

Oct. 2009



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

Greetings Utah Chapter members,

Our thanks go out to Robert Lee for his insightful presentation on Security Metrics in September.

Our next meeting is scheduled for October 15th, where Tim Martin will be presenting on ID Theft and Phishing.

We are also getting the details for the Fall Seminar. Kyle Chugg and Brady Stevensen have arranged to have Cody Hatch with Compunet present on "Securing the Borderless Network". More information should be available at the October meeting.

Although we do everything we can to keep costs low for our members we are no longer able to subsidize the cost of our monthly meetings at the Lion House. Beginning in **October** the monthly meeting costs for members will be \$20 and \$25 for all others (cost to students will remain the same at \$15). Thank you for your understanding.

I'm looking forward to seeing you on the 15th!

Thanks

Julie Park

****Important Notice***

Our web site is currently experiencing some technical difficulties. If you are planning on paying with a credit card please go to the following link: <http://www.acteva.com/booking.cfm?bevaaid=176786>
The link that is currently on the web site to pay by credit card is pointing to the previous month's event. This new link will take you to the correct URL.

If you are going to pay at the door then select the link that is on the web site. <http://www.isaca-ut.org/utahevents.html>

Thanks, the person in charge of the website is currently out of the country so we have to make do for this month.

Monthly Professional Training

Date: Thursday, Oct. 15th
Time: 11:30 – 1:15 pm.
Place: Lion House
Speaker: Dr. Tim Martin
Topic: ID Theft and Phishing
Cost: \$20 for members and \$15 for students, \$25 for non-members

CPE: 1 Credit

Email: utah.isaca.chapter@gmail.com
Include the first and last name with e-mail address for each attendee you are registering.
Register at: <http://www.isaca-ut.org/utahevents.html>

Menu

Sarah Salad
Baked Ham
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. Thanks

Earning CPE

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

I found out from ISACA that there is no limit to the number of e-Symposiums or on-line quizzes that you can take to help fulfill your CPE requirements. If you have any questions concerning CPE credits please email the following: certification@isaca.org and they will answer your questions.

Suggestions for Monthly Speakers

If you have a topic you would like to hear in one of our monthly meetings or if you know of a good speaker please email Jackie Schwartz: Jackie.Schwartz@usa.net

Monthly Article

When IT Security Can Actually Hurt Your Business

As IT becomes considered as a real commodity it also gets better at causing real system outages. Many organizations are directing that IT security leads the way when taking cues for best practices for the enterprise thereby creating chaos when security changes crash systems.

Of course it is given that companies need security for their IT assets and systems. However, many security units are isolated as stand-alone entities working as “I know what is best.” And with this attitude instilled the resulting consequences are disastrous for the organization at large. More often than not, this business practice is due to corporate practices of keeping IT operations and IT security distant from one another. The usual business practice is that of IT being treated to “having security performed on them.” Under the best circumstances IT and security are at odds and security seems a bit elitist and at worst they seem a regulatory liability.

Then there is the example of the security practitioner/auditor that decided that all the passwords used by his organization were “weak.” So he decided to test them and designed a scheme of his own making. This was a good plan at least on paper to impress upper management. The resulting problem was that the password scheme he devised was so strong the users could not remember them so they were forced to write them on small notes near their computer monitors so they might remember them when they signed in. This well-intentioned act by a security practitioner in order to prevent HIPAA violations actually ended up causing more potential violations than the weak passwords.

Here is another typical example of security gone wrong where a security department demanded that a software patch for an operating system was pushed out. The security department saw that it was so important that they skipped testing this patch in a controlled environment and did not follow the organization’s change management policies. Of course as soon as the patch was installed throughout the organization, the system suffered a catastrophic failure. The administrators and help desk persons tried several days to fix their system that in the mean time suffered a serious reputation loss in the market place.

Granted security officers too often find that they must push out security practices or patches expeditiously, however this is the case that “haste makes waste.” If security officers do not act swiftly enough then the results might be devastatingly bad. It is a double edge sword where balance is key.

The burdens of regulatory audits relating to program and change management are not impossible to meet rather it is a matter of understanding IT and business operations. Today is the time to integrate security into these functions and security priorities.

Such consideration can improve decision making in at least three articulated areas:

- Awareness of how IT systems and applications function by participating in their operational activities
- Understanding stakeholder/user risk tolerance and security requirements
- Manage security related changes to the system through the IT change management process

Alan B. Sternecker, CISA, CISM, CFE, CISSP 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

Board of Directors and Officers

President

Julie Park
Weber State University
jpark@weber.edu

Vice President

Jackie Schwartz
Axiom Recovery
Jackie.Schwartz@usa.net

Treasurer

Dan Walker
Intermountain Health Care
Dan.Walker@imail.org

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
Amedica Corporation
jfuller@amedicacorp.com

Membership Director

Michael Carter
LDS Church
carterma@ldschurch.org

CISM Coordinator

Brandon Greenwood
XanGo
bgreenwood10@hotmail.com

Seminar/Education Chair

Kyle Chugg
Questar
Kyle.Chugg@questar.com

Academic Relations Chair

Jeff Davis
Weber State University
jtdavis@weber.edu

Research Chair

Dan Anderson
Intermountain Healthcare
Daniel.Anderson@imail.org

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.