Reputational risk - does it have a bad reputation?

A study of cyber reputational risk

November 2014

ADVISEN CYBER RISK NETWORK

Insurance Intelligence for the Cyber Community

Contents

1 Cyber reputational risk: *A growing strategic concern*

It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.

Warren Buffett

The "Oracle of Omaha" was far ahead of the corporate zeitgeist once again when he highlighted the fragility of a hard-earned reputation in this famous quote (above).

As Buffett warned many years ago, in the current economic climate, reputation is rapidly becoming a company's most valuable asset as it represents the key to gaining a competitive edge by many business leaders.

And cyber insurance is increasingly sold as a tool to safeguard corporate reputation, with pre- and post-breach services added as standard. Some policies even offer indemnity cover for losses as a result of reputational damage.

But just what is 'reputation'?

Global consulting firm Protivi describes reputation as "an interpretation or perception of an organization's trustworthiness or integrity"[1].

In recent years there have been numerous examples of a once-proud company brought to its knees rapidly, and without ceremony, by the media, customers and the stock market; Enron, WorldCom, Adelphia Communications, Lehman Brothers… Corporate arrogance, fraud and blatant disregard for basic risk management were some of the main reasons for these listed corporate failures.

But a new threat to corporate reputation is emerging: a cyber attack by an insider or a third party.

Data breach notification laws in many states require even small companies to disclose breaches. The likelihood of the corporate and consumer public learning about a breach is high.

How a corporation deals with such an event can have significant repercussions on a firm's reputation – or can it?

With information almost instantaneously available to customers and business partners, to what extent are data breaches translating into loss of market value? Has the potential "doom & gloom" associated with reputational risk events eclipsed rational views?

In this report, Advisen's Cyber Risk Network team will consider current perceptions of the reputational risk presented by a cyber event and will apply Advisen research to test these concerns on a set of recent data breach examples.

This paper explores the implications of reputational risk for small, medium, and large size businesses as well as the insurance and risk management solutions designed to help them.

Measuring reputation

From a risk management perspective, reputational risk remains very difficult to identify in a corporation – and almost impossible to quantify.

Unlike cash in a bank account, or a faulty building fire sprinkler system, reputational capital does not carry a clear definition across the corporate sphere. It is "shaped outside the organization" by the media and what its customers, employees and other stakeholders are saying in the public domain, according to Deloitte partner Henry Ristuccia.[2]

Ristuccia added that the tools and analyses for identifying and assessing reputational risk are very different from those used to assess more quantifiable threats. "This kind of risk is at an event level these days, not the company level. And traditional risk management doesn't focus on that nor does it offer the tools to address it," he said.

A report by The Economist Intelligence Unit[3] said that risk managers are divided on whether reputational risk is an issue in its own right or simply a consequence of other risks.

"In industries where risk managers feel they have identified the key first-tier risks facing their business, they may be more inclined to consider reputational damage as simply a failure to manage these risks properly. In contrast, in sectors where first-tier risk is less quantifiable they are more likely to see reputational threats as a class in their own right," the report said.

Reputation through a cyber lens

To complicate matters further, as organizations become more reliant on technology to conduct their business – through retail sales, supply chains, data stored in the cloud and products dependent on technology – cyber risks pose an increasingly fundamental threat to a corporation's reputation and very existence.

Reputational risk is now a strategic concern, with cyber threats at the heart of the debate at the board level of corporations.

Cyber threats can come from such a wide variety of sources and can affect organizations in so many different ways. And many of these threats can have a practical, operational impact on businesses, affecting the public's perception of the company.

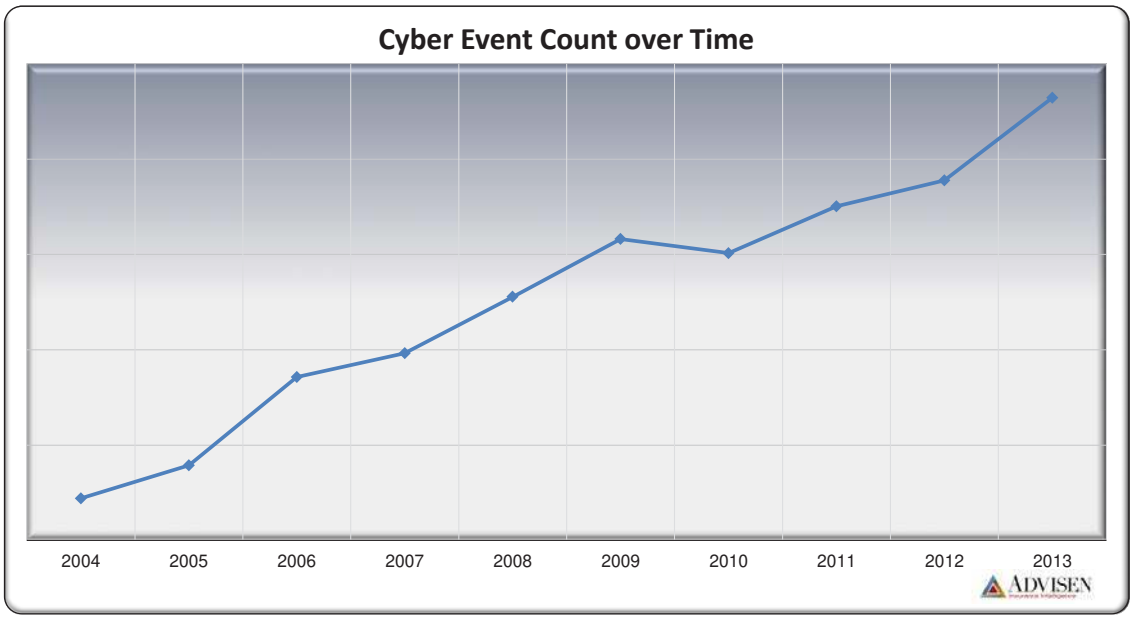
Indeed, in the broader context of cyber reputational risk, can data breaches create a similar level of reputational damage as product tampering, an infection outbreak at a hospital or a crash for an airline.

In a recent report,[4] Experian analyzes the lessons learned from the many high-profile data breaches that have occurred in the past year.

"With the rapid increase in the threat landscape and number of data breaches, concerns over how to manage them have moved beyond corporate IT teams to other major departments of organizations," stated Experian. "The reputational and financial damage caused by a breach is difficult for C-suite or board members to ignore. And, as we've seen with larger breaches, the role of today's chief executives has expanded to now be held responsible for lapses in computer security."

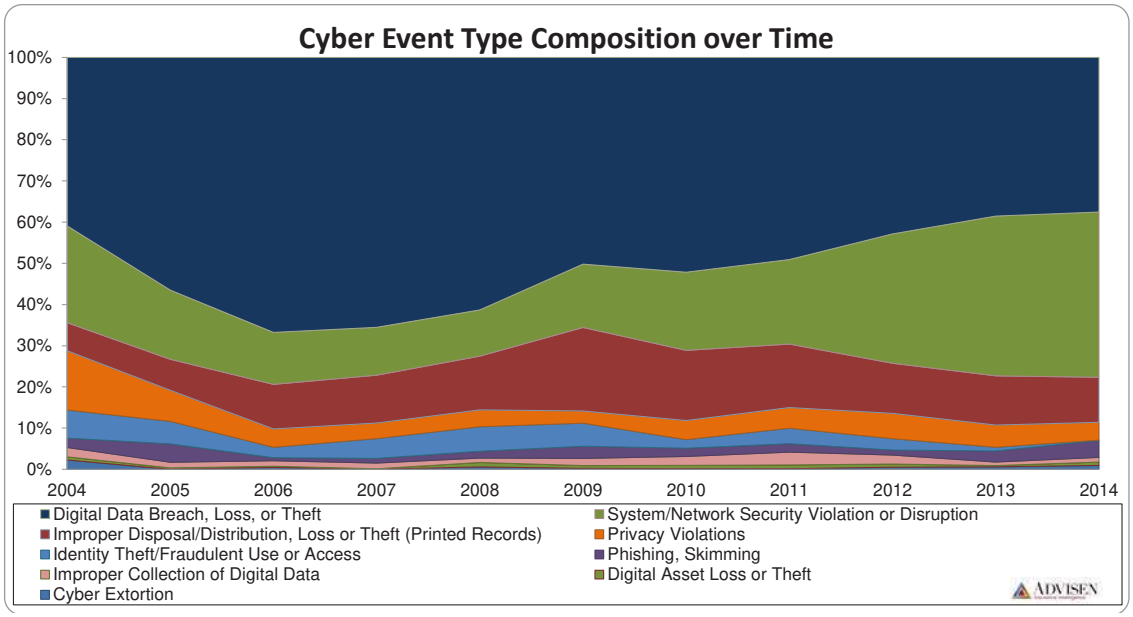
The cyber threat in numbers

To put the cyber risk into context for organizations, Advisen's Cyber Loss Insight data shows a marked increase in the number of cyber events over time.



In the six months to June 30 2014, the number of events in the Advisen database was up 35 percent on the previous year period. 2014 is expected to increase further, once complete.

The Advisen Loss Insights database holds almost 13,000 events with 15,500 associated cases.

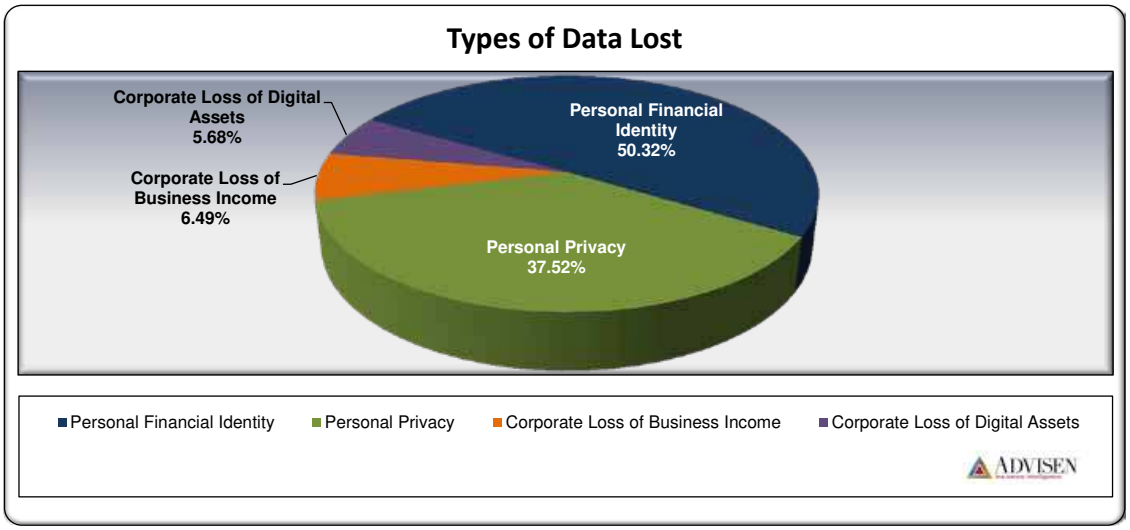


The largest type of event is currently network security violations, which have marginally overtaken data breaches in the past couple of years.

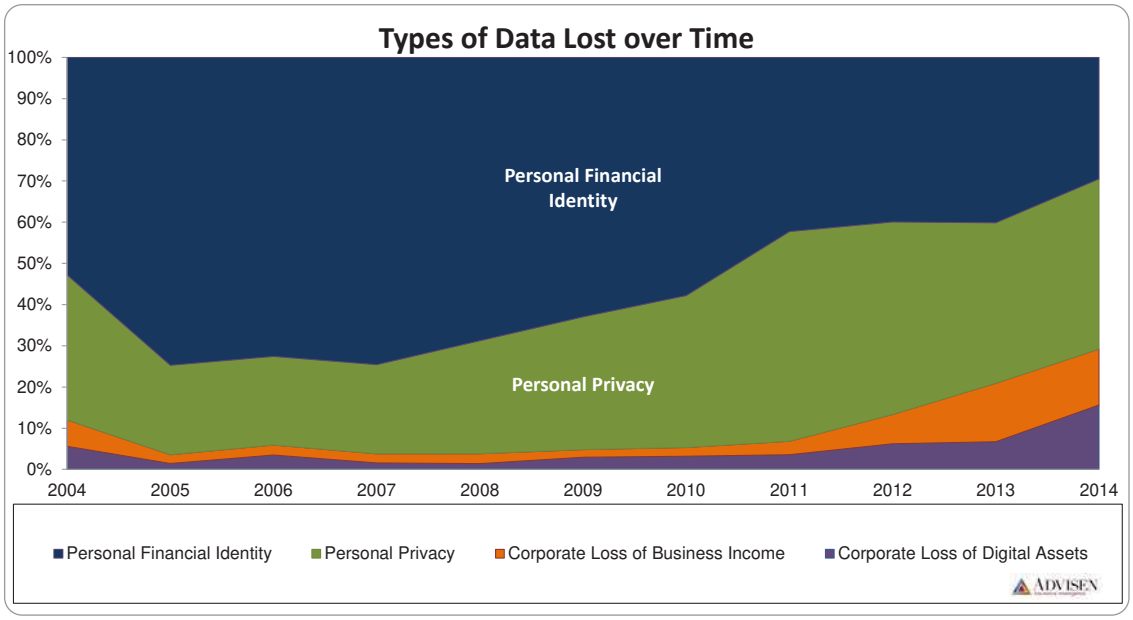
Data breach, having been the largest event type in the past ten years, is a close second, at around 35 percent of the total.

This is notable, as data breach grabs the majority of headlines when the media highlight cyber attacks on corporations. Examples such a Target and JPMorgan's data breaches have garnered many more column inches and affected the reputation of the companies more than network disruptions in the past 12 months.

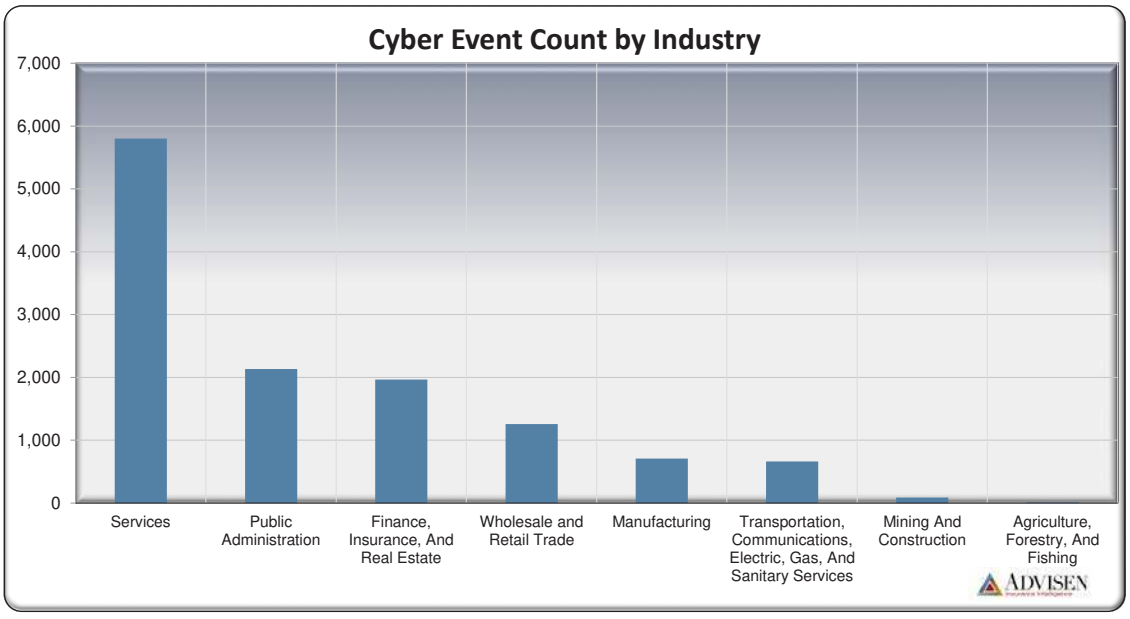
A little over 50 percent of the data lost during a data breach today is personal financial data, with personal privacy data making up 38 percent of the total.



Looking at this developing over time, the loss of personal privacy data is rapidly increasing over financial identity. There are hints that this trend may continue. Recently, Fox Business[5] reported that stolen health credentials can sell for around 10 or 20 times the value of a US credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber crime protection company. Jackson obtained the data by monitoring underground exchanges where hackers sell the information.



When looking at cyber events by industry, Advisen Loss Insights data shows that the services sector – which includes Healthcare - is the worst affected by attacks. Public administration suffers more cyber events than finance or the wholesale and retail trade – two sectors very much in the public awareness currently.



The hardest hit corporations for data breach incidents are in North America and the UK, with Australia chasing behind in third.

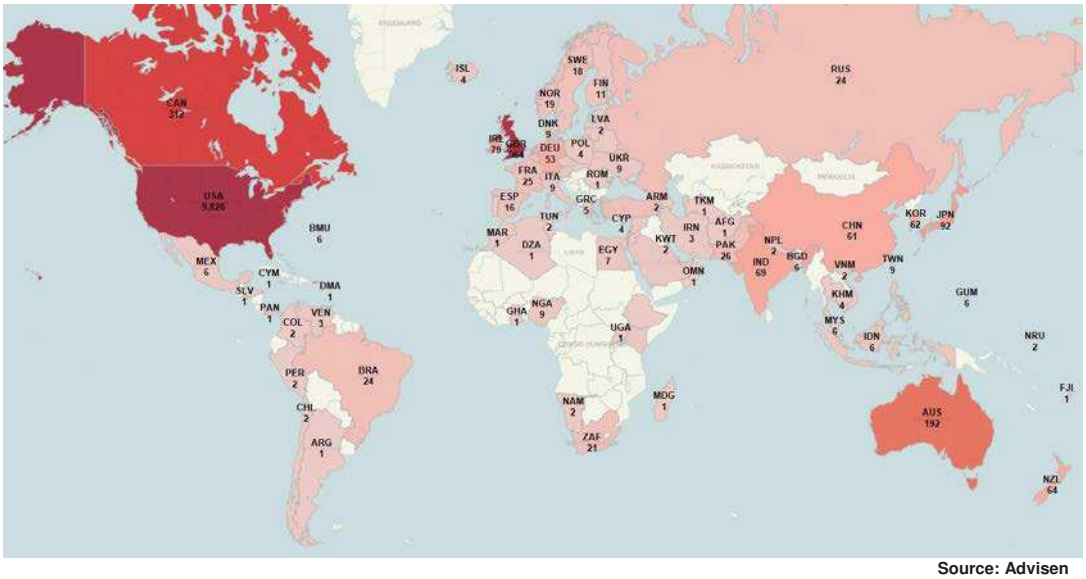
It is not surprising to see North America as the region with the most cyber attacks. Firstly, the US has more onerous data breach notification regulation than other jurisdictions, therefore the public is aware of more events than in other countries.

Secondly, cyber criminals are likely to follow the easiest path to large volumes of personal information and cash. The widespread usage of credit cards among US consumers makes this region one of the most attractive to the underworld.

Data breach notification laws are developing in other regions, notably Europe, but progress is slow and therefore the number of captured cyber events is lower.

Cyber events by country

Cyber events by affected country



Source: Advisen

In the second section of this report, we will explore some current perceptions of cyber reputational risk gathered from surveying risk managers and senior executives at global corporations.

2 Boardroom concern: *Perceptions of reputational risk*

A report from the Economist Intelligence Unit[6] noted that the CEO is the "principal guardian" of corporate reputation. "The chief executive is pivotal in providing an ethical identify for their companies. They also co-ordinate the response of other senior managers to reputational threats and crises," the report said.

With this in mind, it is not surprising that company reputation and the fallout from reputational damage are the number one strategic risk for large companies, according to a 2013 Deloitte global survey of executives.[7] In a sign of the perceived longevity of the problem, survey respondents also highlighted reputational risk as a top-three strategic risk in 2016.

Q. Which of the following risk areas have the most impact on your business strategy (three years ago, today, and three years from now)?

2010	Today	2016
41% | Brand	40% | Reputation	29% | Economic trends
28% | Economic trends	32% | Business model	26% | Business model
26% | Reputation	27% | Economic trends | Competition	24% | Reputation | Competition

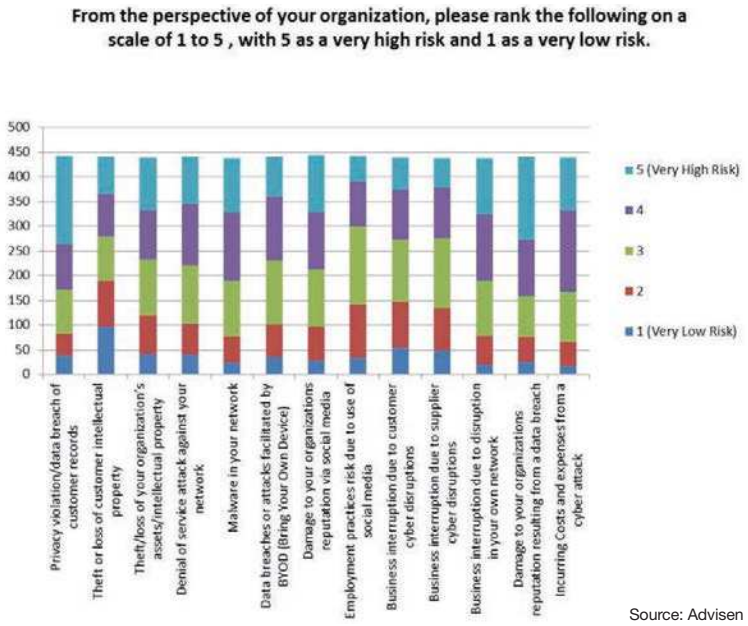
Source: Deloitte

An EisenAmper survey of board members found that reputational risk ranks as their most significant strategic concern.[8]

Putting this priority in the context of other cyber risks an organization faces, reputation ranks highly among theft of records, cost of remediation and business interruption resulting from a cyber attack, for example.

Advisen surveys of risk managers in the United States, Europe and Asia consistently place reputational risk as either the first or second most highly ranked risk as a consequence of a data breach.

In a 2014 Advisen survey of US risk managers for Zurich, more respondents considered reputational risk a "very high" or "high" risk to their organizations than the data breach itself.



Source: Advisen

While long a concern of companies in financial services and a few other sectors, reputational risk has surged in perceived importance to companies in virtually all industries. In the energy sector, for example, reputation risk wasn't even in the top five concerns of executives three years ago, but today it is number one, according to Deloitte.[9]

The growing prevalence and influence of social media is often cited as an important reason that reputation risk has grown as a concern of boards and the C-Suite in recent years. At the very least, social media increases the velocity at which news is disseminated and, consequently, it increases the challenges of maintaining control of a story.

"Social technologies are one of the main factors driving rising concerns about reputation," according to Deloitte, based on interviews with corporate executives. "Given the speed and global reach of social media, companies today are at much greater risk of losing control over how they are perceived in the marketplace."[10]

Data breaches, of course, are only one of many threats that can result in reputation damage. For some organizations, a data breach may not even rank in the top five, or even top ten, perceived threats to brand and reputation.

According to a Ponemon Institute study, however, a data breach can have a material economic impact. Based on input from more than 800 corporate executives, Ponemon researchers concluded that a breach of customer data results on average in a 21 percent decline in the value of a company's brand and reputation.[11] We will consider this assertion in the next section of this report.

Perceived reputational risk from a data breach also may be fueled by a number of surveys that found that

people claim to be less likely to do business with organizations that have experienced a breach. The most recent, conducted by CreditCard.com, surveyed 865 credit card and debit holders and found that 45 percent claimed they would definitely or probably avoid one of their regular stores over the coming holiday if that retailer had experienced a data breach.[12]

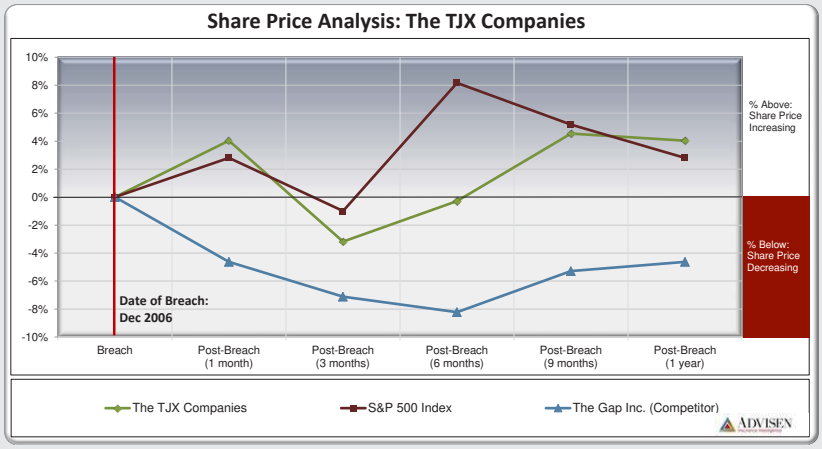
Advisen research, based on an analysis of changes in earnings and share price following a breach, arrives at rather different conclusions than either the Ponemon study or those surveys finding wholesale customer defections following a breach.

Directors and other decision makers implicitly understand the impact that a strong reputation has on an organization's value. They clearly are justified in their concern about reputation risk, but researchers note that a gap often exists between perceived risk and objective threat.

Since risk perception has a strong influence on risk management and loss mitigation decisions, board members and other decision makers need much better information to understand the characteristics of those organizations that are most likely to suffer damage to their reputations as a result of a data breach, the extent to which a data breach is likely to influence earnings and share price, and the strategies that are most effective in mitigating the impact of a breach.

3 Myths and reality: *The effects of a breach*

TJMaxx still a good buy



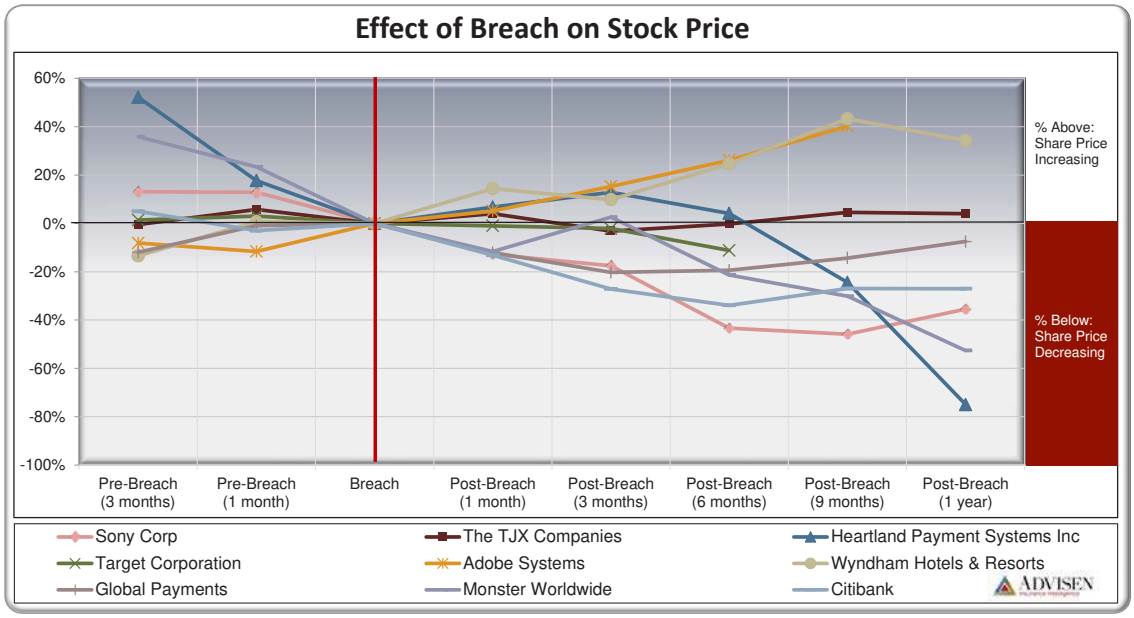
An investor with 100 shares of TJX Companies Inc. stock in April 2007 — about a month after T.J.Maxx, Marshalls and Bob's Stores suffered a cyber breach of 45.6 million consumer credit and debit card numbers — had about $1,400 in his investment portfolio.

Today the same amount of shares is worth about $6,300.

Shares of TJX closed at $63.82 on Nov. 4—just slightly below a high of $64.09 over the last year.

With the extensive direct and indirect costs of a data breach, it could be expected to hit publicly traded companies hard on both their bottom lines and their stock price. However, Advisen research found no strong effect on stock performance after an event.

Advisen conducted stock price research on nine major data breaches in recent years – from TJ Maxx in 2006 to Target in late 2013 – and compared individual share price with a competitor's stock and their relevant stock exchange index over a period of 12 months from the data breach.

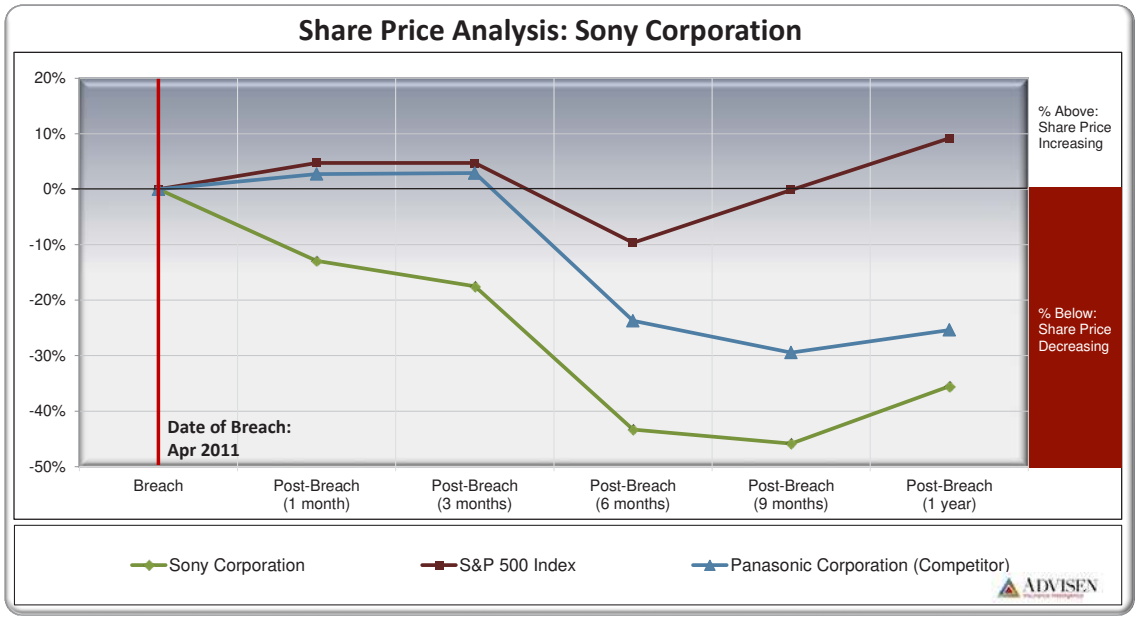


As this graph shows, many stocks were falling in value prior to the breach, including Sony, Heartland payments and Citibank. The cyber event did nothing to stem that decline, but neither can it be identified as the catalyst for the drop.

Alternatively, other stocks were increasing in value and the breach had no discernible effect on that trajectory – Adobe Systems and Wyndham Hotels would still have been considered solid investments, post-breach.

Larry Ponemon, founder of the Ponemon Institute added that his firm similarly was "not able to come up with a stock price effect. There are instances where there is an effect, but it doesn't seem to be consistent."

Sony struggling



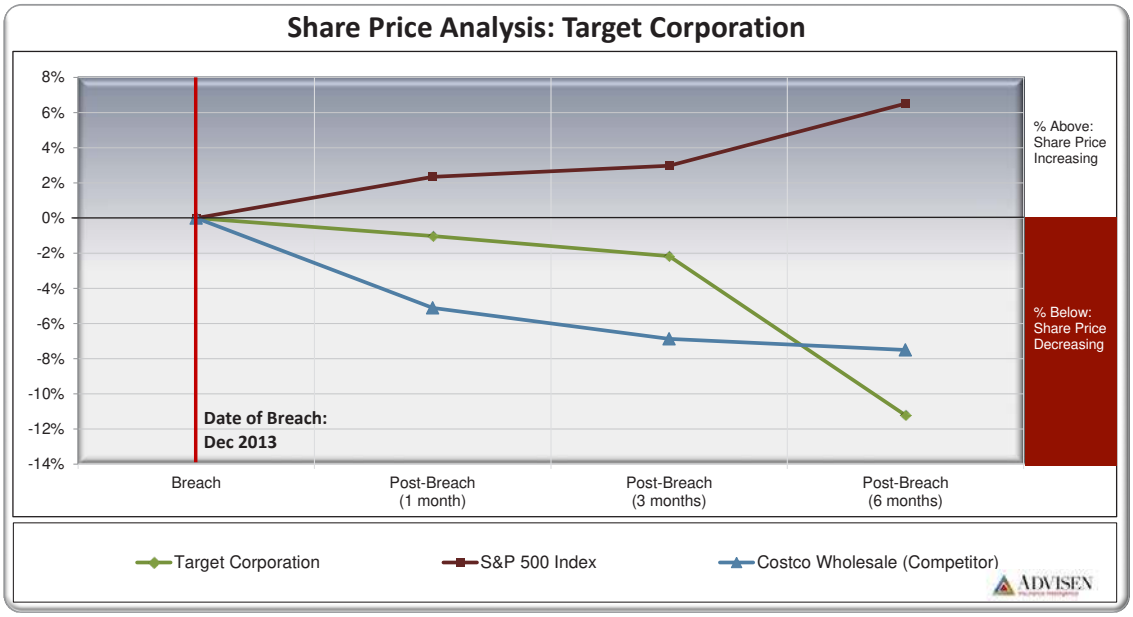
The mega breach Sony experienced in April 2011 could appear to have an effect on its share price, which was selling at about $31.90 at the time and fell to about $16.80 a year later.

However, Sony Corp. stock was consistently dropping before it announced a massive data breach of its PlayStation Network. In February 2011 shares were selling for more than $36 each.

Notably, fellow electronics competitor, Panasonic showed a steep drop in stock price over the same period – without a breach.

Sony continues to struggle, losing billions of dollars according to its last earnings report, as sales of televisions and audio equipment dwindle, while strong PlaySation sales are a redeeming factor.

A Target on his back



More recently, retailer Target experienced a massive breach in December 2013, which produced a stock effect, primarily because it occurred during heavy holiday shopping season.

Target's stock dropped to a year-low in March 2014, but now trades at approximately pre-breach levels.

In fact, the most notable drop in Target's share price came around the time the firm announced it had fired its CEO, Gregg Steinhafel in May 2014. Steinhafel's departure however, was not singularly linked to the data breach incident, with the company struggling under the weight of missed sales expectations and a rocky expansion into Canada.

In fact, financial analysts during a first-quarter earnings conference call in May 2014 barely asked Target Corp.'s interim CEO about its data breach. The retailer may be struggling in the eyes of investors but it has little, or nothing, to do with any loss of trust from a data breach.

"No one has said much about Target's security breach in months, especially after a more extensive one was reported at Home Depot in September," said one site offering investment information.

Home Depot became the victim of a cyber attack just months ago, exposing an estimated 56 million credit cards used at the store. Two lawsuits have already been filed – and yet the home improvement retailer is trading at over $95 a share, nearly a record for the last year. The retailer is credited as being one of a few currently performing well.[13]

Shares of JPMorgan & Chase barely flinched after an early October regulatory filing disclosed that the data of 76 million households and 7 million small businesses might have been exposed by a breach. The bank did not send any personal notifications to customers.

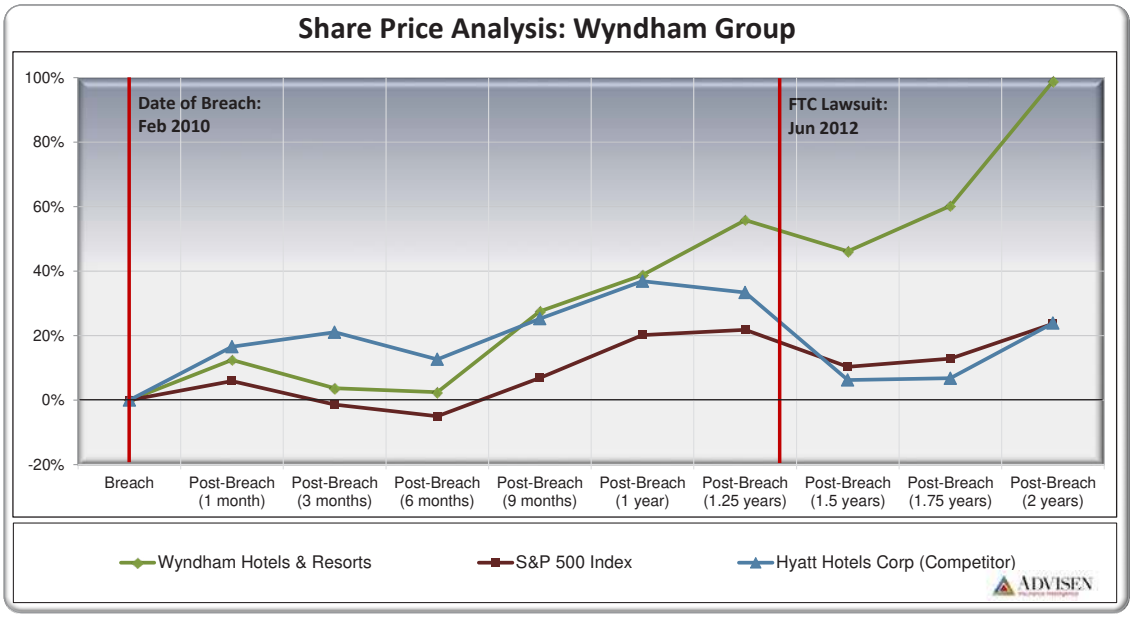
Nevertheless, JPM closed at $60.88 on November 3. Except for a week-long stretch in mid-September, the stock is at its highest point over the last six months.

The last two led the Washington Post to wonder in a headline: "Home Depot and JPMorgan are doing fine. Is it a sign we're numb to data breaches?"[14] This phenomenon is widely referred to as "data breach fatigue".

A reader poll attached to the Washington Post story asked readers why they returned to shop at a data breach victim store. Nearly 37 percent checked off this option: "Breaches seem to be commonplace these days, so I don't particularly blame the retailer".

Could this be why hotel chain Wyndham Worldwide is doing well despite three data breaches in 2008, 2009 and 2010 and a high-profile lawsuit from the Federal Trade Commission?

Wyndham defies logic



A year after Wyndham announced a breach early in 2010, its stock price increased more than 43 percent. Perversely, its stock took another marked upward swing after the filing of a lawsuit against Wyndham Hotels by the FTC in June 2012.

At the start of 2011, Wyndham shares were at $29.83. Today, investors haven't been able to purchase a share for under $75 since the week of June 15. This is despite tens of millions of dollars in alleged fraud losses to consumers from the breach and the FTC lawsuit keeping the hotel's breaches in the headlines.

Ponemon has a few ideas why a data breach doesn't always mean plummeting stock prices for the affected company. This relatively new, constantly evolving business risk carries costs that consumers don't necessarily realize.

"Beyond share price, there are other cost factors. People who are investing in stocks -- not just people, but institutions -- really don't fully understand the long-term impact of a data breach," Ponemon said. From the perspective of the public, "these things seem to get repaired pretty quickly".

Compare a data breach to a product recall. An automobile part recall, for example, garners a great deal of attention and requires consumers to actively engage in the process. In a breach event, consumers generally wait until their banks reissue their cards and, in some cases, keep an eye on their credit report. Unlike a product recall, personal safety seems less at risk.

Negative impacts can also be held at bay by coordinated, effective crisis response management. Sony followed up its breach with "a lot of missteps," according to Ponemon. The corporation announced the hacking event – but it was later revealed the breach was still happening. The 2007 breach at TJX offers

another look at a poorly managed breach. The massive loss of personal financial information combined with a disorganized corporate response to the event caused a loss of confidence at a time when the phenomenon of data breaches was new.

Looking at the stock prices of the even more victims of breaches—Sally Beauty Supply, Michaels, Supervalu, UPS and eBay—the value of a share of each company remains near or slightly above the share price at the time of their data breach incident.

"That's pretty troubling. You want people to care about this," said Ponemon.

Online retailer eBay's May 2014 breach that exposed millions of usernames and passwords is less frequently held up as an example of a mega breach. Customer perception may be as significant as other factors following a data breach.

"They reported it clear and matter-of-fact and were very good at communicating," said Ponemon. "Most people, when they think about mega data breaches, they're not really thinking about eBay."

In the narrower world of banking data breaches, Ponemon completed a study on the effect of "customer churn" after an event. Multiple breaches tend to be more damaging to loyalty.

"If a customer receives communication that there's been a breach, they're not going to leave," he said. "But the second time it happens, there can be a huge customer turnover."

Still Ponemon research found that about 32 percent of consumers said they ignored notifications from breached companies and did nothing. Seventy-one percent of respondents said they did not stop doing business with the company that had been breached.

There is also contrary research. As noted earlier, CreditCard.com, surveyed 865 credit card and debit holders and found that 45 percent claimed they would definitely or probably avoid one of their regular stores over the coming holiday if that retailer had experienced a data breach.

4 Mitigation strategies

Despite a muted investor and consumer reaction to data breach events to date, corporations cannot rest on their laurels. They still need robust planning and smooth responses to pour oil on troubled waters in the event of a cyber attack.

A range of pre and post loss risk mitigation strategies is often considered the best defense. In this section we will explore these strategies and discuss whether or not insurance is an effective component of a reputational risk management program.

As highlighted previously, positive reactions from investors to data breach events were often attributable to a swift, efficient breach response plan.

Reputational risk management

Many companies seek to actively manage public consensus on its products and operations by instilling and reinforcing positive associations in the minds of those who are important to the success of the company such as customers and investors. Managing a reputation also requires a quick response to threats. Deloitte partner and global leader of governance, risk and compliance, Henry Ristuccia[15] highlighted the need for this dual approach:

The challenge is that many organizations still take a rear-view mirror approach to risk, especially reputational risk. For example, in the case of an adverse event to their reputation, they may get legal, corporate communications and PR involved, and then they may do a post mortem to help avoid a similar event.

“That essentially is crisis management, not reputational risk management,” Ristuccia said.

While crisis management is important, it may not be enough when dealing with reputational risk issues as it typically entails taking backward-looking, reactive measures after an event has occurred.

In contrast, managing reputational risk should start with looking at the strategy, what markets a company is entering, what products or services it is offering and what are the critical risks and value killers that could sink the company’s brand.

The next step is developing an early warning system to see and head off an adverse event before it can impact reputation.

“That forward-looking approach is fundamental to anticipating and managing the new risks that the digital phenomenon is presenting,” Ristuccia added.

Corporate governance is at the center of reputational risk management, as well managed companies are more likely to avoid activities that undermine trust, and build goodwill to help cushion the reputational impact of bad news such as a data breach.

But companies should not rely on good corporate governance alone. Proactive steps are also necessary. According to one privacy and cyber security lawyer interviewed by Advisen, organizations that are prepared for a cyber incident both respond quicker and manage the entire process better, which makes the situation more manageable and improves the outcome.

This involves substantial planning and the implementation of both pre and post loss strategies designed to limit the severity of the data breach and reduce the likelihood of regulatory enforcement actions and third party lawsuits.

"Preparedness makes a huge difference," according to another leading privacy and cyber security legal specialist. "The most prepared know who should be involved and what they need to do."

Pre- and post-loss strategies

Pre-loss strategies can include:

- Staying current with exposures and threats, as well as other trends that may spawn new risks.
- Creating a culture of security awareness to avoid, identify, and respond quickly to a breach in cyber security protocol.
- Identifying a leader who is responsible for coordinating the breach response.
- Developing a breach response team with both internal and external resources. "The establishment of a breach team beforehand makes a meaningful difference in terms of time, cost, efficiency, and frustration" a leading privacy and cyber security specialist explains. "There are significant efficiency, savings, and stress reduction if done in advance."[16]
- Developing an incident response plan that spells out the steps that need to be taken and whose responsibility it is to execute them.
- Conducting tabletop exercises that cover a variety of potential scenarios.
- After a data breach occurs, quick implementation of the incident response plan is vital to minimize the reputational consequences of the crisis.

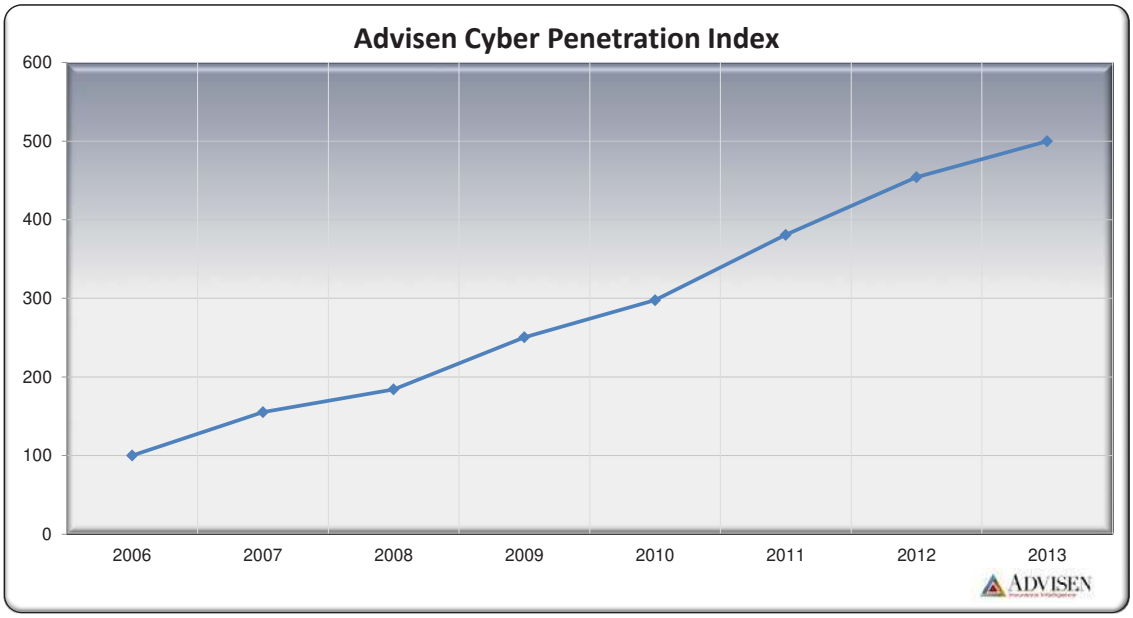
Post-loss, it is vital for organizations to:

- Quickly identify and fix the cause of the data breach and publicly announce what steps were taken to do so. Even if there is no quick fix, it is important that management be seen as moving decisively to remedy the problem.
- Communicate with affected individuals and other stakeholders. When confident as to the breadth and scope of the breach, establish communication that is clear concise, and thoughtful.

- Stay on top of the issue for as long as it takes to repair the damage and regain trust. Repairing a reputation can take years, and companies may be judged on their activities relative to a data breach long after the breach has occurred.
- Turn a bad situation into a positive one. Companies that respond quickly, decisively, take full responsibility for mistakes, and execute an action plan that remedies the problem and attempts to make whole all those that were affected often gain respect.

Insuring reputational risk

According to Advisen's cyber-intelligence database, cyber insurance policy penetration has been steadily increasing every year.



The market is far from saturated, however (see table), and reputational risk is increasingly utilized as a selling point. The challenge is explaining its value.

Penetration rate by company size

Revenue Range ($)	% Purchasing Cyber
<2.5M	3.8%
2.5M<5M	4.8%
5M<10M	6.6%
10M<25M	7.2%
25M<100M	10.0%
100M<300M	17.6%
300M<1B	20.5%
1B<5B	21.8%
5B+	25.9%

Source: Advisen

Cyber insurance has proven effective in indemnifying the quantifiable costs of a data breach. At an average cost of $145 per compromised record, even a comparatively small business could conceivably run up a tab in the hundreds of thousands, or even millions of dollars.

But the ability to quantify, and therefore insure, the reputational impact of a breach is still up for debate. In fact, of the approximately sixty insurers with a cyber insurance product, only a few offer indemnification for losses as a result of reputational damage.

Much less debated is the importance of a breach response team experienced in crisis management. For this reason, when it comes to reputational risk, the most valued aspect of a cyber insurance policy is often the access it provides to third party vendors who are critical to a breach response. In order to increase penetration rates, effective communication of these benefits is a necessity.

Is reputation safe from breach?

In conclusion, Advisen research has found that companies frequently survive breaches with their reputations intact – or at least without much if any negative impact on earning or share price due to reputational fallout.

Nonetheless, some companies have been damaged by data breaches, so the threat is real. The question then is how the risk as perceived by decision makers compares to the actual risk of damaging the organization.

Will “data breach fatigue” take hold among customers, who just accept data breach as part of everyday life, as corporations’ slick public relations teams calm the waters?

Or will the unsettling affect of a data breach – like senior management reshuffles - have irreversible effects on a firm's reputation?

One emerging cyber threat is that of a coordinated attack on a nation's critical infrastructure, for example. The failure of an entire industry or supply chain link may be enough to get investor and consumer attention and any firm not prepared for such an eventuality may suffer badly in the fallout.

In the meantime, we appear to linger in the "resigned acceptance" phase of data breach awareness.

Authors: David Bradford, Josh Bradford, Chad Hemenway, Erin Ayers, Rebecca Bole for the Cyber Risk Network

ADVISEN CYBER RISK NETWORK
Insurance Intelligence for the Cyber Community

Sources

[1] http://www.protiviti.co.uk/en-US/Documents/Newsletters/Bulletin/The-Bulletin-Vol-5-Issue-2-10-Keys-Managing-Reputation-Risk-Protiviti.pdf

[2] Henry Ristuccia, partner, Deloitte & Touche LLP, and global leader, Governance, Risk and Compliance Services, Deloitte Touche Tohmatsu Limited. Appeared in Risk & Compliance Journal 2013 2

[3] http://www.acegroup.com/eu-en/assets/risk-reputation-report.pdf

[4] http://www.experian.com/data-breach/impact-of-mega-breaches-debrief.html?WT.srch=ecd_dbres_iapp_2014_landing_download_mega_breach_debrief#

[5] http://www.foxbusiness.com/industries/2014/09/24/hackers-want-medical-info-not-credit-card-6

[6] http://www.acegroup.com/eu-en/assets/risk-reputation-report.pdf

[7] Exploring Strategic Risk, Deloitte http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_grc_exploring_strategic_risk_093013.pdf

[8] Concerns About Risks Confronting Boards: Fourth Annual Board of Directors Survey 2013, EisnerAmper http://www.eisneramper.com/uploadedFiles/Resource_Center/Articles/Articles/Concerns-Risks-Survey-2013.pdf

[9] Exploring Strategic Risk

[10] Deloitte

[11] Reputation Impact of a Data Breach, Ponemon Institute, sponsored by Experian Data Breach Resolution, 2011 http://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

[12] "Poll: Nearly half of cardholders likely to avoid stores hit by data breaches," CreditCard.com http://www.creditcards.com/credit-card-news/shopping-after-breach.php

[13] http://www.thestreet.com/story/12897352/1/cramer-home-depot-delivers-despite-poor-housing-expensive-stock.html?kval=dontmiss

[14] http://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/

[15] Partner, Deloitte & Touche LLP, and global leader, Governance, Risk and Compliance Services, Deloitte Touche Tohmatsu Limited. Appeared in Risk & Compliance Journal 2013 http://deloitte.wsj.com/riskandcompliance/2013/10/02/why-reputational-risk-is-a-strategic-risk/

[16] Among others, members of a breach response team can include executive leaders, IT, legal, public relations, customer relations, law enforcement, insurance broker, and insurance carrier.