# On the use of market derived estimates of contingent losses: the case of data breaches

Bruce Bublitz
UM-Dearborn

Kirk Philipich
UM-Dearborn

Ramachandran Ramanan
University of Notre Dame

**ABSTRACT**

In this study, the security market reaction to data breaches in two firms, TJX Companies and Heartland Payment Systems (HPY), are examined. Management of firms where such breaches occur claim that it is extremely difficult to estimate losses arising from these events, and refrain from making any disclosure until approximately nine months later. The primary thrust of this exploratory examination is to judge the usefulness of the market's reaction to the breach's occurrence as a proxy for the ultimate loss incurred by the firm experiencing the breach. The market's reaction at the time of the breach is determined using two measures of abnormal returns: (1) market-adjusted returns, and (2) risk-adjusted returns. These abnormal returns (percentages) are then multiplied by the firm's approximate market capitalization at the time of the breach to estimate the dollar amount of potential loss to the firm. The paper investigates whether the market's reaction could serve as a starting point in determining the damages that might be claimed. The results of this study indicate that the losses estimated from the security market are reasonable proxies for the eventual losses reported by the firms. With regard to TJX, the market estimated losses are within 25% of the losses reported later; for HPY the market losses were within 20% of those disclosed by the firm. These results suggest that managers of firms may consider using market estimates of losses to report estimates earlier, with the provision to update these estimates later as more information becomes available regarding the eventual loss.

Keywords**:** Data Breach, Contingent Loss, Abnormal Returns, Intrusion, Data Security

## INTRODUCTION

The instances of corporate computer data breaches continue to increase (see Ponemon Institute (2014)). Recent well-known victims include Target (see Sidel, Yadron, and Germano (2013)), Home Depot (Banjo and Yadron (2013)), Supervalu (Sidel (2014) and Gasparro (2014)), and JPMorgan Chase (Yadron, Glazer, and Devlin (2014)). Company losses resulting from these breaches include items such as: (1) costs related to detecting the intrusion mechanism, (2) the cost of protecting the system from future intrusions, (3) loss of business resulting from reduced trust in the organization's ability to protect customer information, (4) legal and court costs of defending the company from resulting lawsuits, and (5) settlements that usually occur in these cases. Because the total loss suffered by companies due to these breaches may not be known for some time following the breach and/or its announcement, the accounting profession requires that these losses be estimated and reported even before the amount of loss is known with certainty. However, stock market participants must estimate the losses resulting from the breach in order to continue making valuation decisions concerning the company experiencing the breach although the amount of loss is unknown and not reported by management at the time the breach is announced.

The question addressed by the current study is whether external decision-makers, and possibly management itself, should/could use common research techniques to identify the stock market's assessment of the loss and use it as a starting point to make their own estimate. If management believes it is incapable of making such an estimate, then perhaps the market's estimate should be used as it would be the only publicly available estimate. From the evidence provided in this study, the implicit loss observed from stock price changes at the time of an announced data breach is a reasonable estimate of the loss. It is also worth noting that management was unable to estimate the loss when it occurred, however, they were able to estimate the loss within a year, and this estimate changed little thereafter.

## BACKGROUND AND JUSTIFICATION

Financial accounting statements and their accompanying disclosures require the use of many estimates to provide decision makers with the best available and/or most relevant information on which to base their decisions. Management and their auditors are assumed to be best positioned to make these estimates since they have available a plethora of numerical, qualitative, and contextual information that far exceeds what can be published externally. However, management makes these estimates within an internal culture and set of expectations which might bias the estimate from an external perspective. Although the processes through which these estimates are formed is commonly known in many cases (e.g. depreciation, bad debts expense, and inventory valuation), some situations require estimates with far less professional guidance or long-standing practices.

Estimating damages or future damage claims primarily due to litigation is one such perplexing situation for financial statement preparers. Unfortunately, these estimates must be determined with little professional guidance as to how to develop or verify their veracity. In the past, the need for such damage estimates primarily resulted from product deficiencies. However, more recent potential damages and damage claims have arisen from the breaching of companies' data security and the resulting theft and potential illegal use of both customer/client and company employee personal information (see Horst, Mullen, and Rosenberg (2009)). Within this context

of data breach litigation damages, this exploratory examination suggests that stock price movements (declines) be used, at a minimum, as an initial starting point for estimating the resulting damages.

The justification for the use of stock price movements as an initial estimate of data breach damages is both professional and academic in nature. Professionally, the use of stock price and/or financial market valuation estimates is not new to the financial statement preparation process. "Mark-to-market" accounting has become commonplace for both financial assets and financial liabilities. Examples include: (1) trading security treatment, (2) available-for-sale security treatment, (3) transfers among trading, available-for-sale, and/or held-to-maturity treatments, and (4) accounting for derivative securities.

While some believe that financial accounting information should affect stock prices and it would be circular to have a company's stock price changes affect accounting information, research has shown that stock prices react to a wide variety of information other than accounting reports. In the unchartered territory of making these complicated estimates, relying just on internal information may ignore an unbiased and broad based source of information that cannot be replicated with just internal information.

Other examples where a company's stock price, or its attributes, may impact its own financial reports include: (1) a company's average market price may impact the calculation of fully diluted earnings per share, (2) a company's market price can be used in treasury stock transactions, (3) accounting rules incorporate it for the accounting of small stock dividends, and (4) executive compensation from stock options is measured using option pricing models that include the behavior of its stock. In fact, the use of market-based valuation in accounting is becoming so commonplace that its use is not limited to financial assets and financial liabilities (e.g. recognition of and impairment of goodwill). Thus, the use of financial market valuations is viewed as a source of valuation estimates that are the most relevant to decision makers.

Obviously, the use of stock market declines as a starting point in the estimation of data-breach damages can only be justified by evidence that the stock market impounds knowledge of such breaches into security prices. Veltsos (2012) reports that forty-six states require organizations whose data security has been breached to notify those parties whose personnel information has been exposed. Through qualitative analysis, she concludes that the required/suggested scope of any notification is negative in nature.

Additionally, with a sample limited to seventy-seven firm events of data breaches leading to the theft of customer and/or employee personal data, Gatzlaff and McCullough (2010) find that on the date the firm announces the data breach (day 0) the firms' stock, on average, experience a statistically significant negative 0.57% abnormal return. Over the two-day window, (day 0, day +1), the cumulative negative abnormal return increases to a negative 0.84% and remains statistically significant. They also report that over an extended window (day 0, day 180) the average cumulative abnormal return reaches a negative 2.48%. However, they also find that such a large negative cumulative abnormal return to be statistically insignificant, possibly because the stock market considers the potential damages to a firm to be heterogeneous in nature – i.e., the study excludes some unknown control variables. Thus, market participants consider more than the fact that a breach has occurred before estimating the potential loss.

A cross-sectional analysis of their two-day cumulative abnormal returns (day 0, day +1) finds: (1) that those firms that provided little information or refused to respond more directly to the scope of the breach received a significantly more negative market response, (2) that the later breaches saw more negative and statistically significant market reactions, perhaps as more

market participants became more capable of estimating the potential for damages, and (3) the market's reaction was significantly less negative if the breach occurred within a subsidiary of a much larger organization, perhaps indicating the lower severity of the breach to the organization.

In a somewhat related vein, yet very different setting, Menon and Williams (1994) used the stock market's reaction as a signal of potential damages/losses. In a study of the loss of the insurance value provided by external auditors to shareholders, they hypothesize that stock market participants assign a value to the right to recover potential losses from the auditor when an audit failure occurs. They then hypothesize that the amount implicit in stock price for this insurance varies with the probability that the insurance would become necessary (potential losses may occur) versus those situations where the probability of needing the insurance is low or nonexistent. In their analysis of stock price changes surrounding the announcement of an auditor entering bankruptcy, they find that the loss in value to shareholders at the time of the announced bankruptcy varies significantly with the potential for insurance recoveries from the auditor for previous stock price declines.

The above research creates plausibility that the stock price declines around the time of announced breaches could serve as an indication of the potential damage claims that are likely to ensue. Additionally, the use of these stock price declines as a starting point for estimating potential damage claims provides a far less subjective approach than any other that has been suggested (e.g. estimating future cash flow losses).

## EXAMPLES

The primary thrust of this exploratory examination is to judge the usefulness of the market's reaction at the breach's occurrence to proxy for the ultimate loss incurred by the firm experiencing the breach. Obviously, the market is estimating the total loss to the firm, as opposed to the loss experienced by any one claimant or group of claimants, but perhaps the market's reaction could serve as a starting point in determining the damages that might be claimed. Thus, the market's reaction at the time of the breach will be determined using two measures of abnormal returns: (1) market-adjusted returns, and (2) risk-adjusted returns. These abnormal returns (percentages) will then be multiplied by the approximate capitalization at the time of the breach to reach an estimate of the dollar amount of potential loss to the firm. Abnormal market-adjusted returns are calculated as follows:

$$AMR_{it} = R_{it} - R_{mt}$$

Where:
$AMR_{it}$ = Abnormal market-adjusted return for day t,
$R_{it}$ = Return on firm i for day t, and
$R_{mt}$ = Return on the S&P 500 for day t.

In order to calculate risk-adjusted returns it is necessary to calculate $\alpha$ and $\beta$ in the period immediately preceding the breach. One-year of actual returns immediately preceding the breach are used to estimate $\alpha$ and $\beta$ using the traditional market model as follows:

$$R_{it} = \alpha + \beta R_{mt}$$

These estimates of $\alpha$ and $\beta$ are then used to calculate abnormal risk-adjusted returns as follows:

$$ARR_{it} = R_{it} - (\alpha + \beta R_{mt})$$

Where:
$ARR_{it}$ = Abnormal risk-adjusted return for day t,
$R_{it}$ = Return on firm i for day t, and
$R_{mt}$ = Return on the S&P 500 for day t.

These two measures of abnormal returns will then be multiplied by the market capitalization ($MC_{it}$) to arrive at an estimate of the eventual losses ($LMR_{it}$ and $LRR_{it}$) as follows:

$$LMR_{it} = (MC_{it})AMR_{it}$$

$$LRR_{it} = (MC_{it})ARR_{it}$$

$LMR_{it}$ and $LRR_{it}$ can then be compared to the actual losses reported by the firm to provide some indication of their value as proxies for the eventual actual losses. Additionally, these amounts can also be compared to the reported actual incurred losses plus any estimates provided in the financial statements. Obviously, to receive separate reporting in the financial statements, the losses will have to be sufficiently large (material) to receive special mention in the financial statements or other informative releases provided by the company.

For purposes of this exploratory examination, two large breaches (perhaps the largest data breaches as of 2012) that were first reported in 2007 (TJX Companies) and 2009 (Heartland Payment Systems (HPY)) are examined (see Armerding (2012)). The 2008 Heartland breach involved 134 million credit cards and the 2006 TJX case exposed 94 million credit cards. The breach at TJX was first reported on January 17, 2007, and the breach at HPY was first reported on January 20, 2009. In order to control for other possible confounding events, and following prior research findings, the abnormal return measures for a three-day window (-1, +1), the day before the announcement through the day following the day of the announcement (day 0) are calculated. Panel A of Table One provides the estimates for TJX and Panel B of Table One provides these estimates for HPY.

For TJX, the abnormal returns (ARR and AMR), thus also the estimated loss amounts (LRR and LMR), for each day of the three-day window are negative, with the day of the announcement of the breach being the most negative. HPY also reveals negative amounts for all three-days; however, unlike TJX, HPY's largest abnormal returns and estimated loss amounts can be found on days -1 and +1. Information leakage one-day prior to an announcement is not uncommon nor is the fact that the market may still be determining an appropriate new market value for the company through one-day following an announcement. Thus, on their face, these results are not surprising based on previous research findings.

The actual loss due to the breach reported by TJX was approximately $166 million. The estimated loss amounts, as accumulated over the entire three-day window, of approximately $165 million and $130 million both are easily within 25% of the eventual actual loss. Obviously, the LRR of $165 million is almost exactly the eventual amount recorded by TJX. HPY eventually reported an actual loss due to the breach of approximately $115 million. The three-day accumulated loss amounts of approximately $95 million and $94 million both are within

20% of the eventual reported loss. Thus, given that the actual loss amounts are not known and not fully recorded for up to one-year following the announcement of the breach, the market's estimates of these losses appear to be surprisingly accurate! At least for these two examples, the use of the market's estimated loss amounts as a starting point for estimating the total actual loss to the company, or as a starting point for determining possible damage claims, would seem to have some validity.

As an additional comparison, the losses actually recorded by the company and/or estimated by the company over time as reported in their quarterly and annual financial statements were identified. Table Two contains the amounts reported by the companies over time. For TJX (Panel A), if the financial statements were used as an indication of the total loss suffered by TJX, a year would pass before the 10-K financial statements for 2008 would show an estimate that is as close as that of an estimate based on the market's immediate response to the announced breach. For HPY (Panel B), it takes nine months before the estimated expense derived from the financial statements becomes a better estimate of the eventual loss than that estimated via the market reaction at the time of the announcement. By this point in time nearly $23 million has actually been incurred and only $92 million of the eventual $115 million is actually being estimated by the company.

Table Three shows a comparison of the market-based estimated losses and the losses reported in the various SEC reports for these two companies at various times. In these two instances, the market has done an outstanding job of estimating these eventual losses. For these two companies, the total actual losses seem to have stabilized within two years. Therefore, the two-year reported loss can be considered the actual real ultimate loss. Within a day, the risk-adjusted derived estimate of losses for HPY underestimated the ultimate loss by about 17%. At the same time, the financial reports underestimated it by 100%. For TJX, the immediate risk-adjusted estimate was approximately 0.65% too low. The reported loss was 99.999% too low. The company itself, with not only more current information but insider information as well, could only provide a superior estimate nine months after the market made its estimate. Thus, it would seem that whenever possible a company suffering a systems breach should, at a minimum, observe the market's implied loss estimate before making estimates of damages. Currently, users of financial statements would not find accounting financial reports to be useful in estimating the loss from a breach until at least nine months after the public announcement of a breach.

## CONCLUSION

This study used risk-adjusted and market-adjusted returns over the three days beginning with the day before an announcement of a breach for two companies with major systems intrusions. These two companies could only make a superior estimate of these losses 9 months to a year later. Even though these companies had time to assess the effects of the breach between the time when they discovered them and the time when they subsequently issued the first report after publically announcing these breaches, they claimed that they were unable to estimate the loss. Because the securities markets can make reasonable estimates almost immediately after the announcement of the breach, questions could be raised as to whether management of these two firms could not make such estimates or if they simply did not want to do so.

Management may believe that admissions as to the amounts of future settlements might hurt their negotiating abilities for those settlements. Clearly, through the narrative of the SEC reports, the two managements emphasized that they were going to fight court cases vigorously and that they did not believe that the companies were liable for any damages. However, within a year they have negotiated most settlements and reported a loss that changes little after that. Possibly, the accounting profession should require companies to use the market-based loss as the minimum amount to be recorded in financial statements. For the two companies reported here, a more realistic estimate of losses could then be shown in the financial statements beginning in the annual report for the period when the breach was discovered but before it was announced publically. Management could still claim that these estimates are required by Generally Accepted Accounting Principles (GAAP) and not admit that they expect to negotiate this amount of loss.

The many estimates necessary for producing financial reports can be very difficult. When these estimates are based on future court actions or the settlement of these actions, management may have mixed motives, both based on the ultimate welfare of the company. This study reports on two data breaches for which the securities market initially implied a better estimate of the ultimate loss than what management reported. Possibly, management is under additional pressures than a fair reporting of financial information. Currently, the opportunity to avoid any estimate by just claiming that it is not estimable may tempt management to delay making such estimates. However, the burden of proof should be placed on management for it to ignore the estimates already implied by stock market or other external sources. Especially, since wrong estimates must be recorded prospectively, not retroactively, financial statements would reflect a better timing of these losses.

## REFERENCES

Armerding, Taylor, "The 15 worst data security breaches of the 21st Century", (2012, February 15), Retrieved from http://www.csoonline.com/article/2130877/data-protection/the-15-worst-data-security-breaches-of-the-21st-century.html.

Banjo, Shelly and Danny Yadron, "Home Depot Inc. Confirms Breach", ***Wall Street Journal, Eastern Edition***, (2014, September 9), page 1B.

Gasparro, Annie, "Corporate News: Supervalu Hit with Second Hacking --- Data on Customers Possibly Captured", ***Wall Street Journal, Eastern Edition***, (2014, September 30), page 6B.

Gatlaff, Kevin and Kathleen McCullough, "The Effect of Data Breaches on Shareholder Wealth", ***Risk Management and Insurance Review***, 2010, pages 61-83.

Horst, Robert, John Mullen, Sr., and Mark Rosenberg, "The Growing Wave of Data Breach Litigation", ***Risk Management***, 2009, pages 40-44.

Menon, Krishnagopal and David Williams, "The Insurance Hypothesis and Market Prices", ***The Accounting Review***, 1994, pages 327-342.

Ponemon Institute, "2014 Cost of Data Breach: Global Analysis", Retrieved from http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.

Sidel, Robin, "Supervalu Investigates Potential Data Breach", ***Wall Street Journal, Eastern Edition***, (2014, August 15), page 1B.

Sidel, Robin, Danny Yadron, and Sara Germano, "Target Hit by Breach of Credit Cards", ***Wall Street Journal, Eastern Edition***, (2013, December 19), page 1B.

Veltsos, Jennifer, "An Analysis of Data Breach Notifications as Negative News", ***Business Communication Quarterly***, 2012, pages 192-207.

Yadron, Danny, Emily Glazer, and Barrett Devlin, "Big Banks are Hit in Cyber Attacks", ***Wall Street Journal, Eastern Edition***, (2014, August 28), page 1A.

Table One

Estimated Abnormal Returns (ARR and AMR) and Estimated Loss Amounts (LRR and LMR)
For TJX Companies (TJX) and Heartland Payment Systems (HPY)

Panel A:
TJX risk-adjusted estimates:

| Day | ARR | Accumulated ARR | Implied Daily LRR | Implied Accumulated LRR |
|---|---|---|---|---|
| –1 | –0.4293287% | –0.4293287% | $55,812,728 | $ 55,812,728 |
| 0 | –0.6817645% | –1.1110932% | 88,629,384 | 144,442,112 |
| +1 | –0.1614710% | –1.2725642% | 20,991,236 | 165,433,348 |

TJX market-adjusted estimates:

| Day | AMR | Accumulated AMR | Implied Daily LMR | Implied Accumulated LMR |
|---|---|---|---|---|
| –1 | –0.2112639% | –0.2112639% | $27,464,301 | $ 27,464,301 |
| 0 | –0.6453621% | –0.8566260% | 83,897,079 | 111,361,380 |
| +1 | –0.1470415% | –1.0036675% | 19,115,391 | 130,476,771 |

Panel B:
HPY risk-adjusted estimates:

| Day | ARR | Accumulated ARR | Implied Daily LRR | Implied Accumulated LRR |
|---|---|---|---|---|
| –1 | –6.5357393% | –6.5357393% | $43,135,879 | $43,135,879 |
| 0 | –3.3079186% | –9.8436579% | 21,832,263 | 64,968,142 |
| +1 | –4.5821456% | –14.4258035% | 30,242,160 | 95,210,302 |

HPY market-adjusted estimates:

| Day | AMR | Accumulated AMR | Implied Daily LMR | Implied Accumulated LMR |
|---|---|---|---|---|
| –1 | –6.5192983% | –6.5192983% | $43,027,369 | $43,027,369 |
| 0 | –2.9173175% | –9.4366158% | 19,254,295 | 62,281,664 |
| +1 | –0.1470415% | –14.2249764% | 31,600,180 | 93,884,844 |

Table Two

Actual Amounts Incurred and Estimated Contingent Amounts Charged Against Income
For TJX Companies (TJX) and Heartland Payment Systems (HPY)

Panel A:
TJX Timeline of Expense Recognition:

| Date | Vehicle | Already Incurred Expense | Contingent Expense | Total Expense per Vehicle | Total Accumulated Expense |
|---|---|---|---|---|---|
| 1/27/07 | 10-K | $4,960,000 | -0- | $4,960,000 | $4,960,000 |
| 4/28/07 | 10-Q | $15,044,000 | -0- | $15,044,000 | $20,004,000 |
| 7/28/07 | 10-Q | $17,818,000 | $178,100,000 | $195,918,000 | $215,922,000 |
| 1/26/08 | 10-K | ($18,900,000) | | ($18,900,000) | $197,022,000 |
| 1/31/09 | 10-K | ($30,500,020) | | ($30,500,020) | $165,521,980 |

Panel B:
HPY Timeline of Expense Recognition:

| Date | Vehicle | Already Incurred Expense | Contingent Expense | Total Expense per Vehicle | Total Accumulated Expense |
|---|---|---|---|---|---|
| End 08 | 10-K | Company stated that actual costs to date were insignificant. | | | |
| 3/31/09 | 10-Q | $5,269,000 | $7,681,000 | $12,950,000 | $12,950,000 |
| 6/30/09 | 10-Q | $12,662,000 | $6,718,000 | $19,380,000 | $31,970,000 |
| 9/30/09 | 10-Q | $4,811,000 | $68,511,000 | $73,322,000 | $105,292,000 |
| End 09 | 10-K | $6,650,000 | $17,001,000 | $23,651,000 | $128,943,000 |
| End 10 | 10-K | ($14,138,000) | -0- | ($14,138,000) | $114,805,000 |

Table Three

Various Estimates of Losses at Different Time Periods

| Time | Source | Heartland | TJX |
|---|---|---|---|
| Immediate | 10-K Financial Statement | -0- | $ 4,960,000 |
| One Quarter Later | 10-Q Financial Statement | $ 12,950,000 | 20,004,000 |
| Two Quarters Later | 10-Q Financial Statement | 31,970,000 | 215,922,000 |
| Three Quarters Later | 10-Q Financial Statement | 105,292,000 | 215,922,000 |
| One Year Later | 10-K Financial Statement | 128,943,000 | 197,022,000 |
| Two Years Later (ultimate) | 10-K Financial Statement | 114,805,000 | 166,521,980 |
| Immediate | Risk-adjusted | $95,210,302 | $165,433,348 |
| | Market Adjusted | 93,884,844 | 130,476,741 |
| Ultimate Understatements: | | | |
| Risk-adjusted | | 19,594,698 | 1,088,632 |
| Market-adjusted | | 20,920,156 | 36,045,239 |