CTH Technologies, Inc.

Recent Significant Data Breaches

Can companies continue to bury their heads in the sand when it comes to protecting their customer, patient or employee data? Can they afford to continue to take the risk that a data breach or compliancy fines will not happen to them?

The facts unfortunately paint an entirely different picture for every company today. Data Breaches and Compliancy Fines are occurring on a daily basis. In today's world, you must be proactive in protecting your sensitive data from accidental or malicious data breaches and have a plan on how to quickly resolve issues with stolen company laptops.

CTH Technologies provides an enterprise Data Leak Prevention solution that monitors, encrypts, blocks, alerts and audits the activity taking place at your critical data end points, such as desktops, laptops and file servers. The SecureCARE technology can be used proactively to deal with accidental or malicious data breaches by employees and outside contractors from downloading sensitive data on to thumb drives, burning CD's, printing confidential or customer data, and scanning & encrypting outgoing e-mail or IM. In dealing with stolen laptops or desktops, SecureCARE has the ability to scan hard drives and encrypt sensitive data, so your company will know exactly what information was on the equipment, making sure all sensitive data was encrypted while also giving you the location of the stolen equipment.

The list below is a snapshot of recent data breaches which have been tracked since the spring of 2005. The total list has around a thousand data breaches listed and if the trend continues, like it has shown over the last two plus years, there will be considerably more data breaches in 2008. Company brand names can be severely tarnished, customer trust will erode, costly law suits and stiff government fines are being levied on the effected companies on a daily basis. (ie. TJ Max, etc.) In today's world, government compliancy acts, such as PCI, SOX, GLBA and HIPAA are very real and companies are quickly trying to scramble to meet compliancy standards and avoid the penalties, fines and audits.

2005	**NAME (Location)**	**TYPE OF BREACH**	**NUMBER OF RECORDS**
March 11, 2005	Univ. of CA, Berkeley (Berkeley, CA)	Stolen laptop	98,400
April 2005	Georgia DMV	Dishonest insider	465,000
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
June 18, 2005	Univ. of Hawaii	Dishonest Insider	150,000

Dec. 25, 2005	Ameriprise Financial Inc. (Minneapolis, MN) (877) 267-7408	Stolen laptop	260,000
2006	**NAME(Location)**	**TYPE OF BREACH**	**NUMBER OF RECORDS**
Feb. 13, 2006	Ernst & Young (UK)	Stolen laptop	38,000 BP employees in addition to Sun, Cisco and IBM employees.
Mar. 3, 2006	Metropolitan State College (Denver, CO)	Stolen laptop	93,000
Mar. 8, 2006	iBill (Deerfield Beach, FL)	Dishonest insider	[17,781,462] Not included in total below.
Mar. 30, 2006	Marines (Monterey, CA)	Lost Flash Drive (USB)	207,750
May 22, 2006	U.S. Dept. of Veteran's Affairs (Washington, DC) (800) 827-1000	Stolen laptop	28,600,000
May 24, 2006	American Red Cross, St. Louis Chapter (St. Louis,	Dishonest employee	1,000,000
July 18, 2006	CS Stars, subsidiary of insurance company Marsh Inc. (Chicago, IL)	Stolen computer	540,000
Sept. 23, 2006	Erlanger Health System (Chattanooga, TN)	Lost Flash Drive (USB)	4,150 current and former employees
Sept. 25, 2006	General Electric (US Corporate HQ: Fairfield , CT)	Stolen laptop	50,000 employees
Nov. 3, 2006	Starbucks Corp. (Seattle, WA) 1-800-453-1048	Stolen laptop	60,000 current and former U.S. employees and about 80 Canadian workers and contractors
Dec. 5, 2006	Nassau Community College (Garden City, NY)	Lost printout	21,000 students
2007	**NAME (Location)**	**TYPE OF BREACH**	**NUMBER OF RECORDS**
Jan. 1, 2007	Wisconsin Dept. of Revenue via Ripon Printers (Madison, WI) (608) 224-5163 www.privacy.wi.gov	Lost printout	171,000 taxpayers
Jan. 11, 2007	University of Idaho, Advancement Services office (Moscow, ID) (866) 351-1860 www.identityalert. uidaho.edu	Stolen computer	70,000
Feb. 2, 2007	U.S. Dept. of Veteran's Affairs, VA Medical Center (Birmingham, AL)	Lost Flash Drive (USB)	48,000 veterans plus 535,000

	(877) 894-2600		
Feb. 8, 2007	St. Mary's Hospital (Leonardtown, MD)	Stolen laptop	130,000
Feb. 14, 2007	Kaiser Medical Center (Oakland, CA) (866) 529-0779	Stolen laptop	22,000 patients, but apparently only 500 records contained SSNs (the latter number is included in total below)
Feb. 19, 2007	Seton Healthcare Network (North Austin, TX)	Stolen laptop	7,800
Feb. 28, 2007	Gulf Coast Medical Center (Nashville, TN & Tallahassee, FL)	Stolen computer	9,900
Mar. 9, 2007	California National Guard (Sacramento, CA)	Lost hard drive	1,300
Mar. 23, 2007	Group Health Cooperative Health Care System (Seattle, WA)	Two lost laptops	31,000
Mar. 26, 2007	Fort Monroe (Fort Monroe, VA)	Stolen laptop	16,000
Mar. 30 2007	Los Angeles County Child Support Services (Los Angeles, CA)	Three stolen laptops	243,000
May 5, 2007	Transportation Security Administration (Crystal City, VA)	Stolen hard drive	100,000
July 3, 2007	Fidelity National Information Services Certegy Check Services Inc. (Jacksonville, FL)	Dishonest employee	2,300,000 Additional 6.2 million Total 8.5 million
July 28, 2007	Yuba County Health and Human Services (Yuba County, CA)	Stolen laptop	70,000
Aug. 23, 2007	New York City Financial Information Services Agency (New York, NY)	Stolen laptop	280,000 Not added to total. It is not clear that SSNs or financial account numbers were exposed.
Sept. 9, 2007	De Anza College (Cupertino, CA) (408) 864-8292	Thousands of former students might be at risk for identity fraud after an instructor's laptop computer, containing students' personal information, was stolen last month. The computer	4,375

		contained the students' names, addresses, grades and in many cases Social Security numbers.	
Sept. 12, 2007	TennCare / Americhoice Inc. (Knoxville, TN) To sign up for the free ID theft protection you must call AmeriChoice at (800) 690-1606.	There are 67,000 TennCare enrollees at risk of identity theft after a courier service lost their personal information. The lost information includes names, Social Security Numbers, birthdays and addresses.	67,000
Oct. 4, 2007	Massachusetts Division of Professional Licensure (Boston, MA)	Social Security numbers of about 450,000 licensed professionals were inadvertently released. The information was mailed last month to agencies that submitted a public records request for the names and addresses of professionals licensed by the division. The division mailed 28 computer disks to 23 agencies that use the information as a marketing or promotional tool. The disks would normally contain only the names and addresses of individuals licensed through the Division of Professional Licensure and the Division of Health Professions Licensure. However, the disks also included Social Security numbers.	450,000
Nov. 5, 2007	Alabama Department of Public Health (Montgomery, AL)	The personal information, including the names, ages and Social Security numbers of families enrolled in the state's ALL Kids health care coverage	1,554 Not added to total due to unclear total.

		program, were accidentally sent to the wrong families last week. 1,554 affected families were alerted that some of their confidential information might have been released.	
Dec. 17, 2007	West Penn Allegheny Health System (Pittsburgh, PA)	The names, Social Security numbers, phone numbers, addresses and patient care information of 42,000 patients were all on a laptop computer stolen from a nurse's home. Only home care and hospice patients could be impacted, not patients at the hospitals.	42,000
2008	**NAME (Location)**	**TYPE OF BREACH**	**NUMBER OF RECORDS**
Jan. 8, 2008	Wisconsin Department of Health and Family Services	Social Security numbers were printed on about 260,000 informational brochures sent by a vendor hired by the state to recipients of SeniorCare and other state programs.	260,000
Jan. 15, 2008	Naval Surface Warfare Center Dahlgren Division (White Oak, MD)	Officials at the Naval Surface Warfare Center are warning past and present employees that their identities and credit ratings could be at risk. Two pages of a Naval Surface Warfare Center Employment Verification Report was found when four people were arrested in Bensalem Township, Pa., last week for attempted identity fraud. The report included names, Social Security numbers, birth dates, position titles, tenure codes, pay grades, salaries and other information about the employees.	Unknown

TOTAL number of records containing sensitive personal information involved in security breaches	**217,555,182**

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm