TRAVELERS

TRAVELERS RISK CONTROL

Crisis Communications Planning for a Data Breach

Cyber security experts agree that it might not be possible to prevent a data breach from ever impacting your company. Since the cyber threat landscape and emerging technologies are constantly evolving, businesses of any size or industry are vulnerable. One thing you do have control over is how well your company prepares and responds if a breach exposes your customers' private data.

Many companies have a generalised crisis communications plan, in case there's a fire at a factory or a strike. But data breaches are unique in that they can involve private and confidential customer data and are subject to time-sensitive requirements. This calls for a specialised response, according to Mark Greisiger, president of NetDiligence, a firm that provides services for handling a data breach crisis.

"Crisis communications companies are becoming a really crucial component in handling a data breach," says Greisiger, noting that cyber insurance may cover retaining a public relations firm to manage post-breach communications. "It's absolutely a second line of defence once a breach occurs, in terms of protecting your company's brand and reputation."

Preparing for the Unexpected

One of the keys to weathering a data breach is building a plan before you need it, according to Melanie Dougherty, a crisis PR professional at Inform, a global communications firm. She works with companies to get a handle on what others in their industry are doing to prepare for and respond to attacks. She helps develop messaging for specific scenarios and trains company spokespeople to respond on-camera.

Dougherty notes that there is an emotional component to a data breach for companies who have just been robbed of their data. "That's the part people don't typically talk about," Dougherty says. She adds that the media attention can be overwhelming. Having a plan and a response team in place ahead of time can help take some of the emotion out of the situation so companies can respond effectively.

"A well-planned data breach response can convey that you are in control of the situation, concerned about your customers' privacy and committed to tightening security procedures to help prevent future attacks," says Tim Francis, Travelers Enterprise Cyber Lead.

Here are some key elements to consider:

- **Assemble the team.** Choose a company spokesperson in advance. Ideally, Dougherty says, it should be the Chief Executive Officer of the company or another senior leader. Train a backup in case that person is not available, such as the Chief Financial Officer. Record your spokesperson on camera to see how messages are landing with the team.
- **Understand the law.** Companies are sometimes unaware that their public statements, including media appearances and communication with customers, may be admissible in court if a lawsuit is filed. Consulting with a privacy lawyer can help guide language while also helping companies meet regulatory and fiduciary responsibilities.
- **Notify customers.** For breaches that require notifying customers, a communications plan can include guidelines and training for setting up a call centre. The training might include the tone and message for responding to calls, and how any FAQs will be scripted.

- **Communicate on all available channels**. Reach out to audiences on social media, your company website and other channels so you can tell your story, rather than waiting for it to be told in the media. Remember that consumers may find technical jargon and legal terminology confusing, so try to use plain language to express what you are doing to protect them.
- **Remember employee communications.** Communicate with employees so they are aware of the breach before they hear about it in the media. "They can help carry the banner for you," explains Dougherty. "You need them to have faith in your company."

A data breach can be a real test to a brand's resiliency, but customers are increasingly aware that all companies are at risk. To the extent that you can, share what your company is doing to shore up privacy protections. Companies who meet the crisis head on may even be able to emerge stronger, with a closer connection to their customers.