QBE Insurance

Employee Crime: The insider threat of theft and fraud

An evolving internal risk

Employee crime can cause profound financial loss, reputational damage, and diminished stakeholder trust. To better understand how organizations are managing this risk, we gathered insights from a recent survey of 200 U.S. risk managers at companies with a minimum of $500 million in annual revenue. The findings offer insights into the prevalence of employee crime, the concern prevention efforts are insufficient and how companies are enhancing risk mitigation efforts.

In the past 12 months, 80% of risk managers surveyed said their organizations experienced employee crime such as theft, fraud, and embezzlement. Over the past three years, respondents report that the most common type of employee crime at their organizations was billing fraud (36%), followed by payment and check fraud (23%), payroll fraud (19%), cash theft (13%), and non-cash theft (10%). Billing fraud schemes can involve creating fictitious invoices or manipulating existing ones for personal gain. Payroll fraud often includes complex methods like creating "ghost employees," where a nonexistent worker is added to the payroll system, or inflating expense reports with personal purchases.

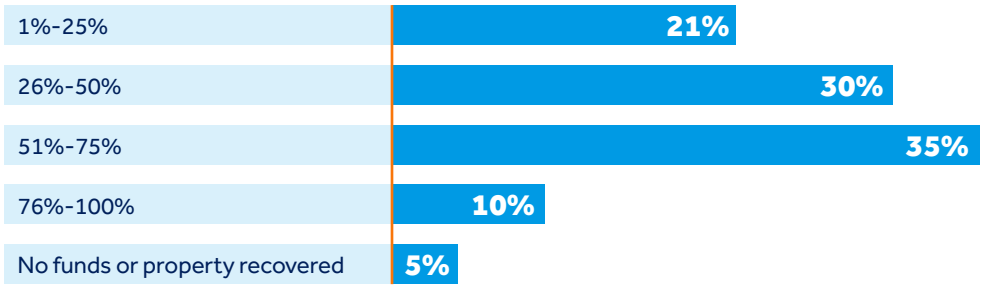
80% of risk managers at companies with $500 million or more in annual revenue say their organizations experienced employee crime in the past 12 months.

The prevalence of specific fraud types is compounded by the fact that internal crimes are often not solitary acts. Nearly 4 in 10 risk managers (37%) indicate the employee crimes at their organizations "frequently" involve more than one employee, while others say it happens "occasionally" (46%) or "rarely" (18%).

The vast majority of organizations (88%) notify law enforcement following the discovery of employee crimes. Those surveyed typically only recover a portion of stolen funds or property, excluding insurance claim payments. For example, 35% of respondents indicated that their organizations recovered 51% to 75% of the stolen funds or property, while 30% recovered 26% to 50%.

More than three-quarters of respondents (78%) indicate the most recent incident was perpetrated by an employee at the manager level or higher. These individuals are often in positions of trust with greater access to company assets. This highlights a significant insider vulnerability that demands attention and robust risk management.

Percentage of stolen funds or property typically recovered through recovery efforts
*(excluding insurance claim payments)**

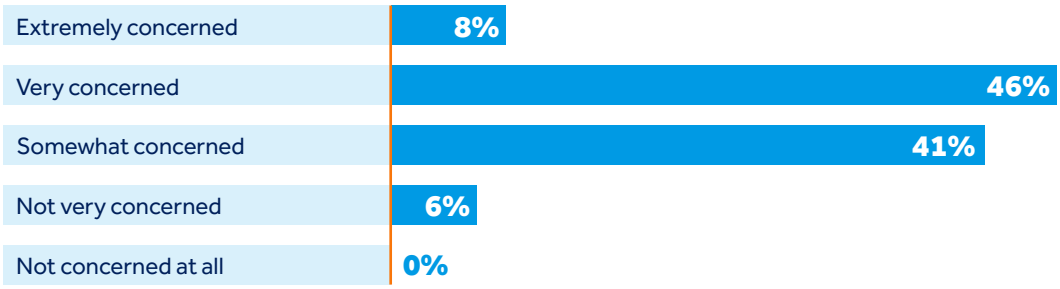


** Totals may not equal 100% due to rounding*

While traditional fraud schemes are currently the most common types of employee crime, an emerging and rapidly escalating threat has captured the attention of risk managers: the potential misuse of artificial intelligence (AI) by internal actors. The very tools designed to enhance productivity may also have the potential of being leveraged by fraudsters for more sophisticated attacks.

Most risk managers (94%) are concerned about employees using AI to perpetrate workplace crimes within their organizations. In response, organizations are taking proactive steps: 45% are already using AI-based systems to detect and prevent employee crimes, and another 50% plan to implement them in the next 12 months.

Level of concern that employees will use AI to perpetrate workplace crimes*



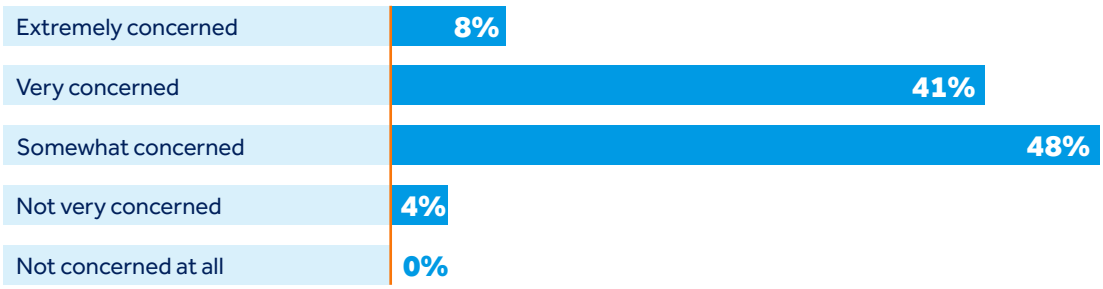
** Totals may not equal 100% due to rounding*

Efficacy and gaps in internal controls

Given the financial and reputational impacts of employee crime, effective prevention is imperative. While risks evolve, the cornerstone of defense remains robust internal controls and proactive risk management frameworks. These systems are essential primary lines of defense against insider threats. However, simply having these controls in place does not guarantee confidence in their effectiveness.

The data supports this, revealing that a significant confidence gap persists in the efficacy of existing internal controls in combating employee crime. Nearly half of risk managers are "very concerned" (41%) or "extremely concerned" (8%) about their sufficiency to prevent and detect employee crimes.

Level of concern that internal controls are not sufficient to prevent and detect employee crimes*



** Totals may not equal 100% due to rounding*

This concern comes even after more than 9 in 10 organizations (92%) addressed weaknesses or gaps in their internal controls within the past 12 months. Most organizations were proactive, realizing gaps prior to a crime being committed (60%). However, a significant third (33%) reacted only after a crime had occurred.

In the past 12 months, **33% of organizations** addressed weaknesses or gaps in their internal control systems only after an employee crime occurred.

Foundational controls and reducing exposure

Organizations employ various methods to prevent or reduce the risk of employee crime, with automated monitoring tools (55%) and employee training (54%) as the most frequent approaches, closely followed by internal audits (50%). Leadership's clear commitment to fostering an ethical corporate culture is a foundational deterrent, alongside the use of anonymous reporting systems.

The backbone of a strong defense, however, lies in fundamental internal controls, primarily the segregation of duties. Many organizations (82%) prevent any single employee from having sole control over a complete financial transaction (e.g., submitting an invoice and approving payment). Routine oversight extends to third-party relationships as well, with 53% of organizations reviewing their authorized vendor list annually and another 46% reviewing it every two to three years.

There are numerous internal controls that organizations can consider if they are not already in place. These may include screening prospective employees and vetting potential vendors. Companies should also establish a formal process to monitor and verify changes to the payroll system for new and existing employees. Ensuring that employees can only access files that are necessary to do their work is a basic yet effective way to deter misconduct. In addition, having an independent accounting firm conduct an annual audit can further strengthen oversight.

Crime insurance as a strategic risk management tool

While internal controls remain vital for prevention and detection, organizations strategically transfer some of the residual risk to build a critical layer of financial protection. Crime insurance, also known as fidelity insurance, is a key strategic tool and a specialized product designed to cover financial losses resulting from criminal acts, including employee dishonesty, forgery, computer fraud, and theft. Its value lies in providing a strong financial safety net, ensuring an organization can weather a significant internal breach without facing catastrophic financial instability.

Given the evolving risk landscape, where AI-powered threats and economic pressures are intensifying, this strategic protection has become even more critical. Consequently, 87% of risk managers report that their organizations carry crime insurance coverage as part of their strategy. Reflecting the heightened awareness of these growing risks, close to two-thirds (63%) of these organizations plan to increase their coverage limits in the next 12 months, while 32% are not planning to change limits and 5% are decreasing limits.

63% of organizations with crime insurance plan to increase coverage limits in the next 12 months.

Opportunities for improvement

Despite widespread proactive management, significant improvement opportunities remain in mitigating employee crime risks. The persistent confidence gap, where risk managers are concerned about the sufficiency of existing controls, indicates a need for continuous assessment and refinement rather than one-time implementation. Furthermore, the fact that a third of organizations act reactively following a criminal incident, highlights a gap in ongoing monitoring practices that thorough internal audits and risk assessments could fill.

The data paints a clear and compelling picture: employee crime is a prevalent and evolving risk that demands proactive and continuous management. The high incidence of crime perpetrated by employees at the manager level and above highlights the critical need for robust controls that transcend traditional hierarchy and hold all individuals and departments accountable. Furthermore, the adoption of artificial intelligence for detection signals a shift in how organizations are preparing for the future landscape of employee fraud. By combining vigilant internal controls, fostering a strong ethical culture, and ensuring appropriate financial protection through comprehensive crime insurance, companies can build a truly resilient defense against these persistent threats, thereby ensuring greater security and trust within the workplace.

Survey Methodology

The survey was conducted by Wakefield Research among 200 U.S. risk managers at companies with a minimum of $500 million in annual revenue, between January 5, and January 15, 2026, using an email invitation and an online survey. All respondents have knowledge of employee crimes (e.g., theft, fraud, embezzlement, etc.) perpetrated at their organizations within the past three years.

About QBE North America

QBE North America is a global insurance leader that gets to the heart of what's at risk for customers. Part of QBE Insurance Group Limited, QBE North America reported Gross Written Premiums in 2025 of $7.7 billion. QBE Insurance Group's results can be found at qbe.com. Headquartered in Sydney, Australia, QBE operates out of 26 countries around the globe, with a presence in every key insurance market. The North America division, headquartered in New York, conducts business primarily through its insurance company subsidiaries. The actual terms and conditions of any insurance coverage are subject to the language of the policies as issued. Additional information can be found at qbe.com/us or follow QBE North America on LinkedIn, Facebook and Instagram.

To learn more about QBE's Crime Insurance coverage, visit Management Liability | QBE US.

QBE Insurance