Global Data Privacy and Security Team

Breach Reputation Management: At A Glance

The reputational injury following a data breach can be severe. Indeed, reputational injury – including lost customers – often surpasses legal liability.

Effective management of the reputational impact of a data security incident requires a proactive and reactive strategy. The proactive strategy assumes that the organization will control when, and what, information will be conveyed to the public, media, and impacted consumers. For many organizations the proactive strategy that they choose is to wait until their investigation of an incident is complete so that they can provide the public with the most accurate and meaningful information.

The reactive strategy anticipates that the public may be alerted to a possible security incident at a time when the organization may not have full or complete information. The reactive strategy must carefully balance responding to requests from the public for details that may not be known to the organization. While the pressure to provide information can be significant, providing inaccurate, incomplete, or preliminary information can confuse consumers, increase the likelihood of legal liability, and, in the long run, lead to worse reputational injury. Due to the complexities involved, many companies retain third party communications, public relations, or reputational consultants to help manage reputational impact.

Percentage of people that reported that they "trusted" family owned businesses.*	Percentage of people that reported that they "trusted" big business.	Percentage of customers that boycott a retailer if a data breach has been reported.
72%	**45%**	**12%**

$0 - $135,000

Range of money spent on a crisis management or public relations firm following a data breach.

What to think about when retaining a consultant to help manage the reputational impact of a security incident:

- ☑ Has the consultant dealt with data breaches in the past? If so, was the strategy advocated by the consultant effective to control the reputational impact and quantity of media exposure?
- ☑ Has the consultant dealt with data breaches in the industry in which you operate?
- ☑ What was the most publicized breach that they handled? (Remember that high publicity does not necessarily signify an effective reputation-management strategy).
- ☑ What other breach-related services do they provide? If reputation-management is not the main focus of the consultant, is their practice sufficiently specialized in that area?
- ☑ What is the consultant's general approach to responding to media inquiries about a security incident when a forensic investigation is not complete?

Bryan Cave's Global Data Privacy and Security Team helps companies safely use, protect, and share information.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: +1 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386 USA
T: +1 303 444 5955

BRYAN CAVE

* 2015 Edelman Trust Barometer at *7 available at* www.edelman.com (last viewed Sept. 2015) (Based upon respondents in developed countries).
† *Id.*
‡ Interactions Marketing, *Retail's Reality: Shopping Behavior After Security Breaches* (last viewed 2015).
§ NetDiligence Cyber Cliams Study (2014)