

March 2008



Newsletter

Serving IT Governance Professionals

Utah Chapter

Our Mission: Provide our members opportunities for career development and networking with peers. Advance and promote the profession by creating awareness of the skills and abilities of IT audit and security Professionals.

President's Message

Hello Utah ISACA members. We will be having our regular monthly luncheon at the Lion House on Thursday, March 20th. A.J. Harring from Check Point will be speaking on Unified End Point Security. We hope to see everyone there. Just go to our Web site at <http://www.isaca-ut.org/utahevents.html> and sign up.

Presenter: A.J. Harring, Check Point.

Bio: A.J. Harring, Director of Sales, Check Point End Point Security
Extensive experience interacting with world-class companies and managing teams that deliver solutions to address their critical IT initiatives. Has helped to grow companies like Platinum Technology, Compuware, Pointsec, and Check Point.

Presentation: Unified End Point Security

Addressing the challenge of protecting critical data and addressing regulatory compliance is not what it used to be. The landscape has changed, but basic principles remain paramount to success.

Our next monthly luncheon will be held on Thursday, April 17th. Also, we are planning on holding our Spring seminar in May. More information on these events will be coming.

As mentioned previously, our chapter is sponsoring the IT Summit conference held on April 16th in the Salt Palace Convention Center. As a sponsor, our chapter members can attend this conference for free. To register for complimentary admission, just visit <http://pwg.groupcommons.com/base/standard/conference/register/9> and enter Discount Code UT08-ISACA. See more information about this conference below and on our Web site.

The next CISA and CISM exams will be held on June 14, 2008. If anyone is interested in our chapter setting up a review course for these exams, please contact Jordan Fuller (jordan.fuller@gmail.com) for the CISA exam or Sod Chuluunbaatar (schuluunbaatar@deloitte.com) for the CISM exam. We need about 7 people to show an interest before setting up the course. Please contact Jordan or Sod by March 15th.

Have a great month,

Mark Murdock

P.S. Here is an email about the IT Summit from Abe Homan:

Dear ISACA member

ISACA is a sponsor of The IT Summit, coming to the Salt Palace on April 16th, 2008. You are invited to attend, compliments of ISACA.

The IT Summit is the executive technology conference series coming to six US markets this year. The purpose of the educational conference series is to support the proliferation of information technology. Attendees are senior-level IT executives from government, education, and corporate.

You will enjoy the demonstrations, networking, and presentations from:

Robert Clyde, CTO, Symantec, Topic Coming Soon

Darwin John, CIO, FBI (ret) **Are CIO's Focused and Proactive Enough?**
Cheney Eng-Tow, Special Agent, FBI **Cyber Crimes Today**
Beto Paredes, CEO, ApogeeInvent Development Group **Artificial Intelligence for the Web**
Les Squires, President, Group Commons **CIO Collaboration**
Randy Sutherland, Western Regional Sales Manager, Lumension Security **Best Practices for an IT Security Policy**

more to follow.

To register for complimentary admission, please visit <http://pwg.groupcommons.com/base/standard/conference/register/9> and enter Discount Code UT08-ISACA

See you at the conference!

Abe Homan
Paramount World Group
15532 SW Pacific Hwy, C-1B #306
Tigard, OR 97224
(503) 616-3227
(610) 885-7452 - fax
ajh@paramountworldgroup.com
www.itsummit.com

Monthly Professional Training

Date: Thursday, Mar. 20th
Time: 11:30 – 1:15 pm.
Place: Lion House
Speaker: A.J. Harring, Check Point
Topic: End Point Security
Cost: Members- \$15, Students - \$15, Non-members - \$18

Please sign up via our web site: <http://www.isaca-ut.org/utahevents.html>

Menu

Tossed Salad
Beef Stroganoff
Coconut Cream Pie

Monthly Training Registration

The cutoff time period to sign up for the professional lunch meeting is the Tuesday before the monthly Thursday meeting. If you sign up after noon on Tuesday, you may or may not have a guaranteed seat. Since the rooms at the Lion House are small we have to give them a hard count by Tuesday at noon to reserve a room, that is reason for the cutoff time. Thanks

Training Opportunities

ISACA e-Symposium

If you are in need of CPE credits, an easy way to earn them is by participating in an ISACA e-Symposium. These are free online web casts and you can earn 3 CPE credits. For further details, go to: www.isaca.org/webcasts

Another way to earn CPE credits is by taking the Information Systems Control Journal CPE Quizzes that are online at: http://www.isaca.org/Template.cfm?Section=CISA_Certification&CONTENTID=16839&TEMPLATE=/TaggedPage/TaggedPageDisplay.cfm&TPLID=58

Each quiz passed with at least 75% earns 1 CPE credit. There is no cost, which is hard to beat!

IT SUMMIT

For those interested, here is the information on the IT Summit:

“The IT Summit is the executive technology conference series coming to the Salt Palace on **April 16th, 2008**. The purpose of the conference series is to support the proliferation of information technology. Each conference features a full day of presentations, networking, and exhibits. We support certain non-profit IT organizations at no cost.

We propose to provide ISACA with complimentary admission for your members, promotion on the conference website, print work, marketing materials, and conference guide in exchange for promoting the event to your people. We hope you use The IT Summit as a membership drive vehicle.

Below, please see details from our annual Denver conference which took place on May 30th. I have included Denver details as an example because each of our programs is very similar. We welcomed 400 attendees in Denver.

More information is available at the following web link: <http://www.theitsummit.com>

International Training

More information is available at the following link: <http://www.isaca-ut.org/training.html>

Attention

If you did not receive your CPE certificate from the fall 2007 seminar, please contact Kyle Chugg at kchugg@americafirst.com and he will get it to you. Thanks

Training in Oklahoma:

Spring Seminars – March 31 – April 3, 2008
Information Risk Management and
Network Security Essentials
Oklahoma State University / Oklahoma City
Please see the attached pdf file in your email.

Internal Threats and the Way Auditors Can Best Combat Them

As auditors we hear these words frequently that the most pervasive threat against most organization is the internal threat. And they are. The greatest threat is the one having the access to our internal networks. Research from the Department of Defense found that approximately 86 percent of enterprise attacks were found among those having technical positions at the enterprise level and of these an additional 57 percent were performed after termination. In some case studies it requires at least 1,000 man-hours to restore data that has been deleted by a disgruntled former employee of an IT department that gained access to key network systems.

Here are some key areas that should be made part of an IT auditors work papers as part of best practices when dealing with privileged passwords:

-Define the inventory of privileged passwords. Who has them and why. These passwords are “root” on Unix and POSIX platforms and “Administrator” in Windows devices. These are accountable to individual systems administrators and must never be shared among administrators or anyone else for any reason. Policies must be crafted to detail sufficient disciplinary action discouraging this practice.

-Define the role of access management and identity. The greatest mistakes committed by organizations is managing human identities and access management in blanket form without specific accountability and responsibility. Audit trails show that someone downloaded a database of clients at 0136 a.m. on Sunday but further analysis will not allow specific detail to be made to an individual employee. This is a disgruntled employee’s dream that of having little accountability or responsibility for actions on the network.

-Change policies must apply to privileged passwords. For example passwords on a laptop change every 30 days and must be enforced however surveys show that administrator passwords do not change from the default. If mobile devices are lost, the new owner can quickly research the default administrator password and access the data 20 percent of the time. (I know I did exactly this with a CEOs laptop recently.)

-Ascertain the storage of privileged passwords. This might seem overly obvious, but it is omitted often in work papers. Privileged passwords are stored in binders, or cards, notes or other unsecured means. Regrettably, it is too often seen.

-Don’t accept the premise that since “we have never secured these passwords, we never shall” attitude. Privileged passwords are the Crown Jewels and are not going to be left around for just anyone’s collection. Remember that they control the most valuable resources of the enterprise and must be secured with assigned accountability.

-When a holder of a privileged password is dismissed or announces her intention to leave the organization a specific policy must be in place. And once they have left the organization, then an immediate audit is performed of their actions for the previous 60-day period.

Regardless of the craftiness and motivation of the employee, the threat level cannot be overestimated at the enterprise level. However, auditors having a regard for employees with privileged passwords and unfettered access these keys allow, can point the means that provide for their responsible and authorized use.

Alan B. Sternecker, CISSP, CISA, CISM, CFE is a consultant and is the author of Critical Incident Management, ISBN: 084930010X, published by CRC Press, www.crcpress.com. He has written numerous articles and regularly lectures regarding fraud and computer systems security auditing. He can be reached at absterneckert@yahoo.com

Journal Update

The Information Systems Control Journal is seeking articles for volume 1, 2008, to be issued in January 2008. The copy deadline for volume 1 is 24 September 2007, and the theme is **Dysfunctional Operations in IT**. For more information, please view the 2008 editorial calendar at www.isaca.org/journal or e-mail jblader@isaca.org.

Board of Directors and Officers

President

Mark Murdock
LDS Church
murdockma@ldschurch.org

Vice President

Julie Park
Weber State University
jpark@weber.edu

Treasurer

Brandon Brown
Deloitte & Touche LLP
brandonbrown@deloitte.com

Secretary

Kyle Finlayson
Intermountain Health Care
kyle.finlayson@intermountainmail.org

Newsletter/Publicity

David Gibson
Legislative Auditor General's Office
dgibson@utah.gov

CISA Coordinator

Jordan Fuller
América Corporation
jfuller@amediacorp.com

Membership Director

Dan Anderson
IHC / GE Healthcare
daniel.anderson@intermountainmail.org

CISM Coordinator

Sod Chuluunbaatar
Deloitte & Touche LLP
schuluunbaatar@deloitte.com

Seminar/Education Chair

Kyle Chugg
America First Credit Union
kchugg@americafirst.com

Academic Relations Chair

Jeff Davis
Weber State University
jtdavis@weber.edu

Research Chair

Angela Duff
Fiducian
aduff@fiducian.us

Webmaster

Ben West
Protiviti
ben.west@protiviti.com

The views and opinions contained in this publication are solely those of the authors, and do not necessarily represent or reflect the view or opinions of the Utah Chapter. In the event you have any questions concerning an article, you may wish to contact the author directly.