

Sept. 2009



Newsletter

Serving IT Governance Professionals

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

Welcome back from the summer break. I hope everyone had an enjoyable summer.

There have been a few changes to the Utah ISACA chapter board membership; hopefully you will be able to attend our next monthly luncheon and meet the new board members.

We will be holding our regular monthly luncheon at the Lion House on Thursday, September 17th. Robert Lee, from Outpost24, will be speaking on Security Metrics. If you haven't already you can register for the monthly luncheon at our website <http://www.isaca-ut.org/utahevents.html>.

Our next monthly luncheon will be held on Thursday October 15th at the Lion House. More details will follow.

Thanks

Julie Park

Monthly Professional Training

Date: Thursday, Sept. 17th

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Robert Lee, Outpost24

Topic: Security Metrics

Cost: \$15 for members and students, \$18 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

Beef Stroganoff

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

Executive Level Responsibility in Enterprise Information Technology Security

Executive and senior level managers are faced with mandatory legal and regulatory requirements that change often. And they are often expected by stakeholders to be “all knowing” when it comes to the functions of subordinate business units and individuals. It is not just an information technology problem rather it is a business problem to establish, train, audit, and enforce an enterprise-level information technology security program.

There are many reasons justifying the effort and expense of an information security program. However, the most significant motivators have been determined to be concern by upper level executives for legal liability, regulatory compliance and protection of the organization’s business reputation.

To be successful it is necessary for senior managers to foster a relationship that establishes a consistent message throughout the organization that protects human resources, data and physical assets. And it is incumbent on these same executives to know exactly what and where these three areas of valuable assets are located. However due to the size of many enterprises it is likely that executives may know only key individuals in specific business units and the impact of those units within the organization. Often this level of these areas is enough.

For executives to accomplish their roles well there are critical elements that will ensure information security according to an ISACA survey conducted in 2005:

- Management’s understanding of current information security issues
- Information security planning prior to the implementation of new technologies
- Integration between business and information security
- Alignment of information security with the organization’s objectives
- Executive and line management’s ownership and accountability for implementing, monitoring and reporting on information security
- Appropriate employee education and awareness on information asset protection
- Consistent enforcement of information security policies and standards
- Placement of information security within the organization hierarchy

- Budget for information security strategy and tactical plan
- Consistent board and executive management message with regard to information security priorities
- Focus on short-term goals resulting in long-term control weaknesses
- Justify the cost of information security
- Generally accept information security best practices and metrics

At every opportune moment, senior managers should communicate that every employee, that includes contractors and interns, are accountable for information security. Essentially everyone connected to the business enterprise is responsible and accountable for ensuring that information security expectations are clearly understood. These expectations must be spelled-out in the organization's policies and standards. Therefore, employees must clearly understand that violations of these will carry consequences for all without exception.

The organization's policies and standards must have formal review and authorized changes before implementation. In short, there is necessarily a formal means by which changes are proposed, tested outside the production environment and approved before being implemented. Then there is the measurement of control effectiveness. Auditors must ensure that metrics are effective and efficient, that reports have been made on a quarterly basis to the chief legal officer, chief compliance officer or their equivalents and annual summaries are sent to the board of directors.

It is certain that most aspects of the IT security program align with a shared services business model. Consequently, most security initiatives are closely paralleled with the underlying business efforts they protect. But the cost of securing IT and intellectual property must not exceed the actual value of those assets. Business risks and information security solutions must have a cooperative dialogue. It is an overly expensive venture to spend precious resources protecting an executive's pet project that has little intrinsic value to the detriment of other more valuable assets.

Each facet of technology risk must be appropriately viewed and analyzed within the construct of confidentiality, integrity and availability as it pertains to the organization's transaction flow. Additionally, the scope of this analysis must be on the business' transactions that are relevant to the information flow, product flow, and compliance to relevant laws and regulations.

Conflicting priorities frequently fail to support information security initiatives. Conflicting priorities and lack of ownership are generally resolved through the organization's system of performance rewards. With that statement made auditors must assure that performance goals associated with IT must support the information security process. Priorities must be clearly stated and established in the security strategy with metrics approved by executive management. Information security should have a reporting structure that notes accomplishments and views it's governance properly. Key control objectives should be incorporated within the training of all levels of employees as part of their performance measurement. Appropriate levels of supervisory management should have accountability for ensuring that information security violation and other pertinent security measurements associated with their line of business processes are acted upon on in a timely and meaningful manner.

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

Board of Directors and Officers

President

Julie Park
Weber State University
jpark@weber.edu

Vice President

Jackie Schwartz
Axiom Recovery
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.