

Healthcare Security Release

November 2007



GORDON SMITH
President of Canaudit

I am very concerned about the upsurge of identity theft and disclosure from healthcare organizations. In my recent presentation at the AHIA conference in San Diego, I introduced figures that showed that hospitals are a primary target of identity theft. I have since updated my data to reflect several more serious incidents which indicates to me that the healthcare industry is well into an information disclosure crisis.

HEALTHCARE-RELATED IDENTITY THEFT

As you can see to the right, the total is five times last year's numbers and almost 15 times the 2005 number. Even this humble auditor can see that information disclosure is mushrooming at a pace that threatens public confidence. Based on the audits I have performed over the last two years, I can state that this number understates those affected by identity theft. When examining the incidents, you will notice that the most common cause is loss or theft of laptops and workstations. You and I expect information losses through hacking or inside jobs, but the data above does not show this. Why not?

Year	Identities Lost, Stolen or Compromised *
2005	377,425
2006	1,078,216
2007	5,423,339

*Data gleaned from <http://www.privacyrights.org/ar/ChronDataBreaches.htm>. Current statistics are available on their website.

The answer is that the hospitals I have audited do not have intrusion detection or prevention systems. If a hospital does not detect an intrusion there is no need to report it. In my opinion, this head-in-the-sand attitude, coupled with extremely soft controls, makes hospitals the preferred target of hackers. The combination of few controls, no intrusion detection system, and poor incident response procedures places personal health information (PHI) at great risk. Servers, databases, medical devices, laptops and tablets in many cases are not properly secured. In our security baselines and penetration tests, most hospitals are completely compromised within hours of the start of the audit. If our team can do it, I suggest that hackers and disgruntled insiders or contractors could just as easily penetrate hospital defenses.

There is another issue to consider. Not all hackers are careful in their attacks as they may not understand the technology or they do not care if they do harm. Have you had a recent unexplained outage of a critical server, application or database? This could indicate that a hacker tool misfired, causing the intended target to fail. Clearly, an unexplained failure needs to be investigated as a potential network intrusion. It could be an indication that the network has been compromised.

ACTION IS REQUIRED NOW

Hospitals and other healthcare facilities must act now to triage their Information Technology, identify the risks and immediately start remediation. In my January 2007 Healthcare edition of the Canaudit Perspective (<http://www.canaudit.com/Healthcare/GreatestITRisksHealthcare.pdf>) I explained the greatest IT risks facing health care. I do not want to repeat the issues again as you can download the article. By now, I expect that some of you have worked on remediating the items I identified. In the rest of this bulletin, I will update the article with additional information from our recent healthcare audits.

DATABASES ARE POORLY PROTECTED

Oracle and Microsoft SQL (MSSQL) databases are easily compromised due to a failure to implement vendor-recommended controls. In all of our audits this year, we have been able to compromise most Oracle databases and many MSSQL databases. We have noticed an increase in unauthorized versions of Oracle being installed within the network. We found developers who download the Oracle Personal Edition, which is free. They use these in their development effort as it is easier to create new code in these databases. There are two specific risks that I am concerned about with these personal databases. The first is that they often contain Oracle default passwords. Using the Canaudit Oracle Scanner, we are able to gain access to the databases using default authentication information, and then download and crack the passwords. Since the developers often use the same password on the personal edition as they do on the development and production versions of the databases, we may gain database administrator rights to the production or test environments.

Oracle database exports (backup files) remain unprotected. As a result, anyone who gets onto the system can "harvest" the entire database and then import it into their own personal version of Oracle. Why steal a few records when the entire database is exposed? Please check your Oracle and MSSQL implementations for obvious flaws. After all, hackers follow the path of least resistance. Why compromise a server when it is easier to compromise and steal the database?

LAPTOPS AND WORKSTATIONS CONTAIN SENSITIVE DATA, PROTECT IT!

Everyone squawks about the cost of encryption just as they used to complain about the cost of antivirus products. Let me assure you, the cost of providing credit monitoring and possible litigation is far more than the cost of encryption software. Review my AHIA presentation at the following link (<http://www.canaudit.com/Healthcare/HealthcareSecurity.pdf>). Encrypt now or be prepared to have your hospital posted on www.privacyrights.org. The incidents of lost laptops and workstations are rising. There could be a determined effort to steal these machines due to lax physical security in many hospitals.

PASSWORDS AND PATCHES

I cannot say enough about passwords. Hospitals are notorious for having accounts without passwords, accounts with passwords equal to the account name, and accounts with other default passwords. Healthcare application vendors have a tendency to use the same account and password on all of their clients' machines. The last hospital I was at we used an account of "mckesson" with a password of "mckesson". That gave us administrative rights to the server. We were able to leverage this to gain access to most of the Windows machines in the network. Default passwords are a hacker's delight. Please find and change them.

Patches remain a major issue in the Windows environment. We often hear that the FDA will not permit patches to medical equipment. The FDA does in fact have a policy permitting patching of the Common Off-The-Shelf (COTS) Software such as the Windows and UNIX operating systems. An un-patched machine is an open invitation to breach security. Do not tempt the hacker. Patch the machines. I have placed some additional information relating to COTS on the Canaudit website (<http://www.canaudit.com/Healthcare/FDARegPersp.pdf>).

CANAUDIT IS COMMITTED TO HELPING

As always, Canaudit remains committed to assisting healthcare facilities with high-quality audit and security products. At the AHIA conference, I extended a significant discount for AHIA members for projects completed before the end of February 2008 (<http://www.canaudit.com/Healthcare/HealthcareBrochure.pdf>). The \$10,000 discount for our penetration tests and security baselines will expire soon. If you are concerned about the security in place at your organization, contact me so we can get the risk identification and remediation process started.

Project	Standard Pricing	AHIA Pricing *
Comprehensive Penetration Test	\$ 55,000	\$ 45,000
Security Baseline	\$ 55,000	\$ 45,000
Network Vulnerability Assessment	\$ 45,000	\$ 37,500
Internet Review	\$ 15,000	\$ 12,500
Dial-up Review	\$ 5,000	\$ 5,000
Windows Security Assessment	\$ 9,000	\$ 7,500
Web Application Security Assessment	\$ 27,500	\$ 22,500
UNIX Security Assessment (15 systems)	\$ 32,500	\$ 27,500
Oracle Security Assessment (5 databases)	\$ 35,000	\$ 30,000
Microsoft SQL Assessment (20 databases)	\$ 35,000	\$ 32,500
Application Audit (Lawson, Cerner, etc.)	Pricing upon request	Pricing upon request

*To qualify for AHIA pricing, the project must be performed between November 1, 2007 and February 28, 2008 and must be confirmed by January 11, 2008

As always, the comments in this article are mine and mine alone. Please email your comments to gordon@canaudit.com. I read, consider and respond to all of your emails. Also please visit the new Healthcare Section on the Canaudit website, <http://www.canaudit.com/healthcare.html> for presentations, articles and other relevant information concerning healthcare internal auditing.