

Canaudit Perspective

February 2006
Volume 7, Issue 1

TOPICS OF INTEREST:

- Are the organization's databases secure?
- How good is my physical security?
- Can remote control software be used to defeat the firewall?
- Can we really trust our employees and contractors?
- Are our internal auditors permitted to do real security tests?
- Is the data on our computers protected from theft?
- Are our portable devices secure?
- Can our data be stolen and transported out of the facility?
- Is our data safe when it is transported to other locations?
- Is two-factor authentication used for sensitive or powerful access?
- The final question

TEN QUESTIONS THAT THE CEO SHOULD POSE TO THE CIO AND THE GENERAL AUDITOR



GORDON SMITH
Canaudit President

At the beginning of each year, I try to summarize the newest audit issues that my company, Canaudit, Inc., identified during the previous years worth of audits. The biggest single issue uncovered was the requirement to notify clients in California if their personal information has been disclosed to unauthorized individuals or groups. These public disclosures are very embarrassing to an organization that has reportable security incidents. In this article, I have listed the top ten questions that a CEO should ask the internal auditor and the CIO to determine if their processing environment is properly protected. At the end of these ten questions, is one final question that should be asked. The answer to this last question may startle the CEO.

I believe that our primary objective in 2006 should be the protection of corporate information assets. Clearly, this is where the next battle will be fought. For those of you who have been in my cyber-terrorism or information insecurity classes, this article will seem *deja-vu*. The issues are certainly worth revisiting.

ARE THE ORGANIZATION'S DATABASES SECURE?

One of the biggest issues in 2005 was poor database control. This can be broken down into several categories. The most dangerous, in my mind, is poorly secured backup or export files. Databases are usually backed up at least once a day to ensure that the database can be recovered after a processing interruption or disaster. When the backups are completed, the backup files are almost always in a "world readable" state. This means that anyone who can login to the machine can copy the database. Once they have the database, they can simply download the database software onto their PC or a machine they control. When completed, they can import or restore the pilfered data into the database they control and will have full system database administrator rights. This will enable them to view all the data, extract personal or confidential information, and use the information in any manner they choose. To prevent the theft of the database by any user who gains access to the system, have the database administrators (DBA) modify the program or script that creates the export. The program or script should make the permissions on the export or backup file so that only the DBAs can access this sensitive file.

Another common issue we discovered last year, relating to databases, was the failure to implement account lockout. Users who attempt to login to the application or database and mistype the password three times should have their account locked. If a hacker attempts to guess a user's password and fails three times, the account will be locked. If an alert is coded into the lockout function, an email can be sent to the security staff every time an account is locked. This will enable security to then call the user to see if they are experiencing difficulties logging in. If they are not attempting to log in, a probable computer incident is in progress and should be investigated.

Oscanner is a simple software tool used by attackers to gain access to a database. This tool enables them to gain access by trying default passwords or by using brute force to guess the password. Most of our clients in 2005 were susceptible to exploit by this tool, which could be used by anyone who gains access to the network.

My last issue with databases concerns software products, such as PeopleSoft, Banner, Cerner and Lawson. Purchased software often comes with default passwords. These passwords are well known and are readily available on the Internet. It may even be possible to download the manuals for these database software products, which may contain accounts and passwords, from the Internet. It is critical to information security that default passwords are changed.

Even with the best of DBAs, some things fall through the cracks. I believe that a full database security audit should be performed annually by a skilled professional.

HOW GOOD IS MY PHYSICAL SECURITY?

Many of our clients have spent dearly to protect their facility. Key cards, access turnstiles, guard services, cameras and other devices are costly, yet may not be effective. The question to answer is not how much was spent on physical security, but how effective is it. In 2005, all of our attempts to defeat physical security succeeded. You might want to stand by the security desk on a Monday morning during the last-minute rush to get to work on time. Watch to see if everyone uses or shows their badges. Some of our clients have systems that display the badge holder's picture when the card is swiped. Is anyone actually looking at the picture and comparing that to the person entering? This is often difficult to do during the morning rush. Periodically, send someone through security with a borrowed badge. If they get in, then the control is not working.

Another technique that is very successful is to attempt to enter as an EMT or power or phone company employee. Smokers create another significant vulnerability. They tend to congregate outside. A person who stands out in the cold with them for a few days becomes known to them, and they usually hold the door open so that they can enter the building.

Regardless of the technique, once we get into a facility it doesn't take long to locate a machine that is unattended or a live network jack that a system can be plugged into. We can then easily place a system on the network or load software onto a machine on the network that will let us establish an inside-out, outside-in session. Another trick that can be used is to place a word document or an airline reservation document onto a flash drive (also called thumb drives – small devices that hook into the USB port and can store up to 5 GB of data). All an attacker would have to do is ask if they could print out a file. They could then plug in the flash drive to print the file, while really loading the logmein.com software to establish an inside-out, outside-in connection. While the probability of this occurring is small, a breach like this can be disastrous to your organization.

CAN REMOTE CONTROL SOFTWARE BE USED TO DEFEAT THE FIREWALL?

The inside-out, outside-in exploit worked at every client we tried it at last year. The object of this software is to enable people to access another PC even if access is normally blocked by a firewall. You may have seen commercials for GoToMyPC.com or other similar products. The commercial states that you can get at your files at home even if your company has a firewall. Once this software is loaded on an internal machine, a session can be initiated from a machine outside the network, say at a hacker's home. The software has been designed to enable a remote machine to control an internal network machine. Once the connection is established, a hacker can use the connection to attack the internal network, sliding right through the firewall.

My intention is not to ban this type of software. It certainly has its uses. It is a great tool to enable an administrator or support person to gain desktop access to a remote machine. It is also useful for retrieving critical files on demand. (My PC just crashed, but I have my files backed up. I have been using logmein.com to retrieve these files so I could teach a class and do an audit without having to ship the files to me). All I ask is that this software be controlled. Only authorized staff should use it. Be careful of staff or contractors who may use it without permission to transfer your critical data to an offsite machine.

We should also not forget about other remote control software such as VNC, PCAnywhere and Microsoft Terminal Services. VNC is generally very poorly secured. It typically has a simple password that can be easily acquired and cracked using a freely available tool called NBTEnum. Once onto a machine with poorly secured VNC, it is a simple matter to take critical files, passwords, and other information that may be useful to attack other machines. There is a securable version VNC that requires both an account and a password to authenticate; however, a majority of our clients in 2005 did not appear to be using this secure version.

Microsoft Terminal Services can also be used for remotely controlling workstations, laptops and servers. Once an attacker has gained administrator access to the domain or the Active Directory, they have complete control to all the machines on the domain running Microsoft Terminal Services. We urge our clients to use access control lists to determine who can use MS Terminal Services, as well as two-factor authentication for all administrators.

PCAnywhere can also be used to remotely control machines. We actually noted fewer poorly secured implementations of this product in 2005. The recommended implementation of this product is to use account and password authentication and to use an encrypted session. This way the data will be encrypted as it traverses the network or the internal network. In conclusion, remote control software can be a great tool to your organization, provided the correct product is selected and the controls are implemented.

CAN WE REALLY TRUST OUR EMPLOYEES AND CONTRACTORS?

The old-school philosophy was to protect the network from external penetration. Some of the quotes I have heard in the last few years are as follows: "The bad guys are all on the outside." "It is okay to have poorly secured machines on the internal network because we have a firewall." "We do not have to monitor our consultants as they are with a reputable firm." "We only need to protect ourselves from external penetration." "We are willing to accept the risk". A quick visit to <http://www.privacyrights.org/ar/ChronDataBreaches.htm> will provide you with many examples of insiders who stole or sold corporate information. The list includes organizations such as Bank of America, Wachovia, PNC, Commerce Bancorp, Georgia DMV, the University of Hawaii and Atlantis Hotel. Clearly, when the opportunity presents itself, some people will try to steal your data, particularly client information.

Now is the time to start securing the network, the machines within the network, and your business applications and data. Staff and contractor's access and use of data must be monitored. Network activity must be monitored and unusual activity investigated. A full internal network vulnerability assessment should be performed by an external independent firm to test the exposure to insider security breaches and suggest improvements. If your mid-level managers "are willing to accept the risk", then I suggest they be held accountable for an incident when it occurs. Many managers are willing to accept the risk but not the consequences. When estimating the consequences, don't forget to include the public relations cost and the lost profits as customers close accounts or take their business elsewhere. This is 2006, not 1990. We need strong internal control to protect our information assets.

ARE OUR INTERNAL AUDITORS PERMITTED TO DO REAL SECURITY TESTS?

I really love my job, which is very apparent to my audit clients and those who attend my training sessions. Last week I was asked what frustrated me the most in my long audit career. The answer was not the work, the long hours, or the travel. I have auditors come to my classes so they can learn how to identify network, server or application security issues. I show them what to look for. I give them the software to find issues. I even show them how to safely use the software in a lab environment at my IT Audit & Security Boot Camp. Lately I've been asking the participants if they will be running the tools when they get back to the office. Surprisingly, about half of the auditors in my classes will not be permitted to use the network scanners, password crackers or other vulnerability discovery tools. The IT folks will not permit the use of the tools on the network. When I ask them about the audit mandate, each of them says the mandate empowers them to perform such testing as the auditors deem necessary. The audit mandate is not the issue. Upon further questioning, they answer, invariably, that using the tools is not politically correct; the IT folks may have some explaining to do if the testing reveals serious network flaws. This is what frustrates me the most.

I find this both shocking and disappointing. Imagine if the CFO said that the auditors would not be permitted to test the general ledger or cash receipts! How about, "you cannot use audit software to verify that the ledger balances to the control accounts"? Why is it that some IT departments try to hide their poor controls by handicapping the auditors? If an attacker can use a tool to penetrate your security, then your auditors had better find out first! Otherwise your organization is a sitting duck!

I understand that the IT folks may not want to have false alarms regarding intrusion detection software that may be running. For that reason, I have perfected a procedure that permits the auditors to test independently while ensuring that the IT folks do not waste valuable time tracking intrusion events that really is audit testing. Our mechanism involves loading the required software tools onto a special laptop. This laptop is not on the network unless the auditors are testing the network or downloading security and software updates or patches. The IT and security staff are provided with the MAC (hard-coded computer address) of the test machine. If it shows up on the network, they can call internal audit to determine if a test is in progress. This works at several of my clients.

If your auditors are not permitted to test the network, then attackers have an open invitation to exploit unidentified security issues. Internal audit must be permitted to do such testing as they deem necessary, as stated in the audit department mandate, to verify the presence of control and, more importantly, the absence of controls. Only through identifying how data can be stolen can we implement new controls to prevent the loss of confidential data and to ensure early discovery of incidents.

IS THE DATA ON OUR COMPUTERS PROTECTED FROM THEFT?

As of January 17, 2006 there were 26 reported incidents of computer or laptop theft on <http://www.privacyrights.org/ar/ChronDataBreaches.htm>. Boeing reported that approximately 161,000 identities may have been compromised as a result of a stolen laptop. Other companies reporting potential identity theft through lost computers or laptops include Bank of America, UC Berkeley, the Department of Justice, MCI, and San Jose Medical Group.

Laptops can be easily misplaced when going through airport security and screening. Road Warriors often leave their laptops in their hotel rooms when going out to dinner or to the gym. These machines could be accessed by anyone with a master key card to hotel room doors. Airline clubs are also a good place to lose a laptop. Many of us work in the airport lounge. When we leave our workstation to get a snack or to visit the restroom, we lock our computers. This does not prevent them from being stolen or the hard drives removed, copied, and returned. Your organization may want to consider installing PC LoJack on all laptops. When a laptop is then stolen and hooked into the Internet, it can be tracked and recovered. This is good software to consider for every executive and all staff with sensitive information on their laptops.

If I had my choice, I would encrypt all data on all computers. Unfortunately I'm fighting an uphill battle, at least with those who have not had confidential data stolen on a laptop (yet). After the data is gone, everyone wants to start encrypting data. This is closing the barn door after 10,000 horses have left. I strongly suggest that all sensitive data be encrypted on all workstations and laptops. If possible, this data should also be encrypted on the servers. There are several inexpensive products that will encrypt data. XP and Windows server editions come with the capability to define an Encrypted File System (EFS). This is free! Other tools such as PGP are very inexpensive and easy to use. It is best to assume that a laptop or workstation will be stolen and to encrypt the data before it actually is stolen. Staff should also be warned that they are personally responsible for any data they download. Periodic testing should be performed to determine what confidential information is exposed to theft.

ARE OUR PORTABLE DEVICES SECURE?

Portable devices include Blackberry communication devices, PDAs such as Palm and IPAQs, and cell phones. Let's address them in order. Blackberries pose a significant threat if they are not properly secured. They are normally used by senior executives and other important staff. The most common failing is the lack of a password on a Blackberry. In 2005 this was pervasive throughout our client base. A simple test I use is I ask a person to pull out their Blackberry and shut it off. Then I ask them to turn it back on. If it does not prompt them for a password, then this device can be easily compromised.

Blackberries are often carried in a jacket pocket. The jacket may be hung on a door where someone can steal the device from the pocket. I've also seen people in a bar place the Blackberry on the table or the floor under their feet as they don't like it vibrating on their belt. Again, it is easy to steal. Another issue with Blackberries is the bberry server that processes the emails. In several audits last year, we identified an administrator account on the server called bberry with a password of bberry. Using this account we could reconfigure the blackberry settings. Think of the damage that could be done if copies of all executive emails were automatically sent to a competitor. Make sure this password is changed.

PDAs and some cell phones also contain sensitive data. The new Palm Treo combines a cell phone with a PDA and is very similar to a Blackberry. Many people use their personal PDAs or cell phones with Pocket PC, such as the Treo, for business purposes. When they leave the firm, this corporate data goes with them. Add in the likelihood that SD chips can greatly increase the storage capacity, and we have a scenario for large amounts of corporate data being in the hands of a disgruntled terminated employee. At Canaudit, we provide these devices to our staff and retrieve them upon termination. We also have a strong policy on confidential information and how it is to be protected. Clearly the use of personal PDAs, cell phones and other similar devices for business use should be prohibited.

CAN OUR DATA BE STOLEN AND TRANSPORTED OUT OF THE FACILITY?

The easiest way to transfer data from the internal network to an external device or server is to transmit the data out over the Internet. Another method is copy the data onto a portable storage device and walk it out of the building. I use my PDA to store information I need. To increase my storage capacity, I use the 1 gigabyte SD cards. These devices are about ¾ of an inch squared and wafer thin. Some of our clients with highly sensitive data or research actually inspect laptops that are leaving the facility. What better way to beat the inspection than to transfer the data onto 50, 100 or even 200 SD cards, place them in a briefcase and walk out of the building.

I recently bought another 100 gigabyte hard drive the size of a deck of cards. I use this for carrying an image of my PC around with me in case I need to restore it. I have several others for backup and other storage purposes. A dishonest employee or contractor could easily conceal 50 of these devices in his laptop case. I also have several Maxtor drives that we use for forensics work. These drives are the size of a hard cover book and store 400 gigabytes of data. Again, it would be easy to put four of these drives into a briefcase and sneakernet it out of the building. In addition to smuggling the data out of the building, it could be easily couriered or mailed to Mail Boxes Etc or similar service. If your organization has sensitive data, then regular random inspections of personal belongings upon leaving the facility is an option. Also, scrutiny of outgoing courier and mail should be considered.

IS OUR DATA SAFE WHEN IT IS TRANSPORTED TO OTHER LOCATIONS?

Lost tapes have also resulted in serious information disclosure issues. According to Privacyrights.org there have been eight occurrences where tapes have been lost in transit. There were two incidents where tapes were lost while in transit to offsite backup location. Several tapes were lost in transit to credit bureaus. If tapes contain sensitive information, they should be encrypted. If a tape is lost, the data is reasonably protected from unauthorized access or disclosure. I have been recommending this for over 20 years. Now, with these eight reported incidents, my warnings are now being taken seriously.

IS TWO-FACTOR AUTHENTICATION USED FOR SENSITIVE OR POWERFUL ACCESS?

For years, the battle has raged over the length and complexity of a password. Let's get real. Newer password crackers such as RainbowCrack can crack the most complex passwords in less than 30 minutes. Obviously, passwords are not a control in themselves. For this reason, auditors have been suggesting two-factor authentication. In addition to a password, a user is required to have a second form of authentication. This can include a token such as RSA SecurID or Identix. Both of these popular devices are inexpensive and reliable. Biometric authentication using finger print or iris scanners is also very effective. Digital certificates are also excellent tools. Two-factor authentication has been available for several decades. When a company has a computer incident, they quickly understand why they need these additional controls.

In a previous article (http://www.canaudit.com/Perspectives/Volume6_Issue9.pdf), I mentioned the serious exposures relating to web mail. I remain very concerned about web mail and administrative access to servers and databases. I strongly urge your organization to implement two-factor authentication for all those with sensitive access, including system administrators, database administrators, executives and any other staff or contractors with sensitive access.

THE FINAL QUESTION

If the answers to the above questions follow the theme that we do not have any issues here, then I have one last question that the CEO should pose to the General Auditor and the CIO. **If an airplane was built from the controls in the IT environment, would you board the aircraft?** The answer I receive every time I pose this question is the same – No, they would not board. A single serious control failure can cause a plane to crash. I believe a single serious IT flaw can cause organization disruption or public embarrassment.

If I pose this question in another way – Are we Sarbanes-Oxley compliant, the answer would be yes. Is it possible to comply with Sarbanes-Oxley, yet still have serious control issues within the IT environment? The CEO often asks what value the company received from the Sarbanes-Oxley process. My answer is that these are two different issues. You can be Sarbanes-Oxley compliant according to the audits performed by the external auditors and consultants, yet still have a poorly secured network. You have to fund both the SOX audit and the broad scope Vulnerability Assessment audits.

As you can see from this article, 2005 has brought new audit and security risks. The questions I pose in this article focus management's attention on these risks as they are the new security "hot buttons". These items need to be addressed; but as auditors and security professionals, we must ensure that we emphasize all of the essential controls in the audit and security universe, not just those mentioned here.

The opinions expressed in this article are mine and mine alone. I am interested in your comments, positive and negative, relating to this article (Gordon@canaudit.com). I believe in encouraging dialog between audit and security professionals so your comments are valuable to me.

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.

Mini Network Vulnerability Assessment	\$27,500
Full Network Vulnerability Assessment	\$50,000
Full Network Penetration Test	\$65,000

For interest in Canaudit to perform an IT audit for your organization, please call Gordon Smith or Tamra Savage at (805) 583-3723.

PROFESSIONAL DEVELOPMENT

Canaudit also 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 30 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:

King of Prussia, PA

March 20-24, 2006	IT Audit & Security Boot Camp	<i>HANDS ON</i>
March 20-24, 2006	Ultimate Network Penetration Class	<i>HANDS ON</i>
March 27-28, 2006	Control & Security of PeopleSoft	
March 29, 2006	Auditing for Profit	

Bloomington, MN

April 3-7, 2006	IT Audit & Security Boot Camp	<i>HANDS ON</i>
April 3-5, 2006	Advanced Ultimate Network Penetration Class	<i>HANDS ON</i>
April 3-4, 2006	Control & Security of Enterprise Wide E-Commerce	
April 5-6, 2006	Control & Security of Linux	
April 6-7, 2006	Perimeter & Physical Security	
April 7, 2006	Auditing IT Technology	

Registration for a Canaudit public seminar can be performed online at www.canaudit.com. For additional information or interest in hosting a Canaudit seminar, please call (805) 583-3723.