

## TIME TO UPDATE OUR BASIC IT AUDIT TECHNIQUES - By Gordon Smith, Canaudit, Inc.

### Databases Are the Target

What is it the hackers want? They want your data, your clients' data, and your funds. The best way to get our data and our clients' data is by stealing our databases. In the past, I have demonstrated how to defeat intrusion detection, target the databases, gain administrative rights, and steal the data. As auditors, we need to identify the databases that may be at risk. In the past few months I have performed several audits. While many databases were properly protected, test databases and "unauthorized" personal editions of databases were not. This enabled us to gain the information needed to compromise the better protected databases.

Our approach has always been to identify all databases and subject them to a basic security review. Using the results of this testing, we approach the high-risk business databases with the knowledge gained from the basic security review. As a result, databases that were thought to be secure are found to be susceptible to attack. Using the old audit approach, the stand-alone databases were considered secure. The new approach demonstrates that otherwise secure databases can be breached because of a missing control in "unimportant", "beyond scope", or otherwise ignored databases. Trust me; the hackers (external and internal) don't care about scope. They will use every trick to harvest your data or perform transactions to steal your funds.

Clearly, we need to update our audit approach so that databases are not only audited annually, but we use more aggressive techniques to complete the audit.

Continued on Page 2

### ISACA Training Week 2010

May 24-28 - Charlotte, NC

September 13-17 - Orlando, FL

October 11-15 - Indianapolis, IN

December 6-10 - Las Vegas,



ISACA® Training Week is a unique educational event, designed to provide the tools you need to maintain, update and upgrade your skills, and to continue your professional development.

### In this issue:

Time to Update Our Basic IT Audit Techniques—Databases	1
ISACA IT Risk/Reward Barometer	1
Message from the President	2
Time to Update Our Basic IT Audit Techniques—Continued	2

### VOLUME 2 SPRING 2010

#### IMPORTANT DATES

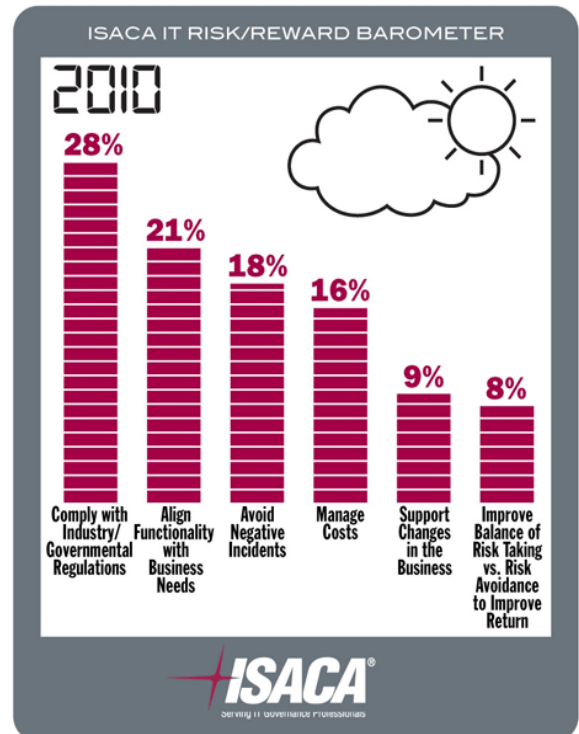
May 15 – CISA Exam Review Course – Day 1

May 29 – CISA Exam Review Course – Day 2

June 12 – CISA, CISM, CGEIT Exam

June 17 – ISACA Austin Chapter Annual Banquet

## What drives IT-related risk management?



## Message from the President - by Kim Bradley

It has been a busy few months since our last newsletter. We held our joint session with the Austin IIA Chapter in December, offered our CISA review course in November/December, and conducted a couple of our monthly chapter meetings/luncheons. The Board formalized and enhanced some of our policies in the form of adopting a Privacy Policy and a Communications Policy, which are both posted on our website.

We plan to offer another CISA review course in the May/June timeframe to help attendees prepare for the June 12, 2010 CISA exam. We had our largest turnout ever at our November/December CISA review course. It appears that those who attended had a good success rate on the exam.

Seventeen of our chapter members passed the December 2009 CISA exam and five passed the December 2009 CISM exam. Congratulations to everyone who passed the exams!

Between October 23, 2009 and February 22, 2010, eleven of our chapter members earned their CISA designations and two earned their CISM. Congratulations to all of our newly certified CISAs and CISM.

I had the opportunity to attend the Central Region PCM in November that was held in Nashville, Tennessee. The Central Region PCM is a leadership conference where the ISACA chapter leaders from our region along with representatives from ISACA International get

together to discuss challenges we face and successes we have in our chapters. Attendees included chapter leaders from Texas, Arkansas, Louisiana, Oklahoma, Ohio, Illinois, Michigan, Tennessee, Minnesota, Nebraska, Iowa and Winnipeg to name a few! It was interesting and insightful to share ideas with the other chapter leaders, and learn that most chapters face similar challenges. Our Board is working to incorporate some of the ideas gleaned during this conference.

Other attendees were impressed by some of the successes and processes I shared from our Chapter as well.

Thanks for reading our newsletter, and please let us know how our board and chapter can meet your needs. I look forward to seeing you at future chapter events!



Texas contingent at the Central Region PCM in Nashville, TN held on November 7-8, 2009 (Diane Nelson from International, on left, Kim Bradley, third from the left)

### Continued from Page 1

#### *The Network Is The Vehicle*

If the databases are the target, then the network is the vehicle. Our organizations do business in a very complex environment. In the "olden days", networks were closed. Our audit approaches changed significantly when the network was expanded to include the connectivity to the Internet. Wireless was next. We rushed to secure wireless connections that seemed to come out of nowhere. My biggest concerns remain unaudited by many organizations. These are outsourced or off-shore trading partners, application service providers, unauthorized connectivity, and web applications.

Let's start with outsourced and off-shore connectivity. When we outsource to a major firm, what security measures are in place to protect our network from their globally dispersed staff? If an organization outsources to XYZ company for new system development, do their developers have access to our "test" network? They may even have access to production data that is used in testing (I know it is a no-no but it happens all the time).

If we outsource the data center, the outsourcers definitely have access to our data and they are directly connected to our network. I am concerned that we often fail to realize that the outsourcer is not only connected to our network but to the networks of every other one of their clients. We depend on the outsourcer's network controls to isolate their other clients from our network. If another client's network is compromised, can the outsourcer identify this and protect their network and our network from the contagion in the compromised network? What if the outsourcer's core switches and firewalls are compromised - will the cockroaches infesting a polluted network be able to crawl into our network?

We often have other trading partners connected to our networks. This can be banks, health care providers, travel and reservation services, ecommerce supply chain vendors and customers, application service providers, and/or consultants. This is just a small list. Does your organization really know who is connecting and what the controls are in place for each one? Are those controls strong enough to protect your internal information superhighway and the data residing within it? Would your controls recognize unauthorized traffic on an approved connection?

I am also concerned with web applications. Last year I made a decision that Canaudit would provide a free Web Application Security Assessment with our IT Security Baseline. I decided to incorporate this \$8,000 assessment into the baseline because our clients did not understand the complex risks in web applications. Since we started offering this, we have uncovered poorly secured web applications that expose the organization to serious data leaks or even manipulation of data due to missing controls. The Web Application Security Assessment is essential to all organizations with Internet-facing applications. This is not a one-time audit. It must be re-performed at least once a year for critical web applications to ensure that changes or modifications have not degraded controls.

Unauthorized connectivity is still a major concern. I have written about inside-out, outside-in exploits for several years. Despite that, the message does not seem to be sinking in. Products like GoToMyPC and LogMeIn are great tools when used properly and with authorization, but remember that they create a pathway for a user to come into your network. Simply blocking the sites is not enough. If a consultant or employee installs the software on their laptop then brings it into your office and connects it to the network, it is likely that they or their fellow staff can log into that laptop from anywhere on this earth where there is an

Internet connection. We can assume that only approved transfers of data will occur or we can audit it to find out.

#### *General Control Audits Are Even More Important*

I know how boring general control audits can be because I have done many of them. They are also one of the most important audits because this audit sweeps through the major control points in an IT organization. Some of my concerns are that many auditors have not upgraded the general control audit program with new risks. For instance, can someone take control of the access control computer that validates badges and opens doors? In my classes, I have shown the participants how to do this. I am also concerned by those who rely on two-factor authentication but do not check to see who can bypass this control. Having RSA tokens is a great control, but if someone loses or forgets their token, do we issue a "temporary" password? If so, is it for single use or for limited duration usage such as a day or two? It is time to revamp our general control audits so that we can take a fresh look at the old issues as well as the new methods used to compromise these controls.

#### *Conclusion*

It is also time to change other areas of our basic annual IT audits. I am concerned about business continuance after a disaster or successful network penetration. Logical security and change management audits have to be upgraded to encompass new risks, some of which were covered earlier in this article. We even need to revise our approach to risk assessment so that it more closely resembles the actual risks we are facing, rather than the financial risk that has been used in the past.

*Reprinted with permission from Canaudit, Inc. All rights reserved Canaudit, Inc.*