ONTIC

Checklist

Mass Layoffs: Getting Prepared and Dealing with the Aftermath

BROUGHT TO YOU BY THE CENTER FOR PROTECTIVE INTELLIGENCE

Mass layoffs have swept across American businesses this year – and as interest rates and inflation continue to rise it's likely more businesses will be following suit to trim back costs.

Corporate security teams play a crucial role in both preparing for and dealing with the aftermath of mass layoffs. But, so do teams like HR, cybersecurity and legal. In fact, according to Ontic's State of Protective Intelligence Report, 91% of respondents agreed that at their company, physical security, legal and HR are trained to address situations should the firing or furloughing of an employee turn violent. But, 87% agree their company does not have a process or tools to alert the same departments or staff if, after they have been furloughed or fired, former employees who have exhibited violent tendencies return to the premises.

While protecting your business during these difficult times may seem like an uphill struggle, having a proactive security protocol in place, as well as a plan for any risks that may come afterward, can offset a lot of 'unforeseen' damages resulting from a mass layoff. It's also important to note that we are dealing with people that have given their hearts and souls to a company that unfortunately now must let them go. This means that although we need to plan for the worst, we should not create an adversarial posture, and do what we can to protect the employees' dignity, as well as their privacy.

Here's a checklist of criteria to assess your level of preparedness as you approach a mass layoff as well as what to do after. Keep in mind that these steps are not the end all be all and you'll likely need to adjust the approach based on your organization's individual circumstances.

STEP 1	PRE-CONVERSATION EVALUATION
□	Assess how the employees who are being impacted, as well as those who are not, are likely to react based on the circumstances, and solicit input from their managers, human resources (HR), legal and campus security.
□	Evaluate an appropriate severance package for those affected by the layoff or recommend an employee assistance program.
□	Evaluate the best environment for the conversation to take place. If there are concerns about past aggressive action or violence, consideration should be given to terminating the group of employees remotely. It is important to handle the situation with absolute discretion. Just like with the threat assessment management process, an improper approach can inadvertently cause a triggering event.
□	Consider the best day and time to conduct the terminations. The most common approach is Friday at the end of the workday, as this minimizes attention and does not interrupt the employee's typical schedule.
□	Work closely with your legal and compliance teams to ensure the layoff is in compliance with the federal Worker Adjustment and Retraining Notification (WARN) Act which requires employers conducting a large-scale layoff to provide 60 days' notice to affected employees.
□	Engage with your HR team on messaging to ensure nothing communicated during the layoff conversation results in increased hostility from employees.

STEP 2 SUPPORTING PERSONNEL AND EMPLOYEE HARDWARE

□ Evaluate who from the Executive Leadership Team (ELT) is best suited to share the news with the group. Be sure that on-site security and the executive protection team are in the loop to ensure they are monitoring for any increase in threats against the executive once the news is shared.

□ Identify who else should be present at the time of the termination besides the ELT member who is sharing the news.

□ Evaluate whether security needs to be present and where they will be during the conversation (e.g. in the room, nearby hallway, or parking lot). An overbearing security presence may make the employee feel offended, and possibly create a hostile termination. If conducting the layoff remotely, ensure you have heightened security at your offices if you believe there are indicators that an impacted employee may come to the office and pose a threat.

□ Deactivate all of the employees' electronic access to work accounts and request they return their company equipment. IT access should be shut off simultaneous to the layoff notification. Doing this too far in advance will likely "tip off" the employees and can create false rumors and disrupt the work environment.

STEP 3 TERMINATION CONVERSATION AND ACTION

□ Determine who will accompany the employees to their workstations to get their personal belongings and company property they need to return (e.g. manager, security, or law enforcement). You may want to consider returning their personal belongings and/or having them return their property by mail to keep the employees away from the premises.

□ Provide HR contact information should employees have any questions or requests post-termination and ensure that you have a system in place for your HR team to report any threats they receive to the security team. Keep in mind that threats are not always direct and may come in the form of veiled comments. For this reason, it is important to notify your threat assessment team of any concerning interactions.

STEP 4 ONGOING ASSESSMENT

□ Regroup to discuss the events, what can improve in future terminations from a security standpoint, and what next steps are necessary.

□ Consider what resources are in place for continuous monitoring of former employees that pose a legitimate threat, and communicate employee information to relevant security teams.

□ Conduct a formal threat assessment on any employee when it is determined necessary to do so. (e.g. How does their behavior compare to the Pathway to Violence?)

□ Establish a technology-supported process to assess potentially violent former employees and their mental state over time (e.g. online behavior, financial difficulties, family difficulties, etc.)

□ Utilize a technology solution to collect, store, and manage threat data through the entire threat lifecycle.