



The State of IT Security in the Healthcare Industry

Challenges and Solutions for Auditors

Prepared by
Gordon Smith - CANAUDIT, INC

Contact Information:

Email: gordon@canaudit.com

Phone: 805-583-3723



Healthcare Security Breaches in 2005

<u>Date</u>	<u>Name/Location</u>	<u>Type of Breach</u>	<u># of Records</u>
2/18/05	University of Chicago Hospital (IL)	Dishonest insider	85
3/11/05	Kaiser Permanente (Oakland, CA)	Exposed online	140
4/8/05	San Jose Medical Group (CA)	Stolen computer	185,000
4/15/05	CA Dept of Health Services	Stolen laptop	21,600
4/26/05	Christus St. Joseph's Hospital (Houston, TX)	Stolen computer	19,000
6/30/05	OH State University Medical Center	Stolen laptop	15,000
10/12/05	OH State University Medical Center	Exposed online	2,800
10/21/05	Wilcox Memorial Hospital (HI)	Lost backup tape	130,000
11/1/05	University of TN Medical Center	Stolen laptop	3,800

TOTAL number of records containing sensitive personal information involved in healthcare security breaches in 2005:

377,425

Healthcare Security Breaches in 2006

<u>Date</u>	<u>Name/Location</u>	<u>Type of Breach</u>	<u># of Records</u>
1/1/06	University of Pittsburgh Medical Center (PA)	Stolen computers	700
1/24/06	University of WA Medical Center	Stolen laptops	1,600
1/25/06	Providence Home Services (Portland, OR)	Stolen backup tapes	365,000
2/17/06	Mount St. Mary's Hospital (Lewiston, NY)	Stolen laptops	17,000
3/1/06	Medco Health Solutions (Columbus, OH)	Stolen laptop	4,600
6/17/06	CA Dept. of Health Services (Sacramento)	Improper disposal	1,550
6/21/06	CapeFearValley Health Sys (Fayetteville, NC)	Stolen computer	24,350
6/21/06	Lancaster General Hospital (PA)	Stolen computer	100s
6/23/06	CA Dept. of Health Services (Sacramento)	Improper disposal	323
7/25/06	Georgetown Univ. Hospital (Washington, DC)	Exposed online	23,000
7/27/06	Kaiser Permanente N. CA Office (Oakland)	Stolen laptop	160,000
8/4/06	PSA Healthcare (Norcross, GA)	Stolen laptop	51,000
8/11/06	Madrona Medical Group (Bellingham, WA)	Former employee	6,000
8/17/06	Hospital Corp. of America (Nashville, TN)	Stolen computers	1,000s
8/18/06	CA Dept. of Mental Health	Tape missing	9,468
8/22/06	Beaumont Hospital (Troy, MI)	Stolen laptop	28,400

Information provided by Privacy Rights Clearinghouse

Healthcare Security Breaches in 2006

<u>Date</u>	<u>Name/Location</u>	<u>Type of Breach</u>	<u># of Records</u>
8/29/06	Valley Baptist Medical Center (Harlingen, TX)	Exposed online	Unknown
8/29/06	Compass Health (Everett, WA)	Stolen laptop	Limited
8/31/06	Labcorp (Monroe, NJ)	Stolen computer	Unknown
9/9/06	Cleveland Clinic (Naples, FL)	Dishonest employee	1,100
9/15/06	Mercy Medical Center (Merced, CA)	Lost memory stick	295
9/16/06	MI Dept. of Community Health (Detroit)	Lost flash drive	4,000
9/16/06	Beaumont Hospital	Exposed by mail	3
9/18/06	DePaul Medical Center (Norfolk, VA)	Stolen computers	100+
9/21/06	Pima Co. Health Dept (Tucson, AZ)	Improper storage	2,500
9/23/06	Erlanger Health System (Chattanooga, TN)	Stolen records	4,150
9/28/06	Stevens Hospital ER (Edmonds, WA)	Dishonest employee	30
10/13/06	Orchard Family Practice (Englewood, CO)	Improper disposal	Unknown
10/19/06	Allina Hospitals & Clinics (Minneapolis, MN)	Stolen laptop	17,000
10/20/06	Manhattan VA Medical Center (NY, NY)	Stolen laptop	1,600
10/25/06	Swedish Medical Center (Seattle, WA)	Dishonest employee	1,100
10/26/06	Akron Children's Hospital (Akron, OH)	Hacked	235,903

Information provided by Privacy Rights Clearinghouse



Healthcare Security Breaches in 2006

<u>Date</u>	<u>Name/Location</u>	<u>Type of Breach</u>	<u># of Records</u>
11/2/06	McAlester Clinic/VA Med Ctr (Muskogee, OK)	Lost disks	1,400
11/2/06	Intermountain Health Care (SLC, UT)	Improper disposal	6,244
11/25/06	Family Health Center (Jeffersonville, IN)	Stolen computers	7,700
11/28/06	Kaiser Permanente CO (Denver, CO)	Stolen laptop	38,000
12/2/06	Gundersen Lutheran Med Ctr (LaCrosse, WI)	Dishonest employee	Unknown
12/14/06	Electronic Registry Sys (multiple hospitals)	Stolen computers	63,000

TOTAL number of records containing sensitive personal information involved in healthcare security breaches in 2006:

1,078,216


Healthcare Security Breaches in 2007



<u>Date</u>	<u>Name/Location</u>	<u>Type of Breach</u>	<u># of Records</u>
1/2/07	Deaconess Hospital (Evansville, IN)	Missing computer	128
2/2/07	VA Medical Center (Birmingham, AL)	Stolen hard drive	1,835,000
2/7/07	Johns Hopkins Univ. & Hosp. (Baltimore, MD)	Missing tapes	135,000
2/8/07	St. Mary's Hospital (Leonardtown, MD)	Stolen laptop	130,000
2/14/07	Kaiser Medical Center (Oakland, CA)	Stolen laptop	22,000
2/19/07	Seton Healthcare Network (North Austin, TX)	Stolen laptop	7,800
2/28/07	Gulf Coast Medical Center (Nashville, TN)	Stolen computer	9,900
3/1/07	Westerly Hospital (Westerly, RI)	Exposed online	2,242
3/2/07	CA Dept of Health Services (Sacramento, CA)	Exposed by mail	54
3/20/07	Health Resources, Inc. (Evansville, IN)	Exposed online	2,031
3/23/07	Group Health Cooperative HCS (Seattle, WA)	Missing laptops	31,000
4/5/07	DCH Health Systems (Tuscaloosa, AL)	Missing disc	6,000
4/10/07	GA Dept of Community Health (Atlanta, GA)	Missing disc	2,900,000
4/12/07	University of Pittsburgh Medical Center (PA)	Exposed online	88
4/24/07	Baltimore County Dept of Health (MD)	Stolen laptop	6,000
5/11/07	Univ. of CA Irvine Medical Center (Irvine, CA)	Missing file boxes	287

Information provided by Privacy Rights Clearinghouse


Healthcare Security Breaches in 2007



<u>Date</u>	<u>Name/Location</u>	<u>Type of Breach</u>	<u># of Records</u>
5/11/07	Highland Hospital (Rochester, NY)	Stolen laptops	13,000
5/17/07	Georgia Div. of Public Health (statewide)	Improper disposal	140,000
5/22/07	University of Pittsburgh Medical Center (PA)	Exposed by mail	6,000
5/24/07	Beacon Medical Services (Aurora, CO)	Exposed online	5,000
6/4/07	Stevens Hospital (Edmonds, WA)	Exposed online	550
6/6/07	Dearfield Medical Building (Greenwich, CT)	Improper disposal	Unknown
6/9/07	Concord Hospital (NH)	Exposed online	9,000
6/20/07	University Community Hospital (Tampa, FL)	Exposed by mail	Unknown
7/11/07	South County Hospital (South Kingstown, RI)	Stolen briefcase	79
7/24/07	St. Vincent Hospital (Indianapolis, IN)	“Security lapse”	51,000
7/28/07	Yuba County Health & Human Services (CA)	Stolen laptop	70,000
8/10/07	Legacy Health System (Portland, OR)	Stolen paperwork	747
8/11/07	Providence AL Medical Center (Anchorage)	Missing laptop	250
8/15/07	Greater Detroit Hospital (MI)	Paperwork exposed	Unknown
8/15/07	Sky Lakes Med Center (Klamath Falls, OR)	Exposed online	30,000
9/1/07	Johns Hopkins Hospital (Baltimore, MD)	Stolen desktop	5,783

Information provided by Privacy Rights Clearinghouse

Healthcare Security Breaches in 2007



<u>Date</u>	<u>Name/Location</u>	<u>Type of Breach</u>	<u># of Records</u>
9/9/07	McKesson	2 stolen desktops	"1,000s"
10/2/07	Athens Regional Health Services (GA)	Missing computer	1,400

TOTAL number of records containing sensitive personal information involved in healthcare security breaches in 2007 as of October 24, 2007:

5,423,339



Difficult Times for Healthcare Auditors

- ◆ Cyber attacks against hospitals, medical centers and clinics are frequently in the news
 - The healthcare industry is known to be poorly secured and is targeted by hackers
 - Insufficient funding
 - Patient information is readily available
 - Who has access to patient records?
 - A better question is who does not have access?
 - The mindset is to avoid security
 - Patient care is often used as an excuse (i.e. security will delay or impede care)
 - Vendors falsely claim that the FDA does not permit changes to COTS
 - Many facilities lack technical IT auditors and security personnel



HIPAA Has Not Improved Security

- ◆ All of the facilities we audit are HIPAA compliant yet they consistently fail penetration tests and vulnerability assessments
 - Not a single healthcare facility has passed one of our tests
- ◆ After several years of HIPAA, our penetration team is gaining access more quickly than ever before
- ◆ Executives are very concerned about their “investment” in HIPAA controls versus the results found during our audits
 - “How could we pay \$3.6 million and not be secure?!”
 - Network security and HIPAA compliance may not correlate
- ◆ The business effort required for HIPAA detracted from other critical security projects
 - Deferral of critical upgrades to applications and server security
 - Diversion of internal audit resources



Laptops and Workstations Are TTB's

- ◆ As can be seen from the reported incidents, stolen laptops and workstations are a major source of compromise
- ◆ The answer is simple: Encrypt all hard drives, whether on a workstation or a laptop
- ◆ Also encrypt all backups, particularly those being transported to another location
- ◆ I know the OUCH! factor is high on this, but you can pay to encrypt now, or pay up to \$200 for each identity stolen later
- ◆ Remember the Fram oil filter commercial: “You can pay me now, or you can pay me much more later”



Active Directory Issues

- ◆ Active Directory promised security improvements
 - Many organizations did not implement the required enhancements such as Kerberos
 - Patches not installed
 - Two factor authentication only partially implemented
- ◆ HIPAA did not focus on security reviews of critical machines
 - One poorly secured machine can give us access to the entire Windows Active Directory environment



Other Windows Issues

- ◆ Windows is the Achilles heel of hospital security
- ◆ Account lockout not in place on most machines
 - A weak security policy may exist on the AD and domain controllers, but not on local machines
- ◆ LanMan passwords still used
- ◆ Cross-over accounts are a serious unresolved issue
- ◆ MS-SQL creates some vulnerabilities
 - We can test 5,000 machines an hour, so why can't the IT folks?
- ◆ VNC still used in an unsecured manner
- ◆ LSAdump2 enables us to dump LSA secrets including unencrypted admin passwords
- ◆ Service accounts with default passwords are TTB/DAS



Solutions for the Windows Environment

- ◆ Identify the machines on the network (first step in all technologies)
 - Scan the network with Solar Winds IP browser standard edition (\$145)
 - We selected this product as it does not harm machines
 - Use NMAP to identify devices and ports
 - Contact the presenter for the safe settings for this product
 - Create a spreadsheet that classifies the devices on the network and services open on each device



Test All Windows Machines

- ◆ Use chklock to document the security policies on the machines
 - Identify machines with poor settings and no account lockout
- ◆ Use CIS or NBTenum against machines that do not have account lockout
 - Identify accounts with simplistic passwords
 - Identify accounts with unchanged passwords
 - Identify default accounts
- ◆ Use pwdump3e to download password files
 - Identify passwords that do not conform to the security policy using l0phtcrack
- ◆ Identify cross-over accounts to the domain



Test All Windows Machines

- ◆ Run patch tests using hfnetck to identify unpatched machines
 - Domain controllers, sensitive servers, etc. should be carefully scrutinized for missing patches
- ◆ Scan for the SQL ‘sa’ accounts with no password or a default password
- ◆ Test for VNC (ports 5800, 5900) on machines
 - Use NBTenum to determine VNC password(s)
 - Test all machines with VNC with the VNC passwords gleaned above
- ◆ Use LSAdump2 to identify passwords stored in “secrets”
 - Reduce setting of buffered passwords to 2 for workstations



Email and VPN's are not properly protected

- ◆ Exchange mail or Lotus Notes may be in the AD
- ◆ Blackberrys are not secured
- ◆ Two factor authentication often not used with outlook web mail
- ◆ VPN's may use encryption, but two factor authentication may not be used by all
 - Tokens for normal users, secondary passwords for other users
 - Trading partner resistance



Solutions for Email and VPN

- ◆ If the email server is on the AD, then administrators may have access to everyone's email
 - Also default service accounts, etc.
 - Remove the email servers from the AD if possible
 - Restrict those with administrative access to the email product
 - Executives and administrators should require tokens to authenticate to email
- ◆ Poorly secured VPNs are a hackers delight
 - Implement two factor authentication
 - Identify bypass accounts using passwords
 - Watch out for vendors who have a pathway through the firewall



Solutions for Blackberries

- ◆ Change the default passwords on the AD or Blackberry servers
 - (bberry:bberry, besadmin:besadmin)
- ◆ Ensure all communications are encrypted
- ◆ Most importantly, ensure that all Blackberrys have access passwords
 - Executives detest this control, but it is for their own protection
- ◆ Be prepared to “kill” lost Blackberrys
 - Be aware that a hacker could “kill” all Blackberrys



Network Devices are Not Properly Secured

- ◆ Community string issues
- ◆ Unnecessary ports and services
 - Port 80
- ◆ Clear text services permitted
 - telnet, ftp, http



Solutions for Network Devices

- ◆ Remove unencrypted services (ftp, telnet, tftp, http) with free secure versions
- ◆ Eliminate default community strings
 - Periodically test the two above items using Solar Winds IP browser
- ◆ Remove Cisco servers from the domain
 - Do not name them cs2000, ciscoworks or cisco
- ◆ Ensure all Cisco devices patched (html exploit, etc.)
- ◆ Search for, find and encrypt password cheat sheets
 - Use password safe or other product to secure the shared passwords



UNIX and LINUX machines

- ◆ Finger, EXPN and VRFY enable account enumeration
- ◆ Blank passwords including root passwords an issue
- ◆ Trust relationships abound!
 - Even + +
- ◆ It is time to eradicate trust relationships
- ◆ Patches an issue, particularly for HP-UX and SUN



Solutions for UNIX and LINUX

- ◆ Run and evaluate the Canaudit Scripts
- ◆ Identify accounts with default or simplistic passwords and change them
- ◆ Eliminate “simple” and unneeded services (tftp, finger, ftp, telnet, echo, chargen etc.)
- ◆ Trust relationships are always an issue
 - Eradicate them
 - If eradication is not possible, then isolate them in a restricted, filtered, VPN or behind a strong firewall.
 - Work with the vendor on a final solution

The Mainframe

- ◆ Logon failures are often not properly investigated
 - For example, we often put 10,000 or more password attempts
 - We normally get OPERATIONS and AUDIT capability within an hour
- ◆ The FTP port is usually not monitored
- ◆ We use cross-over passwords from the Windows environment and attack port 21 using Brutus



Solutions for the Mainframe

- ◆ Ensure that the FTP port is closed, use SFTP
- ◆ If FTP port cannot be closed, place account lockout on password violations against port 21
 - Shut down the port and generate a high priority alert if automated attack is detected
- ◆ Do not permit cross-over accounts
 - This is particularly true of those with sensitive access such as systems programmers and security folks
 - If cross-over accounts are used, then ensure the passwords are different from the passwords used in the Windows environment



Inside-out, Outside-in Exploits

- ◆ Remote control software slices through firewall security as the session is initiated internally
 - Examples are gotomyPC, logmein, remotely anywhere, BomGar, cryptcat, netcat, etc.
 - Contractors and employees can bring these tools preinstalled into the facility, or download it from within the facility
 - Once installed, the firewall is converted into an unauthorized hacker superhighway for attacking the internal network and harvesting data
- ◆ Physical security is ineffective in most hospitals as they are public venues
 - Placing Trojan machines on the network is simple



Solutions for Inside-out, Outside-in Exploits

- ◆ Work with the vendors to prevent or restrict network egress and ingress
- ◆ Monitor firewall for unusual data transmissions
- ◆ Ensure all internal machines are properly secured
 - If the machines on the internal network are secure, there will not be any targets.
- ◆ Unfortunately, it is difficult to close these doors



Oracle Databases Seriously Exposed

- ◆ Port 1521 open and not protected
- ◆ Oscanner and better tools available
- ◆ We gain DBA access in minutes
- ◆ Poorly controlled database links
- ◆ Off-shore development and testing
- ◆ Patches not installed



Solutions for Oracle

- ◆ Where possible, put passwords on the Oracle Listener port
- ◆ Ensure that all accounts have complex passwords, especially default accounts with DBA access
- ◆ Identify, secure and encrypt all authorized database links
 - Eradicate unauthorized dblinks
- ◆ Ensure that all exports (backups) are properly protected



The Best Advice I Can Offer

- ◆ Perform detailed technical security reviews of the Active Directory, all Windows and UNIX machines, Oracle and SQL databases, and network devices
- ◆ Perform a security baseline or vulnerability assessment
 - Security baselines provide metrics to monitor improvements and new issues over time
 - Vulnerability assessments are useful to ensure management understands the state of the network and the devices within it
- ◆ Once the network is considered secure, perform a penetration test

Conclusion

- ◆ We missed the boat from an IT audit standpoint
- ◆ 2008 must be the year we emphasize security
- ◆ Audits that skim the surface jeopardize security
- ◆ We need to hasten the return of **Real IT Auditors!**
 - The profession has dumbed down over the last 5 years and we must reverse this trend
 - Testing must be more aggressive
 - If auditors can't run scanners and other security tools, then hackers will succeed!



END OF PRESENTATION