

The Canaudit Perspective

January 2004
Volume 5, Issue 1

New Priorities for Difficult Times

Written by: Gordon E. Smith - President, CEO

Points of Interest

- Hardening the external perimeter
- Hardening the internal perimeter
- Patch, Virus, and Malware Management
- Staff Acquisition
- Professional Development is Essential
- Available Seminars and Presentations



A handwritten signature in black ink that reads "Gordon E. Smith".

As we enter a new year, it is time to set objectives, redefine goals and renew our corporate security efforts. 2003 was a difficult year for the security and audit profession. Overseas outsourcing, corporate downsizing and early retirements took their toll on our profession. New exploits, viruses and worms ensured that the survivors had much to do.

As the 2003 earnings reports come in, many companies are meeting or beating expectations. This bodes well for our profession as corporate belt tightening may be reduced, purse strings may be loosened, and yes, there may be some selective staff acquisition in the picture. Our profession has a small window of opportunity to make our case for the much-needed budget and staffing resources before other resource strapped areas requisition the cash flow. The security and audit functions need this funding to prepare the corporation for the new challenges we will face in 2004. To get the funding required, you must get managements attention and motivate them to enhance security. Here are a few issues you can use to build your business case for augmenting the security and audit function.

Keep the Organization off the Front Page of the Wall Street Journal

Recently, many organizations have been the brunt of negative publicity. Not only does this destroy the public's confidence in a company, but it also causes a sharp drop in the share price. One of the fastest ways to become headline news is to have your customer's personal data lifted from your servers and databases. Identity theft and violations of Gramm Leach Bliley (GLB) can rapidly destroy your organization's public image.

You can expect a series of class action suits once your company is front-page news. Failing to properly protect your customer financial or medical records is perceived as a major corporate sin. Executives may look for a designated inmate when the stock is falling and the organization is mired in public litigation. That inmate is often the security officer or the internal auditor.

This is the time to go through the unresolved security issues that are on your plate. Document and rank them by risk. Present them to management as part of your 2004 focus document. Plainly state the issues, the impact of an occurrence and the resources required to mitigate the risk. Don't forget to track and document the responses, and more importantly, record the areas where you did not get management support. If management is "willing to accept the risk", document it and send them a gentle email noting that they have accepted the risk related to this particular security event. Keep this and any responses handy in case you are selected to be the person honored to "take the wrap". Facts are your friends! By keeping good records, you can ensure that you are a part of the solution, not the person who must accept the blame for the incident.

Hardening the External Perimeter

I have some good news on the external network access front! In 2003, a few of our clients detected our Internet penetration tests. These clients are still in the minority, but any improvement is welcome. The positive shift indicates that firewalls are trapping and logging security events. More importantly, security folks are receiving automated alerts or identifying attacks through log review. Yes, there is progress, but there is still a long way to

go. Many organizations still do not have intrusion prevention and detection software. Those that do may need to improve their use of the software, particularly the automated alert functions.

The business community relies on firewalls to block penetration attempts. Those of you who have read my books or attended my Control and Security of Telecommunications Network class or the IT Audit and Security Boot Camp know how easy it is to bypass the firewall. No single control is bullet proof, hence the need for intrusion detection (IDS) and prevention software. This software is not a panacea. To be effective, controls must be implemented to detect intrusion attempts, block them, and notify the security analysts that an event has occurred. The analysts can receive timely notification of critical, network threatening events by properly triaging the types of events and prioritizing the response and notification. These "Code Red" alerts need immediate attention.

Another area that is often ignored is the slow careful attack by a skilled hacker. These attacks, if properly executed, stay under the water line of both the firewall and the IDS products. A scanner set to send out one request every 20 minutes may go undetected. The patient cyber criminal will use stealth to defeat your control structure. For this reason it is necessary to monitor less obvious attacks. The firewall logs and IDS data should be mined for the smaller, less frequent attacks on a daily basis. When a low intensity, yet serious attack is detected, a "Code Red" alert should be generated. The security analysts should be called to action by email and a message should be sent to their pager or cell phone.

Don't forget about modems. They remain a serious threat to your perimeter security. Performing a regular automated modem hunt is a necessity. A common flaw is to seed the automated war dialing software with the phone numbers that come through the PBX. Don't forget about the central office (CO) and POTS (plain old telephone service) lines that come into the facility. Often these numbers are not cataloged and, as a result, they are not tested. One of my "crusades" for the year is to focus on capturing these elusive phone lines. We now recommend that the security and IT audit groups ask the carriers to supply a list of all POTS and CO connections that terminate in your facilities. It should be updated regularly.

This process can lead to startling results. A senior executive at one organization wanted to bypass firewall filtering so he could avoid monitoring of his Internet sessions. He simply ordered a POTS line with DSL and had high speed, un-firewalled access to the Internet. At another company we identified phone circuits that were brought into the facility without the knowledge of the phone coordinator. If this person does not know about the circuits, then they certainly will not be managed nor will the proper controls be implemented.

My last issue on external perimeter is wireless. Again, we've seen good improvement in 2003 with regards to wireless security. There is still much to be done, particularly in the area of laptop wireless devices. Often these devices are active, yet the user is not aware that their machine is actively seeking for a wireless access point. When a "bad guy" sets up a wireless access point in the vicinity, the laptop automatically connects. It is a simple task to take control of the laptop and use it to attack the internal network. Clearly we must continue to secure our wireless connections, yet ensure that we provide fast wireless services to those that need them.

Hardening the Internal Perimeter

While I saw progress last year on the external perimeter, sadly I have to admit that the internal network security at many of our clients has actually degraded. Our internal penetration audits revealed that operating systems are not hardened, IDS and honeypots are often not used and machines are not patched. The account without a password is still one of the greatest risks. CIS and NBTenum, two tools that enable a hacker to identify poorly secured accounts, still work on enough machines to enable us to glean the account / password combination required to gain administrative rights on the primary domain controller. Most of the Windows machines can be accessed and compromised once we get this far.

UNIX machines with default passwords or no password enable us to gain access to the UNIX environments. Once onto the device, we take advantage of poorly secured services such as rlogin to gain root access. If this does not work, then we try various exploits, just as a hacker would, to augment our capabilities to the root level. In 2003, we found that SUN boxes were the easiest to capture because of the integer overflow exploit and the sadmind feature. HP machines with unshadowed password files came in a close second. Visit our web site (www.canaudit.com) and download our free UNIX audit scripts. These will help you identify and remediate poorly secured machines.

Network devices are still plagued by poor community strings. Running a tool such as Solar Winds enables us to quickly identify the community strings that give us the ability to download the machine configurations, identify user accounts and crack the passwords. This process often gives us VPN access and can lead to an external network

penetration. We can click on one button and see any accounts on the machine if your Windows machines have a public or private community string. This allows us to identify accounts without using CIS or NBTenum. One of the most important network controls is to disable the Simple Network Management Protocol (SNMP) service or to use complex read and write community strings. If you have HP OpenView, or other network management products, you may not be able to disable SNMP on the internal network. If the SNMP service is required to be open on the internal network use a honeypot to detect SNMP scans.

Sadly, we have noticed an increase in the number of insiders who intentionally attack the network. These disgruntled current or former employees and contractors have the knowledge required to defeat your controls. A poorly secured internal network enables them to obtain the information, over time, that they require to knowingly and purposefully damage or destroy your computing environment. The most disappointing item in 2003 was the dramatic increase in "emergency" forensics investigations we performed for clients who were hit from the inside by knowledgeable employees. While this is a profitable business for us, we prefer that controls be implemented before an attack occurs, rather than after the incident is public knowledge.

Patch, Virus, and Malware Management

Again we noticed improvement in patch management last year. Many of our clients have automated the process of applying patches and new virus and malware signatures. They are regularly patching their machines. We find that there are still machines on the network that are exposed to the DCOM and other exploits when we do our patch level tests. The most common deficiency is with laptops. Often these machines are not set to automatically update the operating system and virus software. The reason provided to us during our audits is that laptops may be connecting through a slow speed modem connection (say at 28.8 Kbps). Downloading an eight-megabyte patch would take a very long time. One solution is to send an email to the users, who do not get automatic updates, notifying them that they must connect to a high speed, fire-walled network, and download the required fixes within 24 hours. They will not be permitted to connect to the network if they do not comply.

Another issue is the lack of personal firewalls on internal network machines. Given the risks, it is now necessary to install and configure this software on all Windows based machines. We can no longer rely solely on large-scale firewalls on the perimeter. We need proven technology to ensure that the desktop, laptop and servers are protected from viruses and malware inserted into the network by accident or, even worse, intentionally.

When reviewing patches and virus updates, one of the areas often under managed are vendor and consultants computers. Only one client last year asked to look at our machines before we connected to the network. This client checked our firewall settings and virus signatures. Then they asked us to run a full disk scan before we were permitted to connect to their network. Consultants with unpatched machines can quickly insert a virus or other malware into your network. Ensure that you include the right to inspect consultant machines in your contracts as well as the requirement to be at current virus signature and patch levels. You should then develop a checklist to be used to inspect consultant and vendor machines before they connect to the network.

Password Crackers Made the Password Obsolete in 2003

Rainbow Crack, a relatively new cracker developed in China by Zhu Shuanglei, makes it a simple matter to crack any password. Using this cracker on a 3.2 GHz machine, we are able to crack any alphanumeric password within two minutes. This cracker uses a precompiled dictionary (you have to compile it yourself) to quickly analyze the LanMan hash, compare it to the dictionary value and "crack" the password. Chris Schroeder, our Senior Manager, used six high-speed machines for a month to generate an alphanumeric/common special character dictionary. Using this dictionary he can crack a password with a common special character within eight minutes. He is currently working on a new dictionary that includes alphanumeric and all special characters. This should enable us to crack just about any password within 30 minutes.

With tools like these, faster computers and networked computer cubes, password controls can and will be quickly defeated. After years of talking about biometrics and certificates of authentication now is the time to implement them. We suggest that all staff with administrative rights to machines, or those with access to high value or extremely sensitive information, be issued tokens, digital certificates or biometric devices to augment security. These devices ensure that critical users are authenticated using comprehensive, yet easy-to-use tools to foil the effects for faster and better password crackers. It is unlikely that a hacker will get the file to crack without using social engineering or other techniques if they needed one of these secondary authentication devices before he or she could download the password file. Now is the time to move into secondary authentication! Do not wait until professional hackers victimize your organization.

[Use Sarbanes Oxley, HIPAA and Gramm Leach Bliley Legislation to Your Advantage](#)

The threat of legal sanctions, large fines and jail time is now a reality. You may not be able to comply if your IT environment is not secure. The GLB and SOX legislation now applies. The IT security portion of HIPAA will come into force in another 13 months or so. Some of our recent reviews of client IT processing environments indicate that they are out of compliance with this legislation. Security and IT audit need the staffing resources and skill sets to identify out of compliance issues and ensure that these issues are resolved quickly. I will be addressing this issue in my next newsletter, so I'll hold my thunder until then.

[Staff Acquisition](#)

There is now a plentiful pool of under or unemployed security professionals and IT auditors thanks to years of downsizing and outsourcing. **[Now is the time to hire the staff required to identify and correct serious IT control issues!!!](#)** I strongly support insourcing the outsourced IT audit or security functions. I also believe that existing security and internal audit functions need additional, highly skilled staff. Information security needs to be improved in the short term and it takes skilled and experienced staff to make this happen. The security function needs to be augmented to ensure that the job is done properly and that your organization's security issues are contained, until they can be corrected. You might want to consider redeployment of existing qualified staff to the security area if your organization has a hiring freeze or capable staff are facing layoffs.

Let's also reevaluate the role of the IT auditor. A real IT auditor does much more than general control reviews and high level audits. They delve deeply into the technical control structure, use automated tools to ferret out control issues and provide management with an independent assessment of internal IT controls. We need more high tech IT audit professionals and we need them now. ISACA and IIA chapters must reach out to the universities and community colleges to attract the new technical auditors we will need in the future. At the same time, we need to acquire senior skilled and knowledgeable technical IT auditors to assess controls and mentor the new auditors. This is one profession that has withered during the recession and needs to be reinvigorated. Don't wait for ISACA International to promote this idea. You and the chapters in your area must rise to the challenge. Reach out to senior executives. Brief them on the value of IT audit and the requirement to insource this valuable function. As always, I put my money where my mouth is. If your chapter is looking for a powerful free presentation on Rebuilding the IT Audit Function or my highly controversial presentation Outsourcing: Placing Our Nation at Risk, email jennifer@canaudit.com. I have reserved a week in the spring to fly around the country at my expense to make these thought provoking and impassioned presentations. Your chapter must finalize this offer by February 20, 2004 to qualify. For more information on our upcoming seminars, which include the IT Audit & Security Boot Camp, The Ultimate Network Penetration Class, and our Professional Development Weeks, please visit us at www.canaudit.com.

[Professional Development is Essential](#)

Our world is changing rapidly, yet professional development budgets have been decimated in the last two years. As we face new challenges, we need new skills. Each and every security professional and auditor needs a personalized PD program to ensure that they continue to meet their organization's security needs for today and into the future. I believe that we will see a rebound in the security and internal audit functions. When this occurs, and I expect it to occur in the next 18 months, the tables will change. Employees will have the upper hand.

I've talked to many people recently who are just waiting for a sustained recovery so they can jump ship. When this happens, organizations will lose very qualified and capable staff. To replace these staff, they will have to pay higher wages, offer incentives and pay headhunter fees to attract the skill sets required to maintain a secure and controlled IT environment. Roughly half the people hired will not remain with the company for more than three years. So a failure to respect your IT security and audit staff now could have very serious long-term repercussions in the mid term. A strong personalized PD program assists in employee retention. A challenging and rewarding work environment can enhance staffing stability while ensuring that your staff continues to grow and prosper. **[Companies that believe in implementing security will attract the best of our profession!](#)**

The comments and opinions above are mine and mine only. I hope that they provided you with goals and objectives for 2004. As always, I look forward to receiving and responding to your comments. Please email them to Gordon@canaudit.com.

In compliance with Federal Laws, please indicate if you would like to [opt-in](#) or [opt-out](#) of our mail list.