

Feb. 2010



# 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**

Greetings Utah Chapter members,

We had a great January meeting. Brandon Greenwood presented on IT Auditing: Intrusion Detection. A copy of the presentation was emailed to the chapter.

Our February presenter is James Elste, Security Strategist, Symantec Corporation who will be presenting on "The Anatomy of a Breach" - Hackers to Criminals. Please remember to sign up early to make sure we get a room big enough to comfortably seat everyone who wants to attend.

I am looking forward to seeing everyone on February 18, 2010.

Thanks

Julie Park

## Monthly Professional Training

Date: Thursday, Feb. 18, 2010

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: James Elste, Security Strategist, Symantec Corporation

Topic: The Anatomy of a Breach” - Hackers to Criminals

Cost: \$20 for members and \$15 for students, \$25 for non-members

CPE: 1 Credit

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.

Register at: <http://www.isaca-ut.org/utahevents.html>

### Menu

Sarah Salad

Beef Stroganoff

Lemon Chiffon 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.

\*\*\*\*\*

### 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](mailto:Jackie.Schwartz@usa.net)

## Monthly Article

### **Auditing the Cloud**

With the advent of cloud computing tasks usually reserved for servers where one task resides on a machine is disappearing. Cloud computing is virtualized where subscribers are connected to virtual servers. In essence, one hardware machine with a resident operating system and virtualizing application can host many server applications in what might be called an “elastic environment.” In this environment, as traffic increases more virtual servers are added and as traffic decreases they shrink in number to accommodate.

Cloud computing therefore has some easily seen advantages in that they are very scalable having the capacity to serve the needs of individuals and organizations. An example of this is an organization offering a contest to build customer loyalty. As customers login to their accounts where they post their product information and receive product rebates traffic and server utilization increases. Cloud computing environments allow more servers to be added to accommodate spikes in traffic. And as the flood subsides, they can be removed.

And of course, this means that cloud computing need not reside in the data owner’s space. It is easily outsourced to a third party. This has its own risks and advantages as does any outsourced service. The primary security concerns for cloud computing environments are the following:

- Administration of the virtualized server takes place remotely. Since this means there is exposure to others being able to gain access to the remote host. It is imperative that a secure means of communicating to the server be established. And this secure means must be sufficient to allow only authenticated access to the service.

- Trusted borders must be enforced between the cloud computing servers and the business organization. Malicious individuals will take advantage of any or all vulnerabilities existing in any connections between parties.

- Establish security policies and standards for the business organization and ask to see those policies and standards of the cloud provider.

- Store only non-critical data on the cloud provider. Consider using data at rest encryption for Personally Identifiable Information (PII), HIPAA, or other critical data.

Of course, auditors must get involved in auditing their business’s cloud computing efforts mitigating risks right from the start. Here are a few things that auditors must keep in mind when their organization is considering a cloud computing project:

- Where is the cloud located? The country or state of the cloud is important. Such laws as Safe Harbor, SB-1386, GLBA, or other laws may attach. Knowing this is very important also if the cloud is located in an area that is known for being unstable either geographically or politically.

- How critical is the application being sent to the cloud for administration? The cloud should be considered only for non-critical applications and for handling non-critical data.

- Auditors must request a copy of the disaster recovery policy of the cloud provider and subject it to the same review as the business.

- Auditors must review the cloud provider’s security policy and determine how they have responded to incidents.

- Auditors should obtain independent visibility into the controls of the cloud provider. This process may take shape through an independent audit report or even having an audit take place at the cloud provider.

There is little doubt cloud computing is here to stay and will have an increasing effect on business and information flow for users and organizations. For most, cloud computing represents the best and riskiest type of outsourcing. Consequently, it is important that cloud computing users and auditors weigh carefully its implementation knowing strengths and vulnerabilities.

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 [absternecker@yahoo.com](mailto:absternecker@yahoo.com)

## Board of Directors and Officers

**President**

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

**Vice President**

Jackie Schwartz  
Jasper Enterprises  
[Jackie.Schwartz@usa.net](mailto:Jackie.Schwartz@usa.net)

**Treasurer**

Dan Walker  
Intermountain Health Care  
[Dan.Walker@imail.org](mailto:Dan.Walker@imail.org)

**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  
Amedica Corporation  
[jfuller@amedicacorp.com](mailto:jfuller@amedicacorp.com)

**Membership Director**

Michael Carter  
LDS Church  
[carterma@ldschurch.org](mailto:carterma@ldschurch.org)

**CISM Coordinator**

Brandon Greenwood  
XanGo  
[bgreenwood10@hotmail.com](mailto:bgreenwood10@hotmail.com)

**Seminar/Education Chair**

Kyle Chugg  
Questar  
[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**

Dan Anderson  
Intermountain Healthcare  
[Daniel.Anderson@imail.org](mailto:Daniel.Anderson@imail.org)

**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.