHES . . . ?

★★★★

*InformationWeek Behind the Lines* — Oct. 8, 2001

An interesting new “buzz word” has surfaced within the IT community following the tragic events of September 11<sup>th</sup>. “Regeneration” is a term, which has been discussed in stem-cell research, but is now being used to describe the opportunity available to those companies that were obliterated by the September 11<sup>th</sup> tragedy. Attributed to a perspective proposed by Mike Corcoran, marketing VP at Information Builders, Inc., “regeneration” is described as the opportunity a number of companies in and around the center of the destruction have to . . . “build their operations and IT infrastructures in an almost idealized fashion because they're starting fresh. They have a chance to establish policies that before Sept. 11 might not have taken root; they have a chance to pursue that "best of all possible worlds" approach to which everyone always aspired but that always collided with the harsh and typically sub-optimal obstacles of reality (a.k.a. "installed base").”

Whether you consider this version of “regeneration” real or nonsense, the concept is clearly coming to the forefront of business and IT heads as we try to come to grips with the events of 9/11 and the ramifications they impose. As audit and security practitioners, it will be our responsibility to keep management aware of the security and controls aspect, which **must** be part of any “regeneration” effort our employers, clients, or

whomever decide to pursue.

<http://www.informationweek.com>

---

## TO ESCROW OR NOT TO ESCROW . . .

★★★

*SANS NewsBites*, Oct. 10, 2001

In an earlier edition of this erstwhile column, we reported to you that some rather overzealous Senators and Congress' people' were attempting to pass legislation, which would require everyone using encryption to escrow their keys with a "third party". The ink wasn't even dry on that item when news came out that several experts and lawmakers have opposed the legislation. Countering the claim that escrowed keys would allow law enforcement officials to decode communication between terrorists and other criminals, Rep. Bob Goodlatte (R-VA) remarked that such person are not likely to place their encryption keys in escrow anyhow. Somehow, I don't think this issue is even close to being decided yet . . .

<http://www.sans.org>

---

## CRITICAL INFRASTRUCTURE PROTECTION COORDINATION

★★★

*SANS NewsBites*, Oct. 10, 2001

The National Infrastructure Protection Center (NIPC), Federal Computer Incident Response Center (FedCIRC), and Critical Infrastructure Assurance Office (CIAO) are in the "Senatorial Doghouse" after appearing before a hearing by the Governmental Affairs Committee to describe their roles in protecting the nation's critical infrastructure. Senators on the Committee were NOT impressed with the organization of critical infrastructure defense and called for untangling the lines of authority and accountability. However, an IT editorial commentator noted that the Committee *missed* one important point: there needs to be some kind of direction that motivates incident response teams to *cooperate* with each other better!

<http://www.sans.org>

---

## NIST RELEASES NEW SECURITY SELF-ASSESSMENT GUIDE

★★★

*News to Use from Infowar.Com 10-22-01*

With everyone in the security industry focused on New York last month, not many people paid attention to the National Institute of Standards' release of a security self-assessment guide. This is really worth a look.

<http://csrc.nist.gov/publications/nistbul/09-01.pdf>

---

## ISP'S WISE-UP(?)

★★★

*SANS NewsBites*, Vol. 3, No. 42, October 17, 2001

A British ISP has made news by joining leading ISPs in this country by suspending the connections of users whose systems are infected with worms and viruses, or who have not applied appropriate patches. ISPs like UUNET have long had the technology and processes in place quickly sever the connections of computers that are attacking other computers. Smaller ISPs are slowly joining these elite ranks.

[www.zdnet.com/zdnn/stories/news/0,4586,5098072,00.html?chkpt=zdhpnnews01](http://www.zdnet.com/zdnn/stories/news/0,4586,5098072,00.html?chkpt=zdhpnnews01)

---

## SYMANTEC GO OOPS . . .

★★★

*SANS NewsBites*, Vol. 3, No. 42, October 17, 2001

We're wondering how many heads have rolled at Symantec after their researchers said that the SirCam worm will drop an additional payload on October 16<sup>th</sup>, and that infected machines run a 5% risk of having all the files and folders deleted from their hard drives. Further analysis by NAI and other researchers showed that an error in the code blocked the erasure.

<http://www.wired.com/news/technology/0,1282,47476,00.html>

<http://www.wired.com/news/technology/0,1282,47582,00.html>

## NEXT!

★★

*Computerworld*, Vol. 35, No. 41, Oct. 8, 2001

Another item, which seemed to get overlooked, is the Department of Justice's announcement that it filed a federal antitrust lawsuit against Computer Associates International Inc. and Platinum, Inc. on September 28<sup>th</sup> for price-fixing in the wake of CA's \$3.5 Billion buy-out of Platinum in 1999. The DOJ alleges that CA assigned one of its employees to "review and approve" Platinum's user contracts before the acquisition had been cleared by government agencies under antitrust laws — a practice called "gun jumping". Also naming Platinum in the suit, the DOJ claimed that the two companies agreed that Platinum would limit the discounts and special contract terms that it offered to users, prematurely reducing competition between the companies.

A database administrator for a US-based electronics component manufacturer provided an example of these activities: Before CA's buy-out of Platinum, the DBA was paying an annual maintenance fee of \$10,000 for 20 copies of Platinum's Plan Analyzer database administration software. *After* the buy-out, the DBA was told he would have to upgrade immediately to a full Platinum product suite at a cost of \$100,000 *plus* \$50,000 per year in maintenance fees. Later, CA told the DBA he would have to buy into CA's management and middleware products at a cost of between \$5 Million to \$10 Million. When told of the lawsuit, the DBA is quoted as saying, "It couldn't have happened to a nicer company".

<http://www.computerworld.com>

---

## E-MAIL IS IT MANAGERS BIGGEST SECURITY CONCERN

★★★

*TechRepublic, Inc.*, Oct. 24, 2001

Gartner Group's *TechRepublic* published the results of its latest survey of IT Managers biggest security concerns. One-hundred eleven members responded to the survey, of which 70% cited e-mail security as their biggest security concern. Following e-mail security, 26% cited authentication, and 4% cited encryption.

---

## PDA SECURITY

★★

*InfoSecNews*, Week ending October 12<sup>th</sup>, 2001

Asynchrony has unveiled "PDA Defense", an IT security application developed specifically for Palm PDAs and other mobile devices. According to the St. Louis, Missouri-based Company, as well as supporting proprietary features that no other PDA security software offers, the application completes the last segment of the information chain, from desktop to PDA. Two versions of the software have been released - PDA Defense Standard at \$19.95 and PDA Defense Professional at \$29.95 - both for the Palm operating system. Asynchrony say the applications are built around its PDABomb security platform, a multi-tiered security system that uses industry-standard encryption - 64-bit on the standard version, 128- or 512-bit on the professional version - while maximizing performance and response time by decrypting databases only when they are needed.

[www.infosecnews.com](http://www.infosecnews.com)

[www.pdadefense.com](http://www.pdadefense.com)

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

---

[Cntl][Alt]

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" . . .

[Del]

- ☺ Did you see the news bit on October 1<sup>st</sup> about the cracker who was able to alter several Yahoo news stories last month? How many of you are watching your company's web site *content*??? You may want to suggest IT *separate* content creation from web production — that way, if your web site content is altered, it can quickly be replaced with the original content.
- ☺ The number of federal groups formed to fight cyberterrorism continues to proliferate. The latest is the Critical Infrastructure Board established by the executive order of President George W. Bush last week. As with organizations like the National Infrastructure Protection Center and the newly created Office of Homeland Security, the panel will coordinate with private industry to ensure the nation's networks are protected against cyberterrorists targeting critical information systems. Details need to be ironed out, including what Cabinet members and top presidential aides will comprise the board.
- ☺ Network tech dreads assignment to run a new group of network lines from one end of the store he works for to the other. But over the Toy department, he gets an idea. Grabbing a bow and arrow set, the tech ties a string to the arrow and shoots it overhead of the ceiling tiles to the other of the store. Then he ties the string to the cable and pulls it across. Manager pleased at job completion in half the time, but still waiting for an explanation of the bow and arrow set on the inventory transfer sheet.
- ☺ System security is set up to automatically lock out the user after 3 invalid log-in attempts. But users balk at waiting so long before they can try again. So, the Help Desk comes up with a new way to explain it: tell locked-out user they can unlock the Id, but it takes 20 minutes, so go get some coffee while they work on it. For some reason, users are happier with this explanation . . .
- ☺ **WHERE DO I SIGN UP???** A Detroit paper recently ran an ad for an e-commerce manager. The right candidate “will be hands-on and will overlook projects and systems.” Imagine that — getting paid to *overlook* projects . . .

---

## And Finally . . .

For those of you who track Systems Development trends, the Standish Group recently released its' 2001 edition of the *Chaos Report*. Once again, the numbers are up — 200,000 projects, or 76% of all IT development projects, never survive to completion. And we wonder why there's such a high turnover rate in IT . . .



**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](mailto:ldalzell@steelcase.com). Thanks!**



## ***Coming Attractions...***

**December:** *No meeting and no newsletter. We'll catch you again in January 2002!*

**January's Meeting:** TBA

## **Final Words**

**Special thanks to Michael Grinwis for his continued contribution of the Quick Bits.**

*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*