CARLTON FIELDS

Secure Communications: How a Monthly Lunch Can Protect Your Company in a Data Breach

September 01, 2015

After hackers steal customers' credit card numbers or a company's trade secrets, it is far too late for the corporate chiefs of public relations and information technology to learn one another's names and responsibilities. That's why, based on our experience as legal counsel to companies in crisis, we recommend that a company's senior PR person should have regular monthly lunches with its head of IT security. Here, we explain why the IT-PR relationship is critical for an effective media response to a data breach. **A careful strategy**

Without a careful PR strategy, even a routine data breach can morph into a consumer class action, a regulatory investigation and a two-hour CNN special. During a crisis, if the corporate spokesperson lacks a basic IT vocabulary or if IT staffers speak to the press without preparation from the PR department, then a company's public statements will be uninformed, rambling or rogue — rather than accurate, on-message and approved. Soon, even a breach that a company's IT professionals have already detected, assessed and remediated can morph into a disaster for the corporate reputation. And the PR department would bear the blame. One example is the December 2013 data breach at Target, in which hackers accessed the credit card information of 40 million customers and the data files of 70 million customers during the holiday season by infiltrating checkout machines with malware. Target, exhibiting signs of a brushfire mentality, had to correct various initial statements regarding the breach's scope, duration and data types. In particular, Target did not clarify that different types of information were accessed for individual consumers over a period of time. Within six months, both the CEO and the chief information officer had resigned, and litigation had increased. Home Depot disclosed a similar "point-of-sale" data breach in September 2014. The hack was similar in size and scope to Target's, but lasted longer. Unlike Target, Home Depot initially disclosed limited information about the breach, by announcing that the company was investigating a data breach. Home Depot exhibited greater press discipline and didn't make any outside communications until the company had a coordinated message. And when Home Depot updated the press on its investigation, it only announced solid information. This example reinforces the idea that

waiting to say something meaningful beats saying something wrong nine times out of 10. **A focus on education**

One culprit behind poor data breach responses is a lack of effective communication between a company's PR experts and its IT department. Their résumés, backgrounds and cultures differ. Public relations works with wire services, buzzing phones and need-it-yesterday requests for quotes. IT works with systems updates, multiple monitors and all-night coding sessions. But when a data breach engulfs a company, silos don't serve anyone. For these reasons, a company's senior PR person — the person designated as communications lead during a data breach — should regularly connect with its head of IT security. Monthly lunches provide a great environment for these meetings, where there are several goals to keep in mind. Educate the spokesperson about:

- What data the company maintains
- What steps the IT team has taken to safeguard against data loss
- What the most likely threats are to that data and how the company would learn of an attack, if it occurred

Educate the IT chief about:

- The responsibilities of the company's PR professionals and the impact of the company's public messaging on its bottom line
- The types of media that cover the company
- The company's media strategy related to data breaches, how to direct media inquiries, who from IT will interface with PR and vice versa, and whether the company will use an outside agency

The paramount goal is to build "top-to-top" trust and rapport between the two departments. **An improved relationship**

There are also several benefits of this improved relationship:

- Avoids a situation where the IT head has to contain a data breach in real time, while explaining the company's sensitive network infrastructure to a stranger, who must then transform that explanation into an educated public message
- Allows the spokesperson to ask follow-up questions in a non-crisis environment, translate the tech language into effective sound bites and draft a better PR strategy for data-loss events
- Ensures that IT deploys its finite budget to protect against the types of data breaches that would most impact the company's reputation
- Builds a confident, knowledgeable spokesperson — arguably one of the most effective ways to fortify the confidence of a company's customers and investors after a data loss, and reverses or blunts a negative news cycle

Mindful planning cannot stop a breach, but it can result in a well-managed one. The short-term impact of an individual company's media response to a data breach can make the difference in consumers' confidence in that company in the long term. *Copyright 2015 by Public Relations Tactics. Reprinted with permission from the Public Relations Society of America (PRSA.org).*

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology