

# Control Bits & Audit Bytes

Western Michigan *INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION* Newsletter

## SEPTEMBER 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@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

**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

## September 20th Dinner Meeting *Duba's Restaurant* *420 E Beltline NE, GR*

### Internet Security from an Enterprise Perspective By Gregory Hicks

The main emphasis will be on firewall topology and administration.

#### **PROFESSIONAL BIOGRAPHY OF GREGORY HICKS**

Gregory received his BS in Applied Science of Electronic Engineering (Deans List) Louisville, Ky. Since then, he has accumulated over 15 years of industry experience at Heath Zenith, United Parcel Services Airlines, and Meijer, Inc., where he currently works as a Sr. Architect on the IT Strategy Team.

Gregory has been certified with several professional certifications, such as Certified Industrial Engineer (IEEE), Certified Novell Network Technician (first certification ever offered by Novell), Certified Compaq Technician, Certified Networking Engineer (Network General, Sniffer University), and Certified 3 Com Network Engineer. He is also affiliated with several professional organizations, including the International 3 Com Network User Forum, and the International ATM Forum. Gregory has been honored as a Kentucky Colonel (Advancing Technologies that Benefit the Commonwealth of Kentucky) and as a Charter Member World Wide Security Technology Steering Committee (Transportation Industry).

Please make your reservation and meal selection (see below) by September 19th!  
Call Jamie Depuydt and make your reservation today!! **(616) 248-7426**  
OR e-mail Jamie at [jdepuydt@steelcase.com](mailto:jdepuydt@steelcase.com)

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

Dinner menu:  
1 – Sautéed Chicken Breast or  
2 – Prime Rib  
Salad  
Dessert

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

# **CANAUDIT PERSPECTIVE NEWSLETTER**

Volume 2: Number 1; September 2001

## **SECURING THE INTERNET FOR 2002**

**By Gordon Smith, President, Canaudit Inc.**

As we complete more of our Internet penetration and network audits, there seems to be a very disturbing trend. Many organizations have serious Internet issues that need to be addressed. The purpose of this article is to enable you to understand the key risks of an organization's web presence and mitigate those risks. We have presented the issues in an orderly manner, encompassing from initial design to security testing.

### ***CATALOGING YOUR ORGANIZATION'S INTERNET SITES***

Many organizations are not aware of their full Internet presence. They are often aware of their main web site, and sometimes they might even be aware of their full Extranet exposure. However, many of them have "Rogue" Internet connections set up by small groups or large departments within the organization! In several of our recent Internet penetration audits, we penetrated the client's network by identifying and exploiting a poorly controlled rogue site that connected to the internal network. These sites bypass normal IT development, management and security procedures. As a result, the required controls are not in place, and hackers can simply slide into the network.

Once we have penetrated a network using a rogue site, IT management is often upset because they did not even know the site existed. Yet management holds them responsible for Internet security. This is why it is so important that your organization's Internet presence be mapped and catalogued. This can be done by the IT security group or by an outside source such as Canaudit. In fact, cataloging the client's complete Internet presence is the first thing we do when commencing an Internet or Internet penetration audit. You can bet that hackers have already probed your rogue sites for weaknesses in your Internet presence.

### ***DESIGN AND CONFIGURATION***

For many organizations, the Internet presence started out much like the California Gold Rush. Everyone lined up; someone counted to three; and, viola, your company was on the Internet. "Let's just get it up, we'll control it later." "We have to be on the 'net' because our competitors are already there." "We have a firewall." We've heard these and similar phases many times, as I'm sure you have. Despite best intentions, some organizations never revisit their Internet design and configuration. Not only does this lead to poor controls over the Internet presence, but it can also lead to Internet sites that do not have the required functionality to attract and retain your customer base.

Many of the sites we have reviewed are primarily "brochure" sites. These sites provide information about products and services. This is great for clients who simply want to browse an electronic catalog. Unfortunately, it does not capture marketing information about your Internet visitors. Nor does it enable your organization to contact customers, permit customers to order product, or enable your company to push critical information such as price changes and other sales data out to them.

From a security standpoint, poor design and configuration results in very poor security. In most cases, security consists of a firewall. Unfortunately, firewalls can be bypassed through rogue connections mentioned above, or by poorly configured routers, servers and trading partner connections. Internet design and configuration should include the initial design of the Internet sites and the controls required to control those sites. The actual controls are implemented either through firewall, server and application controls and/or the installation of security software.

Internet design and configuration is not something to be reviewed only once. It is an ongoing task that needs to be performed semi-annually. This will ensure that the Internet connections continue to meet the needs of your organization and your customers.

### ***THE EXTRANET***

Many organizations are moving applications out onto the Extranet. As a result, the critical control points must also migrate to the Extranet. Our audits have identified that many organizations have a poorly controlled Extranet environment. Critical customer information, as well as business transactions, can be accessed, copied or even altered by hackers and electronic espionage consultants. These "consultants" data mine the Internet for information that can be sold to criminals and competitors. Effective Extranet security encompasses Internet, server, network, database and application security. Most Extranets have not been subjected to a full security review or audit. One of the priorities for this year should be to complete these reviews so that controls can be enhanced and funding allocated for ongoing Extranet security in 2002.

Many organizations have outsourced their Extranet to an ISP or an ASP. This does not mean that security and control will be any better, nor does outsourcing the Extranet relieve your organization of the responsibility to protect your client's data. We

are currently very concerned that several of the major ISPs may have serious cash flow issues, as the dot-coms turn into dot-busts. If your ISP fails, what happens to your Extranet and your ability to process Internet transactions? Additional information on Extranets is available in our course **Control and Security of the Extranet**.

### ***FIREWALLS***

Firewalls are a great control; however, our audits show that firewalls can be bypassed. Also, if your organization fails to install the required upgrades and patches, then firewall controls may be breached. Another issue is intruder detection and response. We have noticed that many organizations let the firewall block attempts. In many cases, the firewall logs are not reviewed. Hackers can quietly probe the site, document vulnerabilities and, hopefully with success (from their standpoint), execute and exploit the site. If the firewall blocks their IP address, a hacker will just use another account to continue their attack. Only an automated alert, combined with formalized intrusion detection and response procedures, can ensure that a sustained attack is detected and properly investigated. Additional information is available in our seminar **Control and Security of Firewalls and Intrusion Detection**.

### ***VIRTUAL PRIVATE NETWORKS***

VPNs are often marketed as a safe alternative to other connectivity technologies. While this can be true if properly installed and secured, some VPNs have been used by hackers to penetrate corporate networks. In February of 2001, many organizations were successfully penetrated from Eastern Europe using their own VPN connections. Not only were their controls defeated, but these companies had to foot the bill! Some of these companies discovered they were had only once they saw the VPN provider invoice. This could have been discovered much earlier using a query against the VPN data. An effective means of monitoring VPN connections would be to simply have the VPN provider supply a file on a daily or weekly basis with information about your user sessions. This includes account number, origination point, date and time of login, date and time of logout, session duration packets transmitted and packets received. Put this data into a database or spreadsheet and sort it by looking for very long sessions and impossible combinations (logging in from Seattle at 1 pm, then New York at 1:05 pm). Also look for concurrent logins (two or more logins with the same account at the same time). This will enable you to discover compromised or shared accounts. The last simple test is to look for large data volumes from a particular account. This may be a hacker who is downloading your data or uploading his or her data to your servers.

### ***CONTENT MANAGEMENT AND SECURITY***

Many organizations lack controls over web site content. We regularly find site content that has been altered by hackers. Since no one is reviewing the site on a regular basis, these altered pages will only be noticed by your customers! Some changes are made because of poorly controlled CGI code. Other changes are made by exploiting the site software. IIS, as everyone knows, is particularly vulnerable. Every organization should have a formal review process before content is placed on the web, regular reviews to ensure that the content has not changed, and effective security to protect your site and site content.

### ***MANAGEMENT CONTROL AND OVERSIGHT***

We have found that management often delegates web content, management and oversight to low-level staff. This not only demonstrates that management is not interested in the Internet presence, but that a significant part of an organization's customer contact and web content is implemented by project leaders and analysts, not marketing people. Management must take an active role in managing web sites and content. They must determine what information is public and ensure that the information is presented in an acceptable format that will not expose the organization to legal issues. In addition, non-public content and customer information must be protected. Management must also ensure that the Internet presence is secured and that intrusion detection is in place. A senior executive should head the computer incident response team to ensure that incidents are properly reported to executive management and that there are no cover-ups.

As you can see, there are many issues relating to Internet security. This article highlights only a few of them. We highly recommend that every organization's Internet presence be audited or subjected to a security review at least once a quarter. You can perform this review yourself or you can hire someone to do it for you. Canaudit provides a full range of seminars to prepare you for such a review, or we can do the Internet penetration audit for you. Seminars that provide such training will be offered at our upcoming **Professional Development Week** in Minneapolis and at our **Ultimate Network Penetration Class** in Simi Valley, CA, which you can register for at our web site at [www.canaudit.com](http://www.canaudit.com) or by phone at (805) 583-3723.

The Canaudit web site also contains many free software tools that can assist you in your reviews. If you require additional information on our seminars, Internet and Extranet audits, as well as Internet penetration testing, please contact [Gordon@canaudit.com](mailto:Gordon@canaudit.com), [Chris@canaudit.com](mailto:Chris@canaudit.com) or [Paul@canaudit.com](mailto:Paul@canaudit.com).

# 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” . . .

*Well folks* . . . it’s been one *interesting* summer, if you’ve managed to catch even an nth of the business activity. Since there’s been no shortage of “stuff out there”, here’s some of the more major “*eye-grabbers*” . . .

### IT’S A VAX ... NO, A COMPAQ ... NO, WAIT, IT’S AN HP!

★★★★

Hewlett-Packard bucked current industry trends with a bang Labor Day week. First, it announced it was buying Compaq for \$25 Billion. Two days later, HP announces the acquisition of a competitive printer company! (I’m wondering what type of coffee HP’s M&A department is drinking these days . . . if it IS coffee in there . . .) The ink on the announcements wasn’t even dry before the first respondent salvos came in, too. Wall Street is not too happy about the whole deal, and the European Community has promised to give this merger a *very* thorough review. And the media speculation is in “full swing”, too. In one *Computerworld* article, there’s already a proposed list of winners and losers in the industry if the deal DOES go through. Gartner Group’s on-line site, *TechRepublic*, isn’t very optimistic, however. In a “*First Take*” article, the merger is described as “Two once-great companies will likely not live up to their past achievements by combining their assets. The deal would mean many overlaps in products, technologies, distributors, services, facilities, and jobs. The combined HP/Compaq would face the challenge of creating coherent strategies for four server architectures, seven operating systems, four storage architectures, and several service businesses.” In a *Computerworld* sidebar, one analyst stated that HP’s CEO, Carly Fiorina, is already proposing 15,000 job cuts between the two former giants, to help finance the whole deal. You can tell it’s fall again . . . we’re all going to learn some lessons from this one . . .

[http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO63544,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63544,00.html)

<http://www.techrepublic.com/article.jhtml?id=r00620010905ern02.htm>

---

### DOJ DECIDES NOT TO BREAK UP MICROSOFT

★★★★

*CNN Financial News* — Sept. 6, 2001

People in Washington must be singing “Breaking Up Is Hard To Do” a lot these days. The U.S. Department of Justice announced it would not seek the break up of software giant, Microsoft, Inc. during the next phase of its landmark antitrust case. The DOJ said it chose instead to seek court-ordered changes to the way the software maker conducts business. Many of you might remember that the U.S. Court of Appeals for the District of Columbia overturned U.S. District Court Judge Thomas Penfield Jackson’s order in late June that Microsoft be broken into two companies as a remedy for anti-competitive practices. However, the DOJ did uphold the lower court’s conclusion that Microsoft has a monopoly in the computer operating systems market, and maintains that monopoly power by anti-competitive means in violation of U.S. antitrust laws. Guess the “fun times” are a long time from being over for the legal-eagles from Redmond . . .

<http://cnfnfnn.com/2001/09/06/technology/microsoft/>

---

### SABRE SHEDS IT’S MAINFRAME LEGACY

★★★

*Computerworld*, Vol. 35, No. 36 — September 3, 2001

As if we didn’t have enough to worry about, Sabre Holdings Corp., owner of the world-wide airline reservation database system, announced that it will be moving its system over to Compaq Computer Corp’s, NonStop® Himalaya servers at a cost of \$100 Million. The project is viewed as a multi-year process, especially since Sabre serves the reservation processing of more than 50 airlines. An IBM mainframe-based system since the 1950’s, “...this represents...a recognition of the need to respond to the new *e-commerce* travel model”, said Richard Eastman, an analyst for The Eastman Group Inc., in Newport Beach, CA.

[http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO63398,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63398,00.html)

(*Ed. — Could this have been the “icing” that brought on the HP/Compaq deal?*)

---

## 'LAWS' TO WORK BY

★★★

*Computerworld*, "Frankly Speaking", Vol. 35, No. 36 — September 3, 2001

Those of you "faithful readers" of this column know of my respect and admiration for the writings of Frank Hayes, senior news columnist for *Computerworld*. In this issue, Frank lists seven "crucial" IT 'laws' which are surprisingly maligned by many in and outside the industry. In this article, Frank lists the laws' name, the actual quote, who said it, what it means, what too many people *think* it means, and why the difference is important to understand. An example: **Moore's Law**. Intel founder Gordon Moore said "transistor density on a manufactured semiconductor die doubles about every 18 months". This means that improvements to chip manufacturing methods allow manufacturers to double the number of transistors on a given chip about every 18 months. What people *think* it means is a computer made today will process twice the amount of work that a computer made a year and a half ago will do. Why this difference matters is because transistor density does not equal computer power, and computer power does NOT equal the ability to get work done. There's also a nice description of Murphy's Law, too.

---

## DATA: AN ASSET OR A LIABILITY?

★

*InformationWeek Between The Lines*, September 5, 2001

A major controversy is brewing over the sale of Egghead.com to Fry's Electronics. Egghead, an online software and component vendor, recently declared bankruptcy. Fry's, an on-going competitor, agreed to acquire its assets, including its customer database, for \$10 million. As a condition of the sale, Fry's is requiring that 90% or more of Egghead's active customers NOT opt out of the plan to transfer their personally identifiable data to Fry's. Privacy advocates are in an uproar, but its clear that Fry's knows where the value to this deal is. Is customer data an asset or a liability? It's an asset if Egghead's deal goes through, but a liability if the privacy brouhaha nixes the deal. What's clear is that no one is clear on this issue.

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

- ☺ Under the heading of "things that make you go hmmmm", we submit for your consideration two articles published in an on-line newsletter that shall go unmentioned. The first article, on Microsoft Windows XP, contained a comment by a senior MS official expressing his expectations that certain major accounts (names omitted here) would soon step up to the new operating system. In the following article, a senior official with one of those accounts noted that his company had no intentions to even consider the new operating system until later in 2002, "if then". The official cited XP's lack of new major functionality or fulfillment of an outstanding business need.
- ☹ Watch out, any of you who bought a Rex 6000 Micro-PDA from Xircom. Seems Xircom was recently purchased by Intel, and Intel has decided to cease production of the device. To top it off, the on-line support site, [www.Rex.net](http://www.Rex.net), ceased operations as of August 31<sup>st</sup>!

---

**HOORAY?** I-496 in Lansing is finally open to traffic again! Jury's out on the quality of the fix, though.

---

## Coming Attractions...

**October's Meeting:** "Auditing Internet Security" by Jennifer Thompson, Advanced IS Auditor, Meijer, Inc. Social Hour from 5-5:30pm, Speaker from 5:30-6:30pm, Dinner at 6:30pm. Meeting will be held at Duba's. Speaker bio will be published in the next newsletter.

**Professional Development Week:** hosted by the Minnesota IS Audit and Control Association October 1-4, 2001, in Minneapolis, MN. See the web site for further information.

Many of our Chapter Members are also a part of the Institute for Internal Auditors. Per the Lansing chapter's request, we are now publishing their meeting dates and times as well. If you are interested in joining the IIA, please contact the Western Michigan Chapter President for the IIA, Linda Simpson at [SimpsonLD@state.mi.us](mailto:SimpsonLD@state.mi.us).

### Lansing Chapter IIA Program for the 2001 - 2002 Chapter Year

Date	Speaker	Company	Topic	Time
9/18/2001	Bill Papanikolas	Jefferson Wells	Risk Based Auditing	Breakfast
10/16/2001	Mike Stolarczyk	Jefferson Wells	General Computer Controls	Breakfast
11/20/01	David L. Wells	Plante & Moran, LLP	Fraud in the Workplace	Breakfast
12/18/2001	Lambert Lam	Jefferson Wells	Software Piracy and What Every Auditor Should Know	Breakfast
1/15/2002	Dr. Mark Wilson	Michigan State University	Internet Gambling - Issues of Legal Jurisdiction	Breakfast
2/19/2002	John Bengel	Michigan Department of Treasury	Fraud and How It Affects You	Breakfast
3/19/2002	Roger McDaniel	Audit Services	CIA - a Certification NOT a Federal Agency	Dinner
4/16/2002	Kristine Keusch	Blue Cross/Blue Shield of Michigan	Enterprise Risk Management	Breakfast
5/21/2002	Dave Richards	IIA, Chairman of the Board	Peer Review and the New Framework	Breakfast

## CISA EXAM RESULTS

We'd like to extend our congratulations to those members that passed this year's CISA exam, taken Saturday, June 9, 2001. Great job!

Ms. Annie Lea Brautigam  
Miss Leslie Dalzell, CPA  
Ms. Karen Hwee-Ping Koh

Mr. Gregory A Dahinden, CPA, CIA  
Mr. Dale C. Gruber, CDP

Also... and extra special congratulations to those tied for highest score in our area, Gregory Dahinden and Dale Gruber. Also, congratulations to Karen Koh for achieving the second highest score for our area. Outstanding!

## Final Words

Thank you to those that participated in the 2001 Fred Rugg Memorial Golf Outing.

*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*