

# Canaudit Perspective

November 2008  
Volume 9, Issue 3

## AMERICA IS AT RISK: PROTECT OUR NETWORKS AND DATA NOW!



GORDON SMITH  
Canaudit President

My last two articles, *Data Mining* and *Hackers Do Not Take Vacations* (<http://www.canaudit.com/news.html>), were very well received indeed. Now it seems the mainstream press is picking up the story. A recent article in USA Today paralleled the information I released in my articles ([http://www.usatoday.com/money/industries/technology/2008-11-11-thieves-cyber-corporate-data\\_N.htm](http://www.usatoday.com/money/industries/technology/2008-11-11-thieves-cyber-corporate-data_N.htm)). Now I want to provide important information on the new techniques used by hackers and impart a sense of urgency to the IT, Security and IT Audit communities.

Professional data miners are breaching networks and harvesting whatever they can find. These snatch-and-run techniques are extremely effective as they initially defeat the intrusion detection and prevention controls. Once into the network, using techniques described in previous articles or through electronic reengineering of internal websites, they capture the data and transmit it to machines they control. I have identified the main processes in the information-theft-to-merchandising cycle. These processes are infiltrate, confiscate, transmit, vault, catalog, analyze and merchandise. Let us look at these items separately.

The infiltrate process can take several paths. Poorly secured Internet sites are a major cause. Cross-site scripting, which enables hackers to submit code to poorly secured web pages, and SQL injection, which enables the injection of code into database applications, are examples of common techniques used to gain access. In recent weeks, sending mass emails to employees inside the network is becoming more popular. Employees click on what they believe is a valid link. In the process, software is loaded onto their machines and then transferred to other machines. Once embedded, the process moves to the next phase.

In the confiscation phase, corporate data is identified and captured. The major targets are email systems, documents, entire databases and other poorly

protected files. Rather than triaging the data to determine what is worth stealing, they confiscate it all. Once this is done, the other phases are rolled out in quick succession and may be performed concurrently. The data is tagged for transmission, encrypted and then transmitted back to machines controlled by the hackers. There it is stored in encrypted data vaults. Watch out for increased traffic that could indicate that massive amounts of data are being exported to remote sites.

In most cases, this is the first time the data has been encrypted. Could it be that the hackers are the only ones who understand the commercial value of the data? There is an important lesson here. If data has value to your organization, encrypt it before others take it. Note that encrypting hard drives is useful for protecting data when the PC or drive is lost or stolen. It is not effective in protecting data once the user has logged into the encrypted PC. Data on the encrypted PC is viewable on the machine itself or from the network. Separate file encryption must be used to protect the data.

Once the data is in the encrypted vault, the harvesters move to the next stage, that of cataloging the data to determine what they have. We are now entering the critical phases relating to the sale or use of intellectual property. While everyone is worried about credit card and personal health information, the hackers have moved into stealing industrial processes, research and development breakthroughs, competitive marketing strategies, and talent identification (find the best talent in one company and work with a recruiter to have the talent move to a competitor). Once the data is cataloged, it is analyzed to determine the best pricing alternatives for the data and the potential buyers. Lastly, the data is marketed to the hackers' patrons or to the highest bidder. These could be governments or people wanting to build new factories in China to sell cloned American products. Since our current government does not appear to be doing anything about the loss of our technology, it is clear that corporations must protect their data and do it now.

My recent articles have pointed out the various techniques used to compromise corporate networks.

We identified the risks and provided viable inexpensive solutions to mitigating the risk. Now it is time to perform a full 360-degree Security Baseline to identify the flaws in your organization's information infrastructure. While databases are the primary target of late, it is also necessary to identify poorly secured Active Directories, operating systems, workstations and network devices. We must also identify poorly secured trading partner and external Internet connections that can be breached. Once the Security Baseline is complete, we must focus on the rapid implementation of effective controls to remedy the control deficiencies. Every three months, a new

baseline should be run to validate that the required remediation is completed or progressing and to identify new weaknesses.

As a nation, we must act quickly to ensure that our secrets, technologies and innovations are not stolen. We must protect our databases and the data within them. We must do this now. Every day, we read new reports of corporate security breaches. The gaps must be plugged and they must be plugged now so that we can mitigate this new and dire threat to the American economy.

---

*The opinions expressed in this article are mine and mine alone. I look forward to receiving your comments on this article and answering any questions you may have. You can email me at [Gordon@canaudit.com](mailto:Gordon@canaudit.com) My next article will be on Auditing for Profit. This article will identify methodologies to make your organization more cost effective and how to optimize liquidity. It should be available in early December. If you would like to receive articles like this in the future directly, please opt-in to our distribution list on the Canaudit website.*

*If you would like additional information on how Canaudit can assist you with risk identification and remediation methodologies, please contact Tamra Savage Jones at (805) 583-3723 or by emailing her at [Tamra@canaudit.com](mailto:Tamra@canaudit.com).*

---

## **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](mailto:Gordon@canaudit.com) or [Tamra@canaudit.com](mailto:Tamra@canaudit.com), or call (805) 583-3723.

---

## **PROFESSIONAL DEVELOPMENT**

Canaudit provides quality seminars to local chapters and major corporations. These seminars include technical information system audit classes aimed at everyone from an introductory level up to management. With a list of over 20 courses to choose from, we are sure to have a course that will meet your individual needs. In addition to chapter and private seminars, Canaudit also holds public courses. Upcoming public courses are posted on the website, [www.canaudit.com](http://www.canaudit.com).

### **Upcoming Public Courses:**

#### Simi Valley, CA

December 8-12, 2008

December 9-10, 2008

December 11-12, 2008

Hands-On: IT Audit and Security Boot Camp

Control and Security of Web Applications

Computer Forensics for Security and Audit Professionals

#### Albuquerque, NM

January 12-15, 2009

January 12-13, 2009

January 14-15, 2009

Hands-On: Performing an IT Audit and Security Baseline *NEW*

Control and Security of Oracle

Control and Security of Enterprise Wide E-Commerce

Registration for a Canaudit public seminar can be performed online at [www.canaudit.com](http://www.canaudit.com). For additional information or to host a Canaudit seminar, please email [Brenna@canaudit.com](mailto:Brenna@canaudit.com) or call (805) 583-3723.