

January 2012



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,

For January, we will have Gordy Jacobsen from The Cadence Group at our monthly luncheon on January 19, 2012 speaking on the topic "Performing, Using, and Auditing IT Risk Assessments." Here is a brief introduction about Gordy.

Gordy Jacobsen is the President and co-founder of The Cadence Group (www.thecadencegroup.com), a Utah-based compliance and advisory firm. As part of his responsibilities at Cadence, he oversees their Internal Audit Services and Enterprise and IT Risk Management service lines. In that role, Gordy assists several companies with their internal audit function and serves as the Chief Audit Executive for three large Utah-based companies. In addition, he oversees and advises companies on their enterprise and IT risk management programs, focusing on risks related to system development and IT security.

Prior to founding Cadence, Gordy previously worked with PricewaterhouseCoopers for seven years in their System and Process Assurance group in their Salt Lake City, UT, San Jose, CA and Wellington, New Zealand offices. Gordy is an active CPA and a long-time Information System Audit and Control Association (ISACA) member. He has recently passed the ERM 57 exam. He has 15 years of experience in the IT risk management and assurance space.

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

Thanks

Josh Taylor

Communications Director

Monthly Professional Training

Date: Thursday, January 19, 2012

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Gordy Jacobsen

Topic: “Performing, Using, and Auditing IT Risk Assessments”

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

CPE: 1 Credit

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

Parking: You can park at the JSMB underground parking (entrance right in front of the Lion House) and receive parking validation at the ISACA meeting.

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.

Monthly Article

To Block or Not to Block Social Media

In today's world, social networking is an integral part of the business and personal scene. It keeps us connected to one another and in a criminal case on December 26, 2011 Facebook was used by a victim being unlawfully held by her boyfriend in the Salt Lake City metro area to contact local police for rescue.

Social media poses interesting opportunities to explore its vulnerabilities within the IT network as the debate of myth and reality have forced executives to make decisions whether to allow or block it in the workplace. In the 2010 Rotman-TELUS Joint Study on Canadian IT Security Practices it was discovered that organizations that blocked social media Web sites were no more secure than those that did not. However, network threats that were effectively thwarted in the light of known threats made by social media became part of user training and organization policy implementation.

In the referenced study there were some data worth noting such as the losses sustained by organizations that did not block access to social network sites averaged, \$208,333 where organizations that did block access only averaged losses of: \$91,826.

There are some more telling data in this study indicating as follows:

| Types of malware | Organizations not blocking social media | Blocking social media |
|---|---|-----------------------|
| Virus/worms/etc. | 43% | 72% |
| Laptop/Mobile/ Hardware theft | 38% | 59% |
| Unauthorized Access to information by employees | 33% | 42% |
| Denial of service attack | 11% | 24% |

Reviewing the above data suggests that the greater number of blocked breaches in organizations that blocked social media possibly suggests that these organizations were invested in more detection controls thereby increasing their capabilities discovering more possible breaches. These businesses have discovered that social media carry increasing threats to network architectures and might have weighed the risks versus the possible benefits.

There is some further telling data in this section. A portion of respondents reported they were satisfied with their security when blocking versus not blocking social media:

Organizations that do not block access to social media: 58%

Organizations that block access to social media: 68%.

This sense of security might be rested in part in their ability to contain breaches, once they have occurred. However purely from an external view, blocking access to social networks makes security controls far more sensible from an auditor's visibility within an organization. By delivering clear evidence that security controls are present and functioning elicits a stronger response from the user community as a whole.

It was determined that organizations that were blocking access to social media revealed the likelihood that users were not receiving education (only 26% had organization-wide training versus 74% in organizations that did not block). This condition is likely because business chose to block rather than train their users. It is clear that blocking access to social media without training as to the rationale is not a viable recommendation. It might only serve to stimulate circumvention of the blocking thereby creating a threat to the system.

Study respondents indicated they were more likely to block access in an effort to protect their branding if they had a policy addressing information disclosure (57% with a policy vs. 41% without). If there were a rationale supporting a blocking action then the existence of a policy increased the probability that the user could be used as a tool to promote the adoption of the policy.

There are some characteristics that are common among organizations that block social media. Vulnerability management is ranked lower for organizations that do not block. However, it is noteworthy that patch management is equally ranked for both. Disk, email and PKI encryption are used less frequently in organizations that do not block. One might understand that these businesses are less concerned about their security architecture as a whole. Social media are now part of our current culture creating an IT security management priority in the workplace and a headache for auditors. In its current structure, social media sites and technologies force business to make decisions surrounding security sometimes in haste having long term consequences. The perception that social media Web sites are not secure is the rationale that leads organizations to block their use. However, blocking them does not ensure security. Certainly blocking might have benefits however, this decision without levels of user education carries distractions away from ultimate risk management goal.

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

Can be found on <http://www.isaca-ut.org/administration.html>

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.