Developing, Deploying and Managing a Risk-Adjusted Data Security Plan

Ulf Mattsson
CEO
Protegrity

Not too long ago, many security experts believed that the best way to defend data was to apply the strongest possible technological protections to all data, all the time. While that plan may work perfectly in theory, in the real world of business this model creates unacceptable costs, performance and availability problems.

What works from both IT and management standpoints? Risk-adjusted data security.

Protecting data according to risk enables organizations to align their security and compliance profile to their most significant security exposures. This will help them achieve the right balance between business needs and security demands.

Other issues that risk-adjusted security addresses are the unnecessary expenses, availability problems and system performance lags that result when data is over-protected. And cloud-based technologies, mobile devices and the distributed enterprise require a risk-mitigation approach to security, focused on securing mission critical data, rather than the now-unachievable ‘protect all the data at all costs’ model of years past.

Here’s how to develop and deploy a risk-adjusted data protection plan:

Step 1: Know Your Data

Begin by determining the risk profile of all relevant data collected and stored by the enterprise, and then classify that data according to its designated risk level. Data that is resalable for a profit -- typically financial,

continued on page 5

Message from the President

Felix Ramirez
Chapter President
ISACA® NY Metro Chapter

I’m excited about the progress our Board has made in such a short period of time. On the administration side, we have changed our Chapter address and have activated a phone number as well. The new information is:

ISACA® New York Metropolitan Chapter
954 Lexington Avenue #525
New York, NY 10021
Phone: 646-881-4696

On the services side, our continued focus on Education offerings has allowed us to have more courses than ever this Fall, across a wide array of topics. And, despite the down economy, class participation is higher than ever. We are glad people recognize the value of our education classes, and thank you to our Education Committee Chairman for helping to make that possible.

Every Chapter’s goal is to increase membership. We noted a slight fall in our members, which we attribute to

continued on page 8
Membership Highlights

Featured Chapter Member

Cory Notrica – Director of Integrated Audits at a Major Consumer Products Company

Michelle Syskrot
MetroLine Copy and Photo Editor
ISACA® New York Metro Chapter

The Metroline spoke with Cory Notrica, a Director of Integrated Audits at a major consumer products company in the metro New York area. Cory is a CISA®, CISM®, CGEIT®, CISSP®, CIPP® and an SAP Solution Architect with over 17 years of experience in the Information Systems field. Cory specializes in Strategic Development, Information Risk Assessment, Project Risk Management, Network Architecture Analysis, Third Party Due Diligence and Business Process Improvement. Read below to find out more about Cory Notrica.

Metro Line: Which college or university did you attend? What did you study while there?
Cory Notrica: I received my BS in Accounting from Syracuse University; I also concentrated in Musical Theater Performance and Psychology while there.

ML: Describe your career path.
CN: I started my career at Ernst & Young, where I was a Financial Auditor. It was here that I was exposed to Information Systems auditing in my second year and I found the technical aspect of Information Systems auditing to be extremely interesting. I was with Ernst & Young for about 4 years. I later moved to the Information Risk Management group at KPMG (known today as Risk and Advisory Services). After 5 years at KPMG, I went to a client of mine, UBS Investment Bank and was a Director in Security Risk for the Americas. I then went back to Ernst & Young in 2004 in their Technology and Security Risk Services group in the Financial Services Office and left as a Senior Manager. In 2008, I joined my current organization as Director of Integrated Audits, where I am responsible for coordinating and executing IT Audits in support of business processes.

ML: What is a typical day on the job like for you?
CN: There is really no “typical” day for me. I travel about 60 – 70% of the time to various divisions of the company. I enjoy travelling because I meet different people and experience different mindsets and cultures. I like having status discussions with the audit teams in each location because each team member adds a different perspective to the audit. My favorite places to travel are San Francisco and Hong Kong.

ML: How do you keep on top of the latest industry happenings?
CN: I read the bi-monthly ISACA® journal and I find it to be a very valuable resource. There is always an article relevant to an audit I am currently performing, whether it be IT Governance, SAP, or Information Security. I also read the IAPP privacy newsletters, SC Magazine, and I'm a big fan of Maximum PC.

ML: How has networking played an important role in your career?
CN: The key to successful networking is to keep in touch with people on a regular basis, whether it be every six months or once a year. You shouldn’t call someone only when you need something. It’s also critical to know the person that you’re networking with – what is his/her personality, culture, etc. I utilize LinkedIn to keep tabs on my friends and colleagues. It’s any easy way to keep in touch with my former colleagues at Ernst & Young and KPMG. Being a member of ISACA® has also helped build my network. I keep in touch with Board Members and get to see former colleagues at ISACA® meetings and training classes.

ML: What are some of your hobbies outside the office?
CN: I enjoy playing softball and skiing. I built an arcade emulation machine a few years ago that included Space Invaders Deluxe and other classic Atari games. As a child, I was an actor and I appeared in a few professional kids’ shows, off-off Broadway, instructional videos, and commercials. I was also in the movie “Walls of Glass” in 1985. Additionally, I enjoy spending time with my wife, Stacey, and 3 wonderful daughters, Hannah, 10, Nyssa, 7, and Lucy, 3.

We feature a chapter member in each edition of Metro Line! Nominate one of our chapter members by emailing METROLINE@ISACANY.ORG
Chapter Membership Update

Alexander Josephite  
Second Vice President and Membership Committee Chairman  
ISACA® New York Metro Chapter

The Membership Committee has been working hard to implement programs designed to give members of the ISACA® New York Metropolitan Chapter the best value of all ISACA® Chapters. The Chapter is starting a new marketing campaign with strategic guidance from volunteer Michelle Crepeau. New strategies include a presence on Twitter, Facebook, and strong advertising relationships with partners such as the New York Chapter of the Institute of Internal Auditors (IIA). Our Corporate Relations Subcommittee Chair, headed by Chris Westerman, is also making progress obtaining needs from our membership so that we can design successful education and membership events. If you would like to be chapter liaison for your company, please email Chris Westerman at christopher.westerman@isacany.org. In addition, we are now accepting sponsors for our membership meetings. If your company would like to sponsor an event please email membership@isacany.org.

Mentorship Program

I’m happy to announce that anyone mentoring a fellow chapter member will be awarded one CPE per hour of mentoring, up to 10 per year. The mentoring program is loosely structured to allow members to get the most out of the experience. Also, the board approved a small starter budget to allow for the chapter to pay for the first one-on-one meeting, up to $25.

Long Island IT Audit and Compliance Director Roundtable

Lead by Ken Fried and Kevin Fuller

The Chapter would like to extend a big thank you to Estee Lauder for hosting our 4th roundtable meeting on September 24th. Representatives from 18 companies across Long Island were in attendance to share their thoughts and best practices surrounding Vendor Management.

Featured Member Benefit

JournalOnline

JournalOnline (JOnline) is the online-only counterpart to the ISACA Journal. Articles included in JOnline undergo the same rigorous peer review process as articles found in the print version of the Journal. JOnline articles are available exclusively to ISACA members for one year. JOnline is updated bimonthly on the first business day of the month in which no print Journal is released (February, April, June, August, October and December). All JOnline articles are available in HTML and PDF at www.isaca.org/journalonline.

This Member Benefit was featured in ExpressLine, a monthly newsletter for the leadership of ISACA®.

If your company is looking to fill an opening in IT audit, security, management, or operations we would be glad to list it on the ISACA® NY Metro chapter website for free!

To submit a job posting please email the job description and contact information to Membership@isacany.org. The opening will be posted on our site for 30 days unless otherwise directed. This service can only be seen by those logged into our website www.isacany.net.
Chapter Golf Outing

Kevin Fuller
Board of Directors
ISACA® NY Metro Chapter

On Friday September 24th the ISACA® New York Metropolitan Chapter’s 4th annual Golfing event teed off!

The outing which had to be postponed this year for two weeks due to torrential rains was rewarded with crisp autumn air and sunny blue skies.

This annual event was held at the Towers Country Club which is located right off the GCP on the Queens/Nassau boarder just a short drive south of the Throgs Neck bridge which makes it very easy to access.

The day starts as a “shot-gun” which means that all the players start at the same time but begin from different holes on the golf course. The big advantage in that is that everyone finishes around the same time.

The format is a very friendly “Best-Ball” scramble. It works this way: four players hit their tee shot – then they pick the best shot and the other three will pick-up and drop their ball at that spot and all four will take their second shot from that point. So all levels can play and you never know your shot maybe the one that saves the hole.

At the conclusion of a fun-filled day on the links, all gathered back at the clubhouse where a wonderful buffet awaits plus a chance to mingle and enjoy each other’s company. Also people had a chance to win some great raffle prizes. By the way non-golfers were welcome to attend this part of the event as well.

The Golf Event Chair, Kevin Fuller, stated that the intent of the outing is to foster a networking atmosphere that offers the opportunity for members to invite their peers as well as their management to engage and interact in a more relaxed environment. The chapter made every effort to keep the cost as affordable as possible. The outing has been picking up traction and is growing. We are seeing attendance and sponsorship increase every year as members realize that they can anticipate a fall outing. Also, the word is getting out regarding how successful of a day it is.

So next year circle the date on your calendar and we’ll see you out on the links!
Website Continues Moving Forward

Chapter's website continues to grow and mature

Richard Ziegler
Board of Directors and Web Committee
ISACA® NY Metro Chapter

The chapter’s website (http://www.isacany.net) continues to grow and mature over time. This is part of a coordinated effort to better serve the evolving needs of our membership by improving communications, enhancing functionality, and ensuring that content is accurate, timely, and germane to the chapter.

Some of the key initiatives currently underway include:

- Streamlining the event registration process to make it more user-friendly and adaptable to differing registration scenarios. Some of these modifications will refine the online registration process while others will provide administrators with better interfaces for configuring and managing events on the backend.
- Providing the ability to include events from multiple professional organizations in our calendar so that related functions can be viewed centrally. Note that all events will be displayed by clicking on the calendar located in the Events Calendar section on the right side of each web page. However, only our chapter’s events will be displayed in the Upcoming Events section.
- Integrating social networking and micro-blogging capabilities into the chapter’s comprehensive communications plan to provide convenient notification of important announcements, events, and training. Note that our chapter now has a Twitter profile (twitter.com/isacany) and will begin tweeting in the near future.

The Web Committee is proud of our website and our dedication to continuous improvement. Please contact webmaster@isacany.org with any questions, comments, or suggestions.

Message from the President

continued from page 1

people losing their jobs, or switching careers. I happen to believe that when out of work it is the best time to be a part of the Chapter, as other members will provide connections and the Chapter will provide a channel to identify job opportunities. Never-the-less, we’re hard at work looking for more value-added offerings that will continue to attract and retain members.

Our Membership Committee has created several programs and subcommittees to help. This includes activities related to Mentoring, Academic Relations, Corporate Relations and Audit Director Round tables. Additionally, and perhaps most importantly, we provide ways for our members to connect and network at Membership Meetings and holiday get-togethers.

Lastly, I wanted to mention that we have undertaken a major initiative to strengthen the governance framework of the Chapter. The first step in that direction has been to revise our chapter’s By-laws to enable the decisions that need to be made and keep our activities aligned with the needs of our members. Our Board felt that there were some definite improvement opportunities. Our By-Laws Committee has provided a draft which the Board has approved. Among other things, it clarifies some of the roles for each executive Board member and makes our nomination and election processes more transparent and friendlier. The Chapter Board passed the revisions unanimously at our last Board meeting and they are now undergoing a thorough review by ISACA® International. After ISACA® finishes their review, the revised by-laws will be sent to our general membership for final approval.

In summary, we’ve done a lot so far but I’m looking forward to our continued progress as we move into the new calendar year. To continue in our path to better services to our profession and members, we need your continued collaboration and support.
Technical Corner

Diminishing IT Costs with Application Portfolio Management

Jarrett Blankenship
Senior Consultant
Protiviti, Inc.

A year of difficult economic conditions has generated a renewed focus on cost management in companies around the world. Although there are faint signs of improvement in the world’s economy, management teams will continue to scrutinize their budgets to reduce costs for the foreseeable future, and IT will inevitably be one of the targets. However, for most modern companies, their technology is essential to remain competitive. A question many technology executives must now ask themselves is: If budget reductions are unavoidable, where can IT spend less without crippling the company in the process?

It may seem counterintuitive, but information technology departments often spend far more of their budget running and maintaining the applications that they already have, than on new projects or development. Even conservative estimates place the application maintenance and overhead costs at over 50% of the total IT budget. However, there are ways to reduce these costs while still improving the reliability, quality and value of IT. One key way to achieve this goal is through application portfolio management.

Application portfolio management (APM) is a process used to quantify and monitor the value, costs and risks of a company’s applications. Research from Forrester indicates that return on investment from a successful implementation of APM can often be reached within 12 months and that cost savings of 10% - 30% on average are typical.

The application portfolio is more than just an inventory of a company’s applications. When fully realized, application portfolio management identifies redundancies between applications, clarifies the costs and risks inherent in the existing application infrastructure and focuses attention on the purpose and value generated by each application. The metrics it provides support IT management’s decisions to:

- Invest in an application
- Move the application to a new platform (or virtualize)
- Integrate with another application
- Eliminate an application

That information empowers IT management to reduce both the costs and risks of their application environment while increasing the business value of their technology investments. In many cases even small improvements to the environment can provide unforeseen returns on value. For instance, one application may be retired because it is found to be redundant. This will not only immediately reduce costs in terms of licenses, maintenance and system processor usage, but it may provide additional benefits over an extended period as it frees up technical resources to focus their attention on maximizing the value of remaining core applications – especially if the retired application was a problematic system that required a lot of attention.

In order to do this, the Application Portfolio compiles information about each of the organization’s applications and analyzes the data for patterns and warning signs. This information may include maintenance costs, risk and contingency analyses, business value drivers and functionality as well as information to classify and track the applications. The depth of the information required may vary from one company to the next depending on their size and the complexity of their environment.


continued on page 7
Although many companies practice some aspects of application portfolio management already, some have not been able to reap the value they expected from the process. This is because there are a number of challenges that complicate the full integration of application portfolio management into the larger IT strategy of the organization.

The most significant challenge is that APM is more of a philosophy than a tool or a project. To be effective it must become a fully institutionalized piece of the IT governance structure. This may require some discernible process changes within an organization, but the changes aren't an insurmountable barrier. For example, in order to monitor the man hours of support consumed by an application, IT resources may be required to track their time in a more detailed way than they are accustomed. When initially implementing APM, these difficulties can be offset by

- spending significant time building support for APM amongst the affected parties
- investing only modest time and capital implementing new systems

A company wishing to implement APM should initially focus their attention on managing the process changes more than the tools they use to support it. The benefits gained from APM's outputs are much more a factor of the data quality than the portfolio system's features. Although there are several high quality, sophisticated tools for APM on the market, IT could realize many of the benefits without a major investment in new technology. When the process is securely in place, significant value can be realized through little more than well designed spreadsheets, even though the solutions are likely not glamorous. Once the APM process is stable, the organization can consider upgrading to a more robust portfolio management system.

Another serious challenge faced when implementing APM is that much of the required information exists in highly fragmented forms across an organization. For example, a Customer Service group and an Accounting group will have applications with related functions and common integration points. However, the two departments most likely have very different ways of documenting application costs that must be reconciled. To maximize the portfolio's value, these costs must be consistently accounted for across all business groups. For many companies this reconciliation may require the assistance of independent third-parties. To incorporate the entire application infrastructure, business contacts from all areas of the organization will need to be involved as well as the individual IT application owners and experts.

Additionally, there needs to be vocal support from senior management with sufficient authority to ensure that each of the fragmented groups is willing to participate. This is no small challenge, but unlike many other technology projects, the potential return on investment for APM is easily quantifiable in terms of cost savings. That fact alone can make a strong business case for APM when building support amongst senior management.

In most cases, application portfolio management alone can not achieve all of a company's cost reduction goals for IT. However, it can rapidly provide tangible gains when properly supported. With time, IT can then refine the information and the metrics provided by the portfolio to make smarter investment decisions and to maximize the business value of their existing environment.

---

personally identifiable and confidential information -- is high risk data and requires the most rigorous protection. Other data protection levels should be determined according to the value of the information to your organization and the anticipated cost of its exposure -- would your business be impacted? Would it be difficult to manage media coverage and public response to the breach?

There are several models that a business can use to classify data. Larger enterprises will likely want to rely on policy-driven automated tools. Smaller businesses can use the simplest model: assign a numeric value for each class of data; high risk = 5, low risk = 1.

Step 2: Find Your Data

Data flows through a company, into and out of numerous applications and systems. A complete understanding of the high risk data flow is essential to the risk-adjusted process. You can't protect data if you don't know where it is, and assigned risk levels will change depending on how data is being collected, used and stored. High risk data residing in places where many people have access is data that needs the strongest possible protection.

Locate all of the places that data resides. This may include applications, databases, files, and all the systems that connect these destinations (such as data transfers across internal and external networks, etc.). Then determine where the highest-risks reside and who has or can gain access to data (see “Understand your Enemy” below).

Other areas to examine for data stores include your outsourcing partnerships as well as data that is being used for nonproduction purposes such as third-party marketing analysis or in test and engineering environments. It's not uncommon for organizations to invest in protecting production systems and data centers, yet have live data sitting unprotected on the systems of application developers and other outsourced parties. If live production data is being used in a less controlled environment there has to be attention paid to regulatory compliance and security threats. Here too, data de-identification technologies like Format-Controlling Encryption and tokenization can help.

Step 3: Understand Your Enemy

The next step is conducting an end-to-end risk analysis on the high risk data flow to identify the highest risk areas in the enterprise ecosystem and the points where data might be exposed to unauthorized users.

Currently web services, databases and data-in-transit are at high risk. The type of asset compromised most frequently is online data. Exploiting programming code vulnerabilities, subverting authorized user credentials and malware targeting the application layer and data (rather than the operating system) are the attack methods that are being utilized most frequently. These vectors change so keep an eye on security news sites to stay abreast of current threats.

Most data breaches are caused by external sources but breaches attributed to insiders, though fewer in number, typically have more impact than those caused by outsiders. Nearly three-quarters of the breaches examined in the Verizon Report were instigated by external sources. Unauthorized access via default credentials (usually third-party remote access) and SQL injection (against web applications) were the top hacking methods and access to a network was often followed by malware being planted on the system.

Step 4: Choose Your Defenses

Look for multi-tasking solutions that protect data according to its risk classification levels, support for business processes, and their ability to be change with the environment so that you can easily add new defenses for future threats and integrate it with other systems as necessary.
High risk data is best secured using end-to-end encryption or tokenization of individual data fields. Tokenization removes sensitive data from the information flow at the earliest possible point in the process, replacing it with a token that acts as an alias for the protected data. By associating original data with an alias, high-risk data can systematically be removed and protected from malicious hackers over its lifecycle under a fully auditable and controllable process. This practical protection method is perfectly suited for securing high risk data like payment card information and social security numbers.

Newer solutions provide targeted protection for data in use and they don’t interfere with business processes. For example, Data Format Controlling Encryption retains the original format, on a character-by-character basis, of encrypted data, putting an end to the data re-formatting and database schema changes required by other encryption techniques. It’s especially well-suited to protect data that’s being used for testing or development in a less-controlled environment. Partial encryption can then be applied to provide the ability to encrypt selected parts of a sensitive data field based on policy rules.

Policy-Based Masking provides the ability to mask selected parts of a sensitive data field. Implemented at the database level rather than application level, policy-based Data Masking provides a consistent level of security across the enterprise without interfering with business operations and greatly simplifies data security management chores.

**Step 5: Deployment**

Risk-Adjusted data protection enables enterprises to stage their security roll-out. Focus your initial efforts on hardening the areas that handle critical data and are a high-risk target for attacks. Then continue to work your way down the risk-prioritized list, securing less critical data and systems with appropriate levels of protection.

Security is an ongoing process, not a series of events. The level of protection required by data may change according to how it is being collected, transmitted, used and stored. Reevaluate risk levels annually and on an as-needed basis if business processes change.

**Step 6: Crunch the Numbers**

Risk-adjusted data security plans are cost effective. Among the typical benefits of a risk-adjusted plan is the elimination of the all-too-common and costly triage security model which is ineffective whether you’re triaging based on compliance needs or the security threat of the moment. Replacing triage with a well thought-out logical plan that takes into account long-range costs and benefits enables enterprises to target their budgets toward addressing the most critical issues.

By switching focus to a holistic view rather than the all too common security silo methodology, an enterprise will also naturally move away from deploying a series of point solutions at each protection point, which results in redundant costs, invariably leaves holes in the process, and introduces complexity that will ultimately cause significant and costly rework.

Additionally, an understanding of where data resides usually results in a project to reduce the number of places where sensitive data is stored. Once the number of protection points has been reduced, a project to encrypt the remaining sensitive data with a comprehensive data protection solution provides the best protection while also giving the business the flexibility it needs.
Chapter Education Update

James Ambrosini  
First Vice President and Education Committee Chairman  
ISACA® New York Metro Chapter

This year, we have completely re-vamped our education program, offering more courses, on more ‘hot’ topics than ever before. Our fall schedule includes classes on Privacy, SAP, Virtualization, Data Security and Auditing Business Continuity. We also had our chapter’s first webinar on Spreadsheets and Fraud, with over 100 registered members attending.

Additionally, every Fall and Spring, we will have a featured course. This Fall, we are hosting a seminar on Enterprise Governance of IT. We are flying in a world-renowned expert in the field, Dr Wim Van Grembergen from University of Antwerp, to teach this course. The focus of this seminar will be on how IT Governance projects can be measured and how IT’s business contribution can be measured and evaluated. Dr Van Grembergen will also discuss his latest research on IT governance and will discuss case studies from his book, “Enterprise Governance of IT - Achieving Strategic Alignment and Value”.

We decided on Governance for our featured class since this topic is a focus area of ISACA® International. But more importantly, we, as IT auditors and Security professionals, need to be able to assess IT governance and offer recommendations on improving it at our organizations.

As you can see, there’s something for everyone when it comes to our chapter’s education offering. Not only are these classes taught by experts, but it’s at prices you won’t find anywhere else. This gives our members tremendous value while providing relevant courses of the highest quality. There are a few classes left for this calendar year and we have already started planning our Spring schedule. So stay tuned, and check our website www.isacany.net frequently for course offerings and updates.

Chapter CISA Exam Certification Review

Dustin Bradley  
Board of Directors, Certification Coordinator  
ISACA® NY Metro Chapter

The CISA® Exam Review course will be held at St. John’s University from Nov. 14 - December 5 (Four consecutive Saturdays, 9 AM – 5 PM). The CGEIT® and CISM® review courses were cancelled due to low registration.

At the 2009 Annual Chapter Gala and Wasserman Award Dinner, Norman Levine (left) presented Patrick Grant (right), 2007-2009 Chapter President, with a certificate of appreciation from the chapter for his hard work and dedication throughout the years. Thanks Patrick!!
Education Update

Upcoming ISACA® International Seminars and Conferences at a Glance

Faye Reece
Metroline Staff Writer
ISACA® New York Metro Chapter

Here are some ISACA® educational events happening around the Globe.

CANADA
Business Continuity Management & Disaster Recovery Planning, 19-23 October, 09
Delta Hotel, 350 St. Mary Avenue, Winnipeg, R3C 3J2

A presentation on key steps involved in the BCM and DRP processes. Areas of discussion include program planning, business impact analysis, determining recovery strategy, developing business continuity plans, testing and implementing business continuity, maintaining the plans and creating a culture of continuity, technology, data backup alternatives, communications, configurations, alternate site deployment, hardware and software licensing and inventory, maintaining the plans and keeping them current with business change, restoration and recovery. Visit www.isaca-vancouver.org

SPAIN
National Congress of Audit, Security and Government, 22–23 October, 09
Hotel Olympia, Alboraya – Valencia

This is the annual "Rafael Bernal Lecture Series" which brings together eminent personalities from the corporate, institutional and teaching fields related to Information Technology and Communications. The presentation will focus on providing knowledge in areas such as methodologies, best practices, and procedures, standards in the areas of Audit, Control and Governance of Information Technology. http://congreso.isacavalencia.org

UNITED STATES
ISACA® Training Week, 2-6 November, 09
55 Cyril Magnin Street, Market at Fifth, San Francisco, CA 94102

This ISACA® Training Week event will cover three courses: Fundamentals of IT Assurance and Audit, Information Security Management, and COBIT®: Strategies for Implementing IT Governance. These courses are designed to provide the tools you need to maintain, update, and upgrade your skills, and to continue your professional development. The courses will explore aspects of IT assurance, audit, governance and security. See complete training details at www.isaca.org/trainingweek.

e-Learning
GRC and IT: Frameworks, Controls and Implementations Virtual Tradeshow, 3 November, 09
This free one-day virtual seminar is presented by ISACA and SearchCompliance.com. The seminar will focus on demystifying GRC and IT frameworks. Get practical advice for choosing and managing effective GRC frameworks, learn how to create an effective IT governance structure in your organization and simultaneously manage risk and hear from senior GRC expert speakers Brian Banier, Eric Holmquist and Urs Fischer as they break down the complexities of GRC and provide best practices for implementing cost-saving controls and frameworks http://events.techtarget.com/GRC.

Visit http://www.isaca.org/elearning for more Webcasts/e-Symposia learning opportunities.
IT Governance Update

IT Governance Education and Professional Development

Emma Arakelyan
Board of Directors, IT Governance Sub-Committee Chairwoman
ISACA® New York Metro Chapter

The ISACA® New York Metropolitan Chapter IT Governance team is proactively responding to both the needs of the market and our members' need for education and professional development. ISACA® New York Metropolitan Chapter IT Governance committee has planned several series of educational events to cover IT governance measurement, value of IT controls, and maximize performance of the IT investment.

We are organizing a series of IT governance seminars with distinguished professors from the U.S. and other countries as well as industry experts and professionals from top companies.

Fraud, An Evolving Enterprise Risk

A very well attended and successful webinar was held on September 29th by Eric Perry, Vice President, Prodiance Corporation and Michael Hoye, Subject Matter Expert, Jefferson Wells International. The webinar covered the risks involved with uncontrolled EUCs, common spreadsheet fraud scenarios, best practices for preventing and detecting spreadsheet fraud, and highlighted a technology available to help organizations improve transparency and effectively mitigate fraud-related risk. We will be planning additional webinars and one day courses on this subject early in 2010.

Governance Measurement

One of the unique training opportunities is the IT governance measurement seminar for enterprise leaders and management of IT, compliance, audit and risk. A distinguished professor from Belgium, well known University of Antwerp Prof. Dr. Wim Van Grembergen is invited to New York City to run the session. He will be conducting the two-day seminar with Emma Arakelyan from Ernst & Young and the ISACA® New York Metropolitan Chapter Board of Directors. All attendees will receive a complimentary gift from the ISACA® New York Metropolitan Chapter: Prof. Dr. Van Grembergen's 2009 book "Enterprise Governance of IT. Achieving Strategic Alignment and Value".

The following items are the topics that will be covered in theory and real life case studies: maturity measurement of EGIT practices, concepts of the IT Balanced Scorecard (BSC), building a BSC for the IT department and application of the BSC concepts in COBIT® 4.1.

Value of IT

IT value and IT governance continue to be top priorities for any industry and corporation. We are planning to offer a seminar on this topic early in 2010 by Nikhil Lele and Bob Reinhold from Ernst & Young’s Strategic technology advisory, to cover the following key areas based on the real life case study:

- Discover the processes, activities and tools that are required to control and maximize performance across each key phase of the IT investment value chain
- Understanding and quantifying the value delivered by an IT project
- Understanding how can Demand, Execution, Process Portfolio, and Value Management help determine the value of an IT investment.
Editorials

The Value of Mentorship

James Ambrosini
First Vice President
ISACA® New York Metro Chapter

Some of my fondest memories of high school and college were competing in various athletic events. I’ve often said that I wouldn’t be the person I am today if it were not for the discipline, goal setting, and knowing the value of hard work that comes with competitive sports. I could take it a step further and say that whatever fulfillment I got from these activities would not have been possible without a dedicated coach showing me the way.

I look at sports and business as two very similar domains. We are all, or should be, trying to do our best, increase our skills and obtain some sort of enrichment through our work. Also, you can’t have a winning team without a good coach and I firmly believe that the same holds true for business.

Yet I’ve often felt there’s a tremendous lack of coaching and mentoring at most companies. People are busier than ever and working harder just to keep their job, so finding the time to take someone under their wing may seem unthinkable. But, I would say that it’s during these tough times when the right mentor can make all the difference.

Imagine two teams (whether sports teams or within your department). One team has people dedicated to making sure their ‘players’ are properly trained, have acclimated to the culture, and are all working to achieve both personal goals and the goals of top management. The other team doesn’t really make that much of an investment in their people. These team members learn through osmosis, or only by working on things and adjusting through trial and error. Which team would you put your money on?

Seasoned IT Audit and Security professionals have a duty to help the younger or inexperienced employees through their career. This could take many forms but just being there to help guide them and offering proactive insight and instruction is a great place to start. You’ll do more than just create a more competent worker – you’re helping to build a high-performance team that’s willing to give their best to you.

Networking 101

Debbie Morales
Metroline Staff Writer
ISACA® New York Metro Chapter

What is networking? It is the ongoing process of developing contacts through the workplace, personal relationships (friends, family), college alumni groups, professional associations, etc. Networking can help develop new business opportunities, keep you up on trends in your industry, and help you stay aware of potential career opportunities. It is part of our every day lives. We network when we have lunch with co-workers, give referrals for doctors, and when we share information about vacations. You do not have to be selling something, job hunting, or even have an objective in mind when developing a particular contact – you never know when a contact might be beneficial to have in the future.

How can I find a job through networking? Odds are you will not be able to tell which contacts could be helpful in identifying employment in the future – so network as much as possible. Make sure you discuss your career and your professional accomplishments and get this information from your contact. Make sure you get business cards, and follow-up with your contacts if you believe there is an opportunity for employment that you are interested in. Don’t limit yourself to who you contact – you might be surprised at some of the connections you may find.

What can I do to be successful at networking? Try to find a mentor to help support and encourage you through networking.
Networking 101

and your career. Your company may even encourage you to establish a mentoring relationship with a co-worker. Leverage this relationship to expand your network. Find a friend or co-worker to be your “network buddy” and attend networking events together. By attending events together, you will motivate each other and be able to share your contacts. Remember to bring your business cards to all business association meetings.

Utilize the internet by joining networking groups like LinkedIn and Facebook, to keep in contact with people. (Consider creating a ‘professional’ Facebook page separate from your personal page, to avoid privacy issues and inadvertently communicating information that could tarnish your professional image.) Contacts made through these sites can lead to new clients and referrals. Most importantly, proactively build your relationships. Each new connection can provide you with valuable information and advice that can help further your career.

I have a job. Why should I network? Networking isn’t just about job searching – it’s an investment in your career. By networking with others, you are tapping into a wealth of knowledge and expertise of others, and sharing your own knowledge and expertise. In the current economic environment, no one is completely secure in their jobs and to deprive yourself of a good network of people now could mean more difficulty finding a job in the future, should you become unemployed. With a good network, you can find what you need within a couple of phone calls rather than sending out random emails to people you don’t know, buying leads or industry lists, or sifting through resumes for the right candidate. Putting time into developing your network can save you time when you need to get things done or when you need more information. When your networking contacts hear of new opportunities, either within their company or at another company, they will think of you. By getting connected with decision makers, whether or not they have a current opening or whether or not you are looking for one, they get to know you without the pressure of an interview. They may consider you before opening and advertising a new position. Managers tend to prefer hiring people they know rather than interviewing strangers. In fact, over 60% of all jobs are found by networking. Start networking today!

2009 June Gala PHOTO OPS!

On June 15, 2009 the New York Metropolitan Chapter of ISACA® held annual June Gala and Wasserman Award Dinner. Chapter members and their guests are pictured above aboard the Luxury All Glass Yacht Bateaux during a sunset dinner cruise down the Hudson River to the Statue of Liberty.

Above, Deepak Sarup (left) accepts the 2009 Wasserman Award from Peter Wild (right), Long-Range Planning Committee Chairman, at the annual June Gala and Wasserman Award Dinner on June 15, 2009 aboard the Yacht Bateaux.
ISACA® Career Centre and COBIT® Update

Jenny Urena
Metroline Staff Writer
ISACA® New York Metro Chapter

ISACA® Career Center

More than just a job board, the Career Center provides job seekers with a myriad of tools to help them start or continue a career in IT Audit and Information Security. Members can create a professional profile, build their resume and search for jobs even from other job boards. The site also includes job application preview feature, searchable portfolio option and tighter confidentiality.

Freelancers are able to post a job, free of charge, by selecting “freelancer” as a job type while registering as an employer.

Need career advice? Now you can find it at the ISACA® Career Center. Members, both recruiters and job seekers, can take advantage of exclusive tips from the internationally-known career strategist Peter Weddle.

For jobs in the NY Metro area, visit our chapter website at http://www.isacany.net.

Upcoming Release of COBIT® Process Maturity Tool

The COBIT® Process Maturity Tool is a diagnostic and modeling tool that aids management in assessing the maturity of its IT governance capabilities. The tool is developed in MS Excel and it contains three main modules:

1. **Scoping** – helps identify the most important objectives in an IT organization and establish a target maturity level for both interim and desired states. As a result, management would be able to see processes with different priorities in terms of importance and timing.

2. **Analysis** – provides a series of diagnostic questions/comments based on the COBIT maturity model attributes, and a weighing factor that can be adjusted to properly accentuate those questions/comments that are relevant to the overall maturity of the process. Based on these factors, a maturity level is then calculated.

3. **Reporting** – compares the assessed maturity level of each process with the established target level to identify gaps. Additionally, it displays a graphical analysis of the weighted gaps and the maturity outcomes by process.

The tool is now available in the Implementation Guide Tool Kit. For more information visit www.isaca.org/cobit/cobitfocusnewsletter or download a copy of the Implementation Guide Tool Kit free of charge for ISACA® members.

ISACA® eLibrary / Bookstore Update

Members now have exclusive on-demand access to the ISACA® eLibrary. The eLibrary contains virtually all of ISACA® / ITGI® published books as well as 250 additional titles, all at no extra charge.

Titles recently added to the ISACA® eLibrary include:

- Information Security Governance: Guidance for Information Security Managers, by W. Krag Brotby, IT Governance Institute
- Enterprise Value: Governance of IT Investments: Getting Starting with Value Management, by IT Governance Institute
- IS Standards and Summary of Guidelines and Procedures for Auditing and Control Professionals, by ISACA

Visit www.isaca.org/bookstore to view a listing of books on sale now.
THANK YOU TO THE CONTRIBUTORS TO the Metro Line in 2009! Your efforts and support are appreciated!

ISACA® New York Metropolitan Chapter Newsletter Committee

Danielle Henry
Editor-In-Chief

James Ambrosini
Board Newsletter Committee Chairman

Michelle Syskrot
Photo and Copy Editor

Debbie Morales
Staff Writer

Faye Reece
Staff Writer

Jenny Urena
Staff Writer

Contact the NY Metro Chapter
ISACA® NY Metropolitan Chapter
954 Lexington Avenue #525
New York, NY 10021-5013 USA
Phone: 646.881.4696
www.isacany.net

Let us know your thoughts, comments and questions about our Chapter and Chapter activities. Send your messages to membership@isacany.org.

Contact ISACA® International
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
www.isaca.org

Chapter Board of Directors

2009-2011 Officers

Felix Ramirez
Chapter President
Felix.Ramirez@isacany.org

James Ambrosini
First Vice President
James.Ambrosini@isacany.org

Alexander Josephite
Second Vice President
Alexander.Josephite@isacany.org

Norman Levine
Treasurer
Norman.Levine@isacany.org

James Powers
Corresponding Secretary
James.Powers@isacany.org

Nigel James
Recording Secretary
Nigel.James@isacany.org

2009-2010 Directors

Alexander Abramov
Manisha Agarwal
Emma Arakelyan
Dustin N. Bradley
Kevin Fuller
Patrick Grant*
Yonique Malbranche
David Kipin*
Patricia Martin
Robert May*
Andrew T. Robinson
Raisa Serebrenik
Kwongmei To (May)
Chris Westerman
Richard Ziegler

* Past President