Guidepost

SHIELDING YOUR WORKFORCE: STRATEGIES FOR SAFEGUARDING EMPLOYEES DURING MASS LAYOFFS AND HIGH-PROFILE TERMINATIONS

The recent wave of mass layoffs has created an uptick in protests and demonstrations by those affected. In some cases, pay and benefit cuts in lieu of layoffs have also resulted in significant repercussions, as evident by the 700-day Warrior Met Coal strike in Alabama. Unfortunately, some have led to violence or even death, as with the five killed during the 2019 shooting at the Henry Pratt Company in Aurora, Illinois.

The impact on safety:

Bloomberg editor, Sarah Green Carmichael, explains, "At the root of the challenge is that employees interpret layoffs to be what scholars call a 'psychological contract violation', which gives rise to resentment and fear." The *NY Post* reported that disgraced former CNN anchor Chris Cuomo said he, "was so distraught after being 's-t-canned' by CNN that he was 'going to kill everybody and myself.'"

With the rise of doxing, the ease of internet searches to find an HR employee or c-suite executive's home address, as well as personal details about their family, the threat of receiving a disgruntled employee or other threat at their home has become a great concern.

And it's not just physical threats facing employers, but cyber threats too. According to research by Carnegie Mellon's Software Engineering Institute, disgruntled employees have been responsible for sabotage including data deletion, blocking system access, and copying data. "In one case, the insider, who had full access to the company's network and systems, had a falling out with his employer and was terminated. On the day of the insider's termination, he began to remotely attack the organization for four months. The insider deleted crucial files on servers, removed critical backup disks, and deleted numerous records from an important database used by other systems. The insider was able to

attack the organization in such a manner because his credentials were still enabled."

What you need to know:

Most commonly, we see clients who address these personnel matters reactively – either after a disruptive termination that resulted in threats from the former employee, or when someone requests "security" to be present for a high-profile termination on very short notice, or when large groups of employees are dismissed at the same time. In these instances, we always recommend having the security provider present in the room for the termination. While some clients have expressed concern that having "security" present will tip off an employee or it will harm the image they want to present, we believe the benefits of having protection present far outweigh the concerns.

In one recent example, an employer laid off a mid-level manager at a factory in China but did not permit security in the room. The employee grabbed a pair of scissors and held the HR representative hostage while the other employees fled the building. The matter was ultimately resolved peacefully with the assistance of local police, but may have been avoided entirely if security was physically present.

In addition to having security present during the termination, we also recommend having security on-site, for the remainder of the day, until the office closes or the last employee leaves, whichever comes later. We also recommend maintaining a security presence for a day or two afterward to guard against instances where the terminated employee decides to return to the office to harass or threaten his former colleagues, commit vandalism, or damage company property. In jurisdictions where audio and video recording are permissible, security personnel with body worn cameras prove to be a great asset to any claims against the employer made by the former employee.

In instances where employee safety is a concern, it is important to separate rumor from fact. One client came to us with a fear that their US-based Russian employee would become violent after receiving negative feedback in a performance appraisal which coincided with the beginning of the Russian-Ukrainian war. Some of his colleagues had reported concerns about his online social media where he referred to himself as a "mercenary" and was making posts in Russian about the war. Our native Russian-speaking team member reviewed his online profile, determining that this first-generation immigrant was using the term "mercenary" in an archaic sense to refer to taking side jobs for payment, which was understandable given his employment in a gig-based industry. Further, his online posts revealed a high degree of anti-Russian sentiment, and several of his favorite authors were anti-Soviet individuals who advocated for peace.

Take note:

- At a minimum, conduct a social media assessment and updated litigation search for terminations that involve senior leaders or other high-profile employees to determine the employee's current state of mind. An employee in the middle of a divorce, filing for bankruptcy, or dealing with an eviction may be more unpredictable in their behavior.
- Put some thought into the time and location of terminations. If an employee is remote, can or should they be brought into the office to acquire company property? Is termination on a Monday or Friday preferable? If an

employee is a shift-worker, should the termination occur during their regularly scheduled working hours?

- Ensure that terminated employees are immediately escorted off the premises. Do not allow them access to other areas of the building or to company equipment. Consider the use of a plain clothes security consultant with de-escalation training to be present during the termination and escort the employee. If this is not feasible, have security personnel monitoring the termination via real time CCTV and in proximity to act if necessary.
- Based on the employee's behavior after the termination, have a plan to implement social media monitoring, surveillance, and/or security personnel present at the workplace for several days. Specific threats against HR reps, executives, or colleagues should be taken seriously, to include personal protection to the threatened employees and coordination with local law enforcement. In extreme cases, if an employee has been arrested, a company may need to monitor the subject's court hearing schedule to know when the subject is being released from incarceration and adjust their security posture appropriately.

Bottom line:

Whether you are considering a proactive or reactive approach to employee/executive safety, consult a security provider with experience in addressing multiple facets of employee risk. Companies with an international presence should also consider providers who are well connected with local law enforcement agencies that can coordinate responses ahead of time to facilitate the safety of all involved.

CODY SHULTZ PCI, CCI

Director, Investigations + Private Client Protection

Cody Shultz serves as a director of investigations and private client protection for Guidepost Solutions and is based in the D.C. office. Having served with the Central Intelligence Agency, he is now sought out as an expert on reputation and identity management for ultra-high net worth clients and family offices. He holds a Professional Certified Investigator certification through ASIS International and is a Certified Cryptocurrency Investigator.

JUSTIN REID DBA

Security Consultant, Protective Services

Over the course of his career, Dr. Justin Reid has gained extensive experience working within the Department of Homeland Security (DHS) and the corporate security industry overseeing global protective operations, investigations, surveillance, hostile terminations, union strikes and cross border disaster response. He works closely with *Fortune* 500 CSOs and security directors to assess risks and deliver specialized solutions that mitigate

enterprise security threats.