

CONTROL BITS & AUDIT BYTES

Western Michigan *INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION* Newsletter

OCTOBER 2000 NEWSLETTER

OFFICERS

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

VICE PRESIDENT

James Green, CISA
Arthur Andersen
Technology Risk Consulting
Suite 700
171 Monroe Avenue NW
Grand Rapids, Michigan 49503
(616) 653-8364
FAX: (616) 653-6305
james.a.green
@us.arthurandersen.com

SECRETARY

John Blair, CISA
Steelcase, Inc. CH-3E-18
P.O. Box 1967
Grand Rapids, MI 49501-1967
616 / 246-4730
FAX: 616 / 248-7550
jblair2@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@national-city.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

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

PAST PRESIDENT

John Arens, CPA
Meijer, Inc. MC 985/4
2929 Walker Avenue NW
Grand Rapids, MI 49544-9428
616 / 791-3521
FAX: 616 / 791-5341
arensj@meijer.com

DIRECTOR AT LARGE

Kim Coyer
Independent Bank Corporation
623 Washington Ave
Bay City, MI 48708
(517) 892-3511
kcoyer@ibcp.com

NOVEMBER DINNER MEETING

FireWalls and Perimeter Defenses

By Greg Terrell, CTO, Sequoia NET.com

November 8th, Duba's Restaurant

The presentation will be on general security issues focusing partly on awareness, including incident trends, and attack methodologies, with additional focus on counter measures & best practices. One challenge with firewalls is that it requires a thorough understanding of TCP/IP.

Speaker BIO

Over the last twenty years, Greg has witnessed and participated in the evolution of computing technology from the centralized mainframe architecture to the networked computing paradigm of today. His interest in computing technology started while attending Michigan State University and Greg applied his efforts to the information technology industry by starting his own company in 1980. Over his career, Greg has completed assignments in a diverse array of information technology disciplines including software development, field service, system design, network operations, project planning, and technology management. Throughout his career, Greg has kept close to the unique challenges of data communications and networking. This area includes the core of his industry certifications including CISCO Certified Internetworking Expert (CCIE) and Novell, Master Certified Netware Engineer.

AS an employee of both technology provider and consumer organizations, Greg's appreciation for the entire technology delivery process has proved an invaluable aid in his current role as Chief Technology Officer of Sequoia NET.com. Greg's efforts focus on assisting customers in the strategic use of communications and security technologies as the enablers of the eBusiness era.

Please make your reservation now!

Call John Blair and make your reservation today!! **(616) 246-4730**

OR e-mail John at jblair2@steelcase.com

Costs - \$25 Non Members / \$22 Members

4:00 5:00 Board Meeting

5:00 5:30 Social Hour / Registration

5:30 6:30 Presentation

6:30 7:30 Dinner

Internal Audit "Helpers" Continued

ASSESSING RISK

Several considerations, factors and "ingredients" are required when developing an effective risk assessment methodology. One of the most, if not THE most difficult tasks associated with designing a practical methodology is that of defining the audit universe. When developing your audit universe be sure to consider the points noted at www.auditservices.com/runiv.html

XX

TRAINING

Evaluate your training needs for the rest of the year before it's too late! For those who can plan now, a **special offer**: \$800 plus related expenses for a customized in-house seminar to the first three respondents. A list of available dates can be found at our training auction site, www.auditservices.com/auction.html

XX

It's no secret, Continuing Professional Education is expensive. We are continuously looking for ways to provide the internal auditor with quality, professional education at affordable prices. One of our new training initiatives is the "near you" \$800 seminar. Feel free to take advantage of this opportunity if you can; details of this offer can be found at [www.auditservices.com/\\$800sem.html](http://www.auditservices.com/$800sem.html)

And yes, we are NASBA approved.

XX

CERTIFIED INTERNAL AUDITOR (CIA) EXAM

For a list of upcoming Review Courses and some "Help", including some exam taking techniques, go to www.auditservices.com/ciatest.html

XX

Have a nice day,

Roger
www.auditservices.com
615-790-9858
(fax: 209-797-7983)

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 worth–while! Here are some of the latest “discoveries” . . .



Big Brother IS Watching You . . .

USAToday Tech Watch, October 22, 2000

★★★★

www.usatoday.com

- USA Today is reporting that thirteen government web sites are tracking their Internet visitors in violation of privacy rules. One of the U.S. Forest Service sites was apparently sending the information to a private company which generates reports for the agency. Film at ???

“Love virus variant plagues email systems”

CNET.com, October 22, 2000

news.cnet.com/news/0-1005-200-3248692.html

★★★★

Five months after its first disastrous outbreak, the "I Love You" virus is still churning out destructive mutants. The latest mutation is a month-old variation with “new window dressing”, but the same destructive payload that deletes image files and spreads itself via Microsoft’s Outlook address book. The subject header read, “US PRESIDENT AND FBI SECRETS”.

Antivirus companies McAfee and Sophos have both posted alerts on the variant. Microsoft patched its Outlook software to resist viral attacks following the outbreak. One security analyst commented that “Companies have to know that they’re not going to go away. They were designed not to go away.”

Big Brothers are Watching *THEM*, Too . . .

“French Fear Spy in the Sky” *AGE ONLINE*, October 20, 2000

www.it.fairfax.com.au/breaking/20001020/A62985-2000Oct20.html

★★★

A French parliamentary report concluded last week that Echelon, a U.S. and Australian–backed satellite espionage system, exists. “There does indeed exist a system of communication interception, put in place by the intelligence services of the United States, the United Kingdom, Canada, Australia and New Zealand,” French National Assembly member, Arthur Paecht, wrote in a report. European information and communication systems are vulnerable to Echelon and it is not impossible that certain information collected by the spy network could be used for political or economic ends, Paecht said in a critical French-language report that can be found at <http://www.assemblee-nationale.fr/2/rap-info/i2623.htm>.

Listening stations based at the Defense Signals Directorate in Geraldton, Western Australia, and the Pine Gap installation near Alice Springs are being used to monitor communications, the report said. European countries should reinforce the security on their communication and information networks to counter espionage threats, Mr. Paecht said.

Ed. Note — What’s interesting about this is that *Covert Action Quarterly*, a quarterly intelligence newsletter, (www.caq.com) published details about the Echelon system in 1997.

Quick Bits (cont.)

by M. B. Grinwis

Another “bug” fix . . .

Sans News Bites, October 25, 2000

★★★

www.sans.org

Microsoft is warning users to install a patch for an Internet Information Server (IIS) vulnerability that could allow interlopers to read and execute files on IIS-based servers. The patch has been available since August. You can download / get more info at:

<http://www.msnbc.com/news/477722.asp?0nm=TIAN>

http://www.computerworld.com/cwi/story/0,1199,NAV47_STO52573,00.html

These guys are worse than Santa Claus . . .

★

MSNBC News Item, October 18, 2000

<http://www.msnbc.com/news/477749.asp?0nm=T19N&cp1=1#BODY>

Recently declassified documents indicate that *Carnivore*, the FBI’s current e-mail surveillance system, is part of a triad, including programs that can reconstruct a targeted person’s journey through the web. This article also contains the evolution of the FBI’s e-mail monitoring systems. A bonus: The diagram on how Carnivore works (appropriately censored, below).

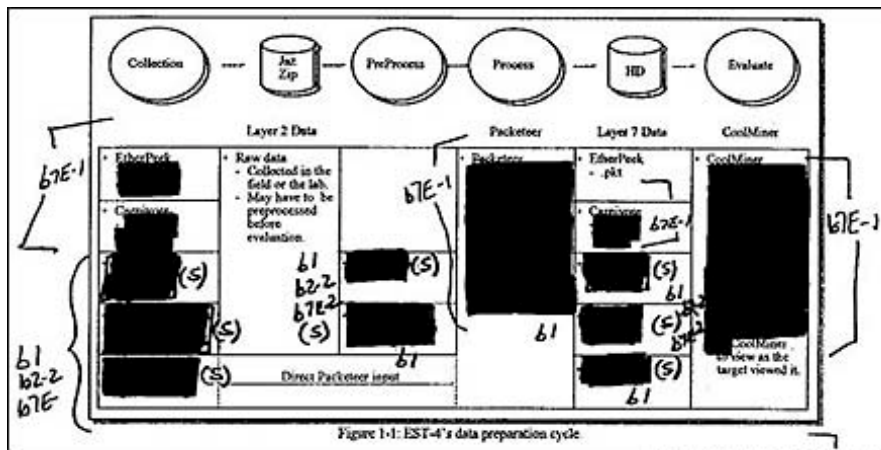


Figure 1-1: EST-4's data preparation cycle

U.S. Department of Justice

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

Taking a hint from “Men in Black”, its somewhat surprising what truthful tidbits can be obtained from the “gossip columns” of the IT world. Here’s some of the latest “fluff” . . .

- ⊗ *Did ANYONE check this guy’s resume???* — New I.S. boss asks if the uninterruptable power supply (UPS) system is adequate. Managers say of course; each server has its’ own UPS with 30 minutes battery time, and they’re paged if it goes down. Boss looks at e-mail server and asks, “What about this one? Is it ready for testing?” Manager nods yes. I.S. boss dramatically pulls power cord right out of the back of the server, which instantly stops dead. Boss then complains, “I thought you said these things were on UPSes!” Result: No e-mail from 11am to 3pm. . . .

Quick Bits (cont.)

by M. B. Grinwis

- ☺ Before you allow your techies to start bidding on new cell phone and wireless hardware in the 700 MHz band, better keep a *very* close tabs on the FCC! Seems the government gave that space to broadcasters (UHF channels 61 through 67) with the proviso that they use it for the fledgling DTV technology until 2006 or until DTV reaches 85 percent of the U.S. market, *whichever comes later!* Guess who gonna win *THAT* one, folks!?!
- ☺ Having trouble reconfiguring that new Dell Dimension with Windows ME for file and printer sharing or Internet sharing??? Seems there's some major discussion on dell's support site concerning the fact that all Dell Dimension Windows ME system shave an error in their installation image of the OS, and the only known solution is to reinstall Windows ME over the existing installation . . .
- ☺ Amid all the other political hoopla, did anyone hear about the New York Senate campaign debate between Hillary Clinton and Mr. Lazio? When asked about Bill 602P, both proclaimed that they were against the bill, which would put a 5 cent tax on e-mail messages. Do you think either of them knew that 602P is an old Internet hoax virus? ? ?
- ☺ And finally, let's have a big round of applause for Nautronix, Ltd! They announced the release of the first underwater laptop. Does this mean that CAD/CAM has finally come to underwater basket weaving???



*Information Systems
Audit and Control
Association*

Looking for Member Feedback – AGAIN!

The Chapter Board and program committee continuously struggles with identifying programs for our dinner meetings. Obviously, we want to provide you with information that is valuable to your work and advancement in the field of IS Auditing. What we struggle with is quality of content. Given that our meeting currently allows for 2 hours (1 hour presentation and 1 hour dinner), how do we balance this with delivering sufficient content to be of added value back at the office. We have taken steps to provide the speaker with areas/guidelines to focus their presentations for our chapter, however, this does not always provide the result we intended.

These are our constraints:

- Presentations are requested to be an 1 hour to 1-15min. in length. As we do not wish to force the speaker to present over the clattering of dishes and servers.
- Presentations are usually volunteered, so delivering more than an hour requires considerable preparation by the presenter.
- One hour is not sufficient time to deliver a subject in any depth.
- Most volunteer presenters have canned presentations already prepared and have been given at other venues.
- Organizations like CANAUDIT and MIS do not (or are reluctant) to speak at “Dinner Meetings” **or**
- Focused presentations from groups like the above become cost prohibitive (one would have cost the chapter over \$2000 for an hour presentation).

We need your input, suggestions and direction. This is YOUR chapter and YOUR education, so tell us what we can do to add value to your needs? Here are a few ideas to help.....

- Expand the presentations to two hours with a break for serving dinner. The presenter would then have to eat their dinner prior to or after the presentation (typically alone).
- Keep venue to hour/hour 15 minutes, with a 15 minute introduction to the subject and the remainder fielding questions from the membership. This would require compiling questions in advance for the speaker in order for them to be prepared and to ensure that we fill the hour provided.
- Focus the presentations for subjects that can be adequately covered in the timeframe given. (I.e. instead of a presentation on Firewalls and Perimeter Defense, the subject would be Audit steps for identifying attacks against your infrastructure....poor example, but you get the idea).

We would like to hear from you!!! Please send your comments and suggestions to Rick Cummings at rick_cummings@MSN.com or our VP of Programs Jim Green at james.a.green@us.arthurandersen.com.

Thank you!

JOB MARKET

Audit Consultant

Michigan's largest writer of workers compensation insurance is seeking qualified applicants for the position of Audit Consultant in our Lansing Office. Internal Audit at the Accident Fund Company takes a proactive approach to auditing by providing consulting services to business units through value-added reviews of systems, business processes, financial and operating controls to confirm consistency with corporate goals, objectives and policies. Performs risk assessments to identify high-risk business processes and applies relevant best practices. Champions and facilitates the company's Control Self-Assessment (CSA) program. The ideal candidate will possess a bachelor's degree in information systems, computer science, accounting, finance or related field. Completion of industry recognized professional designations (CISA, CIA, CPA or CCSA) highly preferred. One to four years experience in information systems audit required. Experience in the insurance, health care or finance industry required. Accident Fund Company is a team-oriented environment and offers an excellent compensation and benefits package, including employer-paid insurance for you and your family. Interested and qualified applicants should submit resume and salary requirements to:

Accident Fund Company

Attn: Human Resources P.O. Box 40790
Lansing, MI 48901-7990 Fax: (517) 342-4305
Email: Lynnem@accidentfund.com
www.accidentfund.com

Final Words

Don't Forget..... December Dinner Meeting

Its on us!! Join us at two of the three dinner meetings from September through November and your dinner and venue will be free! Be sure to make the November Meetings at Duba's Restaurant, Grand Rapids.

The Chapter will also be congratulating those members who have received their CISA in the past year also at the December meeting. More information will be forth coming on both these events in December.

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*