

October 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 two announcements for you. To start, you can now RSVP for the Fall Training Seminar online and take advantage of the early bird discount. Here is a brief description about the course.

Chris Ingram - course description:

This one-day course will introduce the IT Auditor to mobile platforms (iOS & Android) and the process of auditing platform applications. Students will understand the technical and behavioral threats to the enterprise from mobile applications and how to mitigate such risks. Students will take from the class the knowledge to advise on policy, prepare and execute an application audit and handle countermeasures.

This month we will have Alan Sternecker at our October monthly luncheon on October 20, 2011 speaking on the topic "Forensic Investigations and What the Auditor Needs to Know." You may notice Alan's name as he provides the monthly article which is at the bottom of each ISACA newsletter. We'd like to thank him for providing us this quality content. Here is a brief intro about Alan.

For more than 24 years Alan Sternecker investigated and managed sophisticated national and international cases for the Federal Bureau of Investigation. On many occasions, he provided executive level presentations and expert testimony at legal proceedings. Mr. Sternecker developed methods and means for preserving Intellectual Property matters, utilizing innovative steps in collecting evidence for presentation to courts.

After retiring from the FBI, Mr. Sternecker founded Risk Management Associates with offices in Los Angeles, New York, and Dubai. His company provided consulting to provide policy formulation and implementation, business continuity and risk management, critical incident management, intellectual property, and privacy protection services.

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

Thanks
Josh Taylor
Newsletter Editor

Monthly Professional Training

Date: Thursday, October 20, 2011

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Alan Sternecker

Topic: Forensic Investigations and What the Auditor Needs to Know

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

CPE: 1 Credit

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

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 Fall Seminar

- **November 4, 2011** – 8:30 AM to 4:30 PM (7 CPE Credits)
- 2929 Thanksgiving Way, Lehi, Utah (**Rose Room**)
- Early bird special: Registered and payment received (postmarked) until **October 25– NO REFUNDS**
\$175 members of ISACA, ISSA, and IIA
\$225 non-members
- From October 26, 2011 and closes November 1, 2011 (9 a.m.)
\$200 for members of ISACA, ISSA, and IIA
\$250 for non-members

Registration: http://www.acteva.com/ttghits.cfm?EVA_ID=32367

Location: http://www.thanksgivingpoint.com/plan/corporate_events/roseroomcorporate.html

Chris Ingram - course description:

This one-day course will introduce the IT Auditor to mobile platforms (iOS & Android) and the process of auditing platform applications. Students will understand the technical and behavioral threats to the enterprise from mobile applications and how to mitigate such risks. Students will take from the class the knowledge to advise on policy, prepare and execute an application audit and handle countermeasures.

[PERSONAL LAPTOP & MOBILE DEVICE REQUIRED-iPad, iPhone, Android, etc.]

Biography:

Chris Ingram (CISSP, CEH), Director of penetration testing at Emagined Security, is responsible for management of pen-testing operations. He has 7 years of experience in network and application security and an additional 5 years in software and hardware development. His involvement at every level of the hardware and software provides him a unique perspective of security issues.

Mr. Ingram is a professional security consultant with expertise in all aspects of Ethical Hacking/Penetration Testing. He has created security plans, conducted assessments, penetration testing and developed system level security processes. He has lead, designed, and implemented highly technical IT security strategies, policies and procedures. He has a diverse background in enterprise environments as an innovative thinker with an outstanding record of unifying new business concepts, mapping IT to corporate goals, and transitioning infrastructures on schedule and within budget.

Monthly Article

Records Retention

Probably several times a month I receive a legal question about the retention of data. These queries vary from what constitutes data, the regulatory requirements and just how to skirt those requirements. Few if any organizations actually have written policies detailing the enforcement of data collection, complete deletion data; and the prevention of the destruction of critical business records due to applicable legal and regulatory bodies.

It goes without saying that organizations must have formal written, policies in place governing the acceptance of data, its retention and subsequent destruction. Adoption of a universal records management governance framework will deliver cost efficiencies and risk management benefits.

Digital information management for most organizations is literally the 800 pound gorilla in the room. And for most organizations, it is so poorly handled they do not even try. Organizations state they are security-minded and tout they have security structures in place to thwart data leakage yet outlaw “clubs” like LulzSec have routinely penetrated some of the more noted businesses in the world to steal sensitive data. A short list of their victims includes the CIA, Arizona Department of Public Safety, Sony Pictures and News Corp. If their sensitive records had been appropriately stored all they would have stolen would have been unreadable.

With the introduction of new technologies, such as biometrics, back-end social media containing sensitive information, cloud computing, mobile computing devices, and the wide variety of portable media, there is a burgeoning field of business information to manage. In the foreseeable future the widening view is that it is only going to grow larger. Therefore businesses have strong motivation to find a viable means to meet their records management mandates now. By doing so, they will address fewer conflicts in requirements between their headquarters in one state and their branch offices in other states or countries.

So if managers and others are scratching their heads as to exactly what constitutes data or a record. Of course the ISO has a definition. (As John Hannibal Smith says, “I love it when a plan comes together.”) ISO 15489 defines records as, “information which is created, received, and maintained as evidence by an organization in the transaction of business, or in the pursuance of legal obligations, regardless of media.” So reading this definition gives one a fair understanding that essentially any form of data content pertinent to operations or transactions of a business or organization is relevant. Now the factors that are important are the time those records must be kept, the security of those records and how those are to be destroyed.

Information includes content, its associated metadata, and event logs that are produced in the normal course of business operations. It also encompasses all the versions of draft documents, convenience documents such as Messaging or email, versions of documents and accompanying event logs. Information might be declared a record at any point or at all points of its life cycle from beginning to end.

The focus of law often dictates the retention of records. With the passage of the 2006 Amendments to the Federal Rules of Civil Procedure for Electronic Discovery, specifically, Rule 34 defines electronically stored information as “discoverable” and removed from the hearsay test. Now with the application of this rule the potential volume that might be deemed as discoverable as Electronically Stored Information or ESI in litigation or regulatory investigation, the nature of electronic data (read that records) becomes even more important for organizations to adopt formalized retention for “non-records” meaning items that are not part of the business process and not part of security, compliance or preservation obligation. Therefore, records retention management is practiced only in concert with records management policy compliance ensuring that information is collected, retained, stored and destroyed consistently.

Here are some objectives governing retention:

- Mitigate discovery liabilities from keeping information unnecessarily
- Support plans optimizing datacenter storage operations
- Demonstrate legal/regulatory compliance at federal and state levels

In the USA, here are some of the applicable laws and regulations that might reach into most organizations governing their records retention:

-HIPAA The Privacy and Security Rules govern patients’ privacy rights. Covered entities must secure patient records containing individually identifiable health information so that they are not available to those not needing them.

- Individuals must be notified of a data breach, including Web-based vendors storing medical data and HIPAA-covered entities

- Individuals have a right to restrict disclosure of health information

- Sale of protected health information is prohibited and punishable by law

- Retention mandates range from five years to permanent. And for a period of six years, allows the patient to request an accounting of who has accessed their records.

-SEC Rules 17a-3 and 17a-4 of the Securities Exchange Act of 1934 and FINRA Rules 2110. Documents that filed with the SEC by public companies must be kept for five years. Banks must retain records relating to credit transactions for 25 years. Under FINRA, purchase and sale documents, customer records and associated person, customer complaint records and some other records are records must be kept from three years to seven years. These records are email, voicemail, instant messages, and social networking sites as Twitter, and blogs.

-Sarbanes Oxley. SOX covers all publicly traded US companies and foreign companies traded on the exchanges. Section 401 calls for audit and financial records to be retained for not less than seven years after the completion of the audit. (I interpret that to mean after all follow up actions are completed.)

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.