Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

FIRST 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

PRESIDENT'S MESSAGE

Beverly G. Davis
President

Contents

Become A Volunteer!

Planning next year's events calendar and selecting the chapter's leadership is now underway. There are many volunteers who give of their time and their talents to make us a successful chapter. We are proud of their accomplishments but as we move forward we encourage participation from others who wish to become volunteers. This message is dedicated to those individuals who would like to become a chapter volunteer but does not know how they can be of service to the chapter.

The strategy to becoming a good volunteer is to first commit to completing the assignment. I like the definition that a volunteer is a person who performs or gives his/her services at his/her own free will. This challenge, at times, is overwhelming but is possible as indicative of the results demonstrated by the work from this chapter's volunteers. The chapter has the following opportunities where volunteers can give of their time and talents:

The Communications Committee

This group handles the chapter's information dissemination activities. The newsletter including the technical articles is coordinated through this committee. The Web site managed by a volunteer Webmaster is also under the coordination of this committee. A volunteer can get involved in two ways: provide technical articles or serve on the committee to recruit and review technical material.

The Education Committee

This group is responsible for planning, coordinating, and implementing the chapter's educational events. The chapter considers this committee as a critical component to our success. This committee has a sub-committee organized solely for the purpose of managing the fall conference. A volunteer has many opportunities with this committee:

- As a committee or sub-committee member
- As a presenter at an educational event
- As a proctor supporting an educational event
- As an administrative staff support for an educational event
- As a contact person for securing resources

The CISA Review Committee

This group plans and coordinates the CISA Review Course. This is usually a seasonal committee but it is important as many professionals depend upon this course to assist with the preparation for the CISA certification test. The duration is usually limited to 6-8 weeks prior to the examination. Volunteers are needed as instructors and support staff during the classes.

The Membership Committee

This group manages and tracks the chapter's member movement. As an on-going committee, the leadership is always looking for new ideas to retain chapter membership. Get involved as a participant in carrying out the on-going duties or as a planner to provide the creativity and new ideas for membership retention.

The Academic Relations Committee

This group is the liaison for our student chapter at San Francisco and San Jose State Universities. We are proud of this accomplishment and are always open to new ideas for maintaining and supporting the student chapters. By the way, this committee is responsible for the CISA Scholarship Award, which provides at least two students with scholarships for the CISA Review Course. This alone is a rewarding experience as you have the opportunity to make a difference in fostering the development of new IT professionals.

As you can see, there are many ways to add to the value of this organization. We encourage you to take a stand and accept the challenge to give of your time and your talents. We need your help to better the chapter's goals and objectives. Become a chapter volunteer!

Please e-mail me at davisb@fhlbsf.com. The time is now for you to help sustain the chapter's viability!

Thank you and I look forward to adding you as a valuable member of our volunteer roster!

Sincerely,

Beverly G. Davis
President

CALENDAR OF UPCOMING EVENTS

Date	Event	Place	More information
March 18, 2003	SF ISACA Full Day Seminar: "Windows 2002 Security"	The Palace, San Francisco	details to be posted at www.sfisaca.org
April, 2003	SF ISACA Luncheon Presentation	TBD	details to be posted at www.sfisaca.org
May, 2003	SF ISACA Luncheon Presentation	TBD	details to be posted at www.sfisaca.org
September 22-24, 2003	SF ISACA 3-Day Fall eXciting Seminar	The Palace, San Francisco	details to be posted at www.sfisaca.org
National events			
March 23-26, 2003	EuroCACS 2003	Amsterdam, The Netherlands	http://www.isaca.org/eurocacs2003.htm
March 31 - April 4, 2003	IS Audit and Control Training Week	Melbourne, Australia	http://www.isaca.org/trainwk.htm
May 18-22, 2003	North American CACS	Houston, Texas	http://www.isaca.org/nacacs2003.htm

THE PURPOSE OF PENETRATION TESTING

By
Jeff Camiel
Senior Manager,
Deloitte & Touche,
Security Services: Network Security

Jeff has more than ten years of experience working both in information security and internal audit at technology and financial services companies.

Jeff is responsible for directing the Network Security Services team, managing the San Jose Security Technology Center for D&T's Northern California and Hawaii regions. Jeff is also the Technology Professional Practice Director.

Excerpts from the electronic memoirs of Joshua Carter, Network Security

Another late night, people have left the building and the motion sensors are turning off lights through out the building. Through my window, I see lit windows in the neighboring towers are blinking out and buildings are darkening. My coffee is cold. I am working through a new exploit but my mind keeps passing back to a conversation I had earlier today.

After lunch, Dave, from the Internal Audit side of the house, had slammed into my office dumping a report on my keyboard, slouched into my guest chair, and glared. Picking up the report, I read "Internet Penetration Report," looked at Dave, he glared, I continued reading. The report was a typical Penetration Test Report, completed by an experienced security consulting company.

I finished the report and flipped it back to Dave. "Seems like a pretty standard report. What's the issue?

"The issue is; what do I do with it? We have five separate Internet access points. This report indicates that Internet access point B can be penetrated through these three computers, but what about the other computers and the other Internet access points? Are they secure?" Dave was looking very frustrated.

Dave had been caught in a very interesting situation. The penetration test had been carried out by some very knowledgeable individuals. I thought I recognized the style of one of the exploit scripts that had been provided as backup documentation as the work of an extreme hacker I had done some work with. Dave and Dave's client were expecting an exhaustive list of vulnerabilities for each computer in each Internet access point. Apparently, Dave's client hadn't understood the scope and purpose of the Internet penetration test.

Internet penetration tests are truly tests. What is referred to as zero-knowledge penetration test is more than a simulated penetration test; it is the actual set of penetration activities leading to the infiltration of an internal network and the capturing of a specific target. There are only a few critical differences between a consultant's penetration test and an actual intruder penetrating the system. The initial critical difference is the penetration test window. Intruders can spend months working to penetrate a company's network. Normally, consultants are given about one hundred hours for field work. The next critical difference is the consultant's pen test is tightly controlled whereas any attack is fair game for the intruder. And the last critical difference is the consultant is limited by the client to certain type of pen test activities, normally excluding certain type of exploits (i.e. denial-of-service, social engineering, and certain computers are to be avoided), the intruder has no limitations.

Because of the time limitations and because pen tests are based on exploration and discovery – therefore very slow to complete (try scanning over the network 65,535 TCP and UDP ports per computer and you have ten computers in each DMZ!) pen tests are normally against low hanging fruit. The easiest path into the network will be discovered and reported. Some pen tests are single penetration and infiltration; others are multiple penetrations and infiltrations. Therefore the results of the pen test do not produce an exhaustive list of vulnerabilities that can be exploited, but only the vulnerabilities which were exploited to accomplish the infiltration. The results do not yield an engineering report filled with issues for the IT administrators to go fix. If the penetration test is successful, the result is proof positive that an exhaustive vulnerability assessment should be completed to locate the rest of the potential vulnerabilities in each of the access points.

Dave and Dave's client believed that at the end of the penetration test they would receive a vulnerability assessment. What they received was a very clear indication that the client needed a vulnerability assessment and the exploits used to penetrate and infiltrate the company were so common that I would have included a recommendation to engage an incident response team or forensics group to determine if an intruder had already infiltrated the company. An interesting point was brought up in the conversation; a penetration test of a single computer over the network took about 6 to 8 hours to complete depending on the hosted applications. More thorough results could be gathered by a vulnerability assessment originating from the computer's console and could be completed in 3 to 4 hours. The difference again is in the purpose. Penetration tests test the ability of an intruder to discover and enumerate information about an information system and its vulnerabilities from a zero-knowledge base from over network. Vulnerability assessments are full-knowledge projects working either directly at the computers' console or over the network to create a list of vulnerabilities that need to be mitigated and discover operational trends that either created these vulnerabilities or did not mitigate the vulnerabilities when announced to the IT community.

At the end of our conversation, Dave knew that both penetration testing and vulnerability services were extremely valuable services and he knew how he was going to use the penetration test report to recommend the need for a vulnerability assessment and he knew in the future about which service he would request based on his particular need.

It is getting late and the motion detector in my office just turned off the lights, a little magic wave and the lights are back. My exploit worked – allowing me to exploit a test Web site which permitted me to have the test Web site extend an FTP request to my FTP Web server and download penetration tools to the test Web site. Pretty cool!

Joshua Carter, Network Security Services

Joshua Carter and Dave are fictitious characters developed by Jeffrey Michael Camiel

MEMBERSHIP

By
Bill Davidson
Committee Chairperson

The membership count for the San Francisco Chapter as of January 1, 2003, stands at 408 members. Please join me and the San Francisco ISACA Board of Directors in welcoming the following new Chapter members:

Bede O. Anunne, CA, ACA
Hayward, CA

Joe J. DeGregori
Jefferson Wells International

Roy D. Florey, CIA
Wells Fargo Bank

Doris Fung, ACCA
Kaiser Foundation Health Plan

Daniel B. Hansen
Protiviti Consulting

Spencer Mead, CIA, CFE
Alameda County Internal Audits

Jared S. Pickering
DHL

Sandra P. Poon
Federal Reserve Bank of San Francisco

Elaine A. Tsay
Wells Fargo Bank

Ricki Shi-Jye Wang
Union City, CA

Alan Wong, CISA, CCSA
Bank of America

BENEFITS OF BECOMING A CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)

Since 1978, the CISA program, sponsored by ISACA, has been recognized as the one international standard of achievement among IS audit, governance, control and assurance professionals. Passing the examination opens many doors for individuals with various strengths. The accomplishment for some may signify a chance to make more money, for others a promotion or prestige, and for many of us, a sense of accomplishment for reaching a goal in our careers.

Being recognized as a CISA brings with it a great number of professional and organizational benefits. Successful achievement demonstrates and attests to an individual's information systems audit expertise and indicates a desire to serve an organization with distinction. This expertise is extremely valuable given the changing nature of information technology and the need to employ certified professionals who are able to apply the most effective information systems audit, control and security practices, and who have an awareness of the unique requirements particular to information technology environments. Those who become CISAs join other recognized professionals worldwide who have earned this highly sought after professional designation. Although certification may not be mandatory for you at this time, a growing number of organizations are recommending that employees become certified. The CISA designation assures employers that their staff is able to apply state-of-the-art information systems audit, security and control practices and techniques and that these skills are maintained. For these reasons, many employers require the achievement of the CISA designation as a strong factor for employment and/or advanced promotion.

Description of the Examination

The tasks and knowledge required of today's and tomorrow's information systems audit professional serve as the blueprint for the CISA examination. These areas are defined through a Practice Analysis that is conducted at regular intervals and consists of both process and content components in a CISA's job function. Accordingly, exams consist of tasks that are routinely performed by a CISA and the required knowledge to perform these tasks.

CISA Exam Content Areas

The following is a brief description of these areas, their definitions, and approximate percentage of test questions allocated to each area.

Management, Planning, and Organization of IS (11%)
Evaluate the strategy, policies, standards, procedures and related practices for the management, planning, and organization of IS.

Technical Infrastructure and Operational Practices (13%)
Evaluate the effectiveness and efficiency of the organization's implementation and ongoing management of technical and operational infrastructure to ensure that they adequately support the organization's business objectives.

Protection of Information Assets (25%)
Evaluate the logical, environmental, and IT infrastructure security to ensure that it satisfies the organization's business requirements for safeguarding information assets against unauthorized use, disclosure, modification, damage, or loss.

Disaster Recovery and Business Continuity (10%)
Evaluate the process for developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption.

Business Application System Development, Acquisition, Implementation, and Maintenance (16%)
Evaluate the methodology and processes by which the business application system development, acquisition, implementation, and maintenance are undertaken to ensure that they meet the organization's business objectives.

Business Process Evaluation and Risk Management (15%)
Evaluate business systems and processes to ensure that risks are managed in accordance with the organization's business objectives.

The IS Audit Process (10%)
Conduct IS audits in accordance with generally accepted IS audit standards and guidelines to ensure that the organization's information technology and business systems are adequately controlled, monitored, and assessed.

Course Objectives

This review course is designed to assist candidates in preparing for the CISA Examination to be held on Saturday, June 14, 2003.

The eight, four-hour review sessions will be taught by professional IS Auditors and will include lectures, practice questions and exams, and classroom discussions. The instructors for this year's course include professionals from Charles Schwab & Co., Inc., Deloitte & Touche, Ernst & Young, VISA, Bank of America, Fortel, Inc., and Lander International.

CISA Coordination Committee

Questions regarding the review course or the CISA examination should be directed to the CISA Coordination Committee (communications via e-mail are preferred):

Brian Alfaro
CISA Review committee chairperson
e-mail: balfaro@deloitte.com
phone: 408-704-4131

Sumit Kalra
CISA Review committee member
e-mail: skalra99@yahoo.com
phone: 415-636-7686

CISA Review Course Schedule

Date	Domain	Time
Saturday, April 12	CISA Exam Introduction & Content Area 1: Management, Planning, and Organization of IS (11%)	8:00am - 12:00pm
Saturday, April 19	Content Area 2: Technical Infrastructure and Operational Practices (13%)	8:00am - 12:00pm
Saturday, April 26	Content Area 3: Protection of Information Assets (25%)	8:00am - 12:00pm
Saturday, May 3	Content Area 4: Disaster Recovery and Business Continuity (10%)	8:00am - 12:00pm
Saturday, May 10	Content Area 5: Business Application System Development, Acquisition, Implementation, and Maintenance (16%)	8:00am - 12:00pm
Saturday, May 17	Content Area 6: Business Process Evaluation and Risk Management (15%)	8:00am - 12:00pm
Saturday, May 24	Memorial Day	(No Class Scheduled)
Saturday, May 31	Content Area 7: The IS Audit Process (10%)	8:00am - 12:00pm
Saturday, June 7	Practice Exam	8:00am - 12:00pm
Saturday, June 14	Exam Day	

CISA Exam Registration

The International Chapter of the I.S. Audit & Control Association administers registration for the CISA examination. To register for the exam contact the International Chapter to obtain registration materials:

online: www.isaca.org
e-mail: certification@isaca.org
phone: (847) 253-1545

Late registration for the exam ends April 2nd, 2003. Exam registration forms sent by mail must be postmarked by April 2nd, 2003. Registration forms sent by fax must be received by April 2nd, 2003.

Course Materials

Review Manuals Available From International ISACA:
Order the study manuals directly from the International ISACA Chapter (www.isaca.org)

- Auditing & Systems: Exam Questions and Explanations, 10th edition
- Candidate's Guide to the CISA Examination, 2003
- CISA Bulletin of Information (BOI), 2003
- CISA Review Manual, 2003
- CISA Review Questions, Answers and Explanations CD-ROM, 2003
- CISA Review Questions, Answers & Explanations Manual, 2003 Supplement

Pricing and ordering information regarding the above two manuals may be obtained directly from the ISACA International Bookstore (http://www.isaca.org/bk_cisa.htm or 1-847-253-1545, ext 401).

Course Location & Time

Time: Classes start each Saturday promptly at 8:00am and run until approximately 12:30pm.

Location: 425 Market Street (Market @ Fremont), Downtown San Francisco
Room location: 2605 + signs will be posted in lobby

Transportation

BART: The nearest BART station is the Embarcadero station.

PARKING: Available in lot located on Fremont between Howard and Folsom ($2/day). Garage located at 50 Fremont ($6/day)

Review Course Fees

ISACA Members: $275.00

Non-members: $460.00 (includes 1 year ISACA membership)

Repeat Students: No Fee (It is our policy to permit any CISA Review Course participants who do not pass the CISA exam to attend the following year's CISA Review Course at no cost, other than the cost of books and study materials)

Notes:
The cost does not include the Review Book.
Payment MUST accompany registration form.

Review course registration form

Complete and send this form along with payment to:

San Francisco ISACA Chapter
ATTN: CISA Review Registration
P.O. Box 26675
San Francisco, CA 94126

Fee enclosed (Check one):

☐ Member rate, $275

☐ Non-member rate, $460

Name: _____

Company: _____

Address: _____

City/State/Zip: _____

Phone: _____

Fax: _____

E-mail: _____

The SF ISACA Chapter recognizes candidates who successfully pass the CISA examination by hosting a recognition luncheon following the announcement of the CISA exam results. We offer successful candidates the opportunity to invite their immediate supervisor or audit director, gratis, to the luncheon. If you would like your supervisor to be invited to the recognition luncheon when you pass the CISA exam, please indicate so below and supply the requested information.

NOTE: Supervisors will only be contacted if you pass the exam.
Invite my supervisor to the Recognition Luncheon (circle choice): YES NO

If 'YES', supply the following information for your supervisor:

Name: _____

Title: _____

Company: _____

Address: _____

City/State/Zip: _____

Phone: _____

Fax: _____

E-mail: _____

Contact

Deborah Vohasek, USA
Phone: +1.847.590.7466
E-mail: dvohasek@isaca.org

As businesses face increasingly complex IT security threats, executives must ensure their IT security managers have the expertise to reduce risk and protect the organization. To address this need, the Information Systems Audit and Control Association (ISACA) has introduced the new Certified Information Security Manager™ (CISM™) designation.

The CISM certification is designed to provide senior executives with the assurance that those certified have the expertise to offer effective security management and consulting. It is a business-oriented designation for professionals who manage an organization's information security and possess the knowledge and experience to set up, implement and direct a security structure to manage risk effectively.

Overall, CISM denotes expertise in management of information security governance, risk management, program development and incident response. This management-level focus differentiates CISM from other IT security credentials that concentrate on specialist-based skills.

"The integrity and reliability of information and IT systems are crucial to an enterprise's success, so executives need a way to ensure that professionals at the enterprise's security helm are skilled and capable," said Marios Damianides, CISA, CPA, CA, chair of the ISACA Credentialing Task Force and a partner with

Ernst & Young in New York, NY, USA. "CISM is for managers responsible for understanding the interwoven relationship between business needs and IT security. Becoming a CISM demonstrates the commitment, dedication and proficiency to integrate information risk management processes into corporate governance while designing and managing an effective security function."

To earn the CISM designation, security professionals are required to successfully complete the CISM examination (offered in 2003), adhere to a code of ethics and submit verified evidence of at least five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job analysis domains. A grandfathering process that allows qualified information security professionals to apply for certification without taking the CISM exam will be offered through 31 December 2003. Those grandfathered must submit verified evidence of a minimum of eight years of information security work experience, with a minimum of five years of information security management work experience in four or more of the job analysis domains.

"ISACA is the ideal organization to administer this first-of-its-kind management-level information security certification," said Robert Roussey, CPA, ISACA International President and Professor of Accounting at the University of Southern California, Leventhal School of Accounting, in Los Angeles, CA, USA. "Since 1978, ISACA has offered the CISA® (Certified Information Systems Auditor™) certification, which has grown to be the globally accepted standard of IT audit expertise. CISM is modeled after the CISA designation. Both CISM and CISA help professionals distinguish themselves and provide a competitive advantage for their employers and their career development."

For additional details about CISM and CISA, contact ISACA at phone: +1.847.253.1545 ext. 471 or 474, fax: +1.847.253.1443, e-mail: certification@isaca.org or web site: www.isaca.org.

With 26,000 members in 160 chapters in more than 100 countries, the Information Systems Audit and Control Association® (ISACA™) (www.isaca.org) is a recognized global leader in IT governance, control and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal, develops globally applicable information systems auditing and control standards and administers the globally respected CISA® (Certified Information Systems Auditor™) designation and the new Certified Information Security Manager™ (CISM™) designation. CISA certification has been earned by more than 28,000 professionals worldwide. More than 11,000 professionals registered for the 2002 CISA exam (8,210 sat for the exam in 2001), which was offered in 11 languages throughout 73 countries.

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, Christina Cheng at (925) 467-3563, or christina.cheng@safeway.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

SF ISACA FULL DAY SEMINAR

Windows 2002 Security • Tuesday, March 18, 2003 • 7.0 hours of CPE credit

Session description

Audit, Control and Security of Windows 2000

Microsoft Windows presents a tremendous advantage in the workplace with an assortment of solutions for all aspects of your enterprise. Active Directory is a new technology included with Windows 2000 Server and provides many new services that allow you to connect your enterprise across the globe. A few of these new features include:

- Directory Services (using LDAP)
- PKI (Public Key Infrastructure)
- Improved Encrypted File System (EFS)
- Enhanced support for Plug and Play devices
- Granularity in Domain and Group organization
- … And much, much more!

This course discusses these technologies in depth and helps you become aware of the security related aspects involved with each. This course will teach methods of securing and configuring your Windows environment in order to protect your organization from the growing threat of cyber crime.

Speaker Biography

Jason Judkins is a Systems and Network Associate at the Lawrence Livermore National Laboratory. In this role he oversees a team of system administrators in charge of security and other aspects for 900 Windows systems. Before working at LLNL he did network engineering and systems support at AT&T for 2 years. He specializes in Windows NT, 2000 and XP security as well as network design.

Register

To see a detailed outline of the presentation, to read biographies of the speakers, and to find other important details about the seminar, visit our chapter Web site: www.sfisaca.org.

Schedule

Time	Description	Pricing (including Saver Pass info (if applicable)
8:00 am - 8:30 am	Registration and Breakfast	$110 Members (or 3 Saver Passes)
8:30 am -11:30 am	Morning Sessions	$135 Non-members (or 4 Saver Passes)
11:30 am -1:00 pm	Lunch	$75 Full-time students
1:00 pm - 4:30 pm	Afternoon Sessions	

This schedule is subject to change and revision.

Location

Palace Hotel
(415) 243-8062, www.sfpalace.com
2 New Montgomery Street, San Francisco, CA 94105
Located at the corner of Market and New Montgomery Streets – Montgomery Street BART/MUNI Station.

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.

JMS AND MQSERIES SECURITY

By
Robert Grill

Robert Grill is a Senior IT Auditor at Wells Fargo Bank. He has a BS in Accounting, and an MBA with a concentration in Management Information Systems. He is a CISA and a CISSP. Bob is a contributor and grader for the SANS GIAC Systems and the Network Auditor (GSNA) certification program.

In Risk Analysis, the fear of the unknown is a factor in the decision making. Often an unknown is a new technology that users don't see but happens behind the scenes. An example of this is a new paradigm in application interfacing called Java Messaging Services (JMS), it has been gaining popularity, and because it usually only takes place behind corporate networks, it has not received much attention from the security community.

JMS is a set of standard Application Programming Interfaces (API) that are used as a common language (or protocol) for enabling applications to communicate with each other across platforms and applications. JMS provides the API's but it does not provide the routing across the network. The routing is accomplished by a program such as MQSeries (MQ), JMS written for MQ evaluates the content of messages and routes them to the appropriate application.

Data sent by one program can be stored in a queue and then forwarded to the receiving program when it becomes available for processing. Without using a common message transport and queuing system such as MQ, each application must be responsible for ensuring that the data sent is received. Without JMS, maintaining communications between different types of applications as they are revised and eventually replaced with newer architectures creates an enormous programming burden in large companies.

MQ works as a message broker in order to add routing to JMS. A rules engine analyzes the messages and determines which application should receive them, and a formatting engine converts the data into the structure required by the receiving application.

MQ & JMS are analogous to e-mail (Outlook and SMTP) systems that provide similar transport functionality. The primary difference is that MQ deals with transactions between programs, whereas e-mail deals with messages between people. The MQSeries server is an application, similar to e-mail, that runs on Windows NT, the clients run on platforms such as OS/390, OS/400, UNIX, NT, etc.

MQ software provides a central point of communication between applications such as browser enabled applications on a server and legacy applications on a mainframe. Moreover, without a messaging system, each application must be custom programmed to call the other and ensure the data arrives. This adds complexity to the environment and lengthens the time to market for new applications. Once companies conform to a common messaging interface, future connections between applications will be more easily developed, and the message queue will hold transactions that are currently not deliverable due to system or network failure or overload. MicroSoft's version of this model is called .NET.

However, the risks associated with this architecture include:

- **Integrity** – how does one know that a message sent from one application was received by the other without being altered?
- **Confidentiality** – is the data being sent to the correct recipient?
- **Authentication** – is the message sent from a trusted source? If anyone sent a message, would it update data on the target system?
- **Authorization** – is the application sending the message authorized to alter data on the target system? What if a cracker had control of a trusted system, could transactions be made on the target application system?

As these are the Auditor's concerns, they unfortunately may not be the top priority for developers.

JMS Security

In summary, JMS has no security functionality built in; the security mechanisms must be implemented at other locations in the stack. For example, if all transmissions were encrypted using a Public Key Infrastructure (PKI) this would ensure authentication, confidentiality, and message integrity if the digital signature and certificate authority scheme were correct. This would also pose a challenge for administration, having each program with a valid certificate, and saying nothing about authorization.

One noteworthy item is that MQSeries replaced Remote Procedure Call technology, which is a protocol that one program can use to request a service from a program located in another computer in a network without having to understand network details.

MQSeries Security

As noted JMS sends its messages to another middleware application that is responsible for routing the messages to their intended application (this is routing at layer 7). This discussion will focus on IBM's MQSeries but other messaging middleware is available.

The question is, how does MQSeries prevent fraudulent messages without PKI implemented? Additionally, if PKI is implemented, how does MQSeries know that an authenticated application is making an authorized transaction?

Provisions for this eventuality does not appear to be addressed. After someone writes a fraudulent JMS transaction, as a proof of concept, this may be of further interest.

Research

The books on the subject of MQ and JMS focus mostly on getting it to work, with security as an afterthought. The main sources used in this article were a search in Google for JMS security and IBM Redbooks on MQ. Amazon.com indicated two books on JMS, each covering 1 and 3 pages on security according to their index, respectively.

There is an IBM Redbook sg245306 entitled "MQSeries Security", this Redbook talks about how to implement PKI with MQ.

MANAGING RISKS IN AN INCREASINGLY AUTOMATED CUSTOMER CONTACT CENTER

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.

Executive Summary

As enterprises implement customer relationship management (CRM) strategies to focus on customer service, retention and acquisition, customer contact centers (call centers) have increased in strategic importance. Forward-looking executives have leveraged these contact centers with enabling technologies to provide additional services to customers. Customer account inquiries and other transactions that previously involved a live agent can now be efficiently accomplished by Web or telephone self-service applications.

However, the complexity of these innovative technologies, coupled with the automation of customer interactions, significantly increases operational and financial risk.

Contact Center Automation

New capabilities such as voice over Internet Protocol (VoIP), chat and e-mail, self-service Web applications, Interactive Voice Response (IVR) and Computer Telephony Integration (CTI) enabling self-service transactions. These systems provide economic benefits – it decreases agent costs and allows the most common transactions to be performed quickly and efficiently. However, automation increases business risks by hiding problems customers may have accessing or using automated applications. Given the volume of calls in self-service applications, many organizations will not know if calls are being blocked, dropped, misrouted, or queued for an unacceptable period – until it's too late. Organizations may not know until hours or days later that customers received busy signals or were routed incorrectly, or that the wrong prompts or applications were playing.

Without supervisors and agents involved in the customer interaction with the contact center, the company may not have immediate visibility to operational issues and dissatisfied customers. Self-service applications remove the human control that provided companies with assurance over the quality of the customer's experience.

Financial and Operational Risks

As senior executives leverage the latest e-business, CRM and telephony technologies to gain a competitive advantage, they should also be aware of the financial and operational risks that could impact the business. Integrating contact center systems, networks and self-service applications to automate transactions and provide additional services are important contact center enhancements. However, they also increase the probability of contact center operational failures and undiscovered customer service problems. A failure with one multimedia access channel could cause a chain reaction of failures with other multimedia access channels. For example, a recent brokerage Web site outage caused customers to inundate the company's contact center with phone calls. The customers who got through the busy signals experienced wait times exceeding ten minutes.

Service disruptions caused by contact center system failures or other operational issues could significantly impact revenue. An audit of one high-tech manufacturing company revealed that each hour of interrupted telephone service could cost the company $1 million in lost revenue. In some industries with low switching costs such as financial services or the travel industry, highly publicized, negative events dilute brand equity and cause customer churn. When adding up marketing and sales costs to acquire profitable new customers, the total cost of a single lost call or failed Web transaction could be considerable.

Major operational risks in contact center operations include:

- Call handling errors or Web site errors,
- Network performance/availability issues,
- Implementation issues from inadequate application testing, and
- Outsourcing issues.

Call Center Overview

A quick overview of how calls are routed through a traditional call center will facilitate an understanding of operational risks. Traditional call centers include Automatic Call Distributors (ACD), Interactive Voice Response (IVR) systems and Computer Telephony Integration (CTI) systems.

The Automatic Call Distributor (ACD) processes each call and routes it to the Interactive Voice Response (IVR) system, or queues it for distribution to an agent. The IVR prompts callers with a series of menu choices. Working in tandem with the IVR and ACD, the Computer Telephony Integration (CTI) system accesses databases for caller account information and automatically processes the call without agent intervention. When callers "zero out" for human intervention, the CTI system provides caller account information to the agent in the form of "screen pops."

IVR Call Flows

Based on digits selected by the caller, IVRs route calls through pre-programmed call flows using conditional branching. As additional menus are added, the conditional branches become increasingly complex. For example, a typical banking customer might navigate through at least four menus and spend two minutes on a call. If each menu has six options, calls could be routed through any one of the 1,296 unique call flows that involves CTI and other telephony systems.

Stay Tuned for Part II

The growing 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. Because of the growing reliance on contact centers, senior executives should be aware of the risks and resulting impact of contact center failures and inefficiencies even over short periods of times. An effective risk mitigation program requires that the operational integrity of contact centers be closely monitored through a rigorous program of automated testing. In Part II, we'll discuss each major operational risk in contact center operations.

SAN FRANCISCO CHAPTER BOARD ROSTER 2002/2003

Executive Board

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

1st Vice President
Christina Cheng
Safeway, Inc.
925-467-3563
christina.cheng@safeway.com

2nd Vice President
Gloria Lievano
Pacific Exchange
415-393-7933
glievano@pacificex.com

Treasurer
Anne Woodbury
Providian Financial
925-738-4849
anne_woodbury@providian.com

Secretary
Lisa Corpuz
Providian Financial
415-278-8713
lisa_corpuz@providian.com

Directors

Directors
Brian Alfaro
Andersen LLP
415-546-8200
balfaro@deloitte.com

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

Sumit Kalra
Charles Schwab
415-636-7686
sumit.kalra@schwab.com

Carey Carpenter
Deloitte & Touche
415-783-5290
ccarpenter@deloitte.com

Dave Lufkin
Bank of America
925-675-1878
dave.m.lufkin@bankofamerica.com

Jennifer Smith
Wells Fargo
415-396-7955
smithjen@wellsfargo.com

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

Committees

Academic Relations
Sumit Kalra, Chair

CISA Review
Brian Alfaro, Chair
Sumit Kalra
Helen Sun

Communications
Christina Cheng, Chair
Lance Turcato, Web Master
Brian Alfaro
Doug Feil
Robert Grill
David Lufkin
Maria Shaw
Aron Thomas

Membership
Bill Davidson, Chair
Hector Massa

Education
Gloria Lievano, Co-chair
Todd Weinman, Co-chair
Carey Carpenter
Lisa Corpuz
Jim Kastle
Helen Leung
Gloria Lievano
William Luk
Maryam Malek
Cliff Nalls
Jennifer Smith
Roy Vaiani
Stuart White

Volunteer
Todd Weinman
Helen Sun, at large volunteer

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

FIRST CLASS
U.S. POSTAGE
PAID
PERMIT NO. 11882
SAN FRANCISCO CA