Security as Business Risk: How Data Breaches Impact Bottom Lines

By:
Tom Bowers, Security Constructs, LLC
Managing Director

September 2011

The management of data breaches is indistinguishable from "classic business risks" and should be assessed from a traditional business risk perspective.

In his excellent book **The Failure of Risk Management**, Douglass Hubbard divides risk management professionals into four major categories: actuaries, "war quants," economists and management consultants.[1] All of these risk management professionals share a common challenge: how do you define risk? Despite this united question, each kind of professional views risk and its implications in slightly different ways.

This divergence in risk mindset inevitably leads to obstacles for what could be classified as the fifth type of risk manager: the security professional. Particularly in these times of frequent large-scale data breaches, the security professional often navigates as much risk as his business unit colleague, but his opinion is often wrongly interpreted in a completely different context. Upon closer inspection, however, it's clear that the management of data breaches is indistinguishable from "classic business risks" and should be assessed from a traditional business risk perspective.

Classic Business Risks

Risk management typically weighs the business uncertainties within the following key categories:

Strategic

The most fundamental and important risk type of all, strategic risk is future-oriented and thus difficult to foresee and mitigate. New competitors, natural disasters and geopolitical changes are all examples of strategic risks to a company. Modern examples include Internet-based telephone versus traditional landlines, as well as streaming movie content versus brick and mortar DVD rental businesses.

Reputation

Though often overlooked, risk to a company's reputation can cause more long-term damage than any other risk type. Damaged reputations typically shrink shareholder value and may involve negative publicity, loss of clients or key employees and decreased revenue. Reputation risk is so critical that a number of online tools have emerged which use social media to track how corporate reputations are impacted during a crisis.

Brand

To understand brand risk, one must understand brand equity. In its simplest form, brand risk is what a brand means to a customer. Higher equity translates to customer loyalty, premium pricing and expanded stock values; brand risk is anything that detracts from that equity. High brand risk and low brand equity means lower customer trust, loss of sales and higher marketing costs to rebuild equity. As an example, the American automobile industry suffered from a large quality perception gap during the 1980s, so brand equity suffered as global competitors grabbed increasing market share and customer base at the expense of U.S. companies.

Customer

Customer risk is a broad term defining a number of customer-specific attributes and their potential impact on an organization. Demographics, global location and buying habits are three examples of specific demographic types. Concentration locations, reliance on too few large customers and risks to customers themselves may all have a dramatic impact on an organization.

1 Douglass Hubbard, **Failure of Risk Management: Why it is Broken and How to Fix It** (Wiley, 2009).

Shareholder

Because shareholders maintain an equity position in a company, any risks which they face become risks to equity value. A large loss of customers during a crisis may lower equity value such that credit is more expensive, research and development curtailed and changes in corporate leadership demanded. This risk type is very public, though tactical in nature. Most data breaches result in some loss of equity value in the short term.

Market

While typically defined in financial market terms, market risks here refer to those driven by both positive and negative business situations which affect market share. Companies can increase market share by increasing product features, improving performance and making positive changes in perceived value; for example, investing in better manufacturing processes over the long term. Market share is lost as reputation suffers and customers move to alternatives. This type of loss tends to be acute in nature and may prove life-threatening to the corporation. The ongoing battle between Internet browsers is a classic example of this risk type.

Operational

Operational risks include the inner workings of a company, for example internal business processes, IT systems, supply chains and talent recruitment efforts. Paramount to assessing operational risk is the ability to continue or resume normal business operations. The earthquake and tsunami in Japan disrupted many businesses and dramatically changed the supply chain for companies around the world. Large-scale data breaches have had a similar effect on companies globally.

Financial

Financial risk includes that which is both internal (investments, loans and debt) as well as external (economy and competitors). Positive financial risks may drive a company forward via new product development, while negative financial risk may cripple an organization, as seen in the recent meltdown in the financial services sector. For example, large companies may take out 90-day loans to pay operational costs while receivables are collected from customers. Fluctuations in a company's financial risk posture may directly affect the cost of these 90-day notes and thus profit margins on goods and services sold.

Compliance

Though a relative newcomer to the "classic business risk" list, compliance is now commanding more attention from corporate executives around the world. Compliance risks emanate from laws and regulations instituted by a wide range of countries, for example privacy laws from the European Union, India, Japan and the United States. Of course, regulations also exist for specific market verticals, such as for those companies that allow credit cards for payment (PCI) and which possess patient health information (HIPAA).

Market share is lost as reputation suffers and customers move to alternatives. This type of loss tends to be acute in nature and may prove life-threatening to the corporation.

There is now enough evidence to prove that security is a business risk which must be accounted for in every organization's enterprise risk management plan.

The New Risk: Security

While classic business risks are well known and defined, with metrics to demonstrate their effect, security lags behind as a risk category. It may be difficult to tie a hacker's attempt to break a password-protected file to a specific dollar amount, but the earliest denial of service attacks against e-commerce companies – dating back to February 2000[2] – demonstrated that when security suffers, business operations are deeply affected. Though data breaches have been little understood until relatively recently, what has been clear is that breaches negatively impact consumer confidence and shareholder value.

The huge number of high-profile data breaches in the past few years has provided statistically valid data to better measure the connection between a company's security and its bottom line. Moving forward, a growing body of academic and professional research will yield new econometric models for security that are easier to use and implement. In the meantime, there is enough evidence to prove that security is indeed a business risk which must be accounted for in every organization's enterprise risk management plan.

Real World Examples

Measuring security as a business risk is a difficult analysis, one more easily quantified by weighing the effects of a data breach on a company. To aid with this evaluation, we offer three case studies that are best viewed as lessons learned and not as criticism of the companies themselves. The risk outcomes with each of these examples – technology giant Sony Corporation and credit card processing firms Heartland Payment Systems and CardSystems Solutions – vary widely and demonstrate an array of data breach responses and market reactions.

Sony

Corporate Overview

Sony is a highly respected multinational conglomerate based in Japan, with FY 2011 earnings of $86 billion. While the company has many distinct business units, Sony is best known for producing high quality electronics.

Sustained Breaches

Sony's challenges began in April 2011 with a massive breach of its PlayStation Network, later followed by additional breaches, including one directed against its online entertainment division. These breaches resulted in the loss of 100 million customer records and the shutdown of business operations for several Sony units over a period of weeks.

2 Martyn Williams, "EBay, Amazon, Buy.com hit by attacks," 2000, http://www.networkworld.com/news/2000/0209attack.html (accessed August 19, 2011)

Sony Response

Sony's major challenge with its response to these data breaches was to deftly navigate perception and image management. In that respect, Sony failed. The company received tremendously negative media attention for its perceived delay in notifying customers of the breach, which became such an issue that the CEO himself, Howard Stringer, was forced to respond to media questions. Stringer's defense of Sony's one-week response time fell on disbelieving ears and only worsened the furious public reaction.

When considering the public apology offered, it's important to remember that Sony is based in Japan, where an apology of this sort would simply be accepted and the matter closed. Suffice it to say, this broader cultural context was lost amidst the firestorm of damaging publicity. From a security professional's perspective, Sony was technically prudent and responsive. From a consumer's perspective, however, the perception of Sony's misguided response created a backlash.

While meant to be a positive development, the May 2011 announcement that Sony was creating a Global CISO role raised more concerns than it settled.[3] Given the wide range of systems breached and business units affected, the belated implementation of this role begs the question of why didn't Sony have a CISO in place before these breaches. The perception is that security was an afterthought not taken seriously by Sony and that individual business units were left to handle security on their own. Little else can explain the complete disassembly of Sony's cyber defenses.

Sony's initial customer responses included offering credit-monitoring services to affected customers, enhanced customer support, creation of welcome back programs and implementation of new security systems. Direct costs to date are approximately $171 million, but given its legal fees and other potential lost revenues, Sony's total cost estimates from these breaches range from $13 billion to $20 billion over the long term.[4]

Victimology

Sony's breaches invite a specific examination of victimology. Initial reports suggest that the personal information of 75 million PlayStation users was compromised by these breaches. One might imagine these PlayStation users to be teenaged and young adult gamers; the reality is that many of these gamers don't own credit cards, and thus it is their parents or guardians whose information was lost. The real loss, however, is one of trust. Sony's damaged reputation might plant this question in the minds of millions of consumers: if this company doesn't care enough to secure my information, do they really create the kind of reliable high-end appliances my family needs in the future?

The announcement that Sony was creating a Global CISO role raised more concerns than it settled; why didn't Sony have a CISO in place before these breaches?

3 Eric Chabrow, "Breach Gets Sony to Create CISO Post," 2011, http://www.healthcareinfosecurity.com/articles.php?art_id=3599 (accessed August 9, 2011).

4 Larry Dignan, "Sony's data breach costs likely to scream higher," 2011, http://www.zdnet.com/blog/btl/sonys-data-breach-costs-likely-to-scream-higher/491612011 (accessed August 9, 2011).

The loss of consumer confidence and declining reputation always leads to market risk.

Business Risks

Customer

In the weeks following the data breaches, PlayStation trade-ins increased significantly amongst consumers opting for other gaming consoles.[5] While identity-monitoring services are helpful for a consumer whose information has been compromised, each alert is also a reminder of how Sony failed them.

Reputation

According to Yougov BrandIndex, which offers daily monitoring of consumers across seven different variables, the reputation of Sony and PlayStation 3 took a severe beating because of the recent breaches. PlayStation 3 is now in the negative territory of brand perception while Sony itself is ranked behind several of its major competitors. Once viewed as the industry leader, Sony is now in the uncomfortable role of playing catch-up.[6]

Market

The loss of consumer confidence and declining reputation always leads to market risk. In the past few months, gaming console competitors to PlayStation have offered discounts and incentives to consumers to move to their platform. PlayStation sales have subsequently declined and market share has been lost. The longer-term market changes in other Sony business units remain to be seen, but one can suspect that slower growth lies ahead.

Shareholders

It is readily apparent that Sony's shareholders and board are unhappy with the company's present situation. Sony announced that its CEO's pay was cut by 15% at the end of June, and while top management executives have stated that online services continue to be a major source of revenue, Sony shareholders seem less positive.[7]

Heartland Payment Systems

Corporate Overview

Heartland Payment Systems is the fifth largest payment processor in the United States, specializing in Server Message Block protocol. Services include online payment processing, check processing and payroll services. Heartland offers a PCI DSS validated service for card processing, which is an excellent standard although limited to a "single point in time" review process. Primary customers include all of the major credit card issuing companies, with tier two customers including a wide range of small to medium-sized merchants.

Breach

Heartland processes in excess of 10 million transactions per day from 250,000 vendors across the country. To do so within a PCI environment, Heartland uses a PCI Zone for electronic transactions. PCI calls for encryption throughout the network, but to ensure interoperability PCI Zone does not require encryption.

5 Don Reisinger, "Report: PlayStation 3 trade-ins on the rise," 2011, http://news.cnet.com/8301-13506_3-20062596-17.html (accessed August 9, 2011).

6 Steve Ragan, "Seven security incidents in two months - Sony's nightmare Grows," 2011, http://www.thetechherald.com/article.php/201121/7185/Seven-security-incidents-in-two-months-Sony-s-nightmare grows (accessed August 9, 2011).

7 Bloomberg News, "Sony Cuts Howard Stringer's Pay Package as Chairman by 15%," 2011, https://www.nytimes.com/2011/06/29/technology/29sony.html?_r=2 (accessed August 9, 2011).

In December 2008, Heartland and a large credit card issuer discovered a massive breach within the Heartland system. Testimony from the alleged hacker ringleader, Albert Gonzales, and his crew provided proof that the breach persisted over several months. To accomplish this breach, the Gonzales crew put sniffers in place to view PCI transactions in clear text, and then created an outbound data stream with the same look and feel as normal business traffic. The sophistication of the Heartland breach demonstrated that hackers are capable of understanding international security guidelines as well as some of the best security professionals.

Business Risks

Customer

Customer confidence in Heartland surely was shaken, especially in light of the long-term nature of the attack. Given the many choices merchants have in choosing their payment processing vendors, it is easy to see how the breach may have led to a decrease in customer confidence.

Market

As with the Sony breach, the downturn in customer confidence led to a change in market risk. Heartland did an excellent job of controlling information during the subsequent breach clean-up, so the total costs of its data breach can only be estimated at $140 million.[8]

Shareholder

Once again, a change in customer and market risks led to unhappy shareholders. This discontent translated into a drop in share value and increased scrutiny by industry analysts, including questions about the company's protection of its payment algorithms, research and operational system design. In short, shareholder investment was negatively affected[9] by the breach.

CardSystems Solutions

Corporate Overview

In 2005, CardSystems Solutions was one of a growing number of credit card processing companies; note the key word "was." The company's clients included most of the major credit card issuing companies.

Breach

A significant data breach in 2005 demonstrated that CardSystems was keeping copies of its transactions in unencrypted form, in violation of its contract terms. Additionally, the breach proved that CardSystems' IT infrastructure was highly accessible to hackers. The breach was the largest of its time, compromising the records of 40 million consumers, and was the first to launch scrutiny from politicians at both the state and national levels. The aftermath of this breach encouraged the credit card industry to rethink security standards and begin a process of intense self-regulation.

In 2005, CardSystems Solutions was one of a growing number of credit card processing companies; note the key word "was."

8 Jaikumar Vijayan, "Heartland breach expenses pegged at $140M -- so far," 2010, http://www.computerworld.com/s/article/9176507/Heartland_breach_expenses_pegged_at_140M_so_far, (accessed August 19, 2011).

9 Noreen Seebacher, "Data Breaches Could Cost Investors," 2011, http://www.investoruprising.com/author.asp?section_id=1296&doc_id=206164 (accessed August 9, 2011) .

Data breaches clearly have major consequences on business operations.

Business Risks

Customer

The intent of the stored data which was hacked was to provide for testing of new software upgrades. The fact that this was done in unencrypted fashion resulted in the loss of all CardSystems' customers within a matter of days. Had the company's customer base been broader, CardSystems may have survived the crisis, but instead the company was forced into emergency measures to save itself.

Corporate

In 2005, CardSystems Solutions was purchased by Pay by Touch, which permanently ceased the company's operations two months later. The breach of trust and customer confidence was simply too overwhelming to recover. Six hundred CardSystems employees lost their jobs.

Integrating Security into Overall Risk Management

Data breaches clearly have major consequences on business operations. From a simple loss of market share to complete corporate collapse, the loss of data profoundly impacts an organization and causes tremendous risk to an organization's bottom line.

Accordingly, security professionals should no longer be marginalized as mere technology executives but instead be considered business executives whose voices are included as a necessary part of a company's overall risk management process. Keeping an eye on business goals while creating security systems to enable that vision can lead companies to adopt more flexible and secure working environments that provide greater protection from harmful risk throughout all of their organizational divisions.

To learn more about data breach resolution, visit **www.Experian.com/DataBreach** or contact Experian® at **databreachinfo@experian.com** or **1 866 751 1323**.