

June 2008



# Newsletter

**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. Please join us this month for a **free lunch** at our Annual General Meeting (AGM) on Thursday, June 19, 2008. We will give you an update on our local chapter proceedings as well as provide information on ISACA International initiatives. We look forward to seeing each of you there.

After the AGM, we will take a break from our monthly luncheons for the summer. Our next luncheon will be held on Thursday, September 18<sup>th</sup> at the Lion House.

Have a great summer!

Mark Murdock

## Monthly Professional Training

Date: Thursday, June 19th  
Time: 11:30 – 1:15 pm.  
Place: Lion House  
Speaker: Annual General Meeting  
Topic: Membership business  
Cost: Free

Since there is no charge for this month's meeting you can register directly to me at:  
Email: [utah.isaca.chapter@gmail.com](mailto:utah.isaca.chapter@gmail.com)  
Include the first and last name with e-mail address for each attendee you are registering.  
Please **RSVP** to David Gibson by 6/16/2008

### Menu

Sarah Salad  
Lemon Thyme Chicken  
Poppy Seed Cake

## 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](http://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](mailto:certification@isaca.org) and they will answer your questions.

\*\*\*\*\*

## **International Training**

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

## **A Big Shout OUT!**

A big thanks to Alan B. Sterneckert for providing the monthly article to our newsletter.

## Logging

Implementing recognized security protocols as ISO 17799, ISO 27001, ITIL is a sound business practice. Integral to these protocols is activity logging. On the surface logging might seem mundane even trivial, but logging serves a vital business function reaching across most organizational lines. Logging data is the organization's richest asset for its security posture, tracking threats and meeting its active and passive audit requirements both regulatory and internal. Because of their possible evidentiary value logs must be maintained as complete, inventoried, accurate and verifiable. Of course records retention must include administrative finality, civil finality and the criminal statute of limitations. Activity logs are no longer just tools of the trade for network administrators these data are a significant implement of the legal trade with impact for most stakeholders.

With the spiraling up of activity logs so has the confusion surrounding their legal and moral issues. Many believe these logs must be preserved in pristine, unalterable format to be considered legally valid. And there are some that believe that there are practical standards allowing more flexibility in their storage. The truth is actually in the former rather than the latter. All original logs must be pristine and unaltered. That is the short truth. All logged data that are going to be reviewed by administrators, auditors and other practitioners must be replicas of these originals. There must be tangible and documented means of how replicas of the originals were created including the why, how, when, how and who. What actions are performed with the replicas is a simple matter of practices done within the organization for their own purposes be it auditing, review, sampling, filtering, etc.

Complete logs tell-the-tale enabling the digital chain of custody proving the method that the evidence, or in this case the log, passed from each person to another person. A full and complete set of logging data delivers visibility into the networks activity landscape. It makes it possible for investigators, auditors, administrators, and legal folks to gain vital insight and reach a logical conclusion based on facts not conjecture.

Analogous to completeness is accuracy and is prerequisite to successful logging in business and audit functions. Legal due diligence, legal and business due diligence are intended to ensure the accuracy of functions to the extent the criminal and civil enforcement actions are actively sought against violators. Electronic copies must exactly replicate the original but the original must not be disturbed in any fashion, not one single bit.

Once logs are determined to be complete and accurate they must be determined to be verified. Techniques such as hashing provide a digital fingerprint of logs. This one way hash is a proven way of verification for both the original and the replica that they are unchanged. These verification hashes show that the organization took the steps of proper due diligence in business functions, administrative, civil and criminal proceedings.

Auditors must ensure that logged data are complete, accurate, and verifiable. The next successive step is ensuring that the terabytes of data is in compliance with current legal standards. These data must be human readable and useful in administrative and legal actions. Administrative actions include those internal actions taken by executive and managerial ranks. Logged data that must be interpreted by technical folks will not likely be acceptable. The key goal here is for self-policing and cooperation with business executives, investigators and law enforcement officers with out the force of court orders unless absolutely required by law.

As an aside here, Sarbanes/Oxley requires businesses to disclose information in a timely fashion to the public regarding material changes to the financial condition or operations of the company. Additionally, the Federal Trade Commission details in its Safeguards Rules the criticality of monitoring use, reviewing access records and logs.

Internally CIOs, legal departments, HR departments, and CFOs are just a few of the non-system administrators that commonly request logged data looking for their content to support actions. Often systems access and activity, IM, email, and Web browsing are the focus of their attention. Consequently, logs are increasingly used as primary evidence to demonstrate the footprint of the employee on the company network. With auditors ensuring the confidentiality, integrity, and authenticity of these logged data businesses can reduce the potential of losing administrative and legal actions.

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](http://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](mailto: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](http://www.isaca.org/journal) or e-mail [jblader@isaca.org](mailto:jblader@isaca.org).

## Board of Directors and Officers

### President

Mark Murdock  
LDS Church  
[murdockma@ldschurch.org](mailto:murdockma@ldschurch.org)

### Vice President

Julie Park  
Weber State University  
[jpark@weber.edu](mailto:jpark@weber.edu)

### Treasurer

Brandon Brown  
Deloitte & Touche LLP  
[brandonbrown@deloitte.com](mailto:brandonbrown@deloitte.com)

### Secretary

Kyle Finlayson  
Intermountain Health Care  
[kyle.finlayson@intermountainmail.org](mailto:kyle.finlayson@intermountainmail.org)

### Newsletter/Publicity

David Gibson  
Legislative Auditor General's Office  
[dgibson@utah.gov](mailto:dgibson@utah.gov)

### CISA Coordinator

Jordan Fuller  
América Corporation  
[jfuller@amediacorp.com](mailto:jfuller@amediacorp.com)

### Membership Director

Dan Anderson  
IHC / GE Healthcare  
[daniel.anderson@intermountainmail.org](mailto:daniel.anderson@intermountainmail.org)

### CISM Coordinator

Sod Chuluunbaatar  
Deloitte & Touche LLP  
[schuluunbaatar@deloitte.com](mailto:schuluunbaatar@deloitte.com)

### Seminar/Education Chair

Kyle Chugg  
America First Credit Union  
[Kyle.Chugg@questar.com](mailto:Kyle.Chugg@questar.com)

### Academic Relations Chair

Jeff Davis  
Weber State University  
[jtdavis@weber.edu](mailto:jtdavis@weber.edu)

### Research Chair

Angela Duff  
Fiducian  
[aduff@fiducian.us](mailto:aduff@fiducian.us)

### Webmaster

Ben West  
Protiviti  
[ben.west@protiviti.com](mailto: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.