

Dec. 2008



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. We will be holding our regular monthly luncheon at the Lion House on Thursday, December 18th. Quinton Jones, from Qualys, will be speaking on Vulnerability Management.

I hope you all enjoyed the Fall seminar on Linux Security and Audit Fundamentals,” and I look forward to seeing you at our December luncheon. Have a happy holiday season!

Our next monthly luncheon after December’s will be held on Thursday, January 15th at the Lion House. The speaker will be Eric Gentry from Verizon Business. The topic is Investigative Response. More details will follow.

Merry Christmas,

Mark Murdock



Monthly Professional Training

Date: Thursday, Dec 18th
Time: 11:30 – 1:15 pm.
Place: Lion House
Speaker: Quinton Jones
Company: Qualys
Topic: Vulnerability Management
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

Sarah Salad
Pork Chop/Mushroom Gravy
Poppy Seed 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.

Reminder

Please remember to renew your ISACA membership. Also, as you are renewing remember to report your CPE credits for the year.

As a new year draws closer, you may be thinking about making plans for 2009. Be sure to include ISACA's educational events on your list of priorities! Start off 2009 by making preparations to acquire the most innovative resources, cutting-edge information and extensive knowledge you need to succeed in today's business world.

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!**

Economic Espionage

A short time ago the People's Republic of China launched a manned spacecraft that achieved orbital status and subsequently a space walk. Several analysts commented this remarkable feat was performed by stolen technology taken from western industries and governments by PRC agents. The ever escalating stakes of corporate and government espionage is being played on a grand scale by individuals representing corporations and governments. These players use any means, ethical or not, to acquire information giving them an edge over their competitors.

Once critical data is in the hands of a competitor whether it is a corporation or government it is very easy for them to use these data. Recovering their lost competitive edge through legal means is virtually impossible. Take for example if the information is in the hands of a competitor located in Russia or the PRC pursuing legal actions in either of these countries against offenders is impossible. Stolen technology and customer data results in lost revenue, jobs, market share, and sometimes bankruptcy.

Compounding the problem is the action by industries that locate some of their facilities overseas or outsource some of their work to foreign entities. This practice can be compared to putting the fox in charge of the hen house. According to J.J. Smith of the Society for Human Resources Management, there has been a marked increase of theft of personnel records from companies located in India alone.

Here are a few tools of the trade used in the corporate technology espionage trade.

The preferred tool used by most corporate spies has been the installation of the key logger on a critical workstation. It can take the form of either software installed on the computer itself where it records the keystrokes and takes an image of the screen at specific intervals. According to the configuration set at the time of its installation, it will be completely transparent to the user. It will email the results to the spy using the corporation's email system at a pre-configured time or it will store it until it is requested to disclose it based on a specific input and password. There is an ongoing battle between the programmers of key loggers and anti-virus makers. When the key loggers are updated they are often undetected by the AV makers but eventually the AV advance and detect them. However, there is always a time lag before this happens and sometimes there is a period of several weeks or months before this lag is closed. These applications are extremely difficult to detect when professionally installed. If carefully configured, these might be detected by a workstation firewall or by scanning by several different AV applications.

There are key loggers and similar applications that do not require physical access to the target workstation. These applications are installed by tricking the user into installing them. They then record all the keystrokes and email them to the spy. Often this type of software is detected by anti-virus software or workstation firewall.

There are key loggers that are hardware devices placed inline between the keyboard and the CPU. These devices record all keystrokes and are then recovered by the spy at a later time. This device requires that the spy have physical access to the target device. The only means by which these devices are detected is by visual inspection.

It is easy to detect a rogue wireless AP attached to the organization's network. Today however, IT professionals have a more sophisticated tool to copy data from a distance without being detected. It is called Ethernet over Power (EoP) that has emerged allowing an insider to covertly access a network and send the data outside the corporation's guarded domain using the electrical system. By inserting a network cable into a device similar to Netgear's XE1027 and plugging it into an electrical outlet a spy can turn a building's wiring into a DES encrypted network that cannot be sniffed or detected like a wireless AP. By using a second EoP device a spy can be anywhere in the building or she might even implement a wireless AP to reach outside the building to send data. If the EoP is seen it will likely be dismissed as a surge protector or some type of power supply.

The only way to detect this device is to physically inspect AC outlets for small devices that are plugged into them and have an RJ-45 connected to that same device.

Probably the most shameful way organizations lose data is having employees or persons associated with the organization take data from the workplace and remove it. This is often attributed to these individuals having too much access to data, having too much trust from the organization, or being insufficiently screened by the organization at the time of hiring, or insufficient auditing controls. The preferred tools of these spies are the corporation's email system where the spy finds their intended data and they merely email it to their recipient. Or this spy will copy the data to a high capacity media such as a thumb-drive that they have concealed on their person. These drives merely plug into any easy accessible USB drive port and the corporate spy is in business.

Detecting this type of spy is summarily difficult particularly if this employee has legitimate access to the data. Some enterprises have gone so far as eliminating USB ports on workstations. Others have eliminated personal cell phones and other electronic devices from the work place. Many will not allow any media to be introduced or removed from outside the work place. Investigate employees working at hours when they are outside their normal work hours.

Fast arriving in the organization is the mobile computing policy of having all mobile devices with strongly encrypted hard drives. Recently, it has been reported that some customs officials have taken the laptops of entering travelers and imaged the hard drives. Also, there are more than 250,000 stolen or lost laptops in the U.S. in 2006. Some laptops have devices that will locate them if stolen. A laptop stolen from a parked vehicle, hotel room, restaurant, office cubicle or airport, with a strongly encrypted hard drive will likely result in the data being safeguarded regardless of the efforts of the corporate spy. The corporate spy must have physical access to the mobile device, but verifying that the hard drive is encrypted is simple to verify.

Many other tools of the corporate spy include:

- Cameras concealed in the workplace

- Concealed recorders/transmitters in the workplace

- X-ray envelope spray turning opaque paper translucent for about 30 seconds allowing the spy to view the contents of an envelope without opening it.

These tools might be detected by physical inspection or by the spy bragging or by exhibiting suspicious behavior. Reporting these activities to federal authorities is required by federal law, Title 18 U.S.C. section 4. If the spy used any of these techniques, it is very likely she committed a felony even if she did not glean any data. And stealing data is a federal felony described in many federal criminal statutes; Title 18 Sections 1831-1839, Title 18 Section 2319, Title 18 Section 1343, Title 18 Section 1341, and Title 18 Section 2314.

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.