

Jan. 2009



Newsletter

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

Hello Utah ISACA members. I hope each of you have had a great holiday season. I look forward to seeing you again at our next luncheon.

We will be holding our regular monthly luncheon at the Lion House on Thursday, January 15th. Stan Kang, from Verizon Business - Security Solutions, will be speaking on Investigative Reporting. Stan is the co-author of the Verizon Business 2008 Data Breach Investigations report which is the basis of his presentation.

See you then,

Mark Murdock

Monthly Professional Training

Date: Thursday, Jan 15th

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Stan Kang

Company: Verizon Business - Security Solutions

Topic: Investigative Reporting

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

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.

Menu

Caesar Salad

Lemon Thyme Chicken

Coconut Cream Pie

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.

ISACA Conferences—Innovation. Be a part of IT.

By attending an ISACA educational event, you will:

- Earn CPE credits toward CISA, CISM and CGEIT certification
- Learn from industry experts from around the world
- Network with an unmatched group of experienced peers
- Receive the most up-to-date research information from the IT Governance Institute® (ITGI™)
- Stay current with professional knowledge and trends

Get a head start on your 2009 plans and make arrangements now to attend one of ISACA's global conferences or Training Week events. Plus, earn continuing professional education (CPE) credit hours!

Register TODAY for upcoming 2009 events

ISACA Training Week—Providing the tools you need to maintain, update and upgrade your skills

Presented in an interactive environment for enhanced learning, Training Week is a unique educational event, tailored to suit all experience levels. Courses are aligned with CISA® and CISM® job practice areas, and revised for 2009. *Eight locations, four courses, at least one combination perfect for you!*

Early 2009 dates and locations:

- Houston, Texas, USA -- 2-6 March
- Nashville, Tennessee, USA -- 6-10 April
- Denver, Colorado, USA -- 18-22 May

Additional Training Weeks have been planned for the second half of the year. For a complete listing and to register, please visit www.isaca.org/trainingweek.

To help round out your training and educational plans, be sure to check out our many online training offerings: e-symposiums, COBIT and CISA online reviews. www.isaca.org/elearning

This conference will build on and include the key elements of information security management practices and information security practices. The conference will cover related business, program and technical issues and the impact of risk management.

We look forward to seeing you at one of our many educational and conference offerings. Please visit us today at www.isaca.org/conferences.

- ◆ **Discover** your potential.
- ◆ **Improve** your performance.
- ◆ **Acquire** new skills.
- ◆ **Enhance** your knowledge.
- ◆ **Register now!**

Computer Laws

Computer information audit professionals are usually responsible for protecting an organization's IT assets from threats both internal and external. There are sophisticated graphs and long narratives detailing relationships between employees, customers, suppliers, regulators as well as the threats posed by identified and unidentified players. Most professionals are efficient and effective at their jobs but are lost in the sea of legal and regulations imposed by federal and state governments. Auditors must incorporate legal requirements in their work papers because they are the only platform for enforcement before criminal or civil enforcement action results. Often systems administrators or managers do not understand that by monitoring text messages without specific permission they are violating federal criminal statutes. It is the auditor that can remedy that misunderstanding and save the organization from costly and embarrassing legal action.

This article covers most of the commonly misunderstood federal statutes with the intention of informing readers of possible legal pitfalls. In each case the law is broken into elements so readers can gain a thorough understanding of it. For reference here, civil penalties result in monetary judgements, where felonies are sentences of incarceration of more than one year.

CFAA - Computer Fraud and Abuse Act

The CFAA, Title 18 United States Code (USC) Section 1030 imposes both civil and criminal actions for a wide variety of acts compromising the security of public and private sectors where computer systems are involved. The underlying provisions for a violation of the CFAA is a "protected computer" meaning one that is "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government [.]"

Or a computer system that is one:

"which is used in interstate or foreign commerce or communication[.]"

This language covers just about every computer in every enterprise with damages determined to be at least \$5000 in a year's time for civil action to be settled.

DMCA - The Digital Millennium Copyright Act

The bane of most music downloaders is the DMCA, 17 USC Sections 1201-05. It provides that no person shall circumvent a technological measure controlling the access to a work protected under this title, meaning a copyrighted work. It prohibits the manufacture, import, offer to the public, or trafficking in any technology, product, service, device, component or part that is designed to circumvent a technological measure effectively controlling access to a copyrighted work or is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure controlling access to a copyrighted work. That is a legaleze meaning one is prohibited from circumventing the means gaining access to a copyrighted work by working around the encryption. If it is done, then a violation of the DMCA has likely occurred.

The DMCA imposes liability for the removal of technological devices then there is the issue of the treatment of the copyrighted works. So there are two issues here. One is the matter of the circumvention or removal of the technological device insuring the copyright with is covered by the DMCA then there is the work itself covered by the copyright. The DMCA imposes civil and criminal penalties as well as recovery of actual damages. Criminal penalties can rise to a felony.

Proprietary Information - Information Security Professionals and Trade Secrets

Most information based-data fall within the categories of intellectual property:

-Trade Secrets

-Copyright

-Trademark and Service marked data

-Patents

Information security professionals and by extension auditors perform important duties in protecting these resources. But they have an individual relationship with trade secrets worth special attention. A trade secret is one that an organization holds in

secret where limited access is granted. It is integral to the operation and might be considered a business or manufacturing operation, secret formula such as Coca-Cola or might be something like a client or supply chain list. Stealing this information is a federal felony to which many federal statutes might apply however this statute specifically applies, Title 18 USC Sections 1831-1839.

The Wiretap Act.

The Wiretap Act imposes civil and criminal liability on any person who in violation of Title 18 USC Section 2510:

“Intentionally intercepts or attempts to intercept a wire, oral or electronic communication, either directly or through another person;

Intentionally uses or attempts to use any electronic, mechanical, or other device, either directly or through another person, to intercept any oral communication: (1) of certain specified types; (2) on the premises of any business or commercial operation that affects interstate or foreign commerce; or the person acts in the District of Columbia, Puerto Rico, or any territory or possession of the United States; Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was intercepted in violation of the Wiretap Act;

Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was intercepted in violation of the Wiretap Act; or

Intentionally discloses, or attempts to disclose the contents of any wire, oral, or electronic communication, that was lawfully intercepted, knowing that that occurred in connection with a criminal investigation, or obtained or received in connection with a criminal investigation, with intent to obstruct, impair or impede an authorized criminal investigation.”

This statute mandates civil and criminal penalties for unauthorized interceptions. In short, employees that monitor text messaging or email in real time without the consent of at least one of the parties is likely violating this statute and guilty of a felony. This law does not refer to electronic data in storage. What this law does define as communications are those being passed real time.

So under federal law at least one of the parties must consent to having their communications monitored. But this all changes under individual state statutes. For example, Maryland prohibits monitoring any type of communications unless all parties provide informed consent. Utah requires only one party to provide consent.

Employers might have employees provide consent as part of their continuing employment at the time of hiring. So monitoring employees' telephone calls, text messaging, email and other real time communications might not violate federal statutes if consent has been obtained.

Stored Communications Act

This act, Title 18, USC Sections 2701-12, protects stored communications from being accessed and disclosed without authorization. It imposes civil and criminal penalties for the intentional and unauthorized access to electronic communication service facility to obtain, alter, or prevent authorized access to a stored electronic communication. This is the set of laws preventing hackers from gaining unauthorized access to data or preventing authorized access to data or systems. The criminal penalty for violating this law is a felony.

Security professionals and systems administrators are those responsible for providing security for the enterprise's data assets, but it is the auditors that are generally responsible for delivering compliance for internal and legal controls. There are many opportunities for employees to stray from generally accepted conduct but with unannounced and regular audits unnecessary legal action can be avoided.

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

Journal Update

The Information Systems Control Journal is seeking articles for volume 1, 2008, to be issued in January 2008. The copy deadline for volume 1 is 24 September 2007, and the theme is **Dysfunctional Operations in IT**. For more information, please view the 2008 editorial calendar at www.isaca.org/journal or e-mail jblader@isaca.org.

Board of Directors and Officers

President

Mark Murdock
LDS Church
murdockma@ldschurch.org

Vice President

Julie Park
Weber State University
jpark@weber.edu

Treasurer

Dan Walker
Deloitte & Touche LLP
danwalker@deloitte.com

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@amediacorp.com

Membership Director

Chuck Sims
BYU
Chuck@byu.edu

CISM Coordinator

Sod Chuluunbaatar
Deloitte & Touche LLP
schuluunbaatar@deloitte.com

Seminar/Education Chair

Kyle Chugg
America First Credit Union
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.