

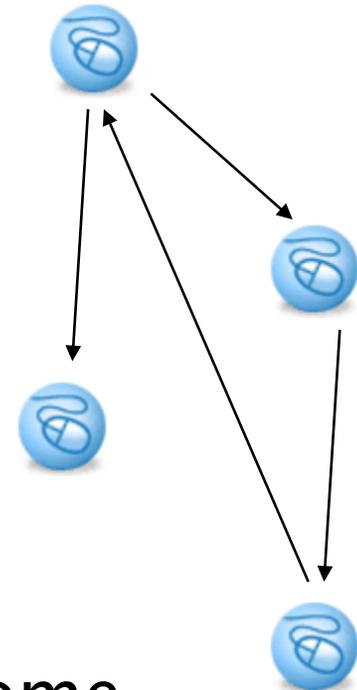


Data Breaches, Identity Theft, and Employees

**Joining the Dots
and Dispelling the Myths**

What you'll learn

- ▶ Data Breaches + identity theft + employees
- ▶ Data Breaches or Data Donations?
- ▶ Data Breaches + Identity Theft
- ▶ The True Cost of Data Breaches
- ▶ Who's to blame?
- ▶ Join the dots and change the outcome



We are the data!

- ▶ Data breaches *rarely* result in identity theft.
- ▶ Data breaches *rarely* involve hackers or other criminals
- ▶ **Most** data breaches are an inside job, but *not* a crime
- ▶ **Most** data breaches can be avoided by better employee awareness and education
- ▶ Awareness is *the* cheapest security on the block
- ▶ And it doesn't even have to work, to work!



What is a data breach?

“The definition of a breach is so broad, almost nothing is excluded.”

- ▶ Failure to encrypt data before sending it out (to a payroll service, for example)
- ▶ Failing to properly erase data from hard drives before transporting or disposing of the computer.
- ▶ Failing to properly protect credit card information after a transaction.
- ▶ Failing to properly protect employee payroll information from other employees.



What is a data breach?

- ▶ Losing a laptop with unprotected data.
- ▶ Dumping data in the trash without shredding it first.
- ▶ Inadvertently posting sensitive information unprotected on a computer, server, or web site.
- ▶ Copies of data, such as computer discs, that can't be accounted for.
- ▶ A computer sent out for repair without protecting or removing sensitive data first.



What is a data breach?

- ▶ Failing to adequately protect backup data.
- ▶ Losing a flash data drive containing sensitive data.
- ▶ Failing to restrict access to sensitive data only to employees who need access.
- ▶ Storing sensitive information on a network or internet-connected computer without a properly installed firewall.

And data doesn't have to be credit card information. It can be home address, phone numbers, order histories, or email address.



Drip, Drip, Drip.

The Year of the Data Breach

- ▶ Data breaches up 40% in 2007, 443 reported breaches, exposing 127 million records
- ▶ In the first half of 2008 there were 342 reported data breaches.
- ▶ TJ Maxx breach (Jan 07) may have exposed nearly 100 million customers.
- ▶ TJ Maxx originally estimated \$3–5 million, then admitted \$250m. Ultimate cost could exceed \$1 billion



Do data breaches = identity theft?

- ▶ Anywhere between 7 and 15 million Americans fall victim to identity theft every year.
- ▶ Identity theft may cost businesses and individuals as much as \$50 billion
- ▶ **There's little evidence that data breaches lead to identity theft**
(Source: The Government Accounting Office (GAO))
- ▶ Although previous studies have proven that only a fraction of fraud in the U.S. is due to data breaches, **77% of consumers intend to stop shopping at merchants that suffer from data breaches.**

(Source: Javelin Research, April 2007)

The Real Cost to the Losers

Money

Profits

Share value

Trust

Reputation

Brand

Customers

Jobs

Lawsuits



The financial cost to the losers

- ▶ Data breach incidents cost companies \$197 per compromised customer
- ▶ Lost business opportunity, including losses associated with customer churn and acquisition, represented the most significant component of the cost increase – \$128 in 2007
- ▶ Average total per-incident costs in 2007 were \$6.3 million
- ▶ The cost of lost business increased to \$4.1 million in 2007, approximately two-thirds of the average total cost per incident.



(Ponemon Institute 2007 Annual Study: Cost of a Data Breach.)

The cost of a data breach

- ▶ Breaches by third-party organizations such as outsourcers, contractors, consultants, and business partners were reported by 40 percent of respondents.
- ▶ Breaches by third parties were also more costly than breaches by the enterprise itself, averaging \$231 compared to \$171 per record.

“Although companies are responding to data breaches more efficiently, consumers seem to be less forgiving when their personal information is compromised.”

Dr. Larry Ponemon, chairman and founder of The Ponemon Institute.

The Impact on Customers

- ▶ 84% of American consumers have reported increased concern or anxiety due to data loss events.
- ▶ 62% of consumers have been notified that their confidential data has been lost.

(Ponemon Institute)



The Impact on Customers

- ▶ **“12 million consumers have switched banks to reduce the risk of becoming victims of identity theft.”** Financial Insights
- ▶ **More than two thirds of the American public have lost confidence in the handling of their personal information.”** Privacy and American Business and Harris Interactive study



The Impact on Customers

- ▶ 62% of consumers said that they would be more upset with a company that lost their information due to negligence than if that company lost their information as the result of theft.
- ▶ 85% will reward companies who are perceived as security leaders with increased purchases.

(Source: Javelin Research)



Ready to meet the bad guys?

- ▶ “Employee misconduct and unintentional actions like errors and omissions are the greatest cause of data security breaches.”
(2007 Global Security Survey, Deloitte Touche Tohmatsu)
- ▶ “Insider misuse and unauthorized access to information by insiders are the No. 1 and No. 2 security threats worrying IT security professionals.”

Computer Economics' "Trends in IT Security Threats: 2007"

"Security awareness training is arguably the most important part of a successful security program."

Computerworld, 2007



Employees and Data Breaches

- ▶ In the first six months of 2007 there were more than 70 publicized data breaches attributed to employee or insider error.
- ▶ In June 2007 alone, 24 reported data breaches attributed to user error or dishonesty exposed the personal records of nearly 3 million Americans.
- ▶ Of more than 342 data breach incidents in the first six months of 2008, the vast majority were traced to employees and insiders, including human error, dishonest actions, and the loss of computers. Only 14% were a result of outside hackers.

(Privacy Rights Clearinghouse)

Why are employees such a risk?

1. Lack of security awareness training.
2. Inadequate security awareness training.
3. Failure to create or enforce security policies
4. Lack of security awareness champions
5. Lack of management commitment to security awareness



Other insiders are to blame too

- ▶ Senior management either doesn't "get it" or doesn't want to admit it.
- ▶ Most security/IT professionals either don't believe in the value of awareness or don't believe they have the necessary resources to make a sufficient difference.
- ▶ Building awareness is unlike all other security measures because it requires all employees to devote some of their time to security, as opposed to just a handful of security employees devoting all of their time.



What's wrong with the dots?

- ▶ Management is not enthusiastic because they don't know how important employee awareness is, don't believe it helps security, or won't invest without a clear ROI.
- ▶ Deploying security awareness often requires the cooperation and consensus of too many competing interests, including IT, security, HR, finance, legal, and senior management.



Lose Your Data, Lose Your Liberty?

“Civil servants face prison for leaving the public vulnerable to dangers of identity theft”

“Civil servants face being jailed for gross failures to safeguard citizens’ personal information under a clampdown following the disappearance of two discs that held the child benefit records of 25 million people.”

The Times (UK), December 18, 2007

It's time for a clean up!

- ▶ Things change when champions rise
- ▶ Lead by example
- ▶ Sell, sell, sell to top management!
- ▶ Bring in the lawyers
- ▶ IT should be the last to know



Focus on employee awareness

- ▶ Create a culture of security through saturation security
- ▶ Make awareness a daily, not annual event
- ▶ Focus on reinforcing the top security issues, and not covering everything
- ▶ Use email – it's the most powerful communications tools
- ▶ Don't forget third parties like partners
- ▶ Track progress and measure results



Auditors are made for this

- ▶ Security professionals pay attention to the title “auditor.”
- ▶ Effectiveness and efficiency of operations.
- ▶ Reliability and integrity of financial and operational information.
- ▶ Safeguarding of assets.
- ▶ Compliance with laws, regulations, and contracts.

About Neal O'Farrell

- ▶ CEO of My Security Plan and working in information security for more than twenty five years.
- ▶ Taught security to more than 3 million users in 120 countries,
- ▶ Creator of the nation's first Cyber Security Day, on November 4th 2002
- ▶ Founder of Think Security First!, the nation's first community –based cyber security awareness initiative and a unique experiment in raising the security awareness of an entire city.
- ▶ Creator of the Identity Theft Score

About My Security Plan

- ▶ My Security Plan helps employers to build greater security awareness across their workforce.
- ▶ Our flagship product is Mentor, the Gold Standard in employee security awareness. Mentor enables employers to create an organization-wide and even worldwide security awareness program in less than a day.
- ▶ Recent projects include a nationwide consumer id theft awareness campaign in partnership with NBC11; and creating a national standard in security awareness training in the workplace.
- ▶ Based in Walnut Creek CA, and on the web at www.mysecurityplan.com