

“We Have Seen the Enemy and He is Us”

Walt Kelly, via Pogo



ZECURION

Treats Internal Threats

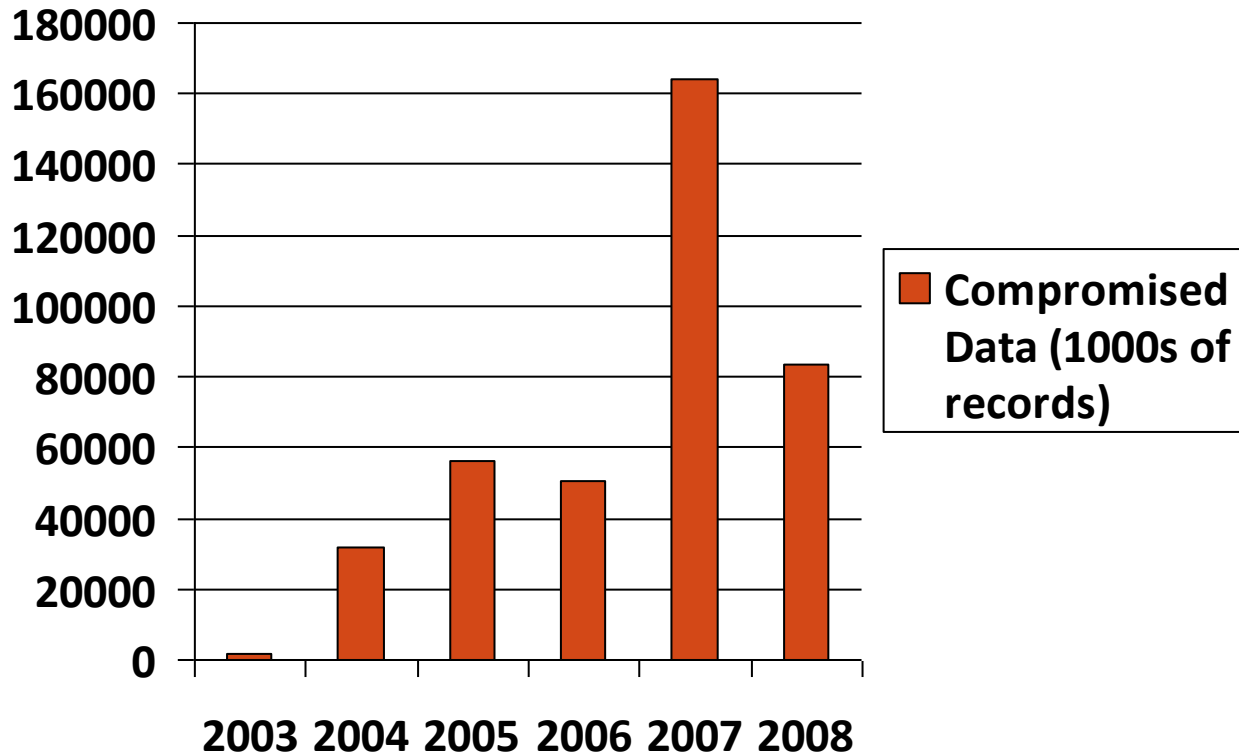
Why Focus on Internal Threats?

- Insiders are the number one cause of all data breaches, with hackers ranking a distant 5th
- External sources, “hackers,” commit only 1% of data breaches (Compuware Survey)
- 79% of IT practitioners reported at least one incident of data breach in 2008
- Rising number of government regulations and security protocols

A Growing Problem

- In 2000 more than 371,400 records were compromised through loss and theft
- Estimated financial cost to businesses:
 - \$75,022,800*

A Growing Problem

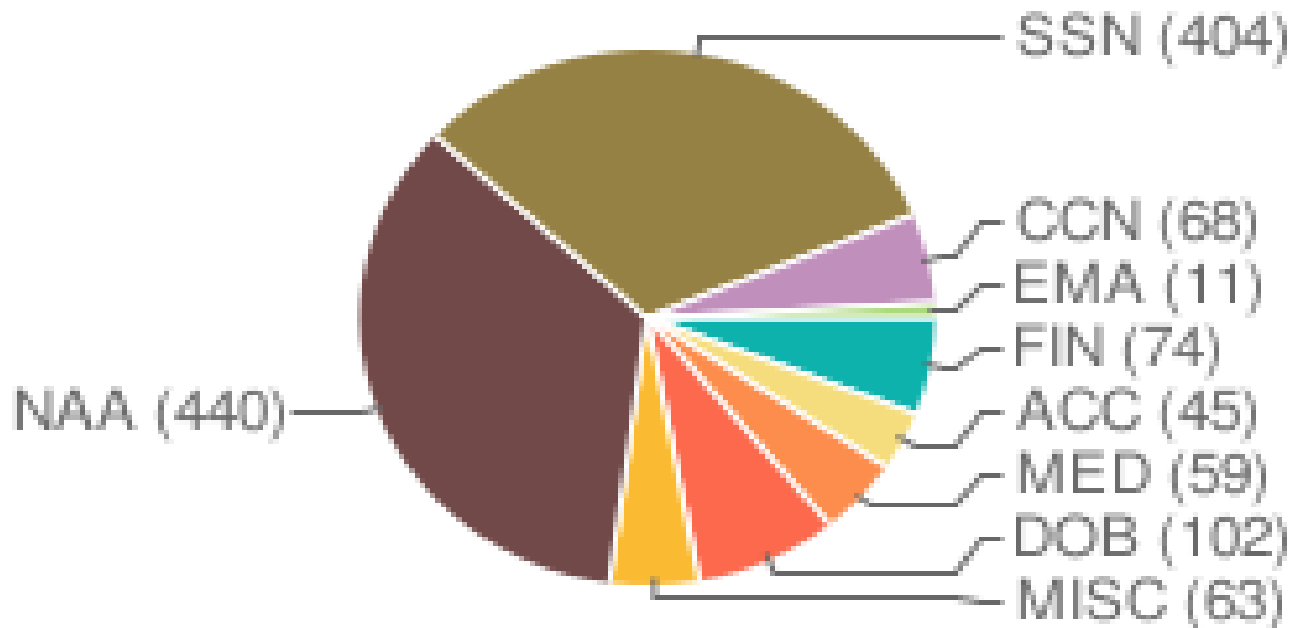


And by 2008...

- Total records compromised:
 - 83,490,075*
- Nearly a 225% increase in 8 years
- Estimated cost to the economy:
 - *\$16,864,995,150**

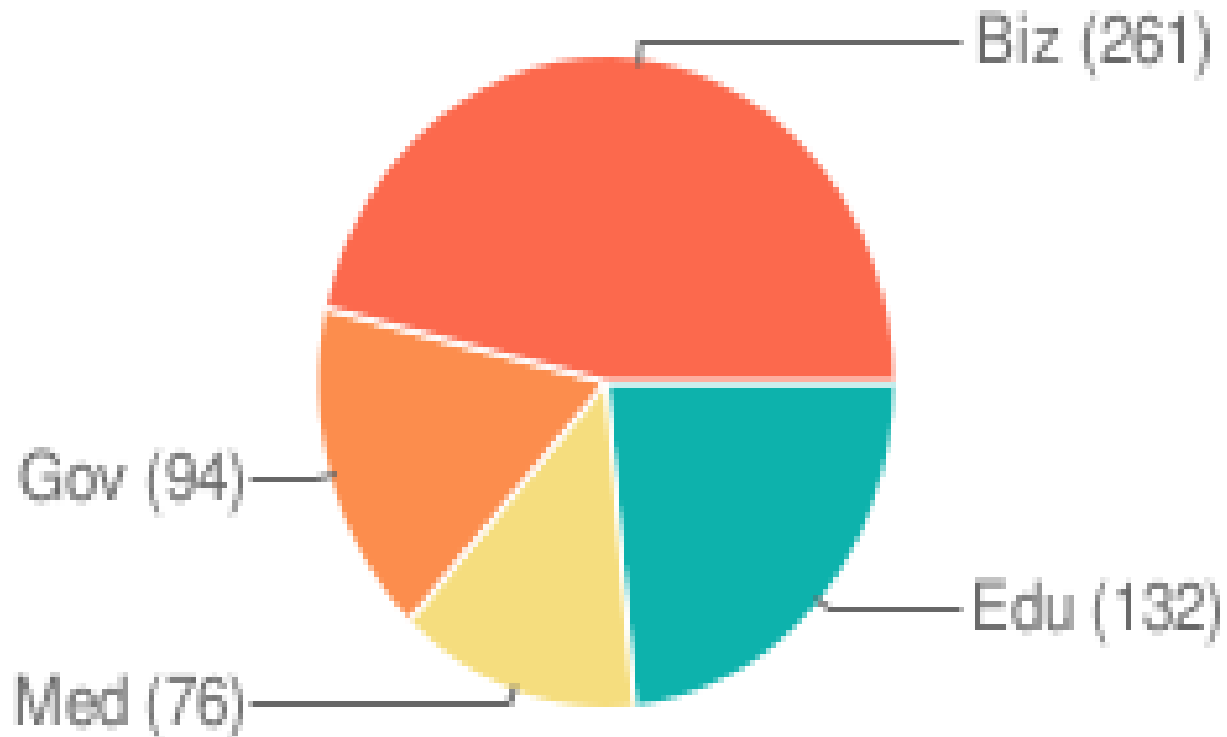
What Types of Data are Affected?

Incidents By Data Type



Every Organization is a Target

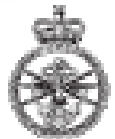
Incidents By Sector



In Bad Company – Case Studies in Damages



GE Money
UNITED STATES



defence



MARINES
THE FEW. THE PROUD.



IRON MOUNTAIN®

HARVARD UNIVERSITY

JPMORGAN CHASE & CO.

kraft foods
Make today delicious

Georgetown
UNIVERSITY
est. 1789

GS Caltex

In 2008 alone more than 83 million records were compromised. Nearly 12.5 million customers and employees of the organizations above had their personal records compromised from the loss or theft of poorly secured data.

In Bad Company – US Veterans Affairs



Theft of vets' data kept secret for 19 days, Social Security numbers of 26 million-plus veterans stolen

May 23, 2006;

- **WASHINGTON (CNN) -- Authorities waited almost three weeks to alert the public that personal data on more than 26 million U.S. veterans had fallen into the hands of thieves, a government source said Tuesday.**
- **The data were on a laptop and external drive stolen May 3 in an apparent random burglary from the Montgomery County, Maryland, home of a Department of Veterans Affairs computer analyst, said the government source, who has been briefed on the issue.**
- **The computer disk contained the names, Social Security numbers and birth dates of every living veteran from 1975 to the present, Veterans Affairs Secretary Jim Nicholson said Monday.**

In Bad Company – US Veterans Affairs



- The analyst is a longtime department employee but was not authorized to take the information home, he said.
- "They weren't after this [data]," he said. "There's a pattern of these kind of burglaries in this neighborhood."
- **But the missing information could be gold for electronic identity thieves, who operate hundreds of Internet sites where personal information is bought and sold.**
- "It's a pretty dire situation," said Rutrell Yasin, technology editor of Federal Computer Week, which covers computer and information technology issues in the federal government. "You have to hope that information is not in the hands of people who know what to do with it."
- **Yasin said the theft should be a wake-up call to federal agencies.**
- "They should certainly have the necessary security on their computers, secure communications links that would protect personal data," Yasin said.

In Bad Company – US Veterans Affairs

Lawmakers cite concerns

- "I've got to ask -- and certainly I have to ask it of not only the VA but all of government -- why can a data analyst take all of this information home?" the Idaho Republican said. "That's a breach of security -- in today's concern about ID theft -- that is huge."
- "Of course, I think it awakened the secretary to the vulnerability within his own organization, and that's true, I would guess, across government."
- "I expect VA's inspector general and the FBI to work closely together so that we can identify and eliminate the flaws that allowed this leak and prosecute any criminal acts," the Indiana Republican said in a written statement.
- "I know that VA is taking steps to notify veterans and provide help on consumer identity protection. The committee will examine this incident in the context of previous data compromises, to ensure that veterans' information is safeguarded."

Threats from Portable Memory Units

Can you be sure that your employees don't print or copy confidential information onto removable memory units?



Challenges to Protecting Portable Memory

- Huge array of various devices
- No adequate way to control use or extraction by employees or consultants either done deliberately or accidentally
- Traditional control methods may interfere with normal business practice
- Small size of storage units with high memory capacity make each information/data extraction a potential loss disaster

How Much is Your Data Worth?

In a recent customer meeting, one of Zecurion's consultants asked a banking manager what his data was actually worth. He replied simply, "About 15 years of my life if I lose it."

Pepperdine University's Graziadio School of Business and Management estimates that ensuing network downtime caused by data leakage can range anywhere from \$50,000 - \$1,000,000 per hour depending on the size and operational deployment of the network.

How Much is Your Data Worth?

- Average cost of a data breach in 2008:
 - \$202 per record
- Average total cost per breach event:
 - \$6.6 million (up from \$4.7 million in 2006)
- Average cost of lost business per breach:
 - \$4.59 million (\$139 per record)

And the Survey Says...

The Ponemon Institute, an independent research and advisory organization focused on information security and privacy, found the following in their 2008 survey of data breaches occurring in 43 organizations:

- 44 % of respondents experienced a breach traceable to consultants, partners or outsourced labor
 - The cost of these incidents are about 29% higher than if the breach is caused by a regular employee
- 49% are creating additional manual procedures and controls
- 44% have expanded their use of encryption technologies, followed by identity and access management solutions to prevent future data breaches

And the Survey Says...

The Ponemon Institute conducted another survey in February 2009 interviewing just under 1000 staff who had changed jobs in the last year.

- 59% of employees who leave or are asked to leave a company and have access to proprietary information steal company data
- 67% of respondents who stole data used the stolen information to leverage a new job
- The stolen information consisted of customer data, email lists, contact lists, employee records, financial reports, confidential business documents, software and other intellectual property.

An Urgent Need

- Regulation is driving the need
 - HIPPA
 - Sarbanes Oxley
 - Data Protection Act (UK)
 - Massachusetts / Nevada Personal Data Protection Laws
- Security breaches are up nearly 225% since 2001
- Healthcare, banking and insurance are closely watched
- Data breaches costs topped \$16 billion in 2008
- Privacy Rights Clearinghouse has identified more than 250 million records of U.S. residents that have been exposed due to security breaches

Laying Down the Law

- 44 states, along with the District of Columbia, Puerto Rico and the Virgin Islands, require that individuals be notified if their confidential or personal data has been lost, stolen or compromised
- When a regulatory breach occurs, organizations must notify all affected individuals, attempt to minimize downstream brand consequences and put solutions in place to prevent a recurrence
- Specific conditions for notification vary by state, yet organizations may not be required to notify individuals when the breached data is protected by encryption or the breach was stopped before information was wrongfully acquired

Where You Least Expect

- In June 2008, Adam Penenberg wrote an article titled, “The Black Market Code Industry,” for *FastCompany*
- He uncovered two HP employees actively selling exploit code in their spare time, with one selling exploits in HP’s own software
- According to the article, HP knew about one of the employees at the time of the article and were conducting an investigation

The Bottom Line...

- Research by the Ponemon Institute revealed that insiders of companies were the number one cause of all data breaches, with hackers ranking a distant fifth
- Insider threats are behind about 75% of all breaches in the U.S., while external hackers committed only 1% of breaches
- Most IT departments focus on outside threats, but may not fully realize the potential dangers posed by employee theft of critical business intelligence and proprietary data
- Traditional network perimeter security systems such as VPNs, firewalls and intrusion detection/prevention systems (IDS/IPS), cannot prevent threats of physical access by unauthorized employees, loss or theft of the media

Defense Plans

- Peripherals are necessities for normal business operations; the only secure solution is to manage and monitor access to these ubiquitous devices
- IT departments must exert full control over computer hardware resources and peripherals
- User or user groups policies giving full, read-only or no access to each physical or logical device must be implemented
- A software log of all access attempts and shadow copies of any protected data copied to an external media storage device, must be created and maintained

Defense Plans

- Administrators must identify individual storage and peripheral devices using a number of criteria including serial number, type and manufacturer
- For each device or device class, administrators should create as many policies as necessary with options to make these policies permanent, recurrent or one-time only
- Additionally, security policies can be assigned to printers, along with “shadow copy” printing, for complete control over physical copies of corporate information
- Administrators must gain full control over peripherals
 - Not only to prevent employees from walking out with confidential information copied on a CD, but also warning the IT department of potential threats

Where the Vulnerabilities Exist

- Theft of disk drives and magnetic tapes
- Breaches during server or hard drive maintenance
- Theft during transportation of computers and storage
- Access control to drives and storage media
- Theft and loss of computers and drives

Realities of Securing Data

- No company is immune, regardless of size
- Theft and loss will likely continue to rise
- Requires multiple levels of protection
- Being inside the “fort” is not enough
- Small form factor mass storage = single point of failure
- Major reasons for security include:
 - Protect integrity of data, Intellectual Property and proprietary information
 - Protect against liability (SOX)
 - Protect corporate reputation and future sales