

It is always wonderful to have an opportunity to share about our profession, earn continuing educational credit, and network with fellow professionals at our regular luncheon meetings. Once again welcome to our April luncheon at the Brio Tuscan, Polaris, with Mr. Mick Douglas from OCLC presenting on: **COOPERATIVE AUDITING: BREAKING THE "YOU VS. THEM" MOLD.**

We hope that you will find this presentation to be both insightful and of interest to you.

We appreciate your attendance and would like to encourage you to invite your colleagues and business partners. You also earn one credit hour towards your CPE.

In this newsletter you will find information on this month's presentation, a recap on the February meeting, and other key announcements. In addition, you will find our member spotlight and information on programs and activities sponsored by ISACA international.

## CONTENTS

CHAPTER NEWS.....	1-2
PRESIDENT'S MESSAGE.....	2
INFORMATION & COMMUNICATION.....	3-4
MEMBERSHIP SPOTLIGHT.....	5
TECHINICAL EDUCATION.....	6-7

## COOPERATIVE AUDITING: BREAKING THE "YOU VS. THEM" MOLD

All too often, auditing is seen as a high stakes showdown. The techs being audited don't want to be "caught", the sponsor wants to "get away with" as much as possible (they think it's cheaper that way). What if you could "socially engineer" the entire audit process such that audits are seen in a positive light by everyone? The SANS 507 auditing class has a section on this very topic. This presentation is a condensed version of this section. After attending, you should be able to implement changes in your day-to-day dealings with your coworkers and clients to help smooth the rougher edges and make everyone view auditing and the audit

process in a more positive light.

### PRESENTER'S BIO:

Even when his job title indicated otherwise, Mick Douglas has been doing information security work for over ten years. He received a bachelors degree in Communications from the Ohio State University and holds the CISSP, GCIH and GSNA certifications. He currently works at OCLC as the Senior Systems Engineer for Information Security where he acts as an auditor and analyst. In his spare time he hacks with the PaulDotCom crew and is a recent addition to the weekly podcast.

## WHERE & WHEN

Brio Tuscan Grill, 1500 Polaris Parkway, Columbus, OH 43240 (670 to 71 N, 71 N to the Polaris Pkwy Exit (exit 121), turn left on Polaris Pkwy, turn right into the Polaris Mall, park and enter at Brio). The meeting starts at 11:15 a.m. with an opportunity for members to network. A presentation from Mr. Mick Douglas follows at 11:30 a.m. and lunch is served at 12:30 p.m.

The luncheon menu includes: Cheese Ravioli, Brio Chopped Salad, Chicken Fra Diavolo, Grilled Salmon with Citrus Pesto, Crispy Potatoes with fresh Rosemary, Tiramisu, and Cheesecake

We are always highlighting our local talent, i.e. our membership in the newsletter. Please feel free to use this post and submit articles, achievements, industry recognition, life, work, etc. Enjoy your reading!

## RESERVATIONS

Please make your luncheon reservation via our web site at <http://www.isaca-centralohio.org/meeting.cfm> before the deadline April 06, 2009 at noon. For your convenience, the chapter currently accepts Paypal, Cash, and Checks. The cost for the luncheon is \$20 for Members, \$30 for Non-Members, and \$5 for Students. Please note that ISSA and IIA will be granted membership price.

### Editorial:

We would like to thank you for taking your time to read our chapter newsletter. Please feel free to send any comments or suggestions you may have for the newsletter or the chapter in general to us at: [jothamn@gmail.com](mailto:jothamn@gmail.com)

Thanks - Jotham Nyamari

## CHAPTER NEWS

### PRESIDENT'S MESSAGE



Networking has become more important these days. I'm not talking about the routers, switches, cables and hardware associated with electronic communications, but the professional and social networking that involves who you know and how you know them. In these tough economic times it is well known that most jobs are obtained through personal contacts.

A strong network is built over many years. The strength and function of networking involves vouching. It involves our relationship to others and giving personal assurance and testimony. Networking is the antithesis of "guilt by association". It is interesting to see how quickly politicians try to break the network between themselves with their "associates" when the associate has negative exposure.

As some of you know, I come from a very large family. My parents had 11 children in 10 years (two sets of twins for those of you questioning the math); ten boys and one girl. I learned at an early age that people associate with me the characteristics of my family. Since some of my brothers were great in sports, people expected I would be great in sports. Obviously, that expectation was

and Communication & Trust. As IT Governance professionals, Mr. Parkes observes that our the challenge is to continuously work to create a sustainable Corporate Governance process. For example, through monitoring, where the IT Auditor would advocate for CP, coordinate monitoring activities, and perform Corporate Governance audits. Also as a

met with disappointment! So too it is with our social and professional networks, people transfer characteristics between people who are associated. This is the basic logic of networking: If person A is associated with person B, and I know person A has desirable traits, person B must also have desirable traits.

I have identified five desirable traits which are core competencies. They include:

1. Work Ethic
2. Moral Character
3. Reliability
4. Technical Competence
5. Social Graces

The absence of any of these traits can doom a professional career and none of these traits is guaranteed by professional or social association.

Networking can originate from our association with family, friends, school, church, workplace and professional organizations. At the very least, having common acquaintances can open doors.

I look forward to seeing you at our April 9<sup>th</sup> meeting.

Brian O'Brien, CISA  
President, ISACA Central Ohio Chapter

principle of good processes, CP ought to be measurable. Mike expounded on this quoting the University of Michigan Business School. "Firms with profitable investment opportunities and with more reliance on external financing have higher quality corporate governance, and firms with higher corporate governance ratings are valued higher". This quote

### PAST EVENTS: - MARCH MEETING

Mr. Michael Parkes with Crowe Howarth LLP, made a very informative, educative, and relevant presentation (especially in the current market) at our March luncheon on Corporate Governance. It is evidently true as Mike presented that Corporate Governance is key to successful organizations.



Members at the luncheon

Mike described Corporate Governance as "the systems and processes and organization has in place to protect the interest of its diverse stakeholder groups, e.g. Shareholders, employees, customer, vendors, community, etc. He also answered the question as to what, where, why, when, who, and how systems and processes direct Corporate Governance (CP) by explaining the functions and roles



Mike presenting to the chapter

of the following: The Board of Directors & Committees; Legal & Regulatory; Business Practices & Ethics; Disclosure & Transparency; Enterprise Risk Management; Monitoring;

emphasizes why CP is important. In addition, Mike stated that Corporate Governance meets legal requirements and fiduciary responsibility to investors, attracts & retains qualified people, and extra. For information on this presentation please visit our website at <http://www.isaca-centralohio.org>.

### UPCOMING EVENT: SAVE THE DATE - 3RD ANNUAL GOLF OUTING

Please mark your calendars and get you foursomes together for a great day of fun and golf.

WHEN: Friday, May 15th, 2009

WHERE: Cumberland Trail GC, Pataskala Ohio

Sponsorship Options:

1. An overall event sponsorship (1 offered at \$1000)
2. Beverage sponsorship (1 offered at \$500)
3. Prize hole sponsorship (6 offered at \$200 each)
4. Hole sponsorship (12 offered at \$100 each)

Please contact Matthew Schondel ([matthew.schondel@alliancedata.com](mailto:matthew.schondel@alliancedata.com)) for more details and availability.

---

## INFORMATION & COMMUNICATION

---

### UPCOMING EVENT: CENTRAL OHIO'S PREMIER SECURITY EVENT

Please join us on May 7th and 8th, 2009 as the Central Ohio ISACA, the Central Ohio ISSA, and the Central Ohio InfraGard chapters have joined together to promote the second annual Central Ohio InfoSec Summit. The goal of this event is to educate regional Information Security professionals and support collaboration by bringing leading speakers in the information security field together to educate the community on the latest industry trends and issues.

This Information Security Conference will provide information security professionals with the most up-to-date information, tools, trends, legislative information, products, services, and strategies for addressing information security issues. The conference will focus on key topics related to information security with presentations provided by recog-

nized experts and exhibits by some of the nation's leading organizations. The program will provide the following highlights:

- Keynote presentations from nationally renowned speakers
- Breakout sessions from top speakers in the industry covering latest trends and issues in the information security industry
- Exhibitor showcase featuring leading security technology and services vendors

Last year's Summit attracted over 200 individuals and sold out. This year, we have expanded this event to a day and a half of content covering both executive and technical tracks from some of the top speakers on information security.

#### WHEN:

May 7th and 8th, 2009.

#### WHERE:

Hyatt Regency, Columbus, Ohio.  
350 North High Street  
Columbus, OH 43215  
(614) 463-1234

#### REGISTRATION:

Registration fees include admission to all sessions, vendor showcase, evening reception, breakfast, lunch, and snacks throughout the day. Fees are defined below:

Prior to April 23rd

- \* \$50 - ISSA, ISACA, and Infragard Members
- \* \$150 - Non Members

After April 23rd

- \* \$65 - ISSA, ISACA, and Infragard Members
- \* \$165 - Non Members

For more information on this event and registration please visit the Central Ohio's Premier Security Event website at <http://www.infosecsummit.org/>

---

### UPCOMING EVENT: KENTUCKIANA CHAPTER OF ISACA FOUR DAY SEMINAR

The Kentuckiana Chapter of ISACA is proud to provide this unique four day (June 8 - 11) seminar with two corporate governance relevant topics taught by Gordon Smith, President and CEO of Canaudit, Inc. In today's environment of change and soon-to-be corporate regulatory requirements, it is essential to become savvy in application

of technical and enterprise governance. The two courses below can be taken individually, or together. Space is extremely limited and given the relevance of the topic, we expect an extremely high volume of interest. Please take advantage of our early bird prices (Through March 31st).

#### WHEN:

1. Monday, June 8 and Tuesday, June 9, 2009 Time: 8:00 am sign-in, 8:30 am to 5:00 pm
2. Wednesday, June 10 and Thursday, June 11, 2009 Time: 8:00 am sign-in, 8:30 am to 5:00 pm

#### WHERE:

Hyatt Regency, Louisville, Kentucky  
320 West Jefferson Street  
Louisville, KY 40202  
(502) 581-1234

#### REGISTRATION:

Please check out the Kentuckiana ISACA website at <http://isauditor.net/> for pricing and sign-up information. For more information, please send email to [mvincent@humana.com](mailto:mvincent@humana.com) (Michael Vincent, KY ISACA President)

#### COURSES:

##### 1 - UNDERSTANDING & PREVENTING ELECTRONIC FRAUD

When: Monday, June 8 and Tuesday, June 9, 2009 Time: 8:00 am sign-in, 8:30 am to 5:00 pm




Instructor: Gordon Smith, President and CEO of Canaudit, Inc.

##### 2 - CORPORATE INSECURITY: PILLAGING INFORMATION ASSETS, DESTROYING ESTABLISHED REPUTATIONS

When: Wednesday, June 10 and Thursday, June 11, 2009 Time: 8:00 am sign-in, 8:30 am to 5:00 pm

Instructor: Gordon Smith, President and CEO of Canaudit, Inc.

## INFORMATION & COMMUNICATION

ISACA 2009 CALENDAR OF EVENTS			
Program			
Date	6-10, April, 2009	3-7, May, 2009	18-22, May, 2009
CPE	Nashville, Tennessee, USA	Orlando, Florida, USA	Denver, Colorado, USA
Location	38	44	38



IT Audit: Challenges and Opportunities (3hrs of CPE)  
29 April 2009  
8:00am PST / 11:00am EST / 4:00pm GMT

For more information on the calendar of events please visit [www.isaca.org](http://www.isaca.org)

### CHAPTER LEADERSHIP

**PRESIDENT**

Brian O'Brien, CISA  
The Ohio State University

**VICE PRESIDENT**

Melissa Justice, CISA  
Ohio Office of Budget and Management

**TREASURER**

Mike Brady, CISA  
KPMG LLP

**SECRETARY**

Schlaine Hutchins, CISA, CISSP  
Cardinal Health

**BOARD OF DIRECTORS**

CHRIS WATSON, CISA  
SCHNEIDER DOWNS

RICH RIDEWOOD, CISA, CISSP, CPA  
B.W.C. INTERNAL AUDIT DIVISION

RYAN HOUK, CISA  
AMERICAN ELECTRIC POWER

MATT SCHONDEL, CISA, CISSP  
ALLIANCE DATA

CHUCK IMWALLE, CISA, CPA, PMP

MICHAEL KIRK, CISA, CIA

JOSEPH PONNOLY, CISM, CISA, CISSP

**COMMITTEE CHAIRS**

**ARRANGEMENTS**  
MELISSA JUSTICE, CISA  
OHIO AUDITOR OF STATE

**MEMBERSHIP**

JIM D'INNOCENZO, CISA  
THE OHIO STATE UNIVERSITY

**CISA COORDINATOR**  
CHUCK IMWALLE, CISA, CPA, PMP

**CISM COORDINATOR**  
JOSEPH PONNOLY, CISM, CISA, CISSP

**AUDIT**

GREG MASON  
STATE OF OHIO, MRDD

**EDUCATION**

RICH RIDEWOOD, CISA, CISSP, CPA  
B.W.C. INTERNAL AUDIT DIVISION

**PROGRAMS**

MICHAEL KIRK, CISA, CIA

**SOCIAL EVENT COORDINATOR**

MATT SCHONDEL, CISA, CISSP  
ALLIANCE DATA

**WEBSITE**

RYAN HOUK, CISA  
AMERICAN ELECTRIC POWER

**NEWSLETTER**

JOTHAM NYAMARI, CISA

#### QUIZ TIME

Previous Question: There are known fundamental weaknesses in perimeter controls—the bad guys are frequently a step ahead of the protection and the insider threat is now recognized to be at least as serious as the threat of attack from outside the organization. . Answer: True

Current: More mature systems development practices, as required for CMMI compliance, can facilitate Sarbanes-Oxley compliance. (The answer will be posted on the next newsletter)

MICHAEL HURD, CISA, CIA  
SENIOR AUDIT CONSULTANT, STATE AUTO INSURANCE COMPANIES

## EDUCATION

Purdue University  
B.S. Management (Accounting), 1995

I started my college career at Virginia Polytechnic Institute and State University (Va Tech). Being somewhat uncertain about whether to pursue a career in medicine (Mom's wish) or as an engineer (Dad's wish), I selected something safely in the middle - Biochemistry. I struggled through a couple of semesters of advanced calculus and other science classes before I realized somewhere during the first semester of organic chemistry that I needed to change majors. Due to a fortunate conspiracy of circumstances, I was able to change my major and also my school. My family relocated to Valparaiso, Indiana. A branch campus of Purdue University was less than 15 minutes away and main campus a little more than 90 minutes. My parents, thankful I finally decided on a new major, were ecstatic to be paying in-state tuition. My younger sister and I both attended Purdue for less than the cost of my out-of-state tuition at Va Tech. Even though my field of study was general management and accounting, most of my work experience during that time was technology related. In the months leading up to my graduation, I was determined to pursue a career that had potential for me to utilize and enhance both my accounting/business skills and also my technology skills. Fortunately, there were a number of excellent firms recruiting at Purdue for entry-level IT audit staff. I was able to transition from full-time student to full-time, job-paying professional employee within two weeks of graduation.



## WORK:

I began my career in 1995 as an Information Systems Auditor at Crowe, Chizek and Company in South Bend, Indiana. At the time, Crowe was experiencing growth through acquisition of new clients and expansion of services to existing clients and I was blessed to share this experience with a group of talented professionals. One memorable experience was when I was chosen to develop the use of microcomputer-based Generalized Audit Software in our firm, which ultimately led to a role of me training other auditors in the firm to use such tools in conducting their financial audits. We provided data acquisition and conversion support as well as first and second level application user support. There are still times when I miss wearing the telephone headset -- made me feel like I was an air traffic controller.

In 1998, I relocated to Indianapolis and accepted a Senior IT Audit Staff position at Ernst & Young. Given my background in data analysis, Ernst & Young relied on me primarily for special projects - mergers and acquisitions due diligence, litigation support, fraud investigation, and strategic process improvements. The work was challenging, fun and certainly rewarding, but the travel schedule eventually led me to find something less mobile. If you look ahead to the life section, you may notice some coincidental timing to this

shift in career focus and a desire to reduce my time away from home.

I have been working for different companies in the insurance industry here in Columbus since 1999. Currently, I am a Senior Audit Consultant and an IT Audit team of one at State Auto Insurance Companies. I am responsible for the entire suite of IT audit activities - including Sarbanes-Oxley compliance. Since we are a small Internal Audit department, I also occasionally assist with financial and operation audits. In today's employment market, I believe a broad resume of experience is a good thing to acquire and maintain. Since December 2007, I have also been working weekends practicing for a career in politics. Yes, I have been working at a horse stable learning how to sling manure. I enjoy getting outside and spending time with the horses at Hunters Creek Equestrian Center in New Albany. I consider it good training for when I purchase a horse of my own. I contemplated calling this recreation, but since I'm usually worn out by the end of my shift and I do get paid... I've decided this is work - though I enjoy it immensely.

## PROFESSIONAL ORGANIZATIONS:

I have been a member of the different chapters of ISACA for the past thirteen years. I earned the CISA certification in 1998. I am a member of the Ohio Society of CPA's, and the Columbus Chapter of the CPCU Society. I serve on the Board of the Columbus Chapter as the Good Works chairperson. In that role, I identify opportunities and coordinate chapter volunteers for community service projects throughout the year.

## RELAXATION (LIFE):

Aside from my career, I am an avid outdoorsman. I enjoy camping, hiking, hunting and fishing. I have even occasionally taken a serious hike. While visiting family in Colorado recently, we hiked Mt. Quandary (peak 14,265) and Mt. Bierstadt (peak 14,060). These peaks are a couple of Colorado's legendary 'Fourteeners.' Between hunting seasons, I enjoy recreational shooting. I learned to shoot clay targets while in college and still love to shoot trap, skeet, and sporting clays. My company also has a shotgun team. We occasionally compete against teams from other insurance companies in Central Ohio. I find it a great way to network with fellow professionals while enjoying the time outdoors. If you have never tried it, but would like to, please let me know. I'd be more than happy to take you to the range. Instruction/coaching would be free.

I'm blessed to be married to a patient woman. She's been able to tolerate my expensive hobbies for the last ten years. I hope that trend will continue. Beth is actually a better shot than I, so she doesn't often accompany me to the range. She also beats me a lot at bowling - both on the Wii and at the Palace. Despite my encouragement, she has so far refused to join the LPBA and go on tour. Maybe some day she'll change her mind and I can quit my day job and focus on my hobbies full-time. In the meantime, I can dream, enjoy her companionship, and look forward to seeing you all at monthly ISACA meetings.

Information security and risk management do not have to be difficult. But, over the last decade, people have treated them as if they were rocket science. A quick glance at the landscape, with every trade magazine in sight talking about data governance, identity access management, end point security, network access control (NAC), intrusion prevention systems (IPSs), patch management and much more, brings the point home. However, the reality is that information security and risk management are much simpler. Instead of rocket science, they are more like basic blocking and tackling (in American football), that is, doing all the little things right.

The little things are what make a good program work. Any authority could expound for days about the latest new and exciting tools, certifications, regulations, data breaches, and standards. But, there is one thing that is truly important: how each individual can make a difference in the program and get the buy-in required.

So much attention is given to what is being written these days that it seems like organizations have fallen under the spell, believing they need to do more, buy more, install more, assess more, etc. And, there appears to be no end in sight. People could accomplish so much in their careers if they would only slow down and really understand what they are doing. There is just one question to ask, and its answer reveals so much. What is the organization trying to accomplish?

Just about everything in life comes down to relationships and how well one handles them. What makes a business relationship work? In general, any solid relationship starts with knowing one's own strengths and weaknesses. In business, it is also important to know the strengths, weaknesses and history of the person or company with whom a relationship is desired.

SO HOW DOES ONE GET BUY-IN FROM THE TOP?

#### 1. GAIN KNOWLEDGE AND HISTORY

This can be illustrated by first looking at it from the point of view of chief information security officers (CISOs), chief security of-

ficers, directors of security or other similar high-level security executives (referred to as CISO in the remainder of this article) who are beginning their first day in the position. The new CISO's first act should be to learn the history of the company. Because understanding a company's history is so important to understanding its present, it creates an advantage to dig deep, interview everyone, find the longest-tenured employee and ask a lot of questions. Reading corporate reports and manuals, conducting Internet research, and taking time to observe operations are also important.

#### 2. LEARN OPERATIONS AND FUNCTIONS SECOND

Once a good grasp of the company's history has been obtained, the CISO should set out to understand what the company does best in its different areas of functioning. If the time is available, it may also be beneficial for the CISO to try to experience how things operate in other departments within the organization in which the CISO does not have direct involvement.

The CISO should:

- Learn all about the company's products and services, how things work, how things are processed, and how they are stored and transmitted
- Document everything
- Spend time with the company's various business units to truly understand how they operate

It is not yet time to learn about security, even though it will be the role's main focus; the first thing to learn about is the business itself—its size, type, culture, and even a little bit about its risk appetite and tolerance. The focus at this stage is on how this machine works and why its people really do what they do.

At this point in the investigation, IT, IT security, risk assessment and treatment, tools, regulations, and standards should not yet be in the forefront of the newly hired CISO's considerations. Remember, the agenda is not to charge into a new business, build a kingdom and do things "your way." There are too many people with overblown egos who could not care less about the business they are considering buying into; they care only about creat-

ing their own program. But, what is truly important is to ensure the confidentiality, integrity and availability of the company's greatest business assets, whatever they may be. The last thing to do is to carry a heavy hammer or have a preconceived agenda, especially early in one's role.

#### 3. CONDUCT ORGANIZATION SELF-ASSESSMENT

After investigating for a couple of weeks and gaining a fairly decent grip on the business, a company self-assessment should be conducted. The first step in this part of the process is to meet with the chairman and chief executive officer (CEO) to understand what is most important to them. After all, these are the people who are ultimately responsible for the business. The next step is to proceed to the legal department to learn about the federal, state, provincial and local laws to which the business must adhere. This requires close attention because, at the end of the day, these laws determine what the CISO really must worry about.

Human resources (HR) should be the next key step in the process. At this point, the CISO will learn about:

- On-the-job policies
- What areas of expertise the employees have and what gaps might need to be filled
- Hiring practices and termination procedures

The next step is the heart of the company: the business units. This is where the CISO will learn how revenue is generated and how far the envelope is being pushed to ensure that the bottom line is reached.

#### 4. INVESTIGATE INFORMATION TECHNOLOGY

Having made all these visits and engaged in all this exploration, it is finally time to investigate IT. Many people might find it surprising that it should take so long to arrive at this point. After all, they might ask, IT security is their job, is it not? Should IT not have been their first stop? The answer: no, their first job is actually to protect the organization's mission statement. So, the first thing that must be understood is the company and the CEO's appetite and tolerance for risk.

Now that the CISO has a full understanding of the business and its operations, it is

time to get acquainted with the IT shop. To do so, the CISO must:

- Learn how the business's assets are processed, stored and transmitted
- Dive down into the architecture at its core to really know how it all works
- Review the logical and physical aspects of all the devices that are utilized
- Conduct interviews to learn about job types and responsibilities
- Once the above information has been gathered to one's satisfaction, begin assembling one's thoughts and document everything that has been learned

So what has the CISO learned? The CISO should be sure to have discovered at least some of the following aspects of the company:

- Its business function
- Its industry
- Its size
- Its organizational structure
- The laws and regulations to which it is subject
- The IT controls it has implemented

If no form of due diligence, such as a risk assessment, has been performed before, it should be undertaken. Now, the CISO can get funding for this because an effective presentation can be made to any level of management. The CISO's homework has been done and the CISO truly knows the business, the areas of concern that the role entails, and what the business impact could be if conformance is not achieved. This is what all of the initial steps of information gathering have enabled the CISO to accomplish. Because a convincing business case for the proposal can be made, the CISO is in a position to get funding for a project that was not funded before.

The CISO has integrated himself/herself into the company and its culture

and, therefore, understands the areas that should be of concern to IT. For this reason, the proposal will have the force of persuasion. That is, the CISO can approach the CEO and describe where security measures are found to be lacking; suggest what needs to be done to implement the necessary protections; and demonstrate what the cost would be if the confidentiality, integrity or availability of company information were compromised. After such a well-thought-out and educated presentation, the CEO will be more likely to see the point and make an intelligent decision about what to do. Procuring and Completing the Assessment

Many requests for proposal (RFPs) are poorly written, do not have the necessary business backing or focus solely on IT. Focusing solely on IT results in an RFP with too limited a scope, since its writers fail to take into account the entire business environment of which their department is only a part.

In contrast, after following the points made here, the CISO is now prepared to write an RFP with intelligence, clarity and conciseness regarding the service that is expected to be delivered. Having equipped him/herself with the knowledge necessary to make this decision and having performed a company selfassessment, the CISO knows what type of assessment the company needs. The CISO is the one who knows how to minimize costs by only contracting to remedy and provide thirdparty validation for the areas that are known to be at risk.

By proceeding in this manner, the new CISO has not ruffled any feathers in his/her short tenure with the business. He/she has done nothing but gather facts and have a thirdparty validate the company's state of security.

When the third-party assessment is completed, the CISO can go back to the appropriate business departments and intelligently explain to them what security flaws were found and what potential damage could occur if they are not remedied. Because the CISO has taken the time to know the business, the laws, and the CEO's risk appetite and tolerance, he/she can make a change that is difficult to argue against. If the CISO had not begun his/her journey by first learning the company's history and making the effort to integrate into its culture, he/she would have been perceived as the bad guy, the sheriff, the security nerd who has to have things done his/her way. Now, the CISO can effectively execute the plan across the entire company, whether it involves IT, HR or any other department.

#### CONCLUSION

This approach seems so easy, why is it not used more often? The reason is that people forget for whom they are working; they forget that it is not their money they are spending and not their business they are managing.

The way to make a difference in the program is to take the time to understand the business and why it exists. These understandings form the foundation for productive business relationships. New CISOs, or any new employee for that matter, should be careful not to fall into the trap of simply trying to do things their way. The CISO has the education, the certifications and the title to make a difference. By following the steps outlined here, CISOs can be truly effective, and the business will appreciate it. Please visit [www.isaca.org](http://www.isaca.org) for more information.

#### CONTACT INFORMATION

Central Ohio ISACA Chapter  
[www.isaca-centralohio.org](http://www.isaca-centralohio.org)  
P.O. Box 151152  
Columbus, OH 43215

ISACA International  
[www.isaca.org](http://www.isaca.org)  
3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443