

# ICON

## ISACA CENTRAL OHIO NEWSLETTER

Volume 11, Issue 9

May 2000

### Meeting News

**DATE:** Thursday, May 11, 2000

**AGENDA:** 11:15 Registration  
11:30 Speaker  
12:30 Lunch

**LOCATION:** Buckeye Hall of Fame Café  
1421 Olentangy River Rd.  
Columbus, OH 43212  
(614) 291-2233

★ Directions on Newsletter Cover ★

**MENU:** Hot Luncheon Buffet:  
Grilled Walleye and Herb Roasted  
Pork Loin, Garlic Smashed  
Potatoes, Steamed Vegetables,  
Mixed Greens with Assorted  
Dressings, Pasta Salad, Fresh Fruit  
Display with Dip, Cottage Cheese  
with Peaches, Rolls and Butter,  
Coffee, Hot Tea & Iced Tea  
Array of Desserts

**PRICES:** \$ 15.00 Members  
\$ 18.00 Non-Members  
\$ 5.00 Student (Student is full-  
time undergraduate, non-  
professionally employed)

**RSVP:** Richard Ridewood 466-4083  
Fax: 728-7199  
e-mail: [rridewood@auditor.state.oh.us](mailto:rridewood@auditor.state.oh.us)

#### RESERVATIONS POLICY

The deadline for reservations is **Monday, May 8, 12:00 noon**. If you do not reach Rich directly, please be sure to leave the following information: Name, Member/Non-Member, and Company. **Cancellation deadline is Tuesday, May 9, 12:00 noon.**

**ALL RESERVATIONS MADE AND NOT CANCELED BY THE DEADLINE MUST BE PAID FOR.**

#### Intrusion Detection

Our speakers this month are Steve Romig and Robert Snyder. Mr. Steve Romig is Manager of Campus Network Security at the Ohio State University. Steve is in charge of the university's Incident Response Team, which provides computer security, incident response assistance, training, consulting, and security auditing service for the university community. In addition, he works closely with Central Ohio businesses to improve Internet security response and practices, as well as with local, state, and Federal law enforcement to detect and deter computer crime.

Mr. Snyder is a contract fraud investigator for the Verizon Wireless cellular company in Ohio. He specializes in the investigation of cellular telecommunications crimes including cloning, subscription fraud, and internal thefts. He provides training and assistance for law enforcement agencies in the investigation of high tech cellular fraud. Mr. Snyder is retired from the Columbus Ohio Division of Police, Intelligence Bureau, where he was assigned to investigate computer and telecommunications crimes since 1983. He was a consultant on the National Institute of Justice video on computer crime scenes and for the MCI Law Enforcement video on telecommunications fraud.

#### Inside This Issue:

Chapter Directory & Agenda	p. 2
President's Message	p. 3
ISACA Updates	p. 3
Monthly Article	p. 4-5
Door Prize Information	p.6
Directions	p. 7



**DIRECTORY OF OFFICERS, COMMITTEE  
CHAIRPERSONS, & DIRECTORS  
1999 - 2000 CHAPTER YEAR**

**ISACA CENTRAL OHIO CHAPTER  
DISCLAIMER STATEMENT**

**OFFICERS:**

**President:** Norman Hofmann, (614) 728-7164  
Ohio Auditor of State

**V-Pres:** Ken Kuss  
Nationwide Ins.

**Secretary:** Jim D'Innocenzo, (614) 466-4085  
Ohio Auditor of State

**Treasurer:** Tim Winslow, (614) 213-6336  
Bank One Corporation

**COMMITTEE CHAIRPERSONS:**

**Arrangements:** Richard Ridewood, (614)466-4083  
Ohio Auditor of State

**Audit:** Greg Mason, (614) 728-0125  
MRDD

**Education:** Richard Ridewood, (614)466-4083  
Ohio Auditor of State

**Membership:** Jim D'Innocenzo, (614)466-4085  
Ohio Auditor of State

**Newsletter:** Tamela Bolte, (614) 995-4834  
Ohio Auditor of State

**Programs:** Ed Bell, (614) 331-9355  
Huntington Bancshares, Inc.

Norman Hofmann, (614)728-7164  
Ohio Auditor of State

**DIRECTORS:**

Ed Bell, Huntington Bancshares, Inc. (614)331-9355

Richard Ridewood, Auditor of State (614) 466-4083

Brian O'Brien, OSU

Claudia Mitchell, Nationwide Ins. (614) 249-4110

Allison Williams, Nationwide Ins.

Larry Frazee, Huntington Bancshares, (614)480-6525

Mike Jenkins, CBSI, (614) 220-4411

Because it is one objective of the ISACA Central Ohio Chapter to be a forum for the free expression and interchange of ideas, statements of position or expression of opinion appearing herein are those of the author(s) and not by the fact of publication necessarily those of the ISACA Central Ohio Chapter. Likewise, the publication of any advertisement in the ISACA Central Ohio Chapter's newsletter is not to be construed as an endorsement of the product or service offered unless such approval or endorsement is specifically stated.

ICON: ISACA Central Ohio Newsletter is published monthly. Articles and advertisements are welcome. The deadline for receiving articles is the 10<sup>th</sup> of the month prior to the month the article is to be published. Current advertising rates: \$30 for full page and \$20 for half page. For further information contact:

**EDITOR:** Tamela Shreve-Bolte  
Ohio Auditor of State  
35 East Gay Street  
Columbus, OH 43271-0386  
**PHONE:** (614) 995-4834  
**FAX:** (614) 728-7199

**E-MAIL:** [tjbolte@auditor.state.oh.us](mailto:tjbolte@auditor.state.oh.us)



**PRESIDENT'S MESSAGE:**

*From the Desk of Norman Hofmann*

This month's meeting brings the 2000 Program Year to an end with a bang. We have two knowledgeable and very interesting speakers this month; Mr. Steve Romig and Mr. Robert Snyder. Both of these speakers have given very interesting presentations to our chapter in the past. This month also marks the election of officers for next year and I urge everyone to participate.

While I was not able to make it to all the meetings because of job commitments, I believe that we had a fairly successful year. We had two sold out education conferences and attendance at meetings was good. ISACA is an organization - like most professional organizations - that depends on the active participation of its membership to be truly effective. I would at this time like to thank the officers, members of the board, and the committee chairpersons for their hard work and support this year. Without your help, this year could not have been a success!

I would also like to thank the membership for giving me the honor of serving as your President this year.

**Dates of Interest:**

- IS Audit and Control Training Week, 17-21 July 2000; Orlando, Florida**
- North America CACS 2000, 7-11 May 2000; Dallas, Texas**
- International Conference 2000, 16-19 July 2000; Lake Buena Vista, Florida**
- Network Security Conference, 21-23 August 2000; Las Vegas, Nevada**
- eBusiness Conference, 21-23 August 2000; Las Vegas, Nevada (Tentative)**

A reminder to everyone that this newsletter is available in a PDF format. A copy of each month's newsletter will be posted on our chapter Website, [www.osu.edu/units/uts/isaca-centralohio/](http://www.osu.edu/units/uts/isaca-centralohio/), on approximately the 20<sup>th</sup> of each month. In addition, we will Email a PDF copy of the newsletter to all members who would like to

receive a copy in that format. Just contact either myself or the chapter newsletter co-ordinator if you would like to receive your newsletter this way.

Remember, due to the breakeven nature of our meeting budget for this year, reservations made but not canceled before the deadline *will* be billed for.

***There will be a board meeting at 10:30 before this month's chapter meeting.***

---

**CISA Review Manuals Being Revised**

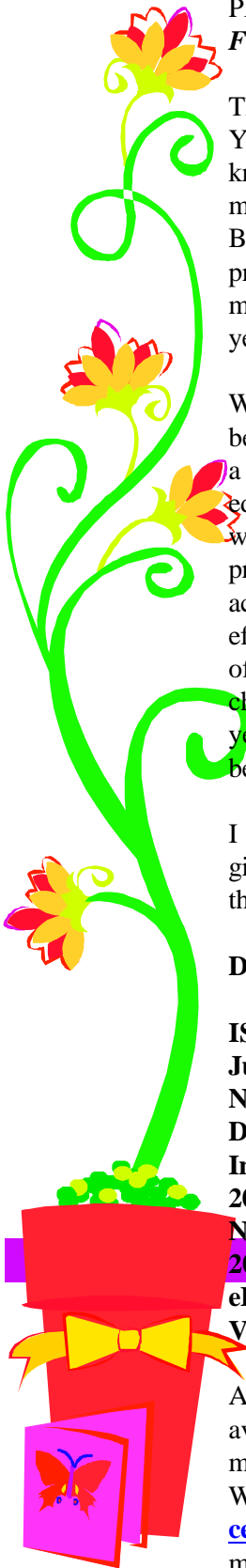
Members of the Quality Assurance Team (QAT) are beginning to revise and update the CISA Review Technical Information Manual and the companion Questions, Answers & Explanations Supplement for 2001.

Additional volunteers are needed to write practice test questions for the manuals. If you or anyone you know would be interested in writing questions and/or joining the QAT, please contact Elia Fernandez at [efernandez@isaca.org](mailto:efernandez@isaca.org)

---

**COBIT Update**

The COBIT Steering Committee is entering the final stages of development of the 3rd Edition of COBIT. The quality assurance process being carried on by the committee for the new edition's management guidelines - key performance indicators (KPIs), critical success factors (CSFs), key goal indicators (KGIs) and maturity models - is nearing its conclusion. The final product will be available in mid-2000 and will contain all-new material on IT governance, including governance KPIs, CSFs, KGIs and a maturity model.



## Intrusion Detection

An intrusion detection system, or IDS for short, attempts to detect an intruder breaking into your system or a legitimate user misusing system resources. The IDS will run constantly on your system, working away in the background, and only notifying you when it detects something it considers suspicious or illegal. Whether you appreciate that notification depends on how well you've configured your intrusion detection system!

Note that there are two types of potential intruders.

**Outside Intruders:** Most people perceive the outside world to be the largest threat to their security. The media scare over "hackers" coming in over the Internet has only heightened this perception.

**Inside Intruders:** FBI studies have revealed that 80% of intrusions and attacks come from within organizations. Think about it - an insider knows the layout of your system, where the valuable data is and what security precautions are in place.

So despite the fact that most security measures are put in place to protect the inside from a malevolent outside world, most intrusion attempts actually occur from within an organization. A mechanism is needed to detect both types of intrusions: a break-in attempt from the outside or a knowledgeable insider attack. An effective IDS detects both types of attacks.

Before we can discuss detecting intrusions, we must define what we mean by an intrusion. All intrusions are defined relative to a security policy. Unless you know what is and is not allowed on your system, it's pointless to attempt to catch intrusions.

An intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusions can be categorized into two main classes:

1. Misuse intrusions are well defined attacks on known weak points of a system. They can be detected by watching for certain actions being performed on certain objects.
2. Anomaly intrusions are based on observations of deviations from normal system usage patterns. They are detected by building up a profile of the system being monitored, and detecting significant deviations from this profile.

As misuse intrusions follow well-defined patterns they can be detected by doing pattern matching on audit-trail information. Anomalous intrusions are detected by observing significant deviations from normal behavior.

An anomaly may be a symptom of a possible intrusion. Given a set of metrics which can define normal system usage, we assume that exploitation of a system's vulnerabilities involves abnormal use of the system; therefore, security violations could be detected from abnormal patterns of system usage.

Anomalous intrusions are harder to detect. There are no fixed patterns that can be monitored for and so a more "fuzzy" approach must be taken. Ideally we would like a system that combined human-like pattern matching capabilities with the vigilance of a computer program. Thus it would always be monitoring the system for potential intrusions, but would be able to ignore spurious false intrusions if they resulted from legitimate user

actions.

Many intrusion detection systems base their operations on analysis of OS audit trails. This data forms a footprint of system usage over time. It is a convenient source of data and is readily available on most systems. From these observations, the IDS will compute metrics about the system's overall state, and decide whether an intrusion is currently occurring.

An IDS may also perform its own system monitoring. It may keep aggregate statistics which give a system usage profile. These statistics can be derived from a variety of sources such as CPU usage, disk I/O, memory usage, activities by users, number of attempted logins, etc. These statistics must be continually updated to reflect the current system state. They are correlated with an internal model which will allow the IDS to determine if a series of actions constitute a potential intrusion. This model may describe a set of intrusion scenarios or possibly encode the profile of a clean system.

### Characteristics of a Good Intrusion Detection System

An intrusion detection system should address the following issues, regardless of what mechanism it is based on:

1. It must run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a "black box". That is, its internal workings should be examinable from outside.
2. It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.
3. On a similar note to above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted.
4. It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.
5. It must observe deviations from normal behavior.
6. It must be easily tailored to the system in question. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.
7. It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.
8. Finally, it must be difficult to fool.

The last point raises an issue about the type of errors likely to occur in the system. These can be neatly categorized as either false positive, false negative, or subversion errors. A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. A false negative occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior. A subversion error occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.



**\$100 Door Prize for 1999-2000**



Last Name	First Name	Company	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	Total
Winslow	Tim	Bank One	1	1	1		1	1	1	1	7
Kohler	Sharon	Auditor of State	1		1		1	1	1		5
Bolte	Tamela	Auditor of State	1	1	1	1	1	1		1	7
D'Innocenzo	Jim	Auditor of State	1	1	1	1		1			5
Reichenbach	Ryan	Nationwide	1	1	1	1	1	1		1	7
Swonger	Jim	Auditor of State	1	1	1	1	1	1		1	7
Ridewood	Richard	Auditor of State	1	1	1	1	1	1	1	1	8
Buckham	Katherine	Deloitte & Touche	1	1	1		1	1			5
Miller	Lisa	Auditor of State	1	1	1	1	1	1	1		7
Crawford	Mary Anne	Audit Force	1	1		1	1		1	1	6
Kabelac	Dennis	Audit Force	1				1	1	1	1	5
Breitmoser	Gary	Nationwide	1	1		1		1		1	5
Bell	Ed	Huntington Bank	1	1			1	1	1	1	6
Frazee	Larry	Huntington Bank	1	1	1			1	1	1	6
Kopp	Chuck	Huntington Bank	1		1		1		1	1	5
Vance	Russ	Huntington Bank	1	1	1	1	1		1	1	7
Imwalle	Chuck	Huntington Bank	1		1	1	1		1	1	6
Hysell	Wallace	Motorist Insurance	1			1	1	1	1	1	6
Kelley	Maureen	Motorist Insurance	1			1	1		1	1	5
Scott	Jeff	Bank One	1	1			1	1	1		5
McKitrick	Jason	Nationwide		1	1		1	1	1		5
Gingras	Barb	Nationwide		1	1	1		1	1	1	6
Slate	Brian	Nationwide			1	1	1	1	1	1	6
Hofmann	Norman	Auditor of State			1	1	1	1	1		5

**NOTE: TO BE ELIGIBLE FOR THIS DOOR PRIZE, AN INDIVIDUAL MUST ATTEND AT LEAST SIX (6) LUNCHEONS DURING THE 1999-2000 SEASON. IF YOU HAVE ATTENDED ONLY FIVE (5) MEETINGS SO FAR THIS SEASON, YOU MUST ATTEND THE MAY 11, 2000 MEETING TO BE ELIGIBLE FOR THE DOOR PRIZE.**

**IF YOU FEEL THAT YOU SHOULD BE ON THIS LIST, AND ARE NOT, PLEASE CONTACT RICHARD RIDEWOOD AT (614) 466-4083 AND LEAVE A MESSAGE WITH YOUR NAME AND PHONE NUMBER OR CONTACT HIM AT THE MEETING PRIOR TO THE DRAWING.**

**Directions to Buckeye Hall of Fame Café  
1421 Olentangy River Rd.  
Columbus, Ohio (614) 291-2233**

**From the North:**

Take 315 S. to Kinnear Rd. exit. Go left around Lenox Square. Stay in the right lane. The Café is one block away on the right hand side.

**From Downtown:**

Take High St. or Neil Ave. (north) to 5<sup>th</sup> Ave. West (left). Turn right at Olentangy River Rd., after the bridge and the Café is on your left.

**From the East:**

Take 670 W. to Neil Ave. and travel north to 5<sup>th</sup> Ave. Turn left at 5<sup>th</sup> Ave. Once over the bridge, turn right onto Olentangy River Rd. The Café is on your left.

**From the South:**

Take I-71 N. to 670 W. Exit at Neil Ave. and go north to 5<sup>th</sup> Ave. Turn left at 5<sup>th</sup> Ave. Once over the bridge, turn right onto Olentangy River Rd. The Café is on your left.

**Membership Information:** [www.isaca.org/memb1.htm](http://www.isaca.org/memb1.htm)