

April 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. We will be having our regular monthly luncheon at the Lion House on Thursday, April 17th. James Sayles, Chief Risk and Compliance Officer with Favored Solutions, will be speaking on "Changes in Auditing and Information Security." We hope to see everyone there. Just go to our Web site at <http://www.isaca-ut.org/utahevents.html> and sign up.

Presenter: James Sayles, Chief Risk and Compliance Officer with Favored Solutions

Bio: James Sayles is VP, Chief Risk and Compliance Officer for Favored Solutions and has provided Governance, Risk and Compliance solutions to more than two dozen of the world's largest banks and financial institutions, managed business and information risks, secured and audited several of the largest Oil and Gas companies. He has over 12 years of industry experience, is a proven leader in working with organization to implement governance, risk and compliance solutions. He is experienced in compliance regulations and frameworks such as SOX 404 and 302, GLBA, HIPAA, PCI DSS, FISCAM/FISMA, SAS 70, FFIEC, COSO, ISO and PCAOB.

We will be holding our one-day Spring seminar on May 22nd at Thanksgiving Point. Our speaker will be Steven Fox, and he will be presenting on the topic, "Developing and Implementing an Organizational Risk Assessment Process." Kyle Chugg will be having a brochure sent out to all the members shortly, which will contain more detailed information on the seminar topic, speaker, and price.

Our next monthly luncheon will be held on Thursday, June 19th at the Lion House. This will be our Annual General Meeting. Come and enjoy a free lunch.

As mentioned previously, our chapter is sponsoring the IT Summit conference held on April 16th in the Salt Palace Convention Center. As a sponsor, our chapter members can attend this conference for free. To register for complimentary admission, just visit <http://pwg.groupcommons.com/base/standard/conference/register/9> and enter Discount Code UT08-ISACA. See more information about this conference below and on our Web site.

Have a great month,

Mark Murdock

P.S. Here is an email about the IT Summit from Abe Homan:

Dear ISACA member

ISACA is a sponsor of The IT Summit, coming to the Salt Palace on April 16th, 2008. You are invited to attend, compliments of ISACA.

The IT Summit is the executive technology conference series coming to six US markets this year. The purpose of the educational conference series is to support the proliferation of information technology. Attendees are senior-level IT executives from government, education, and corporate.

You will enjoy the demonstrations, networking, and presentations from:

Robert Clyde, CTO, Symantec, Topic Coming Soon

Darwin John, CIO, FBI (ret) **Are CIO's Focused and Proactive Enough?**

Cheney Eng-Tow, Special Agent, FBI **Cyber Crimes Today**

Beto Paredes, CEO, ApogeeInvent Development Group **Artificial Intelligence for the Web**

Les Squires, President, Group Commons **CIO Collaboration**

Randy Sutherland, Western Regional Sales Manager, Lumension Security **Best Practices for an IT Security Policy**

more to follow.

To register for complimentary admission, please visit

<http://pwg.groupcommons.com/base/standard/conference/register/9> and enter Discount Code UT08-ISACA

See you at the conference!

Abe Homan

Paramount World Group

15532 SW Pacific Hwy, C-1B #306

Tigard, OR 97224

(503) 616-3227

(610) 885-7452 - fax

ajh@paramountworldgroup.com

www.itsummit.com

Monthly Professional Training

Date: Thursday, April 17th

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: **James Sayles, Chief Risk and Compliance Officer with Favored Solutions**

Topic: Changes in Auditing and Information Security

Cost: Members- \$15, Students - \$15, Non-members - \$18

Please sign up via our web site: <http://www.isaca-ut.org/utaevents.html>

Menu

Sarah Salad

Chicken Cordon Bleu

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.

IT SUMMIT

For those interested, here is the information on the IT Summit:

“The IT Summit is the executive technology conference series coming to the Salt Palace on **April 16th, 2008**. The purpose of the conference series is to support the proliferation of information technology. Each conference features a full day of presentations, networking, and exhibits. We support certain non-profit IT organizations at no cost.

We propose to provide ISACA with complimentary admission for your members, promotion on the conference website, print work, marketing materials, and conference guide in exchange for promoting the event to your people. We hope you use The IT Summit as a membership drive vehicle.

Below, please see details from our annual Denver conference which took place on May 30th. I have included Denver details as an example because each of our programs is very similar. We welcomed 400 attendees in Denver.

More information is available at the following web link: <http://www.theitsummit.com>

International Training

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

Securing the Perimeter

Every organization has their most valuable assets reachable through the perimeter of their business enterprise. Protecting these assets however requires they conduct IT security audits in order to obtain some type of snapshot of the security risks so they might address threats and be prepared to mitigate or eliminate them.

Accordingly here are a few steps to conduct a basic IT security audit. While these steps aren't intended to be comprehensive this version will be sufficient to get anyone on at least on the path to protection.

Start by creating an assets list and define a security perimeter. Decide what are the assets of the organization. Usually these are most easily broken down by physical items as servers, routers, etc. Start by defining the "security perimeter" of the organization. The security perimeter is the conceptual and physical boundary of any business organization. It is the focus of where the security audit begins and the limit outside of which it will be ignored. It is the boundary of the organization's control. Remember it will include mobile computing devices such as mobile phones, PDAs and laptops.

Once the security perimeter has been determined, it is necessary to consider the actual asset list within the within the boundary. Here is a partial list of potential candidates:

- Computers and laptops
- Servers
- Routers and networking equipment
- Printers
- Scanning equipment
- Data
- Software Copyrights
- Wireless phones/ PDAs
- VoIP phones, IP PBXs
- Email
- Security cameras
- Employee access cards.
- Access points (i.e., any scanners that control room entry)
- Points of Sales and Related Credit Card Equipment

Create a list of threats and prioritize them. Simply stated an organization cannot defend itself against an unknown enemy. So at this stage the list of threats must be made and compiled combined corresponding to the assets to which they pose a danger. This compilation must include the frequency these threats occur. Usually the frequency of threats occurring within a given time period of a year is acceptable. There is a margin of idiocy in this stage where resources are not spent to protect "junk." An example of this unacceptable resource expenditure is the hardening of a server and subnet where programmers are developing software where it should merely be isolated from the network all together.

Here is a list of commonly overlooked threats to consider when creating an organization's threat list:

- Network and workstation passwords. Is there a log maintained of all passwords, what type of passphrases are used to gain access to network assets and how secure is this access control list?
- Access to physical assets. Can employees or visitors gain physical access to cables, servers, non-encrypted media, workstations, access points, routers, PBXs or can laptops be removed from offices unobserved?

-Are there complete records of physical assets? Where are these records maintained and are they backed up?

-Data backups. Are data backups existent, where are they maintained, are they encrypted, and when was the last full restoration made from these backups?

-Logging of data access. Each time data access is attempted is this item logged along with attendant relative information?

-Has system development been subject to requirements of SDLC including disposal of hardware in accordance to local and federal requirements?

-What are the policy requirements for safeguarding personal identification information (information that identifies sensitive personal information of any kind) within the organization. Who has access to this information? How is this information logged? Where is this information logged? Is this information encrypted? Who has the keys to the encryption?

-Are long distance telephone calls restricted? Should they be restricted?

-Are email spam filters in place? Do employees require training to identify spam and phishing email? Are there policies in place that govern spam?

Basically at this point this outline provides a simple list of many currently overlooked security threats common to most organizations. A good security audit will account for best practices in the future. One of the best steps is to speak to the long-time employees of the organization and examine the existing documentation. Many threats will repeat themselves over time. Consequently there is an institution of knowledge in the organization's experiences.

Look also for repeating and emerging trends in a particular industry. The Web site, www.itsecurity.com offered a white paper in 2007 and also a Blog that provides updated information on current threats. These often apply to particular industries. Browse their resources and see emerging trends and their impact in particular businesses. There are two sections of special interest in *Meet the Expert* and *Ask the Expert*.

Assets must be cataloged along with their corresponding security threat level. Data is an asset and thereby must receive a level of classification. Often data can be classified as Vital, Important, Useful, Routine, and Non-essential. These levels of classification basically cover all data levels within any organization. An architecture such this will determine the security necessary for most levels of data classification.

Perform a risk /probability calculation. The greater the risk the higher the priority must be dealing with the threat. The formula is simple: Risk = Probability x Harm. This formula simply means that the likelihood of a security threat occurring times the damage. The number comes out of that equation is the risk of a particular threat poses to an organization. How much damage would occur if a particular threat happened? There are many risk-formulae, but whichever one is used the implementation must be uniform across the Security Response Plan and tested at least once annually.

Network Access Controls (NACs) check for the authorized access to the network by any user attempting to access the network from any location. Regardless of the means, Web site, VPN, or network access, NAC must have an Access Control List indicating the user has permissions to certain assets and resources on the network. NACs might include user names, tokens, encryption, digital signatures, IP address verification, user names, cookies, etc.

Intrusion prevention is a separate system from NAC and deals with threats from unauthorized attempts by taking steps notifying of malicious attacks. The most common form of IPS is the second generation of firewalls. Remember that IPSs are not foolproof and generally notify after the fact. This brings up the concept of identity and access management (IAM). IAM simply defined means controlling users' authorized access to specific resources and assets. Under authentication, they are granted access to those assets. Management, through specific policy, grants employees and contractors, the ability to use those resources for a finite period of time and for a specific purpose. IAM is a solution for keeping users from accessing data when they are not authorized to do so. For example it is considered a threat that users are attempting to steal customers' personally identifiable information when they are not authorized to do so outside normal business hours.

Creating viable data and configuration backups. Although it isn't an attractive concept, but many organizations don't have a viable implemented solution of data and configuration backup. And these same businesses have never attempted to restore data and configurations from their backed up media. In the event of having to do so, it doesn't profit them at all to have these backed up solutions if in the event of an emergency these backed up recordings will fail to provide adequate restorations.

Preventing physical intrusions includes threats like attacks from exterior and interior sources as well and the perils from missing data from stolen laptops and PDAs. Have policies been crafted and enforced to screen employees ensuring that undesirable candidates are removed from consideration before hiring? Are there physical locks at doors and other barriers to critical office entries? Are laptops and PDAs secured by encryption?

And in the worst case scenario has the organization crafted a policy where data-owners are notified when their personally identified information is suspected of having been compromised? No one wishes to expect the perimeter as having been breached, but it does happen so having a policy in place will save embarrassment and time should such an event happen.

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
América Corporation
jfuller@amediacorp.com

Membership Director

Dan Anderson
IHC / GE Healthcare
daniel.anderson@intermountainmail.org

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.