DISASTER RECOVERY JOURNAL

FALL 2017 ◆ VOLUME 30, NUMBER 3
$4.00

The Journal Dedicated to Business Continuity

WWW.DRJ.COM

The Threat of Absenteeism

When Disgruntled Key Employees Don't Show Up

INSIDE ...

Photo by © kieferpix – Fotolia.com

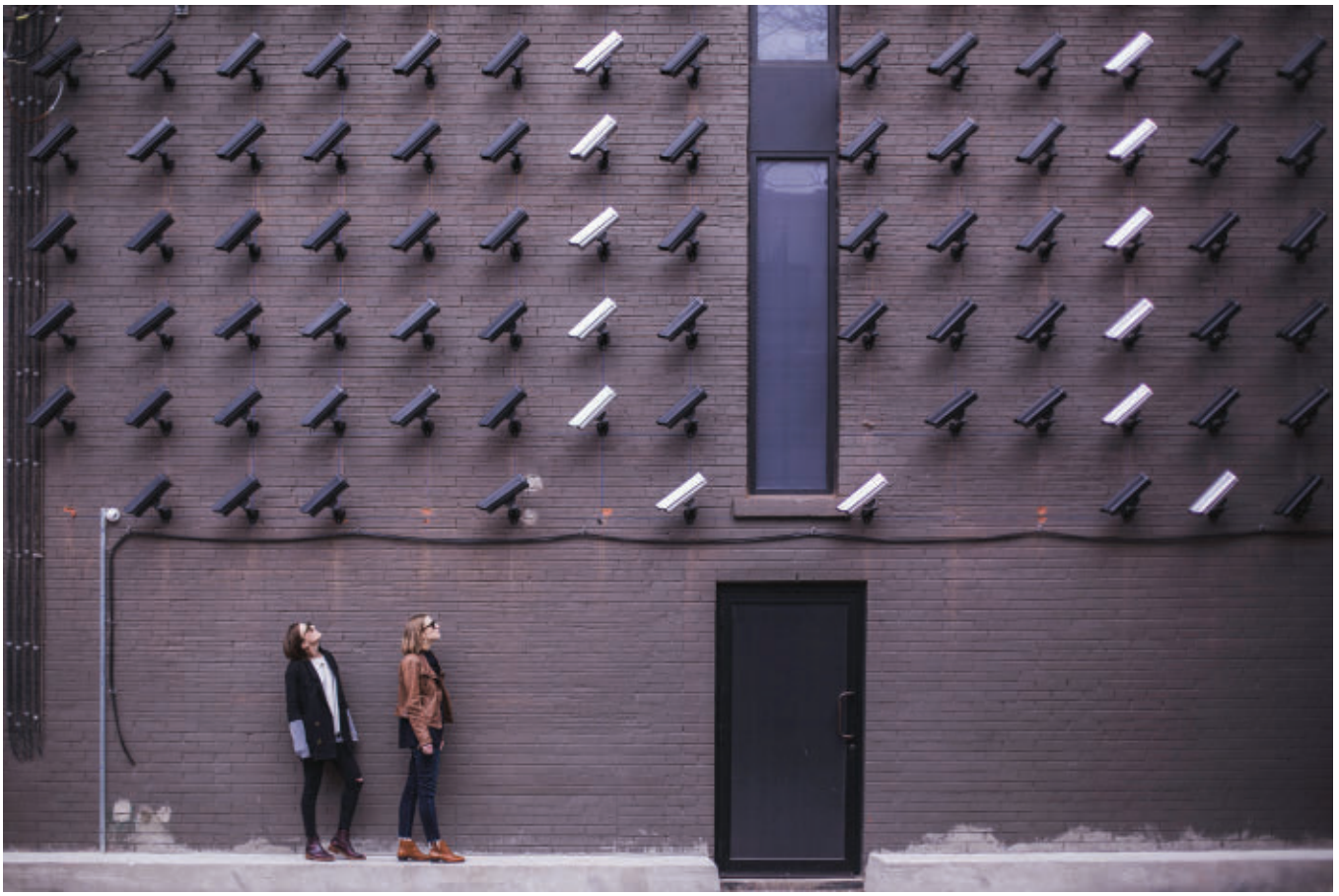

Photo by Matthew Henry

PERSONNEL ISSUES

Crisis and Reputation Management in the Age of Cyber and Physical Threats to Corporate Workplaces

By RYAN SCHONFELD & EDEN GILLOTT BOWE

Crisis. Disaster. Attack. These emotionally charged words catapult our brains into overdrive.

You've heard it countless times: be proactive. Maybe you roll your eyes and say, "I know." Perhaps it is coupled with an audible groan of annoyance. We hear you.

But be practical. Do not let yourself become overwhelmed or you will suffer decision paralysis.

If the thought of tackling the unknown beast has you breathing into a paper bag, you won't glean much benefit from this article, and you will make mistakes when the real thing happens.

Best place to start: slow down and take a deep breath.

After you have calmed yourself, assess the situation. Only then will you have the clarity to focus on the future. If you don't know from where you are starting, you will end up spinning your wheels, wasting time and money, and losing your opportunity to take control of the situation from the outset.

Anticipating Workplace Threats

If a truck careens into your office, do you know what to do? How about an employee becoming an active shooter? Or you have become the latest victim of ransomware, you have been locked out of your computer systems by nefarious cyber attackers, and your employees' productivity is instantly stopped in its tracks?

Before a threat, physical or cyber, occurs, it is important to have a crisis team in place. This includes (but is not limited to) the CEO/COO (ultimate

decision maker), legal, HR, operations or facilities manager, security, and communications.

Each member should know they are on the team and what their responsibilities are. (You may laugh, but this is often overlooked.) There should also be at least one back-up person for each primary team member in the event someone is unavailable during an incident.

Once you have built your team, it is all about collaboration and practice.

Because it can be hard to coordinate schedules, a working lunch is perfect. Invest an hour to conduct regular tabletop exercises at least quarterly and run through semi-real-time scenarios. The meeting should consist of 35-45 minutes of content with 15-20 minutes of debriefing to assess what went well and what needs improvement. Make adjustments and tweaks where necessary.

You also need a business continuity plan that includes service-level agreements with your vendors and providers. Understand what their response times will be in various situations when you are counting on them. Consider security, investigators, generator fuel, power, Internet, etc.

Handling Workplace Threats

Workplace violence is a dirty little secret which companies do not want to discuss.

According to OSHA's most recent statistics, homicide is the fourth-leading cause of fatal occupational injuries in the United States. According to the Bureau of Labor Statistics Census of Fatal Occupational Injuries, nearly 2 million American workers report having been victims of workplace violence each year. (Think of all the additional cases that go unreported.)

How do you prepare? You must be willing to have difficult conversations. It is literally a matter of life or death.

A certain amount of monitoring should take place at any office or setting. It can range from the motto of Homeland Security and New York City's MTA, "If you see something, say something" to friendly conversations at the water cooler to routinely scouring electronic inbound and outbound communications for keywords or phrases such as shoot, gun, blow up, bomb, or explosion. Most of the time, people are making a joke and filters do not understand context, but you cannot afford to take that risk.

Each member should know they are on the team and what their responsibilities are. (You may laugh, but this is often overlooked.) There should also be at least one back-up person for each primary team member in the event someone is unavailable during an incident.

Often, you'll hear the complaint, "But that's a violation of my right to privacy!" Wrong.

Your employees may not realize there is likely a clause in their employment agreement or handbook that their computers, online and email traffic, and activity may be monitored. This can apply to work devices that are taken home to bringing your personal device to work and connecting to the office network. It is all considered company property.

If a threat is discovered, a team consisting of – at minimum – HR and legal should interview those involved. Bringing in a skilled investigator and interviewer may make sense for these types of situations because HR and legal may be less experienced in workplace violence. Depending on the severity, security, and law enforcement may also be called upon. At the very least, the employee must receive counseling or training. At worst, it may be necessary to suspend the employee or terminate. Many jurisdictions also have Workplace Violence Restraining Orders (or similar) that are filed by the employer with the assistance of legal counsel.

Depending on your company's needs, you may decide to take advantage of one of the several platforms available to monitor internal communications and social media. The goal is to see how people are responding to a certain topic or within a specific geographic area. This is often referred to as sentiment analysis and has usefulness in security as well as for advertising and business intelligence.

A common pitfall is the "set it and forget it" attitude. Clients invest money to install a slew of fancy gadgets, but they do not secure the systems' back ends or keep them updated with the latest security patches. The result: a false sense of security. You may feel secure, but you have exposed yourself to cyber threats.

One certainty in life is that threats are constantly changing. You need to set policies and actually follow them. If your company does not have the internal resources to dedicate to protecting your technology, you need to contract with an outside firm that specializes in cybersecurity. (Many IT companies are not cybersecurity experts.)

Working with Law Enforcement or Other Government Officials

Do not wait until you need them. Over time build a relationship with your local law enforcement and other government officials.

Remember that behind the uniforms, police have feelings too.

Simple gestures such as offering to let officers use your company's bathroom on duty can make a big difference. Or consider opening up your cafeteria so they can grab a cup of free coffee. You are providing them a place that is clean and safe, and they will appreciate it.

In return, you now have a relationship that is evolved organically. Officers will feel closer to your employees, which in turn will make your employees feel more at ease.

By contrast, avoid the common pitfall of talking down to law enforcement and other government officials in a demean-

ing way. This includes the "CSI Effect" in which you expect everything to be handled like it is portrayed on TV. It is the quickest way to burn the bridge of trust you have built.

They took the job because they want to protect people. Be reasonable. Talk to them like you would talk to your friends, not your adversary.

How to Communicate During Evacuations

When you are facing a fight-or-flight situation, analyze each situation carefully. There are lots of moving parts and different factors that can dramatically influence your strategy and what you communicate.

It must be clear that you take the situation seriously. Reaffirm your company's core values. Let your employees, the public, and the media know what you are doing to fix it.

Different audiences have different needs. Reporters want a pithy quote. Investors want to be reassured their money is safe. The public wants an explanation that is reasonable and comforting. But even though their needs are different, the essence of your message must be consistent for all the audiences.

Informing the Media and the Public

When the media comes calling, it is natural to feel threatened and want to hide. Don't. Instead, seize every opportunity you can to shape the story to your benefit. Your ultimate goal is to tell your story on your terms.

In any situation, your underlying goal is the same: be reassuring.

Make it clear that you have things under control. Do not say too much. Stick to the two or three key points that are most important to you. Do not speculate. Do not go beyond what you know is factual.

Never say, "No comment." That makes it appear you are hiding something, which makes you look guilty. There is always something you can say or do to make the situation better.

Moving Past the Crisis

Debrief with key participants, preferably within 24 hours.

Memories get fuzzy quickly. People should make notes, or they will forget details. Your goal is to see what did and did not work. Even if the debrief is only at the executive level, accept feedback from everybody because they may have experienced the situation from a different perspective as the executive or may have caught something the executive missed. Then the crisis team should put together a debrief or memo. You want to document it. Make changes based on the "lessons learned." Then practice again.

❖

Ryan Schonfeld is president of RAS Consulting & Investigations, a security consulting and private investigations firm based in Hermosa Beach, Calif. Schonfeld has a background in global security, IT, and law enforcement. He works with companies of all sizes on their security master plan, security technology, workplace violence, prevention programs, and investigations.

Eden Gillott Bowe is president of Gillott Communications, a crisis and reputation management firm, based in Santa Monica, Calif. She frequently appears in publications such as the Los Angeles Times, Wall Street Journal, NPR, the Washington Post, and Forbes. She is a former business professor and author of "A Lawyer's Guide to Crisis PR" and "A Board Member's Guide to Crisis PR."