**CHAPTER NEWSLETTER**

August 2009

ISACA®
Serving IT Governance Professionals
**Rhode Island Chapter**

## Join us for our September Meeting!

Our September meeting features a discussion of both IT Governance and SAS-70s. Ted Wolff, Senior Manager, Vanguard will present 'Building IT Governance into the Audit Plan.' Ted presented this training session at ISACA's 2009 North American CACS Conference. Additionally, Tom Tuniewicz, Senior Manager – IT Assurance Services, Wolf and Company will discuss 'The Role of SAS-70s in IT Governance.'

This meeting is scheduled for the morning of Friday September 18 at Amica Insurance in Lincoln, RI. Please see our website for additional details and registration.

## CONTENTS



## CONTACT INFORMATION

RI Chapter website:
www.isaca-ri.org

RI Chapter webmaster:
webmaster@isaca-ri.org

RI Chapter President:
president@isaca-ri.org

RI Chapter General Information:
info@isaca-ri.org

ISACA Global website:
www.isaca.org

## PRESIDENT'S MESSAGE

Dear Colleagues:

I am honored to assume Presidency of this chapter for 2009-2011. I would like to take this opportunity to thank Camille Rigney, our outgoing President, for her commitment to organizing this chapter. The success of our chapter since its formation in 2007 has been due to Camille's vision and leadership, the dedication of all of our Board Members, and the active participation of our members in chapter events. Please read the interview with Camille that follows.

Our primary goals for the upcoming year will be to:

- Continue offering local, low-cost, quality training events that will cover IT audit, security, and governance. We will offer sessions that are of interest to all of our members. We use the feedback that you provide to select topics and speakers so please continue to forward your suggestions for future topics to **info@isaca-ri.org**.
- Continue enhancing our website. Our website serves as a primary method of communicating our local chapter events as well as ISACA International events, member benefits, and announcements.
- Strengthen our ties with local colleges and universities in an effort to raise awareness of our profession and the rewards that it has to offer.

Our Annual General Meeting and training session on June 23rd was very successful! We received raving reviews of our presenter Stu Henderson for his discussion of security and controls for CICS and DB2. Stu has offered a discount of 15% to chapter members who attend one of his training sessions through Spring, 2010. Please visit http://www.stuhenderson.com.

Mark your calendars for our first training event of the 2009-2010 season**.** On Friday September 18th, we will have two presentations on IT Governance. Our Program & Education Committee is finalizing plans for an October presentation on the Payment Card Industry's Data Security Standard. Announcements of additional events will be forthcoming soon. Please continue to visit our website for current information.

I look forward to the opportunity to work with the Chapter's board and serve all of you.

Pauline G. Lamantia, CISA
ISACA-RI President, 2009-2011

### Chapter Annual General Meeting June 23, 2009

Camille Rigney, President 2007-2009, accepting a small parting gift for her dedication and support to the chapter.

## VOLUNTEER OPPORTUNITIES

Earn up to 10 CPE annually by volunteering to serve your chapter and benefit from the many opportunities for leadership growth and professional development that volunteerism offers. Send an email to president@isaca-ri.org if you are interested in assisting in any of the following areas:

***Newsletter***
***Marketing***
***Certification***

## CERTIFICATION CORNER

The CISA® was named the Best Professional Certification Program by SC Magazine in April. The CISM® was named a finalist. Read ISACA's Press_release for details.

Registration for the December 2009 exams is now open. The early registration deadline is August 19 and the final registration deadline is September 23. To view additional exam registration details visit www.isaca.org/CISAboi, www.isaca.org/CISMboi, or www.isaca.org/CGEIRboi

Exam preparation materials offered through ISACA International at www.isaca.org include:

***CISA***

- The CISA® on-line review course provides a choice of six modules covering the scope of information systems audit and review activity. The modules can be purchased separately or as a bundle. ISACA members receive a discount. Additionally, by specifying the code ISACA197, you will earn an additional 30 days on your course subscription length.
- CISA® Review Manual
- CISA® Review Questions, Answers & Explanations Manual
- A full list of CISA publications is available at www.isaca.org/cisabooks.

***CISM***

- CISM® Review Manual is a comprehensive reference guide. The 2009 edition has been developed to help the candidate understand essential concepts and is organized to facility study by job practice areas.
- CISM® Review Questions, Answers & Explanation Manual 2009 edition.
- CISM® Practice Question Database v9.
- A full list of CISM publications is available at www.isaca.org/cismbooks.

***CGEIT***

- ISACA is developing a Certified in the Governance of Enterprise IT® (CGEIT®) review manual to assist candidates in preparing for the CGEIT exam. The *CGEIT® Review Manual* is scheduled to be completed in late 2009.
- Reference material for the CGEIT exam may be obtained at www.isaca.org/cgeitbooks and www.isaca.org/cgeitreferences.

**For questions concerning any of ISACA's certifications, please send an email to** info@isaca-ri.org.

## ISACA GLOBAL NEWS

### ISACA Adds eLibrary Member Benefits

ISACA has developed the ISACA eLibrary to provide on-demand access to a wealth of readily usable information. The ISACA eLibrary is a comprehensive collection of content from nearly all ISACA/ITGI-published books and more than 250 additional titles—all available free-of-charge as a benefit of ISACA membership. Benefits of this new feature include:

- Access to all books and the ability to browse the content immediately
- Downloads of up to five chapters per month from the available book titles
- A robust search mechanism
- A private bookshelf for the most frequently accessed book titles for each individual user
- The ability to easily purchase a book after browsing online
- Bookmarking ability of the content a user needs most
- Effortless creation of citations

Please visit www.isaca.org/elibrary.

### Conference Spotlight

***Information Security and Risk Management Conference***

*28-30 September 2009*

*Las Vegas, Nevada, USA*

Over the years, the role of the IT security professional has evolved from the key responsibility of securing an enterprise's information to today's expanded role that includes managing the associated risk. In response to this trend, ISACA created the Information Security and Risk Management Conference, an adaptation of the Network Security Conference and the Information Security Management Conference. This conference merges network security, information security management and risk management to be an all-encompassing security event. Attendees can earn up to 32 continuing professional education (CPE) hours—18 for attending the conference, and seven for each day of a workshop. For more information or to register, please visit www.isaca.org/isrmc.

***Future Conferences and Training Weeks***

Other 2009 events to keep in mind include:

- 17-21 August – ISACA Training Week, Boston, Massachusetts, USA
- 14-16 October—IT Governance, Risk and Compliance Conference, Henderson, Nevada, USA

## FREE CPEs

You can easily earn up to **52 FREE CPEs** each year to satisfy your certification requirements. Consider:

- As an ISACA® member you can earn 3 CPE credits for participating in ISACA's® e-Symposia in their entirety and completing and passing a short 10 question quiz at the end of the session. A new e-Symposium is available each month. The past 12 events are archived and available for viewing on demand. The August ISACA® e-Symposium is scheduled for Tuesday August 25. For more information please visit www.isaca.org/elearning.
- Earn 1 CPE for each of the 6 ISACA® Journals by completing the Journal quizzes.
- Earn 10 CPE by volunteering to serve your chapter. Send an email to president@isaca-ri.org

.

**ISACA-RI would like to acknowledge the following organizations for having provided free seminar and meeting space—AMICA, Citizens Bank, and FM Global. The chapter appreciates their support.**

## Interview with Camille R. Rigney, ISACA-RI President 2007-2009

Q. **How did you first get involved in ISACA?**

A. When I returned to the workplace in 1985 after an 11-year work hiatus to raise my children, my employer (Woonsocket Institution for Savings) kindly and frequently sent me to N.E. Chapter EDPAA (now ISACA) meetings to build my technical knowledge base. Three years later, when I joined the audit staff at Brown University, several of my college/university IT Audit colleagues in the Greater Boston area held positions on the N.E. Chapter Board and encouraged me to join their volunteer efforts for ISACA-NE by serving on the Research Committee, which I did for several years. During this period I attended monthly board meetings and became familiar with the ins and outs of chapter administration. Once my personal calendar freed up a bit, I moved into the officer track and became president of ISACA-NE in 2002.

Camille with Int'l President Lynne Lawton

Q. **What were your thoughts and vision for creating the RI Chapter of ISACA?**

A. More times than I can count, I arose at 4 am and by 5 am was on the road or on a train to Boston for a 7:30 ISACA-NE board meeting or for an 8 am ISACA-NE-sponsored training event. (I don't need to explain SE Expressway traffic during rush hour.) Since the IIA and the CFEA had local chapters for as long as I could remember, it was always in the back of my mind that their members were lucky in that they didn't have to endure a frustrating, unpredictable commute to Boston to obtain timely, relevant training. During my vice presidency and presidency of ISACA-NE, I learned a great deal about ISACA-NE's demographics. I was surprised to learn that as the chapter's membership was approaching 1,000 members, at best, only 50-100 members actually attended the meetings/training. That meant that at any given event, at least 90% of the membership was not being served. Most members--particularly in Maine, New Hampshire, and Vermont--cited the time and cost of travel to the Greater Boston area as the prime deterrent to attending chapter events. However, business consolidations and down-sizing in response to the commercialization of the Internet and the resulting globalization of business presented financial challenges to ISACA-NE members as their employers' training budgets began shrinking and/or disappearing. At that point, it became very clear that Rhode Islanders would benefit greatly from a local chapter that provided reasonably priced, viable training opportunities within an easy drive of their homes and offices.

Q. **What is the most important benefit you received from volunteering both with the New England and RI Chapters?**

A. I always felt that professional association volunteerism 'rounded me out' as a professional. It offered me opportunities beyond what my employer could provide, e.g., opportunities to enhance my leadership, managerial, analytical, project management, and problem management skill sets; opportunities to be directly involved in the planning, administration, and teaching of technical training; opportunities to meet and interact with an international network of peer chapter officers; and opportunities to have a voice, to be a conduit for addressing the on-going, often-changing technical needs of our IT audit, security, and control community.

Q. **Now that you are retired from Brown University and achieved your goal of creating the RI Chapter, what's next?**

A. First and foremost, I am totally enjoying being a grandmother. Beyond that, my husband and I have been steadily ticking off the travel destinations in our bucket-list. The next big trip will be an Alaskan cruise, followed by a train ride through the Canadian Rockies. I'm also resuming drawing and painting (pre-children, I was a commercial artist and had my own studio). I hope to integrate both digital photography and graphics into my pieces (neither technique was available in my early years).

Q. **Do you have any final thoughts that you would like to share with our membership and board?**

A. It sounds corny, but volunteering for ISACA has always made me feel good just to be involved. I took great pride in being able to give back to my profession, and it was easy to see the fruits of my labor. There always was a fun and engaging group of fellow volunteers on the boards on which I served, there always was a great group of professional colleagues at ISACA International who mentored us, and there always were many opportunities for personal and professional growth. It was a win-win situation in my life's journey.

# Portable Device Use Growing: Secure the Data Before it Disappears

**Matthew J. Putvinski, CPA, CISA, CISSP**

Let's assume that best practices in data security and your organization's policies are one in the same. Management has determined which portable devices are acceptable for use within the network and an incident response policy directs the organization's activities in regards to data loss or breach. The employees are aware of the risk posed by these devices and have taken the necessary steps to adjust behavior. Everything has been covered, right? Well, there's just one more thing… what technologies do you use to keep the data safe from the inappropriate use of portable devices?

While there appears to be an infinite number of tools that any organization can use to mitigate the risks of data breaches in portable devices, this piece will focus on the two methods that are considered to be cost efficient and significantly effective to protect the organization: encryption of the data and keeping unauthorized portable devices from connecting to the network in the first place.

It wasn't long ago when the thought of using encryption on portable devices such as laptops and Personal Digital Assistants (PDAs) was an expensive and often very complicated task. Challenges were many as organizations were in need of the technical employees that could implement, support and recover encryption keys. At that time, utilizing encryption in any way was unusual and it was often de facto practice to deal with the inherent risk of losing the data. The world has changed. The increase in identity theft and highly public data leaks1 has adjusted the public's expectations regarding protection of sensitive information. Fueled by these past indiscretions2 as well as the availability of so many different encryption options, there is very little excuse for not instituting practices to protect data.

Fortunately, as best practices require mandatory data encryption, the number of encryption solution companies has risen tremendously and these companies are selling tools that require little to no training to maintain. This frees an organization from having to hire specialists to fill the role. Whether it is third-party encryption software that is loaded on the portable device or it's the encryption that comes with software, there should be no reason why a device potentially containing confidential information is not using encryption.

As for regulatory scrutiny, unfortunately, guidelines are quiet on any specific requirements regarding this matter. Therefore it is up to the organization to wade thru the mass of encryption vendors to find the solution that works best within the network and has the most cost benefits. When selecting an encryption package, consider the following:

1) **Strength of the Algorithm** – Built inside each of the encryption methods is an algorithm. It is a procedure that spells out how to solve a procedure in a finite number of steps. The more complicated the algorithm, the greater number of steps required to solve the problem, and in this case, access the data. The benefit of using a stronger algorithm is that it becomes increasingly difficult for an unauthorized user to access the lost or stolen data. The downside is that the stronger the method, the more computing resources used, potentially causing significant slowdowns in other work the device might be performing. The organization should select a method that will offer reasonable security but not be so hard to use, or such a drain on systems, that users will avoid the use of encryption and create even greater risk to the organization.

2) **Determine what gets encrypted** – While the costs and maintenance of encryption is improving, there is still a need to determine exactly which devices need some level of encryption. This determination can be made easier through the use of a risk assessment which identifies exactly where confidential information is stored. Once the assessment is complete, it provides a better focus on what to encrypt in line with the organization's policies. If there are a small number of portable devices in your network you may make the decision to encrypt everything rather than trying to go against the tide and justify why encryption should not be implemented at all.

Perhaps the most self explanatory opportunity for protecting data is the restriction of access in the use of portable devices and on what parts of the network the device can be connected. In most cases, the devices use a USB port and the easiest way to restrict the device is to disallow the use of this port across the entire network. The problem is that not only are the computer mouse and keyboard now starting to use this port, there are other devices, such as cameras and external drives that have a business purpose and could be detrimental if restricted unilaterally. To mitigate the restriction there are tools that identify the type of device using the USB port and then check against an approved list of users to determine if access to the network should be granted.

Increasingly, there are also measures built into the portable devices themselves to increase their effectiveness at protecting data. One example is a USB drive that is designed similar to a combination lock. These devices require a security code to be keyed into them before they can be accessed by a computer. Using the physical buttons on the drive, if the wrong key is entered the PC will not register the portable device's existence. In addition, the device will automatically lock itself if removed from the PC, or if the PC is shut down, eliminating the possibility that someone will forget to enable protection for the information on the device. Another example is a USB drive that requires the scanned finger print from an authorized user before the drive can be accessed. The encryption application runs entirely from the USB drive, eliminating the need to install and configure any software.

In the end, data encryption is not the expensive and complicated process that it once was. As the security and business environments change, vendors of technologies and security products have provided the tools to simplify the process and make it more cost effective for even small organizations. Engaging in sound data security can not only keep your organization from an embarrassing public relations event, but also protects your employees from accidentally releasing sensitive data.

For further information on the specific devices and tools discussed in this article, please contact Matt Putvinski at 617-428-5479 or mputvinski@wolfandco.com

1 - http://www.privacyrights.org/ar/ChronDataBreaches.htm
2 - "TJX data theft spawns million-dollar crime spree," Paul McNamara, Network World, 6/12/2007 on-line version.

*Reprinted with permission from Wolf & Company, P.C.*

## ISACA-RI's Newly Elected 2009-2011 Board

| NAME | BOARD POSITION |
|---|---|
| Pauline G. Lamantia | President |
| Kevan Riley | Vice President |
| William C. Soares | Treasurer |
| Ronald J. Roy | Secretary |
| Colleen Sullivan | Programs & Education Co-Director |
| Nitesh Kumar | Programs & Education Co-Director; Web Master |
| William Nowik | Programs & Education Co-Director |
| Susan Baumes | Programs & Education Co-Director |
| Tom Laliberte | Programs & Education Co-Director |
| Donald Borsay | Marketing & Communications Director |
| Barbara Norris | Academic Relations Director |
| Salomon Frangieh | Audit Chair |
| Susan Strakosch | Standards, Bylaws, & Research Chair |
| Deepika Chandarana | Membership Director |
| Tim Schmutzler | Web Master |
| Camille R. Rigney | Past President |