

March 2011



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.

Greetings Utah Chapter members,

We have several announcements for you. To start, ISACA will be looking to fill many board positions soon. If you have interest please reach out to any of the board members (see list at the bottom of this newsletter).

Clear out your schedule for the ISACA Spring Seminar being held on May 19 & 20. We will have E. Eugene Schultz, Ph.D., CISSP, CISM, Chief Technology Officer from Emagined Security presenting on the topic of Cloud Computing Security. See the "Earning CPE" section below for more details.

This month we will have Deena King at our March monthly luncheon on March 17, 2011 speaking on the topic "Compliance Program Controls versus Operational Controls as Applied to HIPPA and PCI." Here is a brief intro about Deena.

Ms King brings almost 30 years of experience to the field of compliance. While her career began in Information Technology, she discovered the field of compliance and audit 10 years ago and has not looked back. Her assignments have included Senior Auditor and Compliance Coordinator with Brigham Young University and Program Manager over IT audit and corporate compliance at NV Energy in Las Vegas, NV. She is currently the managing director of Pure Knowledge Consulting, based in Las Vegas, NV (with a satellite office here in Salt Lake City) specializing in supplying clients with best-practices-based consulting services using a variety of compliance frameworks (OCEG, NERC, FSG, COBIT, etc.). She is a published writer, has global implementation experience, and is cross-trained and cross-educated giving her the ability to apply compliance concepts to a variety of compliance areas including Data Governance, SEVIS, OSHA, EEO, HIPPA, NERC, and FERC. She is currently working on a book entitled "Compliance in One Page" with an accompanying workbook, workshop, and self-assessment tool.

You can register for this event on the ISACA website (<http://www.isaca-ut.org/utahevents.html>).

P.S. See the new SANS training information below in the "Earning CPE" section.

Thanks
Josh Taylor
Newsletter Editor

Monthly Professional Training

Date: Thursday, March 17, 2011

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Deena King

Topic: Compliance Program Controls versus Operational Controls as Applied to HIPPA and PCI.

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

CPE: 1 Credit

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

Menu

Sarah Salad

Chicken Swiss Bake

German Chocolate 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.

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

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.

ISACA Spring Seminar

On May 19th & 20th, E. Eugene Schultz, Ph.D., CISSP, CISM, Chief Technology Officer from Emagined Security presenting on the topic of Cloud Computing Security.

This two-day course covers cloud computing security risks and controls and control strategies for mitigating these risks. The term “cloud computing” means supplying dynamically scalable and frequently virtualized resources as Internet services. Cloud computing is being hailed as a major advance in computing. It offers considerable simplicity, cost savings, improved computing and network performance, and other advantages. At the same time, cloud computing introduces a myriad of security-related risks, many but not all of which exist in conventional networking environments. Cloud computing invariably results in a degree (and in some cases an almost complete) loss of control over information technology environments and data, making control selection and implementation more difficult than usual. Additionally, the legal and regulatory risks resulting from cloud computing can be severe, but they are only beginning to be understood. Furthermore, virtualization and cloud computing usually go hand-in-hand. Virtualization also has many additional benefits, yet security vulnerabilities abound in virtual environments, further exacerbating the risk factor associated with cloud computing. Virtualization risk mitigation will also be covered. All things considered, developing and implementing a suitable strategy for risk identification and mitigation is paramount in cloud security. Attendees will participate in an in-course exercise in which they will develop

such a strategy with other members of their group. Finally, this course covers recent cloud computing security research and probable future directions for cloud computing and types of new risks that are likely to result.

SANS Training

SANS is pleased to announce one of our most popular courses Security 401: SANS Security Essentials, in our signature bootcamp style, in Salt Lake City, March 14 - 19, 2011.

For complete event details, please visit (<http://www.sans.org/salt-lake-city-2010-cs-3>).

For those individuals and organizations that have audit/compliance requirements, SANS Security Essentials, Bootcamp style, addresses 16 of the 20 Critical Security Controls

(<http://www.sans.org/critical-security-controls>)

IMPORTANT:

We offer Security Essentials course in SANS bootcamp format, with hands-on exercises after the first five class days, because our students consistently tell us that hands-on training (including labs and exercises) makes a huge difference in both knowledge retention and practical skills development.

TRAINING EVENT DETAILS:

When: March 14 - 19, 2011

Course: Security 401: SANS Security Essentials

(<http://www.sans.org/salt-lake-city-2010-cs-3>)

46 CPEs

Instructor: Keith Palmgren

Where: Embassy Suites Salt Lake City

110 West 600 South

Salt Lake City, UT 84101

(<http://www.sans.org/salt-lake-city-2010-cs-3/tuition.php>)

For Group Discounts or to Request a Class in your Area contact: community@sans.org.

THE COMMUNITY SANS ADVANTAGE (<http://www.sans.org/info/41114>)

The Community SANS format offers the most popular SANS courses in your local community at a reduced tuition fee. And as with all SANS courses, the earlier you register, the more your fee is reduced.

Small class sizes make it easier for you to get the access you need to your veteran Community SANS instructor. The small class also makes it much easier for you to network with your professional peers throughout the six course days.

SANS promises that you will be able to use what you learn in the classroom as soon as you return to the office.

Does this sound like the kind of training that would help you to be more effective in your job combating Cyber Crime and doing your best to provide a secure networked environment for your organization? Then register today to join us in Salt Lake City by visiting (<http://www.sans.org/salt-lake-city-2010-cs-3>).

Please contact ahogan@sans.org if you have any questions, and thanks for your continued participation in the SANS community.

Monthly Article

Data Breaches-Our State of Utter Confusion

Hardly a day goes by when I don't get an email asking about data breaches and what the exploit "du jour" is. Usually it is easiest to refer the inquiry to <http://datalossdb.org> for perusal. Yea, I know it is probably not business-wise to do it, but as audit and security professionals we fail terribly when it comes to protecting our business' crown jewels, meaning personally identifiable information (PII) and financial information from attacks.

Many professionals are going to ask, what about virtualization (cloud computing for the uninitiated) which is the technology of the moment for business, public organizations and government entities? Isn't this the saving strategy? More on this later.

Referring to the past calendar year, there have been numerous network data breaches in corporate networks and Web sites. Of course, the purpose of these breaches whether through the front door or other means is the theft proprietary information or PII. And of course there is a growing chorus of individuals complaining they don't have any control over their information that is being sold or traded between companies' marketing departments. Proprietary information that is compromised is always a significant media story if leaked. So for most businesses data breaches are significantly reduced or even removed by holding sensitive data in an off-site location or only accessing it at very specific time periods. And when these data are not being accessed they are heavily encrypted. But when unauthorized access to these data is made the damage to the organization's reputation and brand are significant and always headline news.

Within the confines of the black market, sensitive data are important commodities. Critical PII, financial and proprietary data can be leveraged to obtain credit, steal processes, create fraudulent documents, and even create fraudulent organizations. Currently, a data security breach effectively run by even an inept hacker might involve a "kit" wherein malicious software can be introduced on a victim's computer collecting PII that is ultimately used to drain bank accounts and ACH funds to offshore accounts. Banks have been sometimes reluctant to reimburse victims these funds as there is nothing to show the victim didn't authorize these ACH transfers.

There are some states that have data breach laws where victims must be notified where their information has been compromised. Utah hasn't any such law, by the way. Many states penalize organizations and business that are found to possess lost or stolen PII, or purloined business data.

So what is the appropriate level of security of workstations and laptops, you ask. My associates travel the world and their laptops have encrypted hard drives using Truecrypt and very powerful passwords that are assigned by a central location within the company. So often computers are merely password protected which is trivial to crack a password that is user assigned. And there is the problem if the password is a passphrase and that passphrase is forgotten hence the use of a centrally assigned passphrase.

Organizations must have a policy of not allowing any sensitive information being sent via email. IM (Instant Messaging) must never be allowed on an organization's network. There are too many security holes with IM. Organizations should consider using sandboxed environments in every PC. Utilizing this technology allows users to browse Web sites and run applications without worrying about drive-by downloads or exploit links. An economical version of sandboxing is a virtual disk environment such as LiveCD version of Ubuntu or other Linux LiveCD. The LiveCD is held on a CD, DVD or USB drive and inserted prior to startup. Users then browse Web sites at will without worrying about malicious downloads. Many consultants are recommending to their clients that they use this process to perform their personal banking.

There are organizations that are playing a bit fast and loose believing that information doesn't constitute data until it is decrypted. Often disclosure requirements are more often than not exempt if the data have been encrypted. Organizations believe this protects them and the customers trust. Such plans need to be carefully vetted outside their business walls before implementation.

Now comes the issue of reading stored documents and relying on individuals to read them. The more obvious issues are found surrounding data privacy where and who should have access to the data, what privileges must be had and so on. Additionally, there are the applications to read these documents. Do these applications have the latest security patches relevant to the operating system including Windows, Mac OS and Linux? Have these applications had Java Script, Flash and other script execution disabled? Many businesses take longer to deploy patch management merely as a result of logistics and a means to see if these patches pose a possible crash-risk to the system. Consequently, Java isn't updated unless it is forced. Also by way of note, Adobe Reader v. 10 reactivated Java Script and Flash even if the user had disabled it in previous versions. Why does a reader need to have these activated when they pose a possible vulnerability particularly when this application might be used to read sensitive documents?

Cloud security is a virtualized serviced inside and outside the firewall. It isn't new. It allows businesses to outsource IT functions so essentially it has the same data security concerns present with mature networks with a few more. The majority of these concerns exists of course within the firewall space and within the control of the business, but the business must be more concerned for those managed by the third party...within the cloud. Since many companies are constrained by Sarbanes Oxley for security compliance. Security and compliance are merely referenced as SOX. And there are some interesting compliance issues for organizations such as how do businesses document and audit access, storage and security of critical data that are handled by a third party? This is critical since the data management and security aren't under the direct control of the company's owner, so who will be accountable in the event of a data leakage, the business owner of the third party?

Service Level Agreements (SLAs) are the means to address compliance between organizations. SLAs hold third parties to contractual binding agreements. When effectively vetted, SLAs manage the cloud when there is a data breach or violation of the SLA. The downside here is that SLAs are rarely enforced and they are extremely challenging to enforce to a full stop as the cloud is an on-demand service and does not have a fixed infrastructure. Additionally, cloud providers will not wish to provide organizations full visibility to their network operations particularly since their network will likely exist outside the country of the contracting business anyway. Now one can easily see the issues facing most businesses that want to move into a cloud environment.

Just remember for all the strength of encryption and passwords and passphrases, IPSec, WPA2, SSL/TSL and SSH the last line of security management is people. The easiest link in the chain to compromise is the person that has access to the most valuable assets. That is usually the weakest spot in the organization's security armor. And it my experience, that is where I concentrate my network penetration efforts.

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
julie.park.jp@gmail.com

Vice President

Jordan Fuller
Amedica Corporation
jfuller@amediacorp.com

Treasurer

Dan Walker
Intermountain Health Care
Dan.Walker@imail.org

Secretary

Elizabeth Yukman
e.yukman@comcast.net

Newsletter/Publicity

Josh Taylor
American Express
josh.taylor@aexp.com

CISA Coordinator

Brandon Greenwood
XanGo
bgreenwood10@hotmail.com

Membership Director

Deena King
dking@wecc.biz

CISM Coordinator

Brandon Greenwood
XanGo
bgreenwood10@hotmail.com

Academic Relations Chair

Jeff Davis
Weber State University
jtdavis@weber.edu

Research Chair

Kyle Finlayson
Intermountain Health Care
kyle.finlayson@intermountainmail.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.