

Canaudit Perspective

March 2010
Volume 11, Issue 2

TOPICS OF INTEREST:

- New syllabus for IT auditing to combat degrading skill sets
- Updated audit approach to identify all databases at risk
- Security of outsourced and off-shore network connections
- Routine web application audits are essential
- Inside-out, outside-in exploits continue to be a major concern
- General control audits are more important than ever

TIME TO UPGRADE OUR BASIC IT AUDIT TECHNIQUES



GORDON SMITH
Canaudit Co-Founder

In my last Canaudit Perspective, I mentioned that IT audit skills are degrading in many audit departments (www.canaudit.com/volume11issue1.html). I also mentioned that the hackers are gaining new techniques faster than we can build defenses. With this in mind, I have developed a new syllabus for IT auditing. This syllabus brings together the

risks we face and prepares auditors to identify and assess controls and suggest mitigating techniques. Let me walk you through the major issues that I believe we need to include in our basic IT audit skill sets.

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.

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.

If you found the above article interesting, then I invite you to take our new course IT Auditing: The Next Step which is premiering in Fairfax, VA on March 15-16, 2010. Over the next year, I will be turning this course and other new courses into a series of articles for those who cannot attend our classes. If you are not currently on our mail list, please send an "opt-in" email to Brenna@canaudit.com. Also, feel free to forward this article to other audit or security professionals. As always, I look forward to your comments on my articles. Please email them to me at Gordon@canaudit.com.

CHANGE IN STATUS

Some of you may be aware that I relinquished the position of President of Canaudit at the beginning of the year. Don't worry; I have not left the company. It is time for me to do what I want to do. This includes writing new courses, performing audits, and writing another book or two. Running the company just took up too much of my time away from what I originally set up Canaudit to do - write and teach audit courses and do technical audits. Lesley Parks (our co-founder and Vice President), Kevin Nibler, Tamra Savage Jones, and Kevin Kalbfleish have assumed my management tasks.

I am not fading off into the sunset. In fact, you will be seeing more of my articles and new courses throughout this and coming years. I will continue teaching classes both for Canaudit Professional Development Weeks and for chapters, as well as marketing our services to clients. So far it is working out well. I really am writing more, and I continue to enjoy performing my audits. As always, I am available to answer your audit questions by email or telephone. Yes, I have more time for that as well. Life is good - really, really good - and I look forward to spending more of my time serving you, my clients.

AUDIT & SECURITY SERVICES

Canaudit specializes in a variety of information system and technology audits, ranging from periodic network penetration testing to full network and operating system security review. Our tailored audits provide an objective, disciplined, and in-depth analysis to evaluate and improve the effectiveness of risk management, control and security within your organization's technological environment.

For interest in Canaudit to perform an IT audit for your organization, please email Gordon@canaudit.com or Tamra@canaudit.com, or call (805) 583-3723.

PROFESSIONAL DEVELOPMENT

Canaudit provides quality seminars to various organizations including audit and security chapters and major corporations. These seminars range from technical information system audit classes to internal audit classes aimed at everyone from an introductory level up to management. With nearly 20 courses to choose from, we are sure to have one that will meet your individual needs. In addition to chapter and private seminars, Canaudit also holds public courses. Our 2010 schedule for upcoming public training is below:

<u>Fairfax, VA</u>		
March 15 - 16, 2010	IT Auditing: The Next Step	<i>NEW</i>
March 15 - 16, 2010	Control & Security of UNIX	
March 17 - 18, 2010	Control & Security of Enterprise-Wide E-Commerce	
<u>Austin, TX</u>		
May 3 - 6, 2010	Performing an IT Audit & Security Baseline	<i>HANDS ON</i>
May 3 - 4, 2010	IT Auditing: The Next Step	<i>NEW</i>
May 5 - 6, 2010	Preventing Electronic Fraud & Cyber Incidents	
<u>King of Prussia, PA</u>		
October 4 - 7, 2010	Performing an IT Audit & Security Baseline	<i>HANDS ON</i>
October 4 - 5, 2010	Control & Security of Oracle	
October 4 - 5, 2010	Control & Security of Enterprise-Wide E-Commerce	
October 6 - 7, 2010	Computer Forensics for Security & Audit Professionals	
October 6 - 7, 2010	Control & Security of Linux	
<u>Simi Valley, CA</u>		
December 6 - 10, 2010	The IT Audit & Security Boot Camp	<i>HANDS ON</i>
December 6 - 7, 2010	Control & Security of Web Applications	<i>HANDS ON</i>
December 8 - 9, 2010	Control & Security of Windows	<i>HANDS ON</i>
December 10, 2010	Control & Security of Microsoft SQL Server	<i>HANDS ON</i>

For more information on upcoming public courses and to register, visit www.canaudit.com/seminars.html. Questions relating to Canaudit professional development or to schedule a Canaudit seminar, please email Brenna@canaudit.com or call (805) 583-3723.