How to Effectively Mitigate Employee Risk

How to Effectively Mitigate Employee Risk: A Three-Part Series

Every company, across every industry, is vulnerable to insider risk. A human workforce, coupled with internal or external coercion as well as errors in judgment, puts any company unprepared for the worst-case scenario at significant risk.

Over the past few years, issues of employee risk have come to the forefront of the national conversation. Bad actors at any level of a company's hierarchy are dangerous, and most businesses have been largely unsuccessful at intervening before small issues turn into major public spectacles.

Many companies have some version of a risk mitigation plan in place, but for those that don't, or for companies that only have parts of this strategy fleshed out, it's worth the time and money to invest in protecting against any possible problems. The most effective way to do so is through a fully compliant and comprehensive risk mitigation plan, which can be broken down into eight parts.

Part One: Pre-Hire

These first few steps to create a pre-hire strategy must be individualized, in relation to a company's industry and risk metrics, and standardized to avoid bias and develop a clear and consistent way to handle future problems. Even if a business already has a basic plan in place, going through current policies with a critical eye may illuminate ways to strengthen them, and if these pieces are missing from the company's basic framework, this is a great place to start building a solid plan for employee risk mitigation.

1. Develop a background check policy

This first step is one that many businesses have already begun implementing, as 96% of companies conduct some kind of background check during the pre-employment process. However, these policies aren't always clear or consistent, and there are inconsistencies in which employees are covered by the policy and what companies are screening for. In addition, it's less common for employers to run background checks post-employment, but for any arrests or other relevant incidents, it's necessary to have a system in place for identifying any problems as they occur.

ClearForce has found that criminal events increase 2x amongst employees who have been with the company for over 3.5 years. At the same time, industries such as industrial manufacturing and utilities have an extended average employee tenure of over ten years, significantly increasing the chance that an issue will arise from an established employee. But with less than 25% of companies proactively reviewing current employees for risk, these problems go unnoticed, often until it is too late to intervene. For these reasons, establishing a background check policy that goes beyond a routine pre-hire screening is a necessary first step in creating an employee risk mitigation plan.

2. Develop a criminal actions policy

One of the greatest challenges companies face is deciding what to do when an employee is flagged for an arrest. At-will employees can be fired at any time for many reasons, and EEOC guidelines allow employers to terminate an employee based on the conduct underlying an arrest. However, this can be viewed as discrimination and could result in legal complications down the line.

Instead, it's advisable for companies to develop a tiered approach to address any criminal activity, instead of waiting to figure it out when they encounter an issue. These tiers can be broken down into four categories, from most serious to least: violent crime; nonviolent serious crime, such as burglary, theft, fraud, and felonies; crimes that require further investigation based on industry needs, such as a DUI charge; and low-level crimes that do not require further investigation, such as trespassing or reckless driving.

It's also necessary to isolate who handles the decisions for each of these tiers. The most serious crimes, the first and second tiers, should be referred to inside or outside legal counsel, while the third tier could be handled by a company's security team and the lowest tier would be referred to HR for notification and archival in an employee's file. In most cases, the highest tiers will require some sort of adverse action, likely termination, and having this tiered policy in place helps make the process consistent, standardized, and impartial for all employees.

3. Get a quality pre-hire background check

After laying the groundwork with a consistent background check policy and evergreen employee consent, the next step is to ensure that you're paying for a quality pre-hire background check. The concept of getting what you pay for has significant implications when it comes to background checks, and the varying levels of security can be understood as a comparison between an HR check and a security check.

A minimal HR check that searches through the National Criminal Locator Database Search (NATCRIM) can be performed for around $15. However, this kind of check is hit or miss and is unlikely to pull up any major red flags. For a security check, the budget range is closer to $50 per employee, but that includes a county search in the place of the business location and or home residence and, in some cases, prior residence. A security check will also likely include a Social Security Number screen, an alias screen, and oftentimes sex offender registries and criminal watch lists.

Depending on the industry and job, it's also worth checking on an employee's licenses, education, and references. Regardless of your company or industry, running a pre-hire background check shouldn't be a check-the-box exercise, and deciding on what level of background check to run requires forethought into the risk level for your industry and company.

Part Two: Post-Employment

After establishing a strong pre-hire strategy to mitigate employee risk, companies should turn their attention to what happens post-employment. Running a strong background check on each employee prior to onboarding them is a good starting point and will provide a baseline for understanding the level of risk each employee represents. However, it must be stressed that a background check only captures information that is accurate up until that point in time, and building an employee risk mitigation plan on that alone is woefully inadequate.

The next steps towards successfully mitigating people-based risk should occur post-employment and be integrated into the framework of a company's daily operations.

4. Implement - and explain - an employee self-reporting policy

Encouraging employees to self-report should be an obvious way to mitigate risk, but it is much less common than it should be, particularly in regulated industries. Some industries already enforce some version of this policy, such as the requirement for FINRA agents to make a self-attestation that they are in compliance, but it should be commonplace for every company. Having solid and consistent self-reporting policy matters because it is a highly effective risk practice, reduces liability for an organization in enforcing its policies and risk programs, and serves as a form of deterrence for employees against committing crimes in the future.

5. Provide employees with a portal for self-reporting and peer reporting

Once you've locked in a solid policy for self-reporting, it's necessary to provide employees with the tools to adhere to the policy. Providing tools to ensure that the process is simple, intuitive, and efficient will make it far more likely that employees will be compliant with the policy and report any criminal activity immediately. It's also helpful to layout categories of risk, so employees understand what to be on the lookout for. The problems they may already be aware of might fall into the category of physical risks, such as violence in the workplace, but there are other risks, such as information risk, intellectual property disclosure, and cybercrime, that should also be red-flagged and reported. The goal is to equip a reporting tool with as many mechanisms as possible to make it easy for people to report and increase their awareness of the risks.

6. Utilize continuous monitoring to screen for red flags

Even with a self-reporting and peer reporting policy and process in place, those who commit crimes are unlikely to report them, and companies need a more foolproof way to screen for any warning signs. Continuous criminal monitoring is akin to insurance for any effective risk mitigation plan, as it picks up problems regardless of employee adherence to these policies.

If the need to take adverse action against an employee arises, from a legal perspective, now there are two protections against any future problems: the self-reporting policy, which they have violated by failing to report a crime, and the arrest information, which can be used to figure out whether the issue can be investigated internally or requires other action. Some companies may choose not to do anything with arrest alerts out of fear of legal repercussions and only act if a conviction follows the arrest. But by having continuous monitoring in place, employers are alerted the moment a problem begins and have the opportunity to intervene, if possible, and take proactive steps to protect themselves and their workforce.

Part Three: Employee Engagement

Having a pre-hire and post-employment plan in place is the foundation of a strong employee risk mitigation strategy, but it will never be effective without employee buy-in and cooperation. These last few steps are the key to ensuring that the framework that has been created is implemented effectively and will also protect a company against legal issues that could arise in the future. Proactive action here is imperative and could mean the difference between catching a problem early enough to intervene and taking more severe steps to address it after the fact.

7. Notify employees with an evergreen consent form

To remain FCRA compliant, it's necessary for every organization running a pre-employment background check to obtain employee consent. But having employees sign a one-time consent to run a background check before onboarding is limited in its scope, compared to an evergreen consent form. An evergreen consent form gives employers the ability to run subsequent checks on similar material, and it's easiest to obtain this consent during the onboarding process for new employees. There is also an opportunity to get consent from existing employees, but it requires putting it in front of them to explain what they're signing and capture their express consent.

8. Remind employees annually about their consent for risk mitigation policies

Having employees sign an evergreen consent form gives an employer indefinite permission to run background screening and continuous monitoring, but it doesn't remove every possible legal problem. If an employee signs a consent form and there's an issue five or ten years later, it becomes more challenging from a court perspective the longer it's been since the consent was given. Instituting a practice of annual or semi-annual consent reminders or self-certification forms eliminates this issue by reminding employees that the program is still in place and operational. This is a best practice for smoothing the process when a problem arises and makes it more difficult for employees to claim they were unaware of these policies.

9. Communicate the why behind the program

After putting all of the preceding pieces in place, employers will have a strong employee risk mitigation strategy, but there is one final element necessary to make it successful. These policies are necessary to protect against people-based risk, but they won't be nearly as effective if employers can't communicate why they are necessary and secure employee engagement. The bottom line is that companies are investing in risk mitigation strategies to protect their business and employees from bad outcomes, and explaining these motives for what otherwise could be viewed as intrusive policies will help employees recognize that their participation is a crucial part of keeping them and their coworkers safe.

Organizations that implement this approach will have a best-in-class people risk management program.