

May 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 has filled the board positions for the following year. See new members below.

- President: Elizabeth Yuckman**
- Vice President: Paul Newman**
- Secretary: Jonathan West**
- Treasure: Steven James**
- Seminar Chair: Brady Stevenson**
- CISA/CISM Certifications: Brandon Greenwood**
- Research Chair: Gaylene Kenney**
- Newsletter/Membership: Josh Taylor**
- Academic: Jeff Davis**

Don't forget 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.

The June CISA exam prep has been confirmed to be held at the SLC library. See dates/times below.

Date	Start	End	Room
5/18/2011	6:00 pm	8:00 pm	*Conf. Room D
5/25/2011	6:00 pm	8:00 pm	*Conf. Room 2

Note: Due to the change in the Spring Seminar dates, we will also have a date change for the Monthly Luncheon. Typically this falls on the 3rd Thursday of the month, but in May, it will be the 4th Thursday. This month we will have Kevin Abbott, Cadence Consulting at our May monthly luncheon on May 26, 2011 speaking on the topic "Say Goodbye to SAS 70: What the Transition to the new SOC Reporting and SSAE16 Standards Means to my Organization." Here is a brief intro about Kevin.

Kevin is currently Vice President of Information Assurance and Security at the Cadence Group, a Utah-based consulting firm. He specializes in SAS 70 reporting, including helping companies with their preparation, documentation, and testing

aspects of SAS 70, as well as writing and issuing opinion-based SAS 70 reports. He has been at the forefront of the transition from SAS 70 to the new SOC and SSAE16 reporting standards, and prior to Cadence, Kevin worked with Ernst & Young in Texas as a SAS 70 subject matter expert for the southwest region. In addition to SAS 70, Kevin also specializes in PCI security, helping merchants and service providers understand credit card security requirements, performing both consulting and readiness projects, as well as the actual PCI assessments. Kevin is a Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and PCI Qualified Security Assessor (QSA).

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, May 26, 2011
Time: 11:30 – 1:15 pm.
Place: Lion House
Speaker: Kevin Abbott, Cadence Consulting
Topic: Say Goodbye to SAS 70: What the Transition to the new SOC Reporting and SSAE16 Standards Means to my Organization.
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
Roast Baron of Beef
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.

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.

Monthly Article

Best predictions for Cybercrime Vectors for the Coming Year

Before I go too much further I must attribute much of the information for this article to the following hardworking folks at the following sources: FBI (<http://www.fbi.gov>), Verizon (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf), National White Collar Crime Center (<http://www.nw3c.org/>) US Department of Justice (<http://www.Cybercrime.gov>), MITRE (<http://cve.mitre.org/>), National Vulnerability Database (<http://www.NVD.gov>) and the Privacy Rights Clearinghouse (<http://www.privacyrights.org>).

Now with that administration out of the way, let I will get right to the meat of the best predictions I expect cybercrime to likely occur:

- Retail using online presence will likely be the primary target. However, look for financial institutions to be included in this target base as more malware-based attacks like Zeus and its variants are more prolific.
- Hospitals and health care facilities are going to be more than just targets of opportunity and will be more vulnerable as attackers discover that many hospital devices are powered by Windows platforms.
- VM and Cloud will continue to be targeted by criminals resulting in data losses with challenging recoveries and audits depending on existing SLAs.
- Many new and innovative attacks have been and will continue to be seen against all levels of infrastructure, i.e. financial, intellectual, structural and developmental by competitive and rogue nations. A firm paradigm here is Trust No One (TNO).
- Currently there are stages of growing mobile phone and PDA attacks. New vectors will continue through previously trusted download centers.
- Unified Threat Management firewall and IPS exploits have been and will continue to be developed and successfully launched.
- Probably the most successful of all cybercrime profits result from creative social engineering. These efforts become more and more creative each year.
- Governments around the world are clamoring for privacy yet they are demanding the ability to enter the private communications of their residents. This trend is most notable with the installation of Blackberry servers in countries as India and Saudi Arabia indicating that RIM has provided visibility into their customer’s communications. Look for this trend to continue.

If one doesn't have the idea that either nationally sponsored cybercrime or individual-attacks isn't profitable let me dispel that idea right now. It is. The case for such behavior is more than obvious. It is prime time and fully developed. Probably the most egregious recent example of this was the implantation of the Stuxnet malware to thwart the uranium centrifuges being used by the Iranian nuclear development program. This little bit of malware, very well and tightly written, was targeted specifically for a type of control system and performed exactly as developed.

In the private sector, global threat trending reports that criminal's use of their tools available such as botnets, malware and spam have caused millions of dollars of losses, business disruption to consumers, and loss of business reputation in the community. According to the Internet Crime Complaint Center and the National White Collar Crime Center, here is a list of the latest and most successful cybercrime schemes of 2010:

- Auction Fraud
- Counterfeit Cashier's Check
- Credit Card Fraud
- Debt Elimination
- Employment/Business Opportunities
- Escrow Services Fraud
- Identity Theft
- Internet Extortion
- Investment Fraud/Ponzi Schemes
- Lotteries
- Nigerian email aka 419 frauds
- Phishing/Spear phishing

Since most of these are common knowledge it isn't necessary to explore them in any detail here. These topics have been thoroughly explained in newspapers and other literature ad nauseum. But adjunct to these malicious acts is that of state-sponsored malicious behavior and those individuals that rise to that level of sophistication.

There are nations, groups and individuals, rogue and many easily recognized as friendly that participate in efforts to increase their economic advantage essentially two ways. One by stealing the intellectual property of another nation sourced in private or industrial arenas or two by thwarting the developing of that knowledge. These efforts are primarily based on global communications as a tool to accomplish their goals. And of course the primary avenue for this end is the Internet. This vehicle not only delivers the malware payload it also connects the players through covert means in the way of highly encrypted communications, steganography, and private chat rooms. Coordinating a strike at a specific time and date has never been easier. Just look what happened to the sponsors of Wikileaks. And this was done by a number of amateurs. Imagine the consequences if done by professionals.

An ever present danger is that of eavesdropping on wireless networks. This has been done since WEP was adopted. (Please don't use WEP to secure any wireless network.) Compromising emanations is basically the ability to collect electronic or acoustic emanations from the air, and process them for their value. This is also known as Tempest for those coming from that community. With a little bit of knowledge and some readily available equipment, usually as simple as a Pringles Can and a sensitive receiver wireless signals can be captured, recorded and processed. And if these are not sufficiently encrypted, they can be read by the attacker much to the detriment of the sender. The first real attention was paid to this type of Tempest in 1985 in a paper published by Wim van Eck. But trust me when I say it has been known long before that time. Van Eck carried out his research on a real system with a range of a hundreds of meters using about \$20 of equipment.

Remember that it is unnecessary to gather signals if I can compromise an employee into installing a Trojan on the system for me by downloading it, or if I can convince an employee to plug-in a thumb drive I just gave them as part of a promotional.

There will be rhetoric in national and international voices trying to wrench control of the Internet for themselves. Simply stated the less concentrated data is the less chance there is of compromise. The more distributed data is in its environment the more secure it is but only if it meets the test of Confidentiality, Availability and Integrity. Ultimately cybercrime in 2011 as begun and it will be an intriguing year for sure characterized by action, legislation and counter-action.

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@amedicacorp.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.