MANAGEMENT

How to Manage Your Reputation in the Wake of a Cybersecurity Incident

After a cyberattack, customer and partner interactions can determine whether a company survives.

by Eden Gillott Bowe

Eden Gillott Bowe, president of reputation management firm Gillott Communications, is the author of *A Board Member's Guide to Crisis PR*.

Latest Articles

Why Hybrid Arrays Might Be the Goldilocks Answer to Storage for SMBs

Companies Can Wed Tech and Design to Create Great Workspaces

Ergonomics Can Help Reduce Workers' Comp Claims

The Tech Businesses Need to to Maintain Services in the Face of Dire Storms

No business is too small to be ignored by cybercriminals, and the facts back that up.

Here's just one example: A December 2016 survey by Small Business Trends found that **43 percent of cybercrimes were launched against small businesses**. Sadly, **60 percent** of those companies were out of business within six months.

Reputational damage suffered by the targeted companies — and the subsequent loss of customers and clients — were key factors in the closings.

How can a small business **fight the odds and emerge with its reputation and balance sheet intact?** Here are some tips.

Be Honest and Forthcoming After a Cybersecurity Incident

Empathy should drive businesses to treat customers and stakeholders with respect and address any cyberincident with expediency.

News of a security incident should be **disclosed as soon as the company's legal team gives its blessing**.

Businesses that hide information for months or years will **face fierce public blowback**. Company credibility will be lost, and when that happens, the business **might never regain consumers' trust**.

The question of who needs to know what, and when, **largely depends on the severity of the incident and on various requirements of federal and state laws**, so it's important to consult with a lawyer who specializes in both privacy and cybersecurity rules and regulations.

DIGITAL WORKSPACE

5 Retail Tech Trends to Watch in 2018

BUSINESS INTELLIGENCE

How Will Quantum Computing Help Banks?

Trending Now

NRF 2018: Want Digital Transformation In Retail? Break Down Internal Silos

> In the wake of an incident, how a company treats its customers and business partners can make all the difference.

EDEN GILLOTT BOWE
President, Gillott Communications

Typically, when an incident occurs, various stakeholders — **affected individuals, companies and vendors, as well as regulatory and credit reporting agencies** — need to be informed. There is no legal obligation to inform the media, but if it's a big-enough story or a slow news day, **be prepared for the floodlights to be flipped on**.

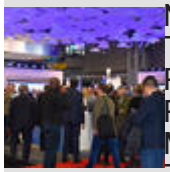
Companies should **carefully select an individual to deliver the news to the public**. The choice of a candidate will depend on the severity of the incident and the spokesperson's qualifications and credibility, as well as his or her comfort level in speaking on the company's behalf.

For a large organization, an appropriate choice would be **a media relations representative, CEO, or the head of IT or security**. A small business **might not have an obvious candidate**.

In this case, the **company's lawyer** may be the best choice as the person most able to speak without speculating, feeding customer or public fear, or making a legal misstep.

Alternatively, **issuing a concise, carefully crafted written statement approved by legal counsel is an effective way to break the news** and circumvent shouted questions from the media.

However the news is shared, the message must be carefully crafted. For example, **don't mislabel a cybersecurity event or incident as a breach**.


NRF 2018: Tech In Physical Retail Stores Must Scale To Succeed


NRF 2018: How Retailers Can Use AI To Solve Problems And Increase Sales


5 Retail Tech Trends To Watch In 2018

These terms have different meanings and possess varying legal disclosure requirements; **essentially, an event is not as bad as an incident, but a breach is far worse**. Stick to the legal team's talking points.

Ensure Employees Deliver a Consistent Message

Finally, make sure all employees understand the importance of **having a single spokesperson to deliver accurate information**.

In response to questions, everyone should be instructed to say, **"The best person for you to speak to about this matter is ..."**

Small businesses that follow this advice may manage to retain their good name, as well as customer and stakeholder loyalty. Most cyberincidents result from negligence by employees or contractors. So in the wake of an incident, how a company treats its customers and business partners can make all the difference.

More On LEADERSHIP POLICIES TRAINING SECURITY

Related Stories

Security

5 Reasons Why Small Businesses Are Targeted by Cyberattacks

Security

Cyberinsurance Helps Companies Mitigate the Fallout from Data Breaches

Security

Apple, Cisco Team Up to Offer Cyber Insurance

BizTech

Technology Solutions That Drive Business

About Us Contact Us Privacy

Terms & Conditions Site Map

BIZTECH: CDW:

VISIT SOME OF OUR OTHER TECHNOLOGY WEBSITES:

EdTech FedTech StateTech

HealthTech

EXPERTS WHO GET IT

3 Reasons Why You Should Run Microsoft Office in the Cloud

Read the Blog

Get BizTech in your Inbox

Browse Email Archives

Subscribe to Biztech Magazine

Browse Magazine Archives

BACK TO TOP

CDW PEOPLE WHO GET IT