SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

Failing to Communicate is a Recipe for Failure

August 29, 2017

Eden Gillott Bowe

Not that long ago, "major" events seemed relatively rare and seared themselves into the public's consciousness. People remembered exactly where they were when JFK was assassinated, when the first plane struck the Twin Towers on 9/11, and when a gunman opened fire at Sandy Hook Elementary School.

Fast-forward to today. Such events are so frequent and common that they blur. Cybercrime, terrorist attacks, workplace violence – It's difficult to come to grips with one unsettling event before another takes its place.

We've reached a point where no company, agency, school or facility can believe with confidence that it won't happen to them. Decision-makers must implement safeguards and find practical solutions.

When confronting a physical threat (potential or actual) or a cybersecurity breach, you must be strategic in how you communicate.

Time is of the essence. You must be reassuring. You must be perceived as in control of the situation. You must show empathy for those who've suffered and be clear about what you're doing to protect those who've been put at risk.

Before you take any actions or make any comments, you must know where you're going and the best way to convey it. After an event has happened, don't waste your time fumbling for ideas and searching for the right words.

Getting Prepared: The First Steps

Assemble your rapid-response team. That's obvious and easy.

Brainstorm what security threats you might face and who's responsible for what. Do it now. The best time to do damage control is ***before*** damage happens. That way, when something happens, you can take immediate action.

Forge relationships now with local law enforcement and other government officials. Don't wait until after you need them. When you and your employees interact with them, treat them with respect. Show kindness, and you'll receive it in return.

Physical Threats and Attacks

These create a greater emotional response. They bring communities closer together. Because such events are relatable, a wider audience will project themselves onto them. People will think, *"What if this were my family?!?!"*

If there's an injury or casualty, your message must show empathy and compassion.

Location matters. If the incident occurs in a private office or factory, the burden is on you to provide and update details. If it's in a public space, local law enforcement or government will handle the details, and you can focus on the broader issues reaching out to comfort and reassure.

Cybersecurity Breaches

After shutting down or taking the affected system offline, call your attorney. You must be certain everything you do or say is in line with the tangle of federal and state legal requirements – before you do it. You can't un-ring a bell.

Remember: What people want most is to be reassured. Were they affected? How? What's being done to protect them?

Don't begin your communication with "We regret to inform you…" Your notification will already include legal jargon that's scary enough. Don't make it worse.

Working with the Media

When the media comes calling, seize every opportunity to shape the story to your benefit. Your ultimate goal is to tell your story on your terms. So, don't hide or say "No comment." There's always something you can say or do to make a situation better.

In today's 24-hour news cycle, you must be fast to get your side of the story told. But don't be too hasty, or you'll make mistakes.

You may have limited time to respond. Use it wisely.

Frame your message so it's smooth and positive. Polish your language so the tone is just right.

Be concise. Reporters love sound bites that fit easily into a short paragraph or a few seconds of airtime. Have only two or three talking points, and don't stray beyond them. If you give a lengthy or convoluted explanation, the media may focus on the point that's least important to you.

Always avoid negative or emotionally charged words. Even if someone else (including the media) is using them, don't repeat words like massacre, disaster, unprecedented, carelessness, exposed (as in "exposed confidential information" or "the back-door left the company exposed").

Communicating with Your Audiences

Don't speculate. If you don't know it to be factual, don't say it. As with the media, stick to the two or three key points that are most important to you.

No matter who your audience is, be reassuring.

Don't tell different stories to different audiences. Be consistent, or it'll look like you're lying to someone.

Working Towards a Brighter Future

After you receive the all-clear, you can breathe a sigh of relief. You've been through the wringer and survived.

Whether it was the real thing or just a test, have your team make notes of what worked and what didn't. For example, were response times too long? Was there any confusion about responsibilities? Do employees need a refresher on how to avoid email scams? Were there too many people speaking off-script,

and therefore no unified message? They'll help avoid missteps next time, because memories fade or are reinterpreted over time.

Eden Gillott Bowe is president of Gillott Communications, a Santa Monica and New York-based strategic communications and reputation management firm, and is author of A Lawyer's Guide to Crisis PR and A Board Member's Guide to Crisis PR.