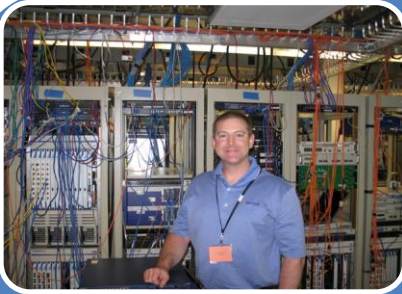




# Data Breach: The Negative Impact on Shareholder Value

Matthew D. Sarrel, Sarrel Group  
matt@sarrelgroup.com  
866-MSARREL x707  
Twitter: @msarrel

# Matt Sarrel



- BA, History (with honors), Cornell University
- MPH, (Epidemiology), Columbia University
- Fourth generation entrepreneur
- 20 years of IT experience
- Expert panelist for FTC workshops on spam and spyware
- Appearances on CNN, MSN, CNBC, BBC, local NY stations
- Quoted in Wall St. Journal, Forbes, CNN Money, Entrepreneur, BusinessWeek
- Technical Director, PC Magazine Labs
- Currently serving as
  - Contributing Editor, PCMag.com
  - Contributing Analyst, eWeek
  - 3G Editor, Backyard Magazine
  - Research Analyst, GigaOM Pro
  - Editor-In-Chief, TopTechDog.com

# An Organization Built for Success

## Lab Testing

- Usability
- Performance
- Competitive analysis
- Security

## Editorial Services

- White papers
- Case studies
- Tech briefs
- Sales battle cards

## Consulting

- Network security
- Software development
- Algorithm based trading systems

Global network of elite technology experts

The Sarrel Group team members have an average of 10-15 years of experience evaluating markets, testing products, and writing technical material

Real world experience yields real world testing

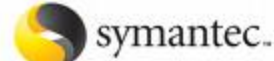
Offshore development teams

- The Philippines
- Cuba

### Global customer base

- New York City
- Seattle
- Miami
- Los Angeles
- San Francisco/San Jose
- London
- Toronto
- Singapore

# Our Clients



# Objectives:

To understand the ramifications of a data breach on company valuation (market cap).

To be able to use this devaluation to influence senior management during budgeting.

- *These guys view IT security as a necessary evil that merely steals money from the sales budget*

To begin to view IT security within the context of the business as a whole.

# My Money Gets My Attention

It was [Heartland CEO and Chairman Bob] Carr's worst nightmare. "It was devastating," says the CEO, who estimates the breach personally cost him about \$100 million in stock losses. -SC Magazine, September 2009

# Introduction - 1

Most IT purchasing justifications today rely on ROI and TCO

What's the ROI on security?

Do we as a socioeconomic culture understand the value of prevention?

Why did my client tell me that he would rather risk a breach than spend to prevent one?

## Introduction – 2

Does my belief in the value of security mean anything in today's business climate?

Why do I keep talking to consumers who don't care that a company compromised their PII?

If companies don't care and consumers don't care, then who does?

# Literature Review

Researchers	Year Pub.	Findings
Campbell et. al	2003	<ol style="list-style-type: none"> <li>1. Breaches result in no statistically significant loss for entire sample</li> <li>2. Breaches involving unauthorized access to customer personal data or firm proprietary data result in an average loss of firm value of 5.5%</li> </ol>
Garg et. al	2003	<ol style="list-style-type: none"> <li>1. Security attacks result in overall loss of 5.3% of value over 3 day event window</li> <li>2. Internet security vendors experience positive returns of 10.3% over the same window</li> <li>3. Property-casualty insurers experience a loss of 2.0% over the same window</li> </ol>
Hovav and D'Arcy	2003	<ol style="list-style-type: none"> <li>1. Breach costs higher for Internet firms</li> <li>2. No overall significant market impact for DOS</li> </ol>
Cavusoglu et. al	2004	<ol style="list-style-type: none"> <li>1. Breaches result in overall loss of 2.1% of value over 2 days following event</li> <li>2. Breach costs are higher for Internet Firms</li> <li>3. Costs not related to breach type</li> <li>4. Breach costs increase over time</li> <li>5. Negative correlation between size and stock market response</li> </ol>
Gatzlaff and McCullough	2008	<ol style="list-style-type: none"> <li>1. The stock market responds negatively to announcements of breaches of customer and/or employee data</li> <li>2. Negative reaction stronger               <ol style="list-style-type: none"> <li>1. High growth company</li> <li>2. Refusal to provide full details</li> </ol> </li> </ol>

# Postulates

P1

- People and businesses act in their own self interest.

P2

- Market capitalization is a reasonable measure of a company's true value

# Hypotheses

H1

- A company loses market value when a data breach is announced.

H2

- This loss is greater when reported in national or global media outlets rather than security specific outlets.

H3

- The loss varies directly with the number of individuals affected by the breach.

H4

- The type of data and company breached affects the magnitude of the loss.

# Methodology - 1

## Monitor security/privacy sites

- [Attrition.org](http://Attrition.org)
- [DataLossDB.org](http://DataLossDB.org)
- [Privacyrights.org](http://Privacyrights.org)
- [Emergentchaos.com](http://Emergentchaos.com)
- [Wikileaks.com](http://Wikileaks.com)

## Monitor the grapevine

- Listservs
- Blogs
- Social networks

# Methodology – 2

## Monitor mainstream news

- Lexis/Nexis
- ProQuest
- New York Times
- Wall Street Journal
- Press Releases

# Methodology – 3

Focus on publicly traded companies listed on

- NYSE
- NASDAQ

Biggest difficulty:

- Determining the true date of the breach

Discard breaches with potentially confounding events

- Earnings announcements
- Mergers and acquisitions

# Categories for Analysis

## Victim

- Customer
- Employee
- Third Party
- Undetermined

## Cause of breach

- Poor security practices
- External attack
- Internal attack
- Hardware theft
- Hardware loss

## Data

- SSN
- Credit card
- Full credit record
- Other PII
- Undetermined
- Undetermined

# Event Analysis

An attempt to explain the stock price's response to an event

## Established methodology

- Brown et al 1985
- Campell et al 1997

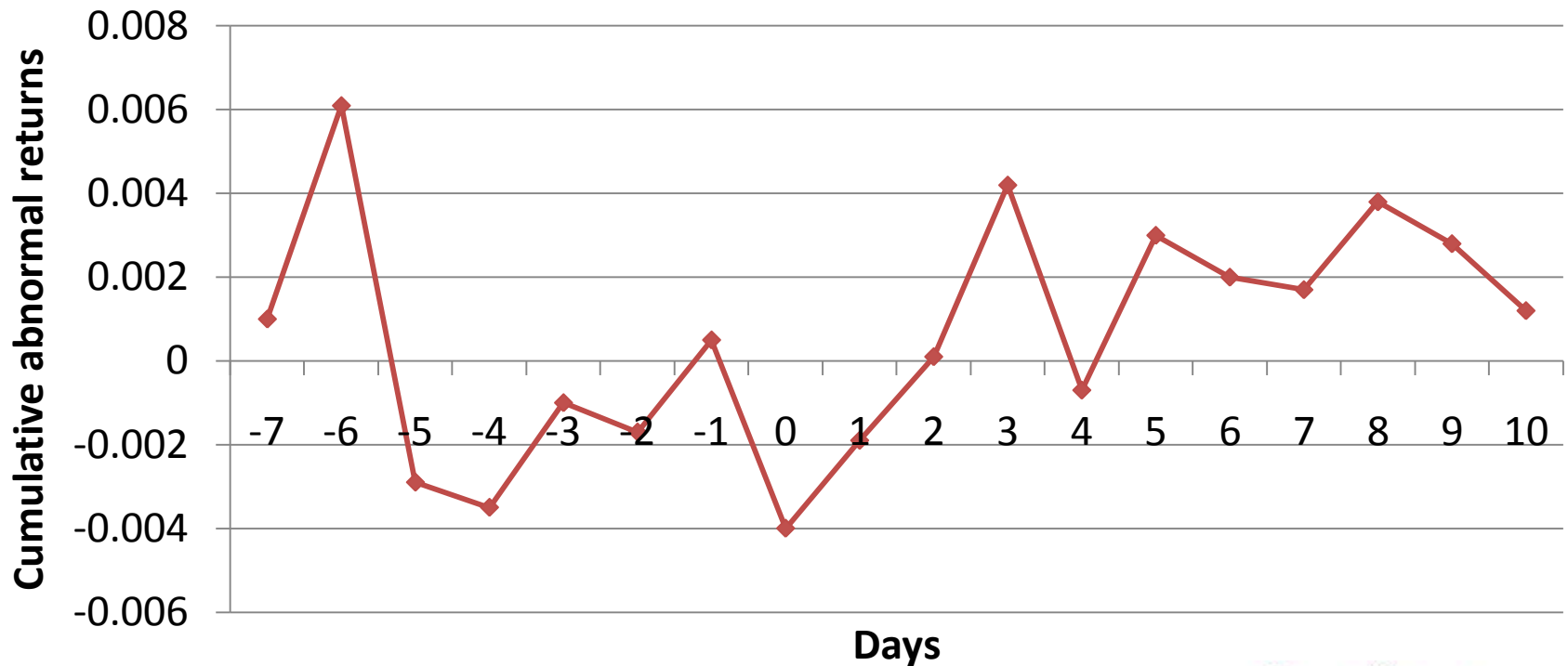
Complex math boils down to comparing the expected return on the stock to the actual return to calculate the cumulative abnormal return (CAR)

## Event window

- -100 to +100 trading days
- Day Zero (0) is the day of the announcement in mainstream media

# Results

## Mean Cumulative Abnormal Returns By Day



# Results Described

Overall small but statistically significant decrease in stock price

The day before (Day -1) is usually positive

Day Zero and Day +1 are usually negative

This represents an immediate bounce of -0.6%

After Day +2 the stock is back on track

# Is That The Whole Story?

It's all relative

- Directly proportional to the number of records breached
- More than 100,000 records
- Indirectly proportional to the market cap of the company breached
- Small company + big breach = big decline

# Time, Time, Time

Difficult to determine the effect of how the announcement changes over time (as more information is released)

- Number of records breached
- Root cause of the breach
- Implications of the breach on core business practices
- Inconsistencies in the story (more on this later)

# Implications of the Breach

Did faulty core business practices and the security around them cause the breach?

Significance of the data

Regulatory compliance – direct costs of notification and repair

Type of business and type of data

- Retail
- Finance
- Data processing

# Example: Heartland Payment Systems

Heartland Payment Systems is potentially the largest and is thus far the most openly discussed data breach to date.

Company officials still maintain that the breach announcement and the Obama inauguration just happened to coincide, and that it was not a deliberate effort on their part to bury the item in the news cycle.

As a publicly traded company whose business is built upon the perceived security and accuracy of processing transactional data for merchants and credit card issuers, most industry analyst had openly questioned the survivability of the company after their January 20, 2009 announcement of “a data breach of unknown proportions”.

Since the incident Bob Carr, CEO of Heartland, has hit the speaking circuit to share lessons learned and to advocate for refinements to the PCI-DSS, particularly in the area of “end-to-end” encryption.

Overview of share price of Heartland common stock (NYSE: HPY)

- Before the announcement: \$15.16
- Immediately after the breach announcement: \$8.18
- February 2009 SEC filings: Heartland included a statement that they did not know the scope of the incident and that they were unsure just how long the breach had existed before it was detected: \$3.43.
- On March 14, 2009 Heartland delisted
- April 30 it was re-certified as a card processor and re-listed on the stock exchanges.

# Heartland Payment Systems Chart



# Heartland Payment Systems Earnings

	Q4 2009	Q3 2009	Q2 2009	Q1 2009	Q4 2008
Total Revenue	420.03	442.57	417.37	372.17	385.93
Income Before Tax	-14.02	-59.39	-4.27	-3.98	12.93
Income After Tax	-9.58	-37.07	-2.60	-2.48	7.98
Diluted Normalized EPS	-0.26	-0.99	-0.07	-0.07	0.21
Dividend	0.01	0.01	0.01	0.02	0.09

# Highlights of SEC Filings - 1

The Company's guidance for 2010 does not include any estimates for potential losses, costs and expenses arising from the previously announced processing system intrusion, including exposure to credit and debit card companies and banks, exposure to various legal proceedings that are pending, or may arise, and related fees and expenses, and other potential liabilities, costs and expenses, including the interest expense on debt incurred to finance any settlements. Except to the extent previously accrued, neither the costs nor the potential liability are estimable at this point, and further the liability is not currently deemed probable.

## Provisions for processing system intrusion:

Q4 2009:  
\$23,651,000

2009:  
\$128,943,000

# Highlights of SEC Filings - 2

The following is an explanation of the adjustments that management excluded as part of its non-GAAP measures for the three and twelve months ended December 31, 2009:

Provision for Processing System Intrusion – On January 20, 2009, the Company publicly announced the discovery of the Processing System Intrusion. For the three and twelve months ended December 31, 2009, the Company expensed a total of \$23.7 million and \$128.9 million, respectively, or about \$0.42 and \$2.16 per share, respectively, associated with the Processing System Intrusion.

The majority of these charges, or approximately \$111.3 million, related to:

- (i) assessments imposed in April 2009 by MasterCard and VISA against the Company and its sponsor banks,
- (ii) settlements reached with VISA (in January 2010) and American Express (in December 2009),
- (iii) settlement offers made by the Company to certain card brands in an attempt to resolve certain of the claims asserted against the Company or its sponsor banks (who have asserted rights to indemnification from the Company pursuant to the Company's agreements with them), and
- (iv) settlements deemed likely to be agreed upon in the near term with certain claimants. Notwithstanding its belief that it has strong defenses against the claims that are the subject of the settlement offers or discussions described in (iii) and (iv) above, the Company decided to make the settlement offers and engage in settlement discussions in attempts to avoid the costs and uncertainty of litigation. The Company is prepared to vigorously defend itself against all the claims relating to the Processing System Intrusion that have been asserted against it and its sponsor banks to date.

# SEC Filings - 3

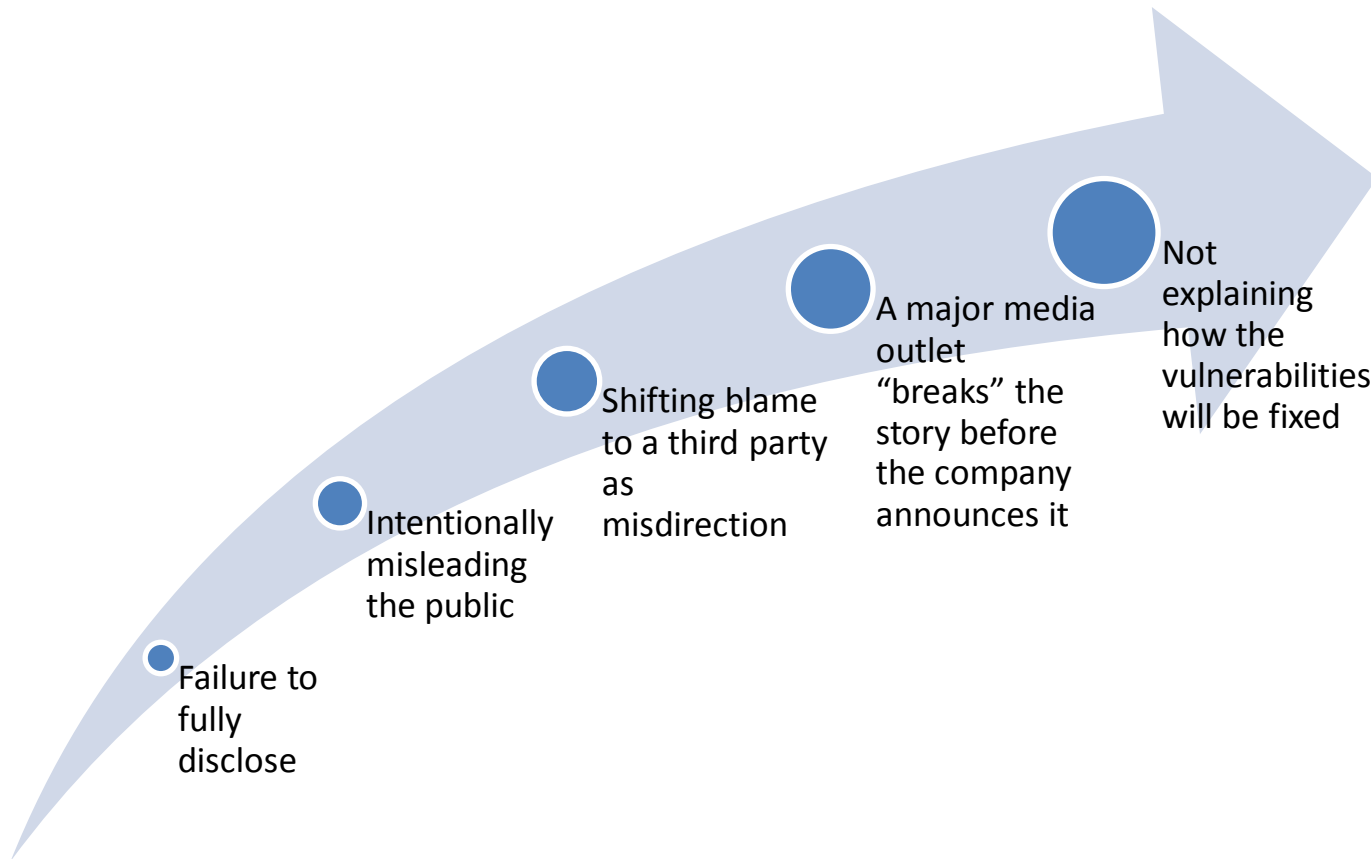
The accrual of the settlements and settlement offers during the twelve months ended December 31, 2009 resulted in the Company carrying a \$99.9 million Reserve for Processing System Intrusion at December 31, 2009. To date, the Company has not reached a definitive agreement with respect to settlement offers noted in (iii) above. Therefore, it should not be assumed that the Company will resolve the claims that are the subject of those settlement offers or the subject of settlement discussions for the amounts of the settlement offers or the settlement amounts deemed likely to be agreed upon. The Company understands that the reserve related to the settlement offers is required by SFAS No. 5, *"Accounting for Contingencies"* (ASC 450-20), based solely on the fact the Company tendered offers of settlement in the amounts it has accrued. It is possible the Company will end up resolving the claims that are the subject of the settlement offers, either through settlements or pursuant to litigation, for amounts that are greater than the amount it has reserved to date. Moreover, even if the claims that are the subject of the settlement offers were resolved for the amount the Company has reserved, that would still leave unresolved a portion of the claims that have been asserted against the Company or its sponsor banks related to the Processing System Intrusion. The Company feels it has strong defenses to all the claims that have been asserted against it and its sponsor banks relating to the Processing System Intrusion, including those claims that are not the subject of the settlement offers.

While the Company has determined that the Processing System Intrusion has triggered other loss contingencies, to date an unfavorable outcome is not believed by it to be probable on those claims that are pending or have been threatened against it, or that the Company considers to be probable of assertion against it, and the Company does not have sufficient information to reasonably estimate the loss it would incur in the event of an unfavorable outcome on any such claim. Therefore, in accordance with SFAS No. 5 (ASC 450-20) no reserve/liability has been recorded as of December 31, 2009 with respect to any such claim, except for the assessments actually imposed by MasterCard and Visa, the amounts of the settlements reached with VISA and American Express, the amounts of the settlement offers made by the Company and the settlement amounts deemed likely to be agreed upon as discussed above. As more information becomes available, if the Company should determine that an unfavorable outcome is probable on such a claim and that the amount of such probable loss that it will incur on that claim is reasonably estimable, it will record a reserve for the claim in question. If and when, the Company records such a reserve, it could be material and could adversely impact its results of operations, financial condition and cash flow.

## SEC Filings - 4

The remainder of the expenses and accruals related to the Processing System Intrusion recorded in the three and twelve months ended December 31, 2009 were primarily for legal fees and costs the Company incurred for investigations, remedial actions and crisis management services. Additional costs the Company expects to incur for investigations, remedial actions, legal fees, and crisis management services related to the Processing System Intrusion will be recognized as incurred. Such costs are expected to be material and could adversely impact the Company's results of operations, financial condition and cash flow.

# What Makes The Hit Worse?



# Commentary

Does Wall Street understand the severity and true cost of data breaches?

Does the public understand the value of their PII?

Are security experts and journalists crying wolf?

Are we risking “privacy fatigue” (Acquisti, et. al. 2009)?

Security experts are not finance experts.

# Costs: The Big Picture

Data breaches cause significant economic burden (over \$1 billion) to publicly listed companies

Market value decreases consistent with direct costs (legal fees, fines, audits, notification)

Wall Street does not take reputational cost into account

Government fines are not currently a deterrent.

# Conclusion

Companies can (and do) go out of business as the result of significant data breach.

C-level executives may not see the value of security, but they do feel the pain of stock price declines.

Budget requests for solutions to protect against data breach should include potential decline in market capitalization.