

Sept. 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. Welcome back from the summer break. Can you believe that it is already September and the cold weather is on its way? I hope each of you had an enjoyable summer, and it will be good to see you again.

We will be having our regular monthly luncheon at the Lion House on Thursday, September 18th. Scott Wright, CISSP, CBCP, MBCI is the CEO of Visual Compliance and will be our speaker. See a link to his business at www.visualcompliance.net. We hope to see everyone there. Remember to go to our Web site at <http://www.isaca-ut.org/utahevents.html> and sign up.

Our Fall seminar is also coming up shortly. We will be holding our one-day seminar on Friday, November 21st at Thanksgiving Point. Fishnet Security will be presenting on the topic of Linux security. Kyle Chugg will be having a brochure sent out, which will contain more detailed information on the seminar topic, speaker, and price.

Next month's luncheon will be held on Thursday, October 16th at the Lion House. More information will be forthcoming.

Hope to see you soon,

Mark Murdock

Monthly Professional Training

Date: Thursday, Sept 18th
Time: 11:30 – 1:15 pm.
Place: Lion House
Speaker: Scott Wright
Topic: Visual Compliance
Cost: \$15 for members and students, \$18 for all others
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.
Please **RSVP** to David Gibson by noon on 9/16/2008

Menu

Sarah 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. 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.

International Training

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



Utah ISACA 2008 Fall Seminar

Date & Time: November 21st, 2008 from 8:30-4:30 (7 CPE credits)

Topic: Linux Security and Audit Fundamentals

Speaker: Ralph Bonnell from Fishnet Security

Cost: \$250 for Utah ISACA members and affiliated chapters (ISSA, IIA)
\$300 for non-members

Registration: Go to <http://www.isaca-ut.org/utahevents.html#fallseminar>

Deadline for any method of registration is November 17th at Midnight MST


Check, Visa, or MasterCard accepted

RSVP to David Gibson via the chapter email address:
utah.isaca.chapter@gmail.com

Location: Thanksgiving Point, Lehi, Utah in the Amber Room

<http://www.thanksgivingpoint.com/information/maps.html>

Questions: Email Kyle Chugg at kyle.chugg@questar.com



Other Training Opportunities

Upcoming ACFE Anti-Fraud Course in Salt Lake City

Topic: Introduction to Digital Forensics

Date: Oct 27-28, 2008

Place:

Hilton Salt Lake City Center

255 S. West Temple

Salt Lake City, UT 84101

Cost:

Member: \$795

Non-Member: \$945

Register by September 27 and SAVE \$95**!

CPE Credit

16

Course Details<<http://eweb.acfe.com/./eweb/DynamicPage.aspx?webcode=topicdesc&topkey=4ee0d451-82b5-4ef8-9fea-06008ef34c99>>

View the Course Outline <<http://www.acfe.com/training/IDFSchedule.asp>>

Course Level

Basic

This two-day course will introduce the fraud examiner to basic concepts of computer forensic investigation and analysis. In this instructor-led course the attendee will learn basic techniques involved in gathering and analyzing digital evidence in fraud examinations, as well as the proper procedures for seizing and securing digital evidence. A software demonstration will also allow you to examine forensic artifacts. The speaker for the course will be James J. Butterworth<<http://www.acfe.com/about/bio-jbutterworth.asp>>.

Breach Notification

Breach notification laws and regulations have contributed to the awareness of information security throughout all levels of an organization as well as informed the potentially aggrieved consumers. Security officers report that breach notification duties have empowered them to implement new levels of access controls, auditing measures and levels of encryption.

As of 2007 there are 36 states that have enacted legislation requiring businesses and government organizations that control personal identifiable information (PII) to warn relevant individuals of security breaches. The state of California led the way with the creation of SB 1386 having been driven by the concerns of identity theft and the apparent lax security surrounding the control of PII. For most purposes PII is categorized as Proper Names, Addresses, SSN, Drivers License Number, Home Address, Telephone Number, Spouse's Name, Mother's Maiden Name, etc.

With the state-patchwork of legislation and regulations there has been an outcry for federal legislation to be enacted to override state laws and create a cogent consumer related set of laws. Data holders have begun to question if consumers actually pay attention to security breaches and if these breaches involve PII theft or not. And here is the \$64,000 question; is the small breach as risky as the extremely large one? The plain answer is both.

As far as ROI is concerned the security of PII is not marketable for most business entities but the downside of declining market share resulting from the proceedings of a noisy lawsuit could prove to be a deterrent. With this aspect in mind, PII security and auditing are gaining ground as vital business features for most organizations. This pressure removes the reputation protecting third party data collectors that lack direct interactions with the general public and moves toward a more uniform set of security practices. For example, a company selling data now allows external entities to audit its systems to determine its internal practices and controls.

Faced with mounting legislation mandating reporting of PII breaches or CISOs in locations that do not have specific reporting requirements here are some best practices:

- Formulate and establish an organizational wide uniform standard that requires public notice of all security breaches to help security professionals track and adapt to incidents at other organizations ensuring that all affected consumers are provided PII breach notices.

- Formulate and establish PII uniform reporting standard requiring notification to a centralized organizational unit in addition to consumers making breaches publicly available allowing industry professionals to reference breach reports for information on security vulnerabilities.

- Clarify and broaden technology for encryption giving better guidance to organizations on what types of security mechanisms are sufficient to prevent lost data from being accessible for the purposes of misuse and to provide research for technologies that render PII useless if accessed without proper authorization. Is the organization's data stored openly or is it stored encrypted onsite and in mobile environments?

- Create and establish a period for notification how notifications must be given for flexibility for organizations to investigation and remedy security breaches.

- Determine the triggers that should be used delivering notification of security breaches.

Many organizations deal with Gramm-Leach-Bliley Act (GLBA) and if publicly traded Sarbanes-Oxley (SOX), or the Health Insurance Portability and Accountability Act (HIPAA). Title V of GLBA authorizes each of the relevant agencies to establish and enforce guidelines ensuring security protecting against unauthorized access of their customer data. SOX efforts are pointed toward safeguarding PII by developing reasonable security measures and developing a formal response plan dealing sufficiency of internal controls. HIPAA has issued their standards regulating identifiable health information that is created or received by a covered entity as it relates to health condition, health care and payment for health care that identifies the individual among covered entities.

It is noted that SB 1386 is not industry-specific as it relates to organizations that do business in California or individuals that reside there suffering a breach of their PII.

Since most notification statutes require that businesses notify relevant parties within a "reasonable" amount of time, there seems to be a great deal of leeway for interpretation. For example, the University of California at San Diego waited three months to notify students and alumni of a potential breach. Obviously, when SB 1386 applied this period was too long if PII had been "in the wild" for corrective action to be taken.

Most executives and auditors know a great deal about identity theft, it is clear that PII theft is a constant problem and one that is becoming one more complex to remedy. CISOs most often are not able to decide the nexus between PII theft and security breaches that have motivated legislation toward consumer protections. Among these well-intended laws are those that raised awareness and vigilance correcting information security through the many levels of security professionals and upper level executives.

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

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
Amica Corporation
jfuller@amediacorp.com

Membership Director

Chuck Sims
BYU
Chuck@byu.edu

CISM Coordinator

Sod Chuluunbaatar
Deloitte & Touche LLP
schuluunbaatar@deloitte.com

Seminar/Education Chair

Kyle Chugg
America First Credit Union
Kyle.Chugg@questar.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.