What is the cost of reputational harm?

It can take years to develop a reputation, but only minutes to damage it. This is true for organizations as well as individuals. Consider these examples:

- Cybercriminals plant malware on a retailer’s point of sale system and steal thousands of customer credit card numbers.
- A national restaurant chain sees its stock price plummet after patrons at various locations become violently ill.
- The head of a major nonprofit organization resigns when an audit discovers fundraising irregularities.

With these types of incidents becoming increasingly common every day, it is no wonder that executives rank “damage to reputation or brand” as the top risk they face—ahead of economic pressures, regulatory and legislative changes, and increased competition.1 At the same time, more than three-quarters of executives admit that it is difficult to quantify the financial impact of reputational risk, given its intangible nature.2

Calculating the cost

While calculating the cost of reputational harm can be challenging, it is not impossible. Depending on the facts surrounding the incident that causes the harm, organizations can use one or more methods to quantify the financial impact for insurance, legal and other purposes.

Calculation starts with an investigation to determine facts that can support a claim or legal position. What revenues were lost as a result of the incident? How much did market share decline? How much did the stock price drop, and for how long? These are among the first questions an organization would address after experiencing reputational harm.

---


Lost profits analysis. This method examines economic damages an enterprise might suffer. Organizations will need to have good records of past business activity to support claims of profits they were unable to generate as a result of an incident.

Relief from royalty method. To calculate the effect on a brand in particular, a company might use the relief from royalty method. This approach examines alternative revenue streams or alternative royalties to be paid, and isolates the effect of the event on the brand, specifically.

Lost enterprise value. Depending on the extent of the damage, a company might go out of business. So instead of just measuring lost profits, an organization might need to determine lost enterprise value.

Event study. This technique measures the effect of an event, such as a data breach, on the value of a firm. This is accomplished by using prices in the stock market to calculate the abnormal return associated with the event and comparing actual returns with those predicted by a market model. This method separates the effect of the event on the firm's stock price from macroeconomic factors.

A case study in cyber-related reputational harm insurance

How does reputational harm insurance work? Consider the following example:

A national retail apparel chain experiences a data breach at several of its stores. Credit card readers were compromised, and data from thousands of customers' credit cards were stolen as a result of malware that infected the system.

Once the breach was reported to authorities, several news stories appeared online, in newspapers and on many broadcast news programs. The headlines scared consumers, many of whom stayed away from the chain for several months, leading to a measurable decline in sales.

Thankfully, the retailer's cyber insurance policy came with a rider covering up to $5 million in reputational harm losses of revenue or profit.

The retailer, working with its insurance company and reputation harm claims adjuster, will assess the circumstances, applying the following process to quantify the reputation harm:

- In cooperation with law enforcement, undertake a forensic investigation to determine the root cause of the breach and to identify the customers, software, systems and devices compromised.
- Based on findings from the investigation, identify the type(s) of data and information lost and type(s) of breach. Losses might differ between customer and financial information versus nonfinancial business information.
- Quantify the associated monetary and profit losses using a method best suited to the type(s) of data and information lost and type(s) of breach in question (lost profits, relief from royalty, lost enterprise value or event study, etc.). Loss mitigation costs as well as other costs avoidable but for the breach should be considered in measuring total losses.

The retailer was able to validate the decline in sales by comparing sales after the breach to prior-year periods and other patterns in the marketplace. An independent certified public accounting firm was called in to provide a valuation of the business losses, and within a relatively short period of time, the insurance company sent the retailer a check for the effects of the breach.

Prepare now

While the financial impact of data breaches can be considerable, perhaps the greater issue for middle market organizations is the effect of breaches on management time. Responding to data breaches requires a lot of executive and staff attention, and can take real dollars away from managing the business. Reputational harm insurance not only helps cover the cost of a breach, but also provides funds to cover the temporary loss of income while an organization recovers. Such policies can be a lifeboat for middle market businesses needing to get through a difficult time.
Just as organizations prepare for business interruptions and other possible crises, they should take steps now to prepare for incidents that might cause reputational harm by developing plans to respond to potential events and identifying external resources that can help mitigate their impact. In the case of potential cyberattacks, pre-incident planning should ensure that network logs are active and that the organization uses a network solution to monitor web-based traffic.

Prepared by:

Boris Steffen, Director, RSM US LLP
boris.steffen@rsmus.com, +1 703 336 6303

Jeremy Barnett, Senior Vice President, NAS Insurance Services jbarnett@nasinsurance.com, +1 818 382 6116