

April 2010



Newsletter

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 March meeting, where Josh Taylor from PWC gave a presentation on Third Party Assurance (TPA).

Our April presenter is Chad Tilbury, who will be presenting on Computer Forensics. Please remember to sign up early to make sure we get a room big enough to comfortably seat everyone who wants to attend.

Also, our spring seminar is scheduled for May 14th. We are very excited to have Cisco come and present, and we will provide more information about the details of the Spring seminar soon.

I am looking forward to seeing everyone on April 15, 2010.

Thanks

Julie Park

Monthly Professional Training

Date: Thursday, April. 15, 2010
Time: 11:30 – 1:15 pm.
Place: Lion House
Speaker: Chad Tilbury
Topic: Computer Forensics
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
Herbed Crusted Chicken
Carrot 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

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

Cloud Computing Security

The latest buzz-words this year are “cloud computing. Or, as it is also called software as a service (SaaS). Cloud computing in its simplest term is expressed when one runs software over the Internet and accesses it via a browser. One of the most common examples is “Google Apps.” If one believes the popular literature cloud computing is the short-term future of computing. And it just might be the bane of professionals involved in auditing and security.

SaaS moves trust boundaries further than they have been previously. Now professionals must trust their software service vendors more than ever. However, it really does not fundamentally change the world, it just means that one trusts another vendor.

With any other technology shifts there are security benefits and risks that must be addressed before the full scope of cloud computing might be understood. There are considerations as regulatory compliance, risk management, identity and access management, and data loss prevention that must be explored when evaluating, managing, implementing, maintaining and deprecating cloud computing solutions.

Here are several salient security points to consider before implementing cloud computing:

Compliance and Risk Management: Organizations shifting part of their business to the cloud are still responsible for compliance, risk, and security management.

Identity and Access Management: Identities coming from different providers. Providers must be able to document from on-premise to the cloud, as well as to enable collaboration across organizational and country-borders.

Service Integrity: Cloud-based services should be engineered and operated with security in mind, and the operational processes should be integrated into the organization's security management.

Endpoint Integrity: As cloud-based services originate and are then consumed on-premise, the security, compliance, and integrity of the endpoint have to be part of any security consideration.

Information Protection: Cloud services require reliable processes for protecting information before, during, and after the transaction.

There are many potential benefits and services cloud computing might create however these also bring new concerns some of which might not be fully understood by executives, administrators and managers. Adopting cloud services usually require businesses to adopt a data management model that is no longer under their direct control. This concept is true in the *hybrid model* where some of the business processes remain on site and others are handled remotely by another IT organization. Now this often means that data traverses from one location to another and one host to another. The responsibility of risk management and security remain with the original business organization and depending on the circumstances will be extended to include the cloud provider.

When critical business processes are migrated to the cloud, internal security matters need to immediately involve allowing cloud providers to participate in these processes as needed. These processes include security monitoring, forensics, auditing, critical incident response and business continuity. Degrees of collaboration must be addressed during the initial cloud setup between the service provider and the customer taking all parties into consideration. Of course, for certain applications and services security requirements are fairly simple but for more complex services more detailed requirements are contractually needed. These often include physical security necessities, logging, in depth employee background investigations, etc. A handshake, nod or verbal agreement is insufficient in this environment.

And any SaaS service agreement must include detailed plans covering management performance problems and completing network, backups and forensics as needed. The service agreement must include and define security monitoring, auditing and system correction intervention timetables provided by the cloud service provider and at what price levels. Of course it is vital to reduce to written form the security for endpoints needed for cloud-based services. Too often discussions of cloud security are narrowly focused on the service itself to the exclusion of the provider's security quality and practices. Failure to effectively evaluate an entire service level from beginning to end can result in flaws in product design and delivery no matter how well developed the application was done. In many cases where a business's security is compromised the issues occur on an individual server or workstation but in the cloud one can easily see the devastation that a compromise might bring.

To partially understand the security and by extension the audit consequences of cloud computing, several specific elements must be addressed: business process, applicable technology, human skills, and relevant controls. Therefore, businesses contemplating the implementation of cloud computing must consider the following base-level practical points before proceeding:

- Compliance program for managing identities, data and devices

- Data classification evaluating risk involving data

- Cloud deployment model depending on data classification security, privacy requirements and business needs

- Business team built to manage risk, security and compliance requirements working with cloud provider

- Auditability, transparency, and compliance controls are essential criteria in the determining the effectiveness of the cloud service provider

- Use of SDLC in developing applications and migrating these to the cloud provider

- Access controls for data needed to operate between different business units and organizational boundaries.

Alan B. Sternecker, CISA, CISM, CFE, CISSP is a consultant and 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
Jasper Enterprises
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.