



# Database Security: A Christmas Carol

David Litchfield

## The Past, Present and Future of Database Security

In 2006 there were 335 publicized data breaches in the U.S. So far in 2007 there have been 276. With the 5th anniversary of the SQL Slammer worm drawing near, now is a good a time as any to look back on the past of database security and ask how far have we come since then and is our data any more secure today? And what of tomorrow? How will our database systems fare in a world of emerging threats? Have we learned our lesson or will we be consigned to the graveyard of statistics?



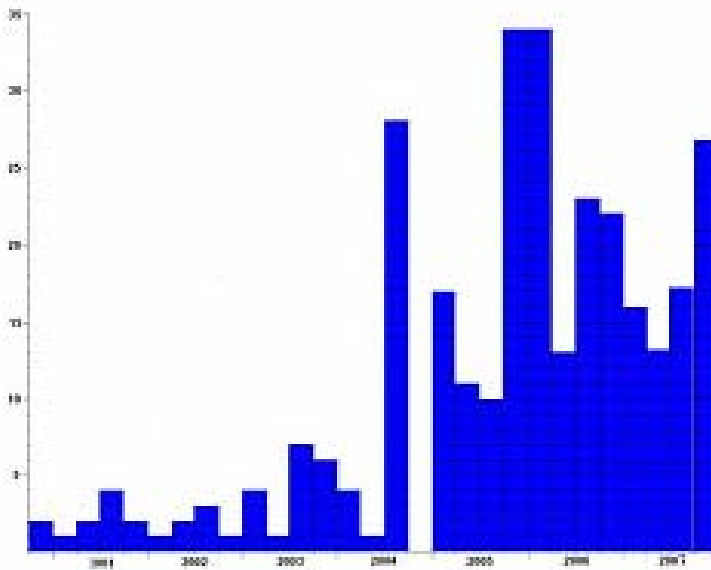
# Agenda

- Vulnerabilities
- Exposure
- Breaches
- Legislation
- Solutions

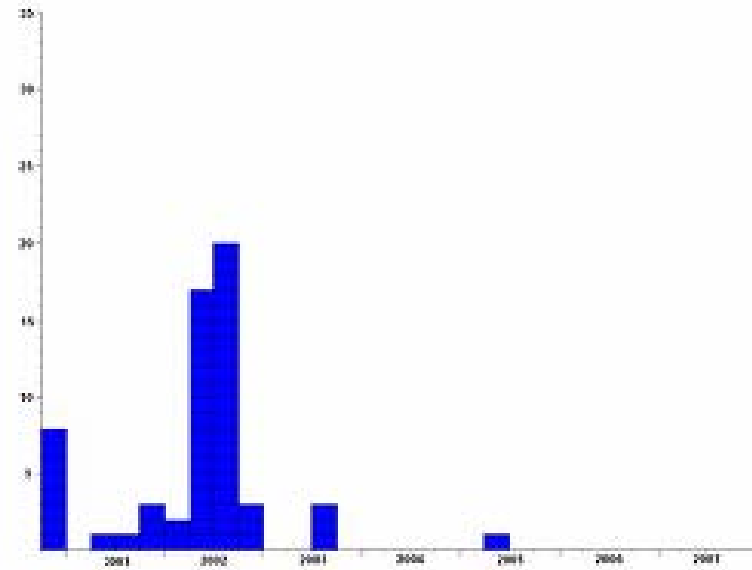


## Vulnerabilities fixed in 7 years

Oracle version 10, 9 and 8, SQL Server 7, 2000, 2005



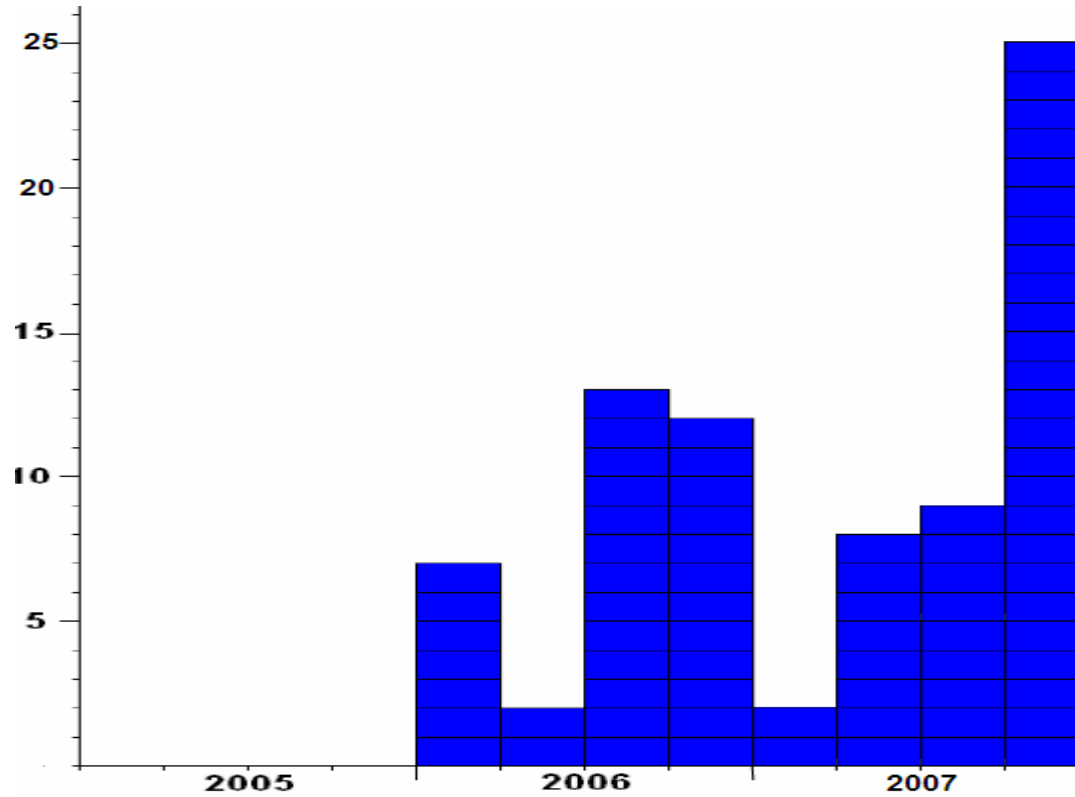
**Oracle**



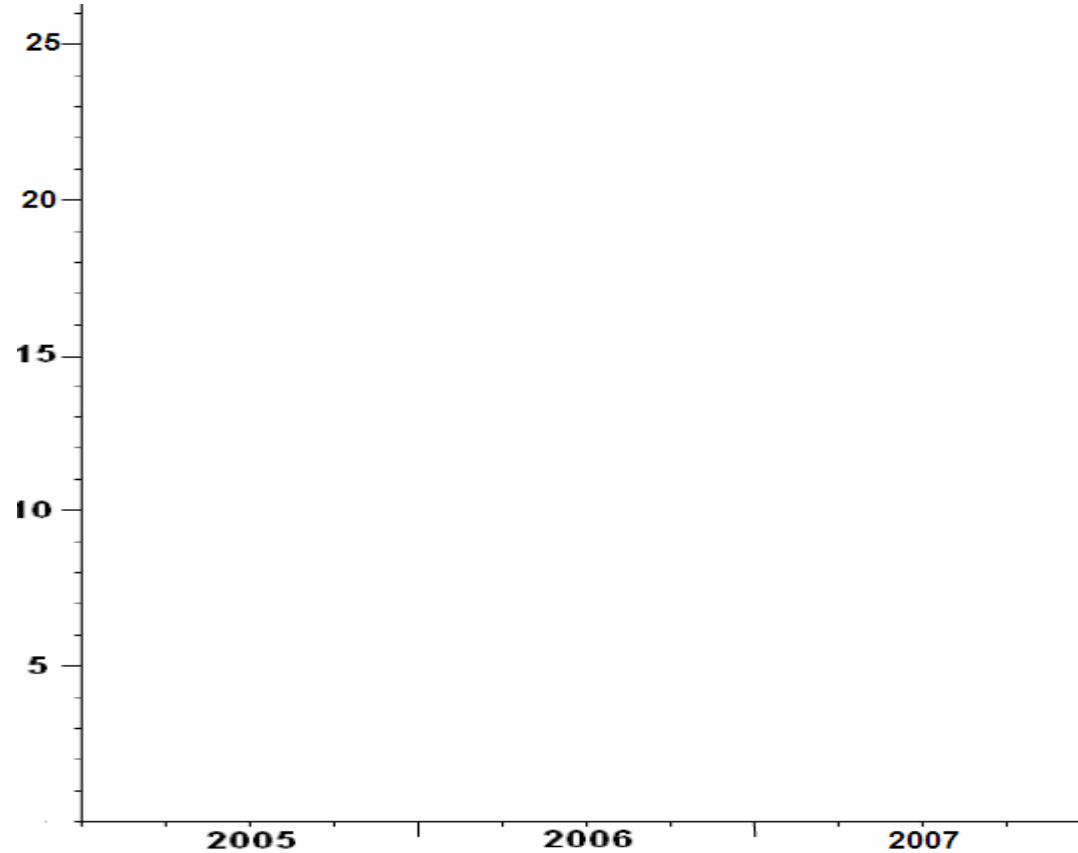
**Microsoft SQL Server**



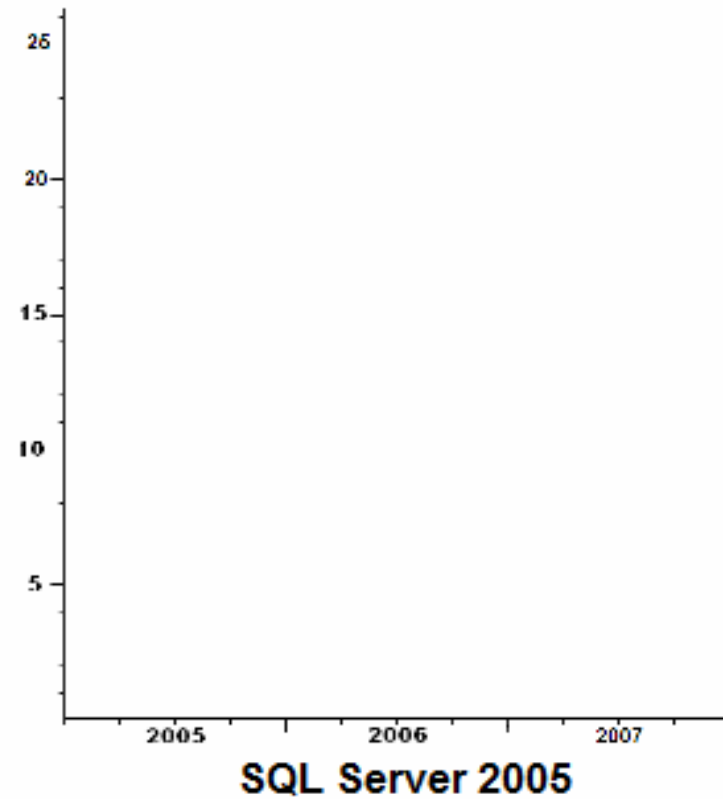
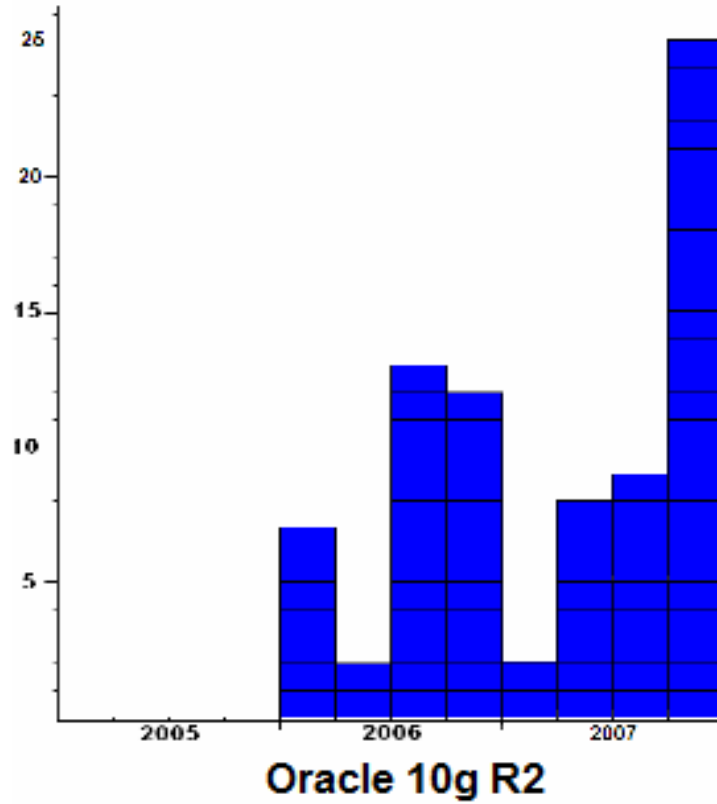
# Oracle 10g Release 2 (source Oracle CPUs, SecurityFocus)



# Microsoft SQL Server 2005 (source Microsoft Security Alerts, SecurityFocus)



# Microsoft SQL Server 2005 vs Oracle 10g R2



## Slammer - timeline

- Flaw found during assessment for bank in Germany in May 2002.
- MS02-039 released July 24<sup>th</sup>, 2002
- Black Hat, August 1<sup>st</sup> 2002
- Slammer launched 25<sup>th</sup> January 2005
- Infection rate doubled every 8.5 seconds
- 10 minutes to reach saturation point

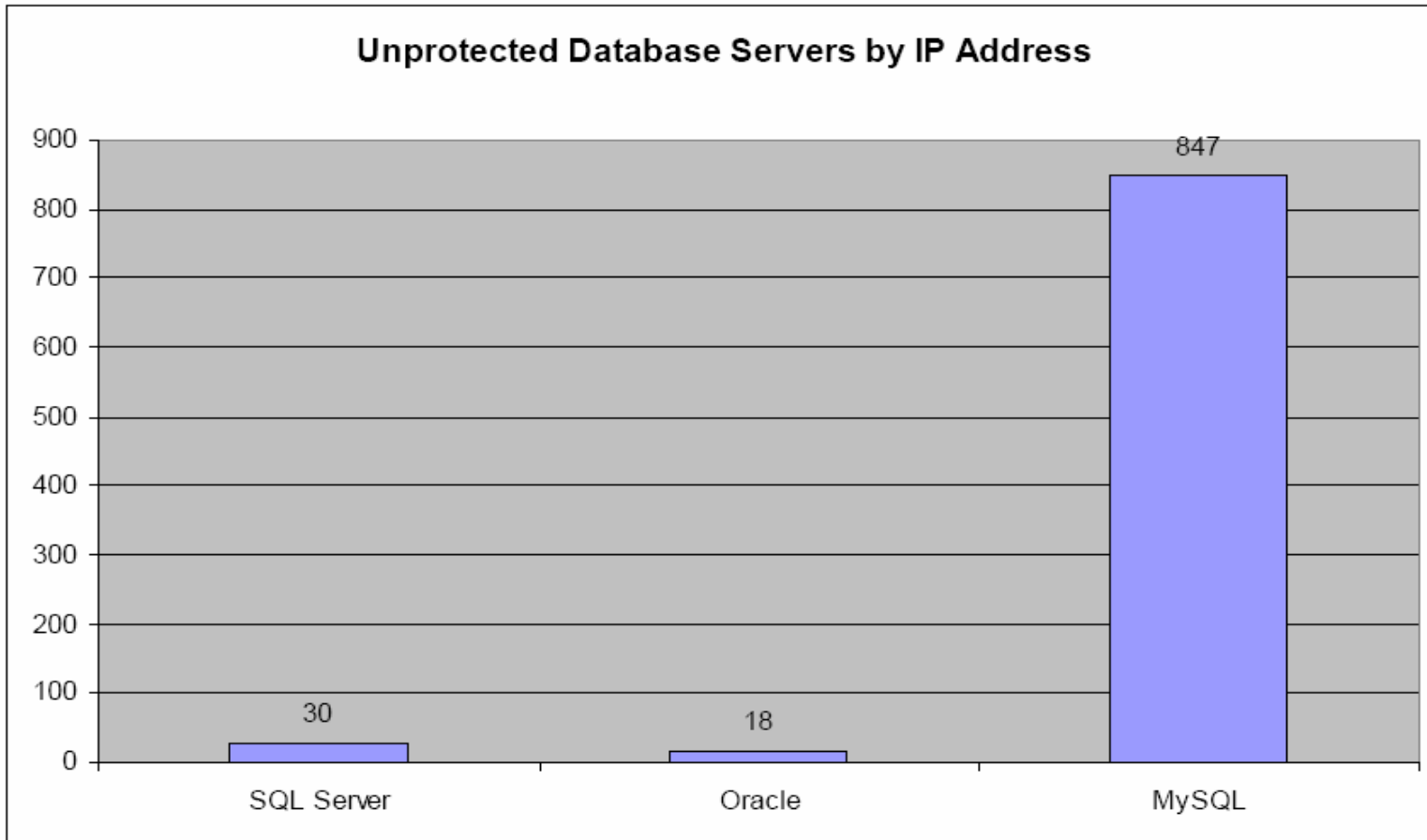


## Database Exposure Survey 2005

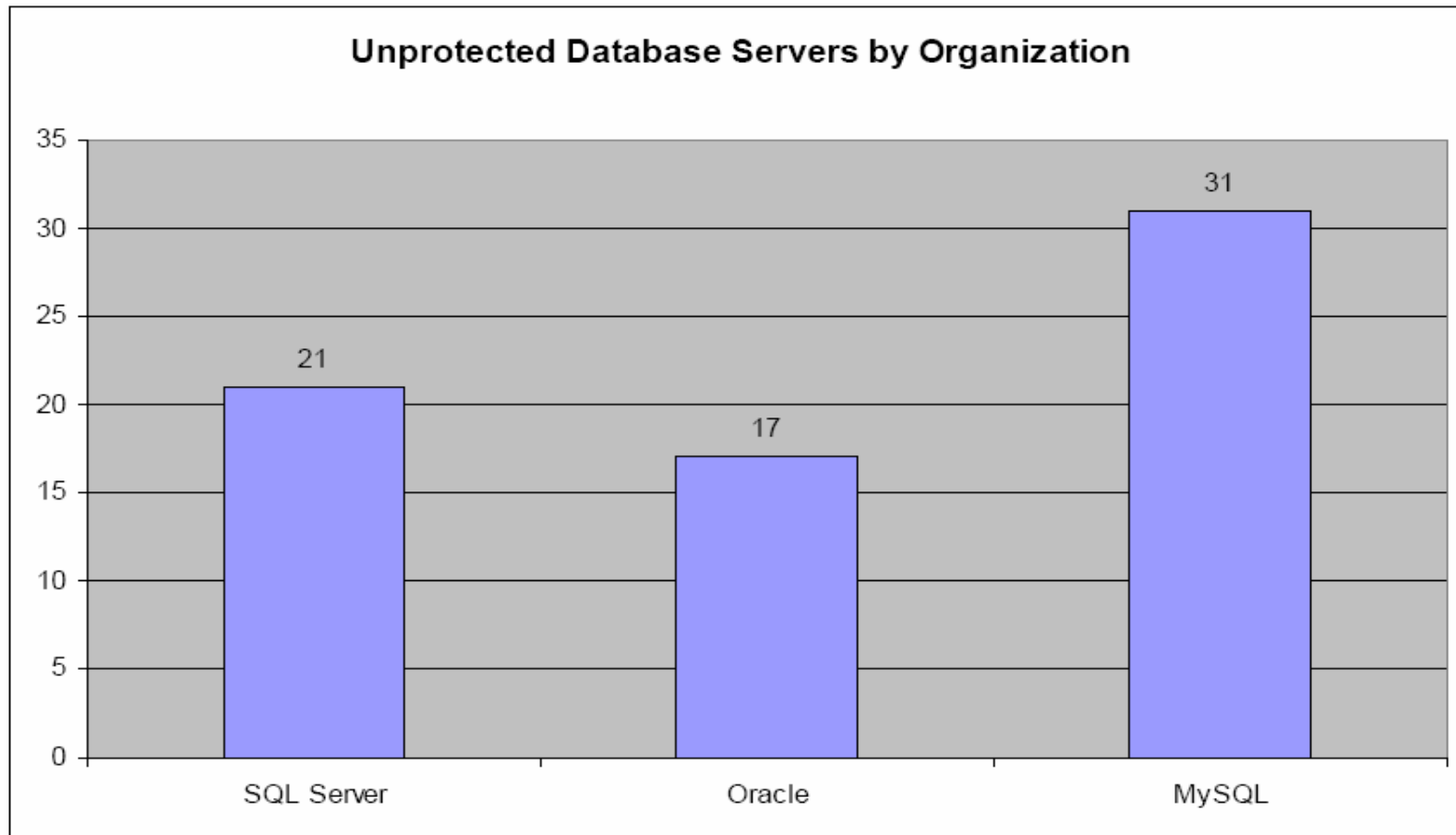
- 8,000 class C networks checked at random
- Total of 480,000 IP addresses checked
- Version check on TCP Ports
  - 1521 – Oracle
  - 1433 – MS SQL Server
  - 3306 – MySQL



## Exposed server numbers



## Numbers normalized by Organization



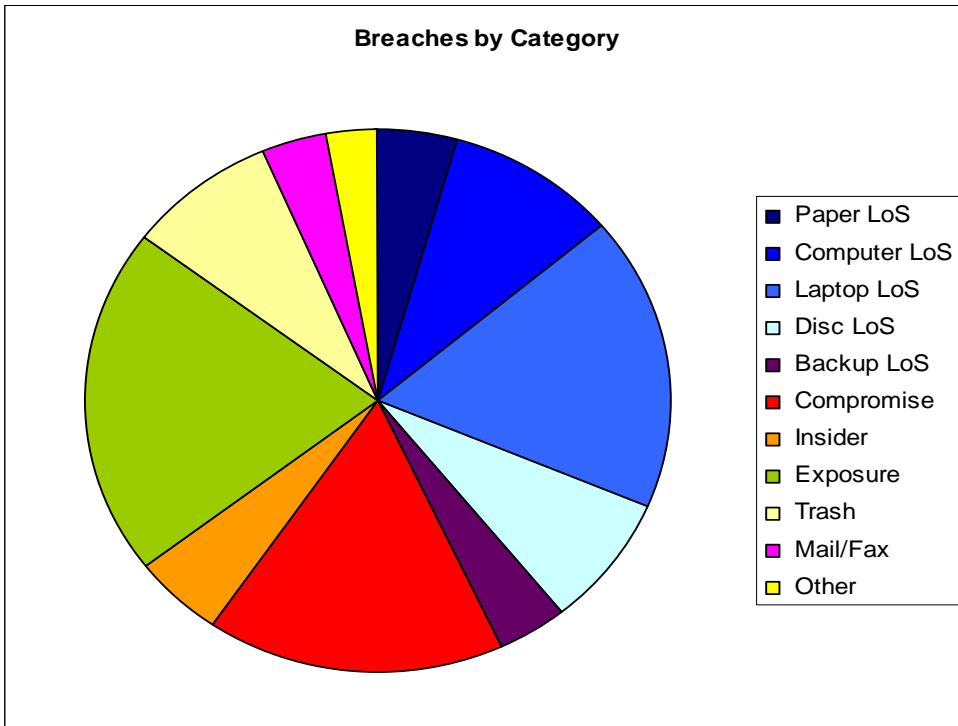
## Results

- 140,000 exposed Oracle servers
- 210,000 exposed SQL Server
- <http://www.databasesecurity.com/>



# Breaches

- From January 1<sup>st</sup> to 23<sup>rd</sup> October 2007 there were 276 breaches according to the Privacy Rights Clearing House (from Attrition.org numbers)



12	Paper
26	Computer
49	Laptop
21	Disc
11	Backup
45	Compromise
14	Insider
57	Exposure
23	Trash
10	Mail/Fax
8	Other



## Guess?, Inc, 3rd March 2002

In the February of 2002 a security aware customer, Jeremiah Jacks, whilst using Guess Inc's website discovered it was vulnerable to SQL injection [1]. He found that he could trivially gain unauthorized access to 200,000 customers' credit card details. After failing to get Guess to fix the problem Jacks contacted SecurityFocus.com to enlist their help. Within an hour Guess had resolved the problem with company spokeswoman Jennifer Munakash claiming, "It was an easy fix." [1] Indeed, when the Federal Trade Commission filed a complaint on 18th of June, 2003 it stated that "the risk of web-based application attacks is commonly known in the information technology industry, as are simple, publicly available measures to prevent such attacks." [2]. Guess settled the FTC charges on August the 5th, 2003.

[1] <http://www.securityfocus.com/news/346>

[2] <http://www.ftc.gov/os/2003/06/guesscmp.htm>



## Tower Records, 4th December 2002

During the November and early December of 2002, in a parameter tampering attack, hackers could gain access to orders purchased on the Tower Records website. The vulnerability (in the orderstatus.asp [1] page of the web application) allowed attackers to cycle through order numbers in their web browser's URL address bar and, if the order number was valid, details of the purchaser, such as name, address, phone number, etc were exposed. This vulnerability was actively exploited and details of the flaw appeared in two Internet chat rooms [2]. On the 21st of April, 2004, Tower Records settled Federal Trade Commission charges [3].

[1] <http://news.zdnet.co.uk/internet/0,1000000097,2127128,00.htm>

[2] <http://www.ftc.gov/os/caselist/0323209/040421comp0323209.pdf>

[3] <http://www.ftc.gov/opa/2004/04/towerrecords.shtm>



## Petco Animal Supplies, 30th June 2003

Jeremiah Jacks, emboldened by the Guess? hack, struck again, this time at Petco whom he discovered via a Google search of ASP pages [1]. Locating pages with parameters that could be manipulated, Jacks gained access to 500,000 credit card details via a SQL injection flaw that took "less than a minute to find". He reported the flaws to SecurityFocus.com who then alerted Petco to the issues. Petco moved to close the holes in less than an hour. Not long after this on the 5th of December the Federal Trade Commission started an investigation and issued a "Civil Investigative Demand". The case was settled just under a year later on the 17th November 2004.

[1] <http://www.securityfocus.com/news/6194>

[2] <http://www.securityfocus.com/news/7581>

[3] <http://www.ftc.gov/opa/2004/11/petco.shtm>



## CardSystems Solutions, Inc, 17th June 2005

On the 17th of June 2005, Mastecard alerted some its customers to a breach in the security of CardSystems Solutions, that had taken place between the end of 2004 and the May of 2005. At the time, it was the largest known breach of its kind. By exploiting a SQL injection flaw [1] in the company's website a hacker gained access to 40 million credit card details, of which they downloaded 264,000. In addition to the fact that CardSystems failed to take simple steps to secure the data, another problem with this breach that made it so egregious was that, in violation of the PCI Data Security Standards, data from each cards' magnetic strip was saved for research purposes. Although CardSystems were PCI certified by Cable and Wireless in June 2004 it seems that this practice was overlooked and not reported to the auditors. Due to this violation, on July the 18th, VISA said it would drop CardSystems [2] and Mastecard soon followed suit. This was the first time in the industry that a processor had been dropped. This effectively spelt the end of CardSystems Solutions. In October 2005 the assets of CardSystems were acquired by "Pay by Touch" [3] and on the 23rd of February 2006 they settled Federal Trade Commission charges [4].



## CardSystems Solutions...

This case is interesting for the class-action suit brought on June 27th by Ira Rothken on behalf of California credit card holders and merchants [5]. It sought to discover who, under California civil code section 1798.82, the data breach notification law, had the responsibility to notify the customers. Should it be CardSystems, or Visa and Mastercard or Merrick, the issuing bank? Or all of them? The judge, Richard Kramer, ruled that neither Visa nor Mastercard were required to alert individual customers [6].

[1] <http://www.ftc.gov/os/caselist/0523148/0523148complaint.pdf>

[2] <http://www.nytimes.com/2005/07/19/business/19visa.html>

[3] <http://www.finextra.com/fullstory.asp?id=14395>

[4] [http://www.ftc.gov/opa/2006/02/cardsystems\\_r.shtm](http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm)

[5] <http://www.techfirm.com/cardsystems.pdf>

[6] [http://www.emergentchaos.com/archives/2005/09/cardsystems\\_bre.html](http://www.emergentchaos.com/archives/2005/09/cardsystems_bre.html)



## Guidance Software, Inc, 20th December 2005

It is perhaps with some irony that Guidance Software found itself requiring the use of their own computer forensics software products in the early days of December 2005. Guidance, the developers of EnCase, discovered on the 7th of December that a hacker had compromised their database server via a SQL injection [1] flaw exposing the financial records of 3,800 customers. It is known that some of these records were abused. For example, one customer received a bill from Google for \$20,000 worth of pay-per-click advertising [2]. As well as having an insecure web application, Guidance had failed to encrypt their customers records in the database and had also stored each credit card's CVV number, both being contrary to the PCI DSS standards. A Federal Trade Commission investigation into the compromise was concluded on the 17th of November 2006 when Guidance settled the FTC charges [3].

[1] <http://www.ftc.gov/os/caselist/0623057/0623057complaint.pdf>

[2] <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121900928.html>

[3] <http://www.ftc.gov/opa/2006/11/guidance.shtm>



## Ohio State University, April 17th 2007

Ohio State University has the largest enrolment of students in the United States; it also seems to be vying to get the largest number of entries, so far eight, in the Privacy Rights Clearinghouse breach database [1]. One of the more recent attacks that took place on the 31st of March 2007 involved a SQL injection attack originating from China against a server in the Office of Research [2]. The hacker was able to access 14,000 records of current and former staff members [3].

[1] <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

[2] <http://209.85.129.104/search?q=cache:bKgj9Tx-CSAJ:www.infosec.ohio-state.edu/Main/Recent+ohio+sql+injection&hl=en&ct=clnk&cd=3&gl=uk>

[3] <http://www.osu.edu/news/newsitem1673>



## Certegy Check Services, 3rd July 2007

In a classic case of an insider job, Certegy, a subsidiary of Fidelity National Information Services, became the victim of data theft by one of its senior database administrators [1]. Named in a suit brought by Certegy, William Sullivan [2], allegedly stole 8.5 million consumer records [3] and sold them to various marketing companies. The investigation was started after one of Certegy's customers linked unsolicited telephone calls and mails to cheque transactions. After finding no evidence of an external compromise the company alerted the U.S. Secret Service who contacted the marketers in order to discover the source. The trail led back to a company called S&S Computer Services owned and operated by Sullivan. By all accounts the data was exfiltrated by physical means. On one hand this could have been physical backup tapes or on the other hidden in an iPod.

[1] <http://www.fidelityinfoservices.com/FNFIS/NewsRoom/20070703.htm>

[2] [http://pubtitlet.co.pinellas.fl.us/servlet/civil.docket.KEAD?CS\\_CASE=07006271C\\_I&CS\\_RESULTS\\_KNT=10](http://pubtitlet.co.pinellas.fl.us/servlet/civil.docket.KEAD?CS_CASE=07006271C_I&CS_RESULTS_KNT=10)

[3] <http://www.sec.gov/Archives/edgar/data/1136893/000089256907000950/a32114e8vk.htm>



## TD Ameritrade, 14th September 2007

TD Ameritrade, a Nebraska based online trading company, announced on September 14th 2007 that one of its database servers had been compromised by a hacker exposing 6.3 million customer records. The breach came to light when a large number of TD Ameritrade's customers started complaining about receiving investment based spam ("pump and dump" stock scams) causing the company to start an investigation [1]. The investigation revealed that a hacker gained access to customer information such as their names, email addresses, snail mail addresses and phone numbers. The investigation concluded that no social security numbers, account numbers or dates of birth were taken despite the fact that such details were stored and available in the same database server. This case is interesting as it clearly shows a targeted attack with a specific agenda. The hacker didn't go after SSNs, etc (which would enable them to commit ID theft); they didn't go after the clients' assets (which could enable them to commit financial theft); they harvested email addresses of people known to engage in buying and selling stocks to target them with their spam stock scam program.

[1] <http://www.amtd.com/newsroom/releasedetail.cfm?ReleaseID=264044>



## Legislation and Contractual

- PCI Data Security Standard
- Federal Trade Commission Act
  - Section 5(a)
- SOX, HIPAA, GLBA
- State Data Breach Notification Laws
  - California Senate Bill 1386
  - 34 more States since



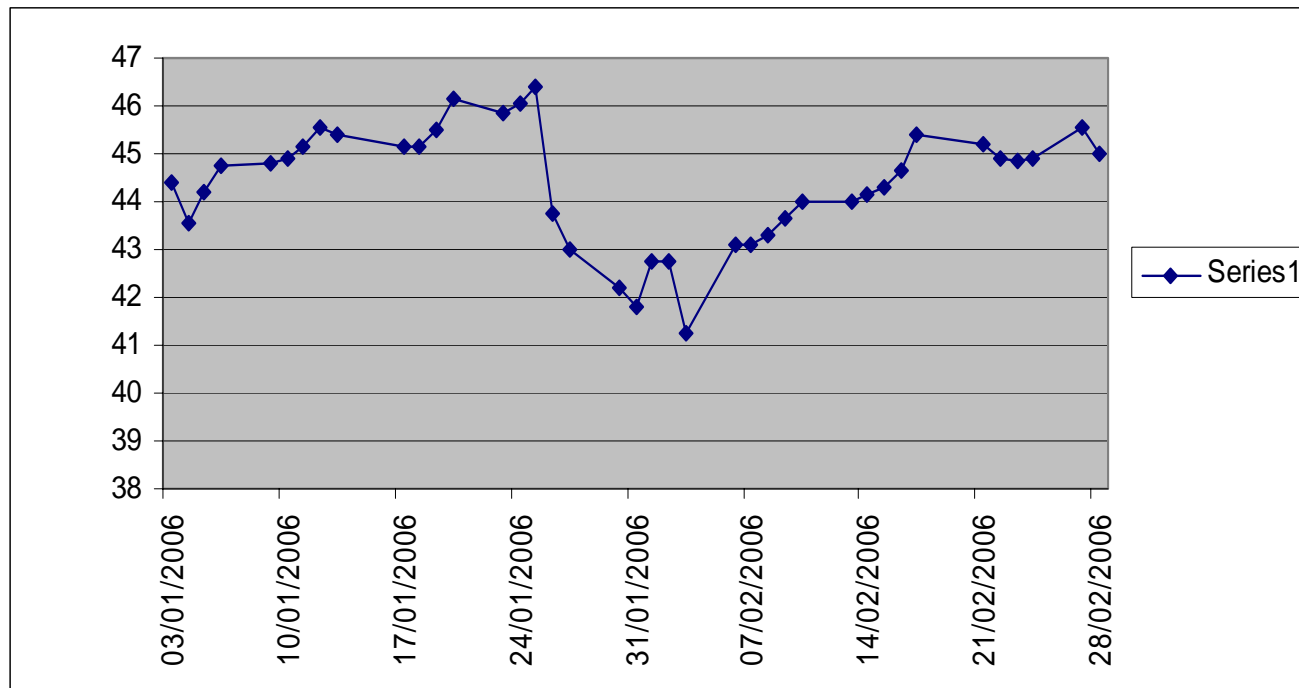
## Punishment for lax security

- Looking after customers' and company's interests should be the motivator
- Doesn't always work like that, though
- Penalties should be much more severe
  - DSW, Choicepoint aside (where financial penalty was imposed) , an FTC slap on the wrist not good enough
  - Perform a security audit biannually. What???
- No one likes the idea of having to punish but examples must be made ~ fear of the punishment must be greater than the fear of the "crime".
- Might be impractical – no-one left???



## Choicepoint – FTC

- Not a breach but lax business practices.
- Fined \$15 million on January 26<sup>th</sup>, 2006
- Stock price dropped sharply



## CardSystems Solutions, Inc – VISA and Mastercard

- Dropped by VISA and Mastercard for PCI DSS violations
- Effectively shut down the business
- Jobs were lost – too harsh?
- Getting the balance right can be difficult!



## Making sure you don't become an FTC case!

- Care about it all!
- Ask, if you were your own customer what would you want?
- Comply with standards, or go beyond, not because you have to but because it's right to do so.
- Acquire better business ethics



## Practical quick hits

- Ensure your databases are protected by a firewall
- Deploy IDS/IPS
- Change default user IDs and passwords
- Encrypt customer data
- Audit database accesses
- Keep on top of patches
- Perform regular vulnerability assessments
  - Pay close attention to SQL injection in web apps!





**Thank You**

<http://www.ngsconsulting.com/>