



NEW YORK REPORTS

GOLD AWARD CHAPTER

August 2005



Dear Colleagues:

Some time after Labor Day each year, I make a point of taking a mental inventory of all the things I was able to do during the summer. I guess it's some kind of therapeutic ritual for me, a way of coping with the end of my favorite season. As I reflect on my summer, the weekend I spent in New Orleans really stands out. I made the trip with several of my long-time friends.

For most of us, it was our first visit to the "Big Easy". Needless to say, we had a great time and were even discussing a return trip for next year when the news of Hurricane Katrina hit the media. Now, it's hard to think about our trip without focusing on the tragedy and hardship that has since overwhelmed the Gulf Coast area. I know that I speak for everyone at the NY Chapter when I offer a wish of sympathy and compassion to all those impacted by Hurricane Katrina. I look forward to the day when I can visit the great city of "Nawlins" once again.

As September rolls in, so does the official start of our programs for the 2005-2006 Chapter year. We are pleased to once again be bringing you some great programs featuring expert speakers and current topics. Here is an update on recent events and a preview of events planned for September and October.

- On **August 12th** we hosted a Business & Industry event: "Continuous Monitoring - A Strategy for Effective Controls and Using Transactional Analysis for Fraud Detection", presented by Derek Warburton of ACL Services Ltd. Over 90 Chapter members attended this half-day event. Special thanks to our Business & Industry committee co-chairs, Mike Lugo, Andrea Perkins, and James Wall for organizing this event.
- Mark your calendars; our first workshop and luncheon program of the Chapter year will be on Friday, **September 16th**. Sandra Miller will be conducting a full-day workshop titled, "Engage, Influence, And Motivate: How Auditors Can Use The Social Sciences To Add Value". Also, we are very excited to have as our luncheon speaker, Sal Marchiano, weeknight sports anchor at WB11 News at Ten.
- Also in September, we're hosting our third Business & Industry event of the Chapter year. We are pleased to welcome Ernst & Young, who will conduct a presentation titled "Auditing Tone at The Top". This half-day event will be held at the Yale Club in mid-town Manhattan on **September 19th**. There is no charge for this event, however, seats are limited to the first 90 registrants. Be sure to check the Chapter's website for registration details.
- On **October 10th-13th** we have scheduled review classes to help you prepare for the Certified Internal Auditor (CIA) Examination. As in the past, the format will be a one-day training session for each part of the exam. For more details and registration information, please check our website. Many thanks to Carol McFarlane, Jennifer VanAlstyne, Pat Murtha, and Juan Perez for their efforts in planning these review classes.

I look forward to seeing you at our first meeting on September 16th.

Luca A. Pagoto, President
IIA New York Chapter

In This Issue

President's Message
Pg 1

Home Network Security Basics
Pg 2-3

CIA Exam Info, Audit Committee
Toolkits
Pg 3

GAO, GAGAS, Structure
Pg 4

Editor's Corner / Chapter Officers
Pg 5

Secrets of Listening Well
Pg 6

Technology Impacts Customer
Protection / Hurricane Katrina Impact
Pg 6 - 7

Letters
Pg 8

Home Network Security Basics

Technology surrounds everything that we do, from the latest RIM communication products to the RFID chips in our E-Z passes. We use technology for banking, shopping, driving directions, and speaking to family members hundreds of miles away. Society has become increasingly computer literate, but it is surprising how often we forget the basics of protecting our sensitive information.

Over a cup of coffee last week, my friend Samantha spoke proudly about how she installed her first home wireless network using a Linksys router. She stated how easy it was to connect her cable modem to her wireless router and how quickly she began surfing the Internet. Being concerned from what I heard, I then began to ask her questions such as:

Did you change the administrator password on the router? She replied, "No".

Did you disable the SSID broadcasting? Again, she replied,

"No".

Did you enable WEP/WPA encryption? Promptly, I received a third, "No".

I wanted to ask her if she is using MAC filtering on her wireless router, but then realized given the previous answers, it would be a definite 'no'. I then began to explain to her why such configuration settings are necessary (which I have outlined below). There are many wireless vendors such as Cisco, Belkin, Linksys, and D-Link and of these wireless products have the functionality to secure your home network.

Default administrator password

I must admit that I was proud of Samantha for purchasing a router instead of plugging her computer directly onto the Internet. A router will provide the initial layer of security for her home network. However, she failed to notice that most routers come with default passwords. With the default password enabled, unwanted guests easily obtain access to your network.

Being familiar with Linksys, I told her that the default administrator ID is blank with 'admin' as the password. I began to show her how easy it was to find the passwords for other products. Within five seconds of searching for default passwords on Google, I found a webpage with default passwords for every network device from 3Com to Zyxel.

SSID Broadcasting

The Service Set Identifier (SSID) is a unique name for every wireless network. However, wireless networks come with factory-default SSIDs, such as Linksys or Belkin. I recommended that she change her default SSID (Linksys) to something that was unique for her network and to disable

SSID broadcasting. This step adds another layer of security, as a computer will not be permitted to join the network unless it can provide the unique SSID.

Wireless Encryption

Without wireless encryption such as WEP or WPA enabled, Samantha's information is being transmitted in clear text. This allows for anyone with a wireless sniffer to read the data being transmitted on her network. WEP/WPA generates a passphrase which acts as a key to authenticate to the network in addition to protecting your data.

MAC Filtering

Lastly, I recommended that she create a Media Access Control Address (MAC address) to filter out computers that do not belong on her network. The MAC address is a unique identifier that is given to every computer or printer. Enabling MAC address filtering will allow only computers with a specific MAC address to obtain access to the network.

Setting up a secure wireless network is not as hard as it seems. Anyone with a little patience and the ability to follow the installation procedures can secure their network in no time. In fact, after coffee, Samantha secured her network in ten minutes and was surfing the Internet again!!!

Duy Nguyen

E-mail: duynguyen@deloitte.com

Audit Committee Toolkits

The AICPA has released two free best practices resources for not-for-profit organizations and government organizations. Visit the AICPA Audit Committee Effectiveness Center , www.aicpa.org/audcommctr to download the AICPA Audit Committee Toolkits: Not-for_Profit Organizations and the AICPA Audit Committee Toolkits Government Organizations.

**Once again the NY Chapter will host a
Review Class in October 2005 for
November CIA Exam**

*The classes will be held at in New York
City at New York Life from Tuesday
October 11 through Friday October 14.*

*Look out for more details in future
newsletters and on the IIA websites*

www.theia.org and www.nyiaa.org

GAGAS=GAGAS + PCAOB?

To avoid confusion and inconsistencies between government auditing standards and standards set by other professional bodies, i.e. the Public Company Accounting Oversight Board (PCAOB), the Government Accountability Office (GAO) will allow auditors to prepare audit reports using both generally accepted government auditing standards (GAGAS) and PCAOB standards.

The GAO sets the standards for auditing government agencies and entities subject to government regulations. Certain companies, e.g. lending institutions that participate in federally funded loan programs, are subject to both GAGAS and PCAOB standards. Under the new guidelines, auditors may prepare GAGAS reports on internal control using the definition of "material weakness" found in PCAOB's "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements".

For more information on complying with GAGAS and PCAOB standards visit www.gao.gov.

GAGAS CPE Requirements Revision

The Government Accountability Office (GAO) recently revised the continuing professional education (CPE) requirement of the Government Auditing Standards, the "Yellow Book". Generally, auditors subject to the Yellow Book standards must complete 80 hours of CPE training every 2 years to maintain their professional competence.

As of June 30, 2005, however, auditors who only perform field work and who devote less than 20 percent to audits conducted using generally accepted government auditing standards (GAGAS) can take 24 hours of training within a two-year period. These auditors must only be involved in audit field-work not involved in the planning, directing, or reporting phases of the audit.

See www.gao.gov/govaud/ybk01 for more information

Structuring

The Bank Secrecy Act requires financial institutions to file a Suspicious Activity Report if it knows, suspects, or has reason to suspect that a customer's transactions are designed to evade the Bank Secrecy Act, i.e., structuring. Structuring is the breaking up of monetary transactions to evade the anti-money laundering reporting and recordkeeping regulations of the Bank Secrecy Act. A customer may try to avoid the law in one two ways: (1) a customer might deposit currency on different days in amounts under \$10,000; (2) or the customer may make multiple deposits or electronic funds transfers in different branches of the same bank over several days

To comply with the Bank Secrecy Act, a financial institution must have an anti-money laundering program that can identify both types of structuring and other money laundering practices. The Bank Secrecy Act require that a financial institution's anti-money laundering policies and procedures be based on its assessment of the money laundering and terrorist financing risks it faces. The Financial Crime Enforcement Network advises financial institutions to consider the type of products and services it offers, the locations it serves, and the nature of its customers when designing its anti-money laundering program.

In a July 15, 2005 letter, William D. Langford Jr., Associate Director of Financial Crime Enforcement Network noted that the goals of the Bank Secrecy Act are: (1) to ensure that financial institutions have systems, procedures, and programs to protect it from money laundering and illicit financing; and, (2) the systems provide the government with useful information to prevent, deter, investigate, and prosecute financial crime.

2005 – 2006 CHAPTER OFFICERS

**PRESIDENT
LUCA PAGOTO**

New York Life Insurance Company
(212) 576-6350
E-Mail: Luca_Pagoto@newyorklife.com

**Executive Vice President
RICHARD M. DAPCIC**

NYSE
(212) 656-2131
E-Mail: rdapcic@nyse.com

**Vice President-Professional
Development
BRIGITTE COLLINS-POWELL**

AXA Financial
(212) 314-5348
E-Mail: brigitte.powell@axa-financial.com

**Vice President-Professional Services
GAIL FORKOSH**

MetLife
(212) 578-3192
E-Mail: gforkosh@metlife.com

**Vice President-Secretary
CAROL McFARLANE**

MetLife
(212) 578-5351
E-Mail: cmcfarlane2@metlife.com

**Vice President & Treasurer
REGINA MULLEN**

New York Life Insurance
(212) 576-7058
E-Mail: Regina_Mullen@newyorklife.com

**Immediate Past President
(2004-2005 Chapter Year)
MARIAN DOUGHERTY**

MetLife
(212) 578-8229
E-Mail: mdougherty@metlife.com

**Newsletter Chair
MICHELLE DUKE**

Guardian Life
(212) 598-7482
E-Mail: michelle_duke@glic.com

Advance Technology

JOEL IPE
Citigroup
(212) 657-0354
E-Mail: Joel.Ipe@citigroup.com

Editor's Corner



I am devastated by the conditions being endured by the victims of Hurricane Katrina. Two stories encapsulate the aftermath of the hurricane to me: One woman told a reporter simply, "All I have is \$80." She cried, "Yesterday I had a home, a job and money in the bank. Now my home is gone, I can't get to my job, I can't access my bank account -- it's all under water, even my car is flooded. All I have is \$80 in my pocket. What am I to do?" She asked helplessly.

Then there's the story of the employee who went AWOL with his employer's boat. He and his friend, a police officer, are looking for survivors. They patrol the now waterways of New Orleans knocking on doors and listening for calls of help. Since the flood they've spent days reassuring and rescuing people.

Through all the commentaries on blame, race, class, politics, and strife, I remind myself of these two people. Their stories show me that we can move from despair to hope through individual efforts of courage and kindness.

Michelle Duke, CPA
Newsletter Chair



The Secrets of Listening Well – source The PAR Group

"Listening is as powerful a means of communication and influence as to talk well." - John Marshall

There is a growing realization of the importance of solid listening and communication skills. In internal auditing, lack of attention and respectful listening can lead to mistakes, misaligned goals, wasted time and lack of teamwork. It can lead to the auditee not buying into an auditor's recommendations.

Auditors are encouraged to ask questions, but asking is only part of the equation. You must understand the meaning and significance of the words heard. An internal auditor must listen in a way that demonstrates understanding and respect. Effective listening can cause a rapport to develop, and that is the foundation from which you can manage the interview, influence the auditee, and obtain reliable information.

The following are some keys to listening well:

1. **Give 100% of your Attention:** Suspending all other activities.
2. **Respond:** Responses can be both verbal and nonverbal (nods, expressing interest) but must prove you received the message, and more importantly, that it had an impact on you. Speak at approximately the same energy level as the other person...then they'll know they really got through and don't have to keep repeating.
3. **Prove understanding:** Saying "I understand" is not enough. People need some sort of evidence or proof of understanding. Restate the gist of their idea or ask a question which proves you know the main idea. The important point is not to repeat what they've said to prove you heard what was said, but to prove you understood what was meant.
4. **Prove respect:** Prove you take other views seriously. It seldom helps to tell people, "I appreciate your position" or "I know how you feel." You have to prove it by being willing to communicate with others at their level of understanding and attitude. We do this naturally by adjusting our tone of voice, rate of speech and choice of words to show that we are trying to imagine being where they are at the moment.

Listening to and acknowledging other people may seem deceptively simple, but doing it well takes true talent. As with any skill, listening well takes plenty of practice.

"I like to listen. I have learned a great deal from listening carefully. Most people never listen." - Ernest Hemingway



Technology Impacts Customer Protection

Companies are using technology to give employees more ways to communicating and to fulfill staffing needs. Estimates show that over 25% of all full-time employees have flexible schedules. However, there are challenges facing companies that allow their employees to use remote access and other wireless technology.

When using a wireless connection, data is broadcast out into the airwaves, making confidential data easier to intercept than if the user used a physical wire. The use of Wi-Fi is another challenge since wireless connections can allow hackers to tap into the user's workstation to gain access to a corporate network. Every workstation connected directly to the Internet creates a separate opportunity for intrusion. In addition to wireless technologic, remote access to corporate networks through VPNs or other technology may raise similar concerns.

The National Association of Securities Dealers (NASD) advised its members to consider whether their current policies and procedures are appropriate before permitting employees to access customer information remotely. Policies and procedures should be tailored to specifically address the technology used by employees with access to customer records and information the NASD added.



Hurricane Katrina Impact

The National Association of Securities Dealers (NASD) temporarily suspended its requirement to maintain Form U-4 information for registered representatives affected by the hurricane. In addition, broker-dealers are not required to submit branch office applications for any newly opened temporary locations established due to Hurricane Katrina.

The NASD advises broker-dealers to make "best efforts" to notify it of changes to locations and other changes in policies and procedures made due to the hurricane. For example, the NASD advises its members to waive procedures requiring written authorizations to move funds, however, it cautions that firms should exercise due diligence in validating the identity of customers.

Question to Members



What information is included on your Internal Audit intranet site?

Send responses to
member_questions@nyiaa.org

Letters

May 17, 2005

Mr. Luca Pagoto
President–IIA New York Chapter
New York Life Insurance Company
New York, NY 10010

Dear Mr. Pagoto,

On behalf of the Port Ministries and the children and families that we serve, thank you for the generous gifts of a DVD player and cameras. All of the items donated will be a great help in with the children/young adults who are served by Port Ministries.

Port Ministries is located in one of the poorest sections of Chicago and the nation. It is a multidimensional outreach facility to the poor and homeless. It was founded by Father Gus Milon, OFM, a Franciscan friar in the south side of Chicago in 1985. Started with a one-room soup kitchen in an old abandoned restaurant, it has grown into three main outreach locations spread over several blocks. It includes food pantries, soup kitchens, shelters, and educational and recreational facilities for children and adults.

The two programs of Port Ministries that focus on children and young adults are administered by Theresa House & Tony's Gym. Theresa House provides a community living arrangement for homeless families. It is the largest full family shelter in Chicago's Cook County. Tony's Gym offers alternate recreational facilities to neighborhood children. It provides the children with the opportunity to receive tutoring, participate in sports, present plays and speaking presentation.

Please find an enclosed brochure that explains all of the services that are offered by Port Ministries.

Thank you,
Mr. David Krug
Executive Director-Port Ministries

Do you have a story to share?
Contact michelle_duke@glic.com. We'll tell all!



You Know You're a New Yorker when:

YOU TAKE THE TRAIN HOME AND YOU KNOW EXACTLY WHERE ON THE PLATFORM THE DOORS WILL OPEN THAT WILL LEAVE YOU RIGHT IN FRONT OF THE EXIT STAIRWAY.