ISACA®
Serving IT Governance Professionals
San Francisco Chapter

SAN FRANCISCO CHAPTER | LOCAL AREA NETWORK

FOURTH QUARTER 2006

PRESIDENT'S MESSAGE

Mike Nelson, CISA, CISM, CISSP, CAP, ITIL, PRESIDENT

YEAR'S LAST ACT: A BALANCING ROUTINE

As we near the end of the calendar year, many of our members are busy with Sarbanes-Oxley audits or responding to any number of other drivers that demand the unique skills and experiences of people like us – information assurance professionals. While it can be rewarding in many ways to be "in demand" in our professional life, we must never forget those who rely upon us to be present and engaged in their lives as well. Just as we constantly remind our CIO or Audit Committee of the importance of balancing business risk with control strength, we must never forget the necessity of achieving balance in our own lives, finding ways to give our time and attention to our family, friends, hobbies and career growth.

Your SF ISACA Chapter offers a number of ways to help with the career growth portion of your priorities. From the ever-growing Fall Conference with its three days, four tracks, vendor fair and fantastic networking opportunities, to the CISA and CISM weekend workshops to prepare you for achieving those valued certifications, to the monthly educational sessions, our team of volunteer leaders is working hard to ensure these kinds of valuable career enhancing opportunities continue to be available locally at a reasonable cost.

In November, our Education Committee arranged for a joint luncheon meeting with the San Francisco Chapter of the Institute of Internal Auditors where we heard Helen Munter of the Public Company Accounting Oversight Board (PCAOB) speak about the lessons learned and future plans for the Sarbanes-Oxley audit guidelines. This well attended session is another example of the relevant and timely knowledge acquisition process that we are committed to bring to our members. Based on feedback from our member surveys, you can look for even more creative ideas from the Education Committee, including more joint sessions with our sister organizations and potentially some breakfast and on-line educational opportunities.

As part of our effort to build on our established relationship with San Francisco State University, we continue to provide support for the ISACA Student Interest Group. In addition to providing speakers on the IT Audit and Security career path at student events, we also now have a seat on the board of the Center for Electronic Business (CEB), founded at the SFSU campus. The mission of the CEB is to:

"Promote interaction among students, faculty, and practitioners that results in the sharing of knowledge, experience, and expertise in electronically-based business activities, and to foster cooperation and collaboration among participants through joint applied research, sharing of best practices, student internships, and related programs."

In August, 2007, we will play host to the ISACA Western Region Primary Contributors (a.k.a. Presidents Council) Meeting. The responsibility for planning, coordinating and hosting this annual event is rotated amongst the ISACA

CONTENTS

Presidents message	1 - 2
Academic Relations Message	2
Challenges in PCI	3 - 4
Members Make A Difference	5
CISA Review Course	6
SF ISACA 2006 Holiday Party	7
Chapter Board Roster	8

PRESIDENT'S MESSAGE - CONTINUED

Chapters in the Western US and Canada. And in 2007, it is our turn. This is an opportunity for future chapter leaders to learn about the nuisances of running an organization such as ours. I've been to several of these meetings and find them to be extremely interesting and valuable. A planning committee has already started the ball rolling, but there is always more room for help. If you're interested in participating in this effort, or in the planning for the 2007 Fall Conference, which will begin shortly after the first of the year, please contact Angie Guzman, our Volunteer Committee Chair at volunteer@sfisaca.org.

As 2006 draws to a close, take measure of your own sense of balance, and ensure you give quality time to all the areas of your busy life. Be thankful in the blessings you have and altruistic in the ways you choose to give back to your community. Have a safe and happy holiday and make 2007 a year of even greater growth and balance.

A Message from SF ISACA Academic Relations

By Wendy Leung
Academic Relations Chair

This past fiscal year has been a great experience for me. Being a committee chair for the first was both exciting and challenging. I enjoyed having the opportunity to work with all of this year's board and committee members. The 2006 SF ISACA Fall conference was a particularly memorable experience. The event was both educational and rewarding for me personally, and I am grateful to everyone who helped and supported this event. Students who volunteered to be a proctor for the Fall conference enjoyed the opportunity to network with professionals. I received much feedback on how much the students learned in the conference.

I am very excited about the upcoming fiscal quarter, and being able to engage with the new students of the upcoming semester. I would like to thank all the current officers (Simi Soho, Natalia Tjandra, Cyrus Makalinaw, Vince Laurel and Meena Bidwal) and others member of SFSU ISACA chapter for their support and time in promoting our student organization.

CHALLENGES IN PCI
BY BARAK ENGEL
PCI AND SERVICE PROVIDERS

The payment card industry (PCI) standard has become a significant compliance driver in the retail and hospitality sectors, and with recent classification changes, more merchants are feeling the pressure. But a segment of the industry that seems to get less attention is service providers – specifically, those service providers that do not handle cardholder data as part of payment processing, but rather incidentally, as a side effect of providing generally unrelated services.

In our practice, we help merchants become compliant, but we also work extensively with such service providers. And we find that every one faces unusual challenges. The PCI standard was written from the point of view of dealing with a merchant or a payment processor; it did not take into account those on the sidelines that may be impacted. As an example, think of a loyalty management vendor that might get transaction logs as part of delivering its solution; even if primary account numbers (PANs), the primary determination in classifying cardholder data, are stripped immediately once they are received by the vendor, they must still be PCI-compliant. Otherwise, merchants will simply not use the vendor's service, due to the PCI requirement that all third-party service providers be compliant (PCI section 12.8).

The problem, of course, is that with incidental handling of cardholder data, curious scenarios might occur that test the boundaries of the PCI standard. One such example that we recently encountered came in the form of digital voice samples.

THE BOUNDARIES OF PCI

The customer, in this case, was a service provider with services focused around voice recognition. The provider supplies its customers with an automated voice response front-end that the customers can then integrate into their infrastructure to enhance their own service delivery platform. A consumer may then interact with a company's automated voice response system that is actually provided by the service provider in question.

How does PCI come into play? Well, some of the customers were "PCI merchants," a type of entity that is required to be compliant with PCI. And because the voice response system could handle discussions regarding the purchase of a product, or upgrade of a service, it would potentially "hear" consumers speak their credit card numbers. Of course, the service provider does not process payments; it simply transfers that data to its customers, who then use their own payment processor. But the system records the voice samples, as they are used continually to improve the responsiveness of the voice system.

Of course, when one reads the PCI standard, it quickly becomes painfully obvious that this sort of scenario wasn't really considered during development. Significant portions of PCI simply do not seem to make sense in this context. For example, investing in technology that ensures that card numbers are not emailed in clear text seems pointless; while it is an important control in an environment that deals with transactions and has sales audit and loss prevention functions, it is not really applicable in our case. Similarly, developing an enterprise user awareness program around the importance of protecting credit card numbers appears somewhat onerous in an environment where credit cards aren't actually being used. There are many other such examples.

But because the system records voice samples, and because consumers may speak their card number, our service provider had to become PCI-compliant. But what to do with those voice files? When we were examining the environment, the main question to us seemed to revolve around whether those files needed to be encrypted – whether, in fact, sections 3.3 - 3.6 of PCI, some of the most challenging to implement properly, were even applicable.

WHERE PCI GETS TRICKY

"What?" I hear you say. How could we even question the need for one of the foundations of the PCI standard? Actually, the concern became apparent almost immediately. Remember that the purpose of PCI, just like any other good data protection standard, is to minimize the risk of compromise. Consider the following:

First of all, card numbers do not actually appear textually in these files. While the newly revised version 1.1 of PCI clarifies much around the issue of what constitutes cardholder data, sound files appear to fall in a gray area. Yes, they are digital. But there is no direct representation of the card number within the file. Instead, there is a manifestation of the card number through a voice sample. In other words, the sample must be "heard" (and interpreted correctly) rather than "seen" in order to discover the number.

The interpretation element brings us to our second point. Analyzing the file is difficult, since the files are stored using a proprietary format, and since the system itself is highly proprietary, it would require reverse engineering of the voice recognition engine to be able to automatically extract information out of the voice files. In other words, for a hacker to be able to extract information from these files using any method other than listening to them would require rebuilding a voice recognition platform similar to the one being examined, from scratch. Not an easy task. Not only that, but even the simple task of listening to them would require at least figuring out their format and how they are stored.

We further noted that there is no special indication of cardholder data. Within the files, there is no specific indication of where cardholder data starts or ends. Moreover, the files contain fragments of multiple conversations. It, therefore, would require not just listening to the samples, but figuring out which parts of the conversation might actually indicate a card number, then find the pieces relating to expiration date and first and last name, and then to figure out which elements combine to form a single conversation. To do that, our hacker would require an army of listeners who would devoutly write down all these various pieces of information, then try to guess which of those pieces may together comprise of a single transaction. To top it off, the system never records its own voice prompts, and thus the recorded voice samples include only the consumer's spoken words, or only one side of the conversation.

Also, cardholder data appears to be spread very thinly. Because the system records many conversations, the vast majority of which contain no cardholder data, it is very difficult to extract useful information from the samples at an acceptable rate. In other words, if you need to listen to several hours of tape in order to have a decent hope of finding a single "live" card number, you may as well look for an easier target. This is especially true since the overall volume of the data is large, since these are voice samples. High quality ones, in very large amounts. That takes a lot of space. Unlike a database that stores text efficiently, these voice files take a tremendous amount of space to store very little textual information, easily three orders of magnitude bigger than a simple text record.

WHERE PCI STUMBLES

After considering all of the above, we reached the conclusion that these files did not represent a significant risk factor, and recommended that they do not require application of sections 3.3-3.6 of PCI, namely encryption. Yet one wonders. Would a VISA auditor figure differently? After all, one could claim that because the files represent a digital storage medium, and because they do contain cardholder data in an indirect fashion, that they must be fully protected according to all PCI requirements. Taken literally, the standard appears to suggest that this is true, even if it makes little practical sense.

And that's where the PCI standard stumbles with regards to some service providers. The current standard appears to make no allowance for reduced risk. With the recent release of version 1.1 of PCI, however, it seems that the compensating controls mechanism has been clarified enough to possibly allow for such disparities. Then again, compensating controls generally refer to controls actively placed for the purpose of compensating for the lack of other controls. In our case, the controls are passively inherent in the nature of the files themselves. The answer, it seems, is not clear.

BARAK ENGEL
ENGEL & ASSOCIATES

Barak Engel is the Principal of security consulting firm Engel & Associates, and has worked for more than 15 years in the information security field. His experience includes creating the information security department at WebEx Communications, working with security-conscious Fortune 500 corporations to develop a secure services environment. In his practice, Engel helps many organizations with security efforts, fulfilling roles such as the CSO at Loyalty Lab, a loyalty marketing solutions provider for the retail industry, and COO at Hackademia, a leading security training company, where he helped develop WorkForce, a unique platform for enterprise security awareness training. He serves on multiple advisory boards and leads the IT Security practice at Vela Global Ventures, a Bay Area venture group. Engel has a particular interest in security awareness as an essential part of a successful security program. In 2003, he helped found Think Security First!, the nation's first community-based cyber security awareness initiative and a unique experiment in raising the security awareness of an entire city, and in 2004 he helped create the Center for Information Security in Walnut Creek. Engel has been a speaker at several SF ISACA events.

MEMBERSHIP MAKES A DIFFERENCE

A Special Welcome to New Members

By Beverly G. Davis
Membership Committee Co-Chair

Members make the difference, and we are looking for new volunteers to support chapter activities. If you are interested in volunteering in support of the chapter contact Beverly Davis at davisb@fhlbsf.com.

On behalf of the San Francisco Chapter Information Services Audit and Control Association, we welcome the following new members and transfers.

As of August 2006

Doreen Lew
Ann Little
Rodney S. Lui
Steven Majourau
Joe N. Martins, II
Ryan R. C. Mendoza
Randy Miramontez
Michael Mojabi
Lien Nguyen
Ansh Patnaik
Eric Roswall
David J. Sanders
Ashish Sanghrajka
Kristine Senires
Mark A. Sloan
Simarjyot K. Sohi
Eugene C. Soriano
David Yam
Troy Yoshiyama
Mokhtar Mofidi

As of September 2006

James Ausman
Seth Bromberger
Shon Burton
Uttam S. Chauhan
Thomas C. Chimento
Paul Cochrane
Michael J. Cordova
Michael J. Corey
Robert Cotnoir
Deura Humayun
Darin Dutcher
Kristi L. Erickson
Pablo Federico
Todd M. Gowervv
Laurie A. Hanover
Nelson Ho
Trung Huynhy
Lance Johnson
Ronald P. Kehoe
Michael T. Kikugawa
Ronald D. Kreklau, Jr.
Stanley F. Kubiak
Ernest Lau
Thomas L. Leserman
Jodi Letkiewicz
Mabrouka Liebhaber
Subbaraman Madhira
Petra Mikesova
Ianne Ramalho Nagem

Eleanor J. Pefferman
Jian Qin
Suzanne Ravera
Jeanie Reth
Chetana J. Sankhye
Pete M. Scheidt
Stephanie M. Scott
Crystal Scott
Shitai R. Shah
Stephen Sims
Greg Sneddon
Ernest Tarasovsky
Bernice Tazbaz
Stephanie Trantow-Pearson
Jennifer Ya-Chen Tsai
Shawn Tu
Christian A. Wagner
Alexander Waher
Jeff Waybright
Jerry Yip
Sugako Amasaki
Ross A. Graber
Marilyn W. Lin
Daniel L. Morrison
Maria D. Gregorio
Jeff Wood
Yi-Chi Huang

CISA REVIEW COURSE

Certified Information Systems Auditor
The mark of excellence for a professional certification program is the value and recognition it bestows on the individual who achieves it. Since 1978, the Certified Information Systems Auditor (CISA) program, sponsored by ISACA®, has been the globally accepted standard of achievement among information systems (IS) audit, control and security professionals.

The technical skills and practices that CISA promotes and evaluates are the building blocks of success in the field. Possessing the CISA designation demonstrates proficiency and is the basis for measurement in the profession. With a growing demand for professionals possessing IS audit, control and security skills, CISA has become a preferred certification program by individuals and organizations around the world. CISA certification signifies commitment to serving an organization and the IS audit, control and security industry with distinction. In addition, it presents a number of professional and personal benefits.

San Francisco CISA Review Course
It's the holiday season and its time to think about passing the CISA examination. The examination is scheduled for Saturday, December 9, 2006. The registration deadline has passed and more than 90 people are preparing to pass the examination this winter.

As in years past, the San Francisco Chapter offered a complete review course for the 2006 CISA examination. This review course is designed to assist candidates in preparing for the CISA examination. The review sessions are taught by professional IS audit, control and security professionals and include lectures, classroom discussion, practice questions and exams. The review classes were held every Saturday from November 4, 2006 through November 18 at PricewaterhouseCoopers facility in downtown and attended by 17 students from various backgrounds.

Like the past, our instructors were experienced in IT audit, IS/IT, and security professionals from various companies. The majority of our instructors have taught the course since the past several years. They have brought in not only real life experience in the technology audit field, but also exam strategy, energy and enthusiasm. Similar to the past, the course included lectures, practice questions, and classroom discussions. Among all these, students most enjoyed the group discussion of sample exam questions and the strategy on how to identify the correct answers to the questions. They all found the discussion very helpful.

The CISA review course would like to thanks its instructors for the course, David Mckenzie - Wells Fargo, James Lucas - Wells Fargo, Vikram Panjwani - PricewaterhouseCoopers, Mike Nelson - SecureNet Technologies, Inc. and Mike Villegas - Wells Fargo. The CISA Review Course Committee would like to thank PricewaterhouseCoopers for providing a great facility to host our course

The CISA Coordination Committee is responsible for developing and coordinating the Chapter's annual CISA Review Course and is co-chaired by James Lucas from Wells Fargo Bank and Vikram Panjwani from PricewaterhouseCoopers. For more information on the CISA exam, please access the Chapter's Web site at: www.sfisaca.org/cisa

December 2006 – SF ISACA Holiday PARTY

Please come join the SF ISACA Holiday PARTY at VinoVenue.

We would like to invite you, to join us for an evening of wine tasting, networking, and Chapter recognitions. Come and mingle within the Chapter over a variety of wines at the slick SF wine bar VinoVenue. For an extra $15, please bring a guest! We will be honoring the CISA and CISM individuals who have recently passed their exam.

Hors d'oeuvres as well as cocktails will be served.

Details are as follows:

Cost:	***SF ISACA Chapter Members***	***Free***
	June 06 CISA/CISM Passers	***Free***
	Non-SF ISACA Chapter Members	***$15.00***

Date: Thursday, December 14th
Time: 5:30 PM - 9:00 PM

Where: VinoVenue (www.vinovenue.net)
Address: 686 Mission & 3rd Streets, San Francisco, CA 94105

RSVP: http://www.sfisaca.org/events/2006-December.htm

***THE REGISTRATION DEADLINE IS DECEMBER 7TH. (We are trying to establish a headcount, so please RSVP!)*

Cancellation Policy: If after submitting your reservation you determine that you need to cancel, please do so at least 72 hours prior to the event by contacting the registration coordinator, Tim Sauer, at either tim@landerint.com or at (510) 232-4264 x24. Please do not be a 'no show'. Our Chapter is billed for reservations made with our facilities provider, and we will have to pass the charges on to you. Thank you for your cooperation.

SAN FRANCISCO CHAPTER BOARD ROSTER 2007

Executive Board

President
Mike Nelson - SecureNet Technologies, Inc.
Office: (866) 660-0249
mnelson@securenet-technologies.com

1ST Vice President
Kevin Fried - Deloitte & Touche
Office: (415) 783-4639
kefried@deloitte.com

2ND Vice President
Conny Cheng - Deloitte & Touche
Office: (415) 783-4176
cocheng@deloitte.com

Secretary
Ashok Kumar - KPMG
ashokkumar@kpmg.com

Treasurer
Sandra Lee - Pacific Gas & Electric
sandra.lee@pge-corp.com

Immediate Past President
Miguel (Mike) O. Villegas - Wells Fargo & Company
Office: (626) 573-6015
miguel.o.villegas@wellsfargo.com

Directors

Directors
Christina Cheng -
Deloitte & Touche
Office: (408) 704-4203
chricheng@deloitte.com

Beverly Davis - Federal Home Loan Bank
Office: (415) 616-2766
davisb@fhlbsf.com

Todd Weinman - Lander International
Office: (510) 232-4264 ext. 17
todd_weinman@yahoo.com

Bill Davidson - Bay Area Rapid Transit District (Retired)
Office: (925) 283-3328
wzdavidson1@comcast.net

Tim Stapleton - Wells Fargo
Office: (415) 283-5937
stapletI@wellsfargo.com

Lisa Corpuz - California State Automobile Association
Office: (415) 565-3940
lisa_corpuz@csaa.com

Michele Ling -
PricewaterhouseCoopers LLC
Office: (415) 498-7482
michele.ling@us.pwc.com

Committees

Academic Relations
Wendy Leung - Protiviti
Office: (415) 951-1536
wleung524@gmail.com

CISA Review Co-Coordinators
Vikram Panjwan, PricewaterhouseCoopers
Office: (415) 498 7332
vikram.m.panjwani@us.pwc.com

Jim Lucas, Wells Fargo
Office: (415) 396-7585
jim@loukas.com

Communication Chair
Steve Owyoung, KPMG
Office: (415) 963-7603
Sowyoung@kpmg.com

Volunteer
Angie Guzman - Protiviti
Office: (415) 402-6438
ANGELINA.guzman@protiviti.com

Education Co-Coordinators
Brian Alfaro -Deloitte & Touche
Office: (415) 951-1536
balfaro@deloitte.com

Education Co-Chair
Jason Kobus -Deloitte & Touche
Office: (415) 951-1536
jakobus@deloitte.com

Advisory Board

Robert Abbott
Kathryn Dodds
Chuck Dormann
Doug Feil
Carol Hopkins
Roberta Hunter
Edmund Lam
Dave Lufkin
Lance Turcato

ISACA – San Francisco Chapter
Communications Committee
PO Box 26675
San Francisco, CA 94126