Gallagher

Corporate Crime and Risk Report

The enterprise risk implications of AI-enabled fraud



Crimes committed against businesses are becoming a board-level resilience issue as AI accelerates deception, fraudsters exploit trust, and financial losses spill across cyber, commercial crime, and executive liability policies.

According to the Gallagher 2026 Corporate Crime and Risk Survey, 75% of senior decision-makers reported having been targeted by at least one form of corporate crime in the past year, and 88% of affected organizations incurred financial losses.

As AI makes deception cheaper, faster and more convincing, these incidents are becoming an enterprise-level risk for organizations and their senior managers.

Key insights

Corporate crime is evident:
75% of senior decision-makers reported that their organizations were targeted by at least one form of corporate or enterprise crime (commercial crime) in the past year, and 88% of those affected incurred financial losses.

AI is amplifying deception:
Six in ten respondents noted an increase in AI-generated content in the attempted crimes their organizations faced over the same period, and more than half found those attempts more sophisticated than traditional schemes.

There is a protection gap:
Although 81% of respondents said they had relevant coverage in place, insurance covered only an estimated 50% of commercial crime losses among insured organizations that experienced financial losses.

Three in four organizations faced corporate crime in the past year

24%
experienced no commercial crime in the past year

33%
experienced between one to two attempts or incidents in the past year

42%
experienced three or more attempts or incidents in the past year

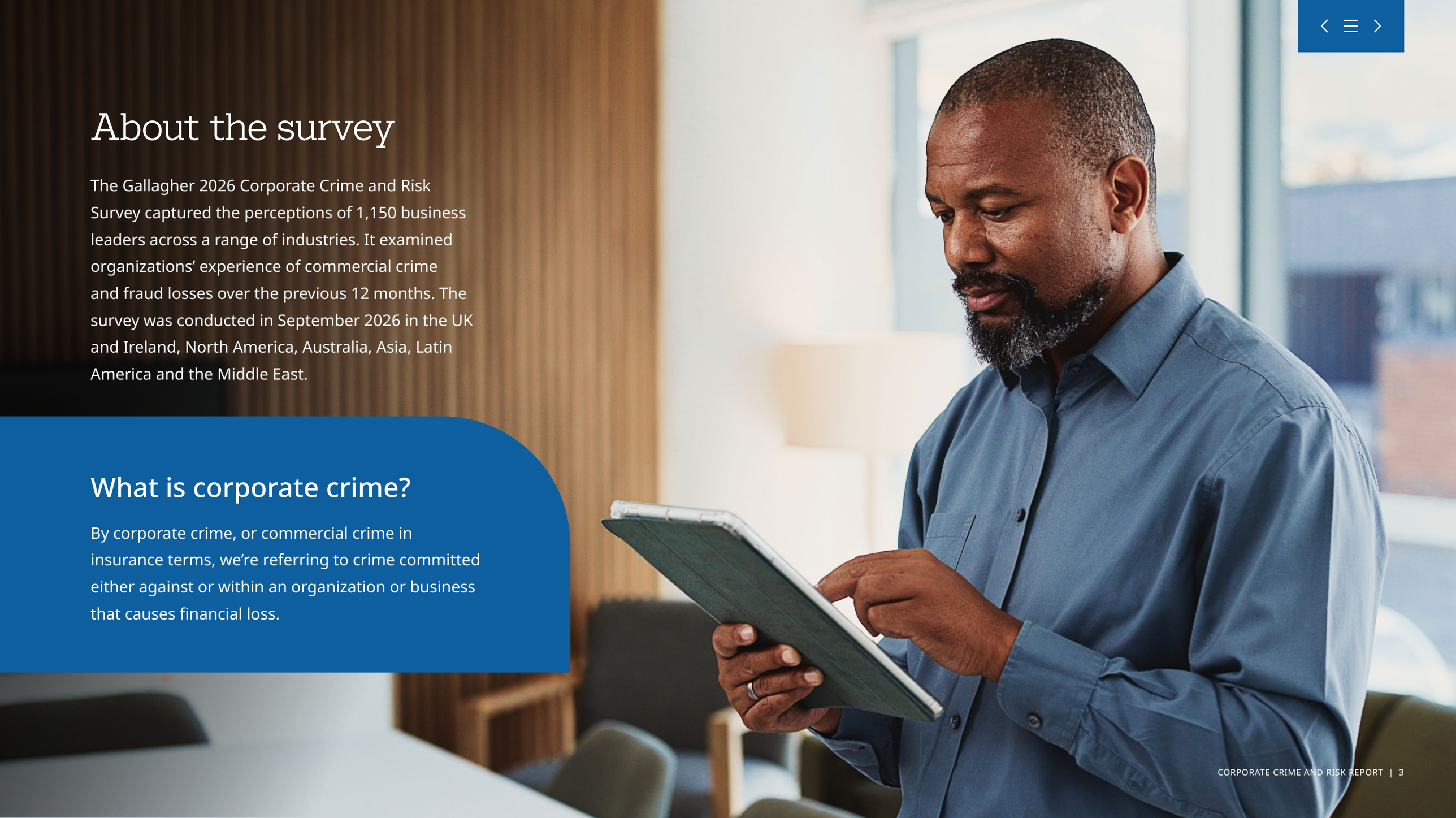
Source: 2026 Corporate Crime and Risk Survey, Gallagher

About the survey

The Gallagher 2026 Corporate Crime and Risk Survey captured the perceptions of 1,150 business leaders across a range of industries. It examined organizations' experience of commercial crime and fraud losses over the previous 12 months. The survey was conducted in September 2026 in the UK and Ireland, North America, Australia, Asia, Latin America and the Middle East.

What is corporate crime?

By corporate crime, or commercial crime in insurance terms, we're referring to crime committed either against or within an organization or business that causes financial loss.



How technology is fueling the crime and fraud threat landscape

Corporate crime attempts are becoming more sophisticated, tech-enabled and frequent. Six in ten respondents reported an increase in the use of AI-generated content in attempts over the past 12 months. And more than half reported increases in sophistication (56%) and frequency (51%).

Recent data from different markets illustrates the growing role of AI in fraud and cybercrime. In the US, FBI data shows that the Internet Crime Complaint Center received more than 22,000 AI-related complaints in 2025, associated with approximately USD893 million in losses.[1]

Across England, Wales and Northern Ireland, meanwhile, the City of London Police's Fraud Annual Assessment 2025-26 reported a 395% year-over-year increase in reports of cybercrime involving the suspected use of AI.[2]

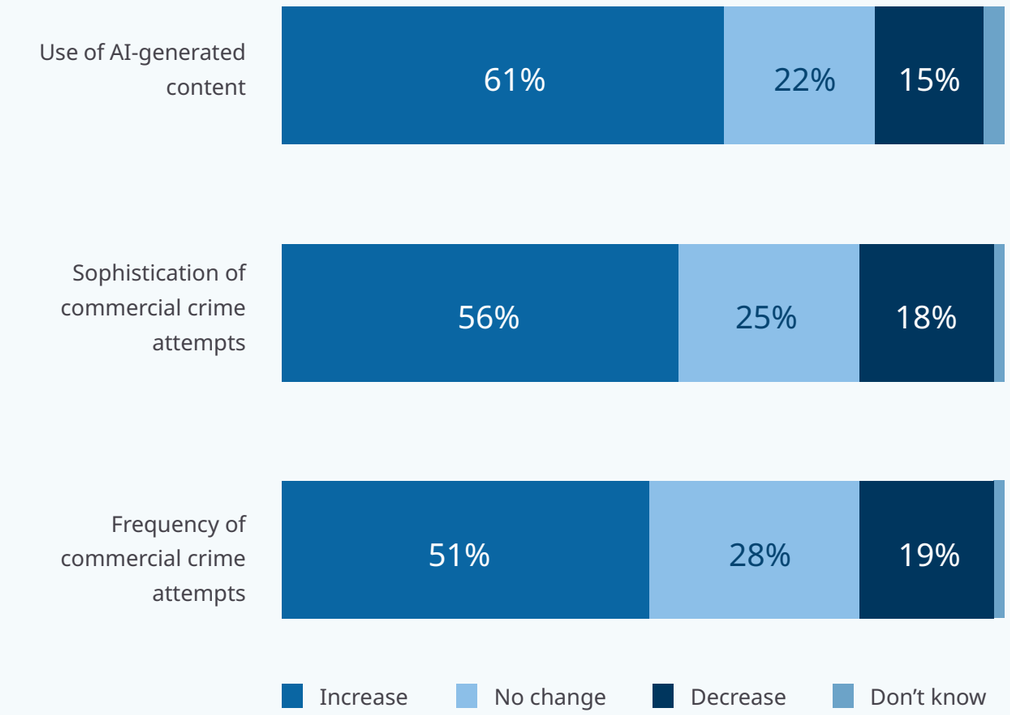
AI does not create the underlying fraud motive; it changes the economics of deception by increasing the speed, scale, personalization and credibility of established schemes at a fraction of the previous cost and effort.

> "AI collapses the cost of producing deception. If the internet gave people the ability to do mass deception, AI gives them the ability to do mass personalization."

J.D. Crouch
Managing Director and Specialist in Embassy and Diplomatic Mission Risk Solutions, Gallagher

Corporate crime attempts are becoming more sophisticated and AI-enabled

Percentage of respondents reporting changes in commercial crime attempts over the past 12 months



Base: All respondents, n=1,150

Source: 2026 Corporate Crime and Risk Survey, Gallagher

> “On one hand, we’re dealing with highly technology-driven fraud, and on the other, we’re still seeing very traditional methods. When check fraud started resurfacing around 18 months ago, it even caught the underwriting community off guard, as you’d expect people to be moving away from paper-based transactions like writing checks.”

Eileen Yuen
Managing Director, Financial Institutions Practice, Gallagher

AI is scaling business fraud by amplifying phishing, malware and business email compromise. Just over a quarter (27%) of survey respondents identified AI-generated phishing emails as the most common tech-enabled attack, followed by fake websites and portals (22%), and AI-assisted malware (21%).

Attackers can use public information to replicate an organization’s tone, use AI to remove familiar warning signs such as poor grammar and produce credible messages at scale.

The technology can also be used to doctor the surrounding paper trail of such scams, making fabricated requests harder to distinguish from genuine communications. “Every company has to be aware that the people perpetrating fraud or crime now have better resources and are now able to take a more sophisticated approach,” says Charlie Lamberta, EVP, Claims Operations — Liability, Gallagher Bassett.

At the same time, more traditional forms of corporate crime — such as check fraud, vendor fraud and the physical theft of goods — remain a significant challenge for many businesses.



Depending on their motivation, criminals may seek to steal money or high-value goods and materials. Others, in cases of industrial espionage, target confidential business information.

Pressure, opportunity and rationalization are the three factors that influence whether a person will be motivated to commit fraud, with white-collar theft too often considered a "victimless crime."

The risk extends beyond an organization's four walls through to its supply chain. A business may have solid internal procedures and still receive a fraudulent wire transfer request or forged bill of lading from a compromised third-party vendor.

With money, high-value assets, data and trade secrets all at risk, and the means to defraud steadily being amplified by technology, the pressure is on to build and maintain robust security and risk management frameworks.

Organizations face traditional and modern crimes at the same time

Percentage of respondents selecting each type of commercial crime experienced in the past 12 months



Base: All respondents, n=1,150

Source: 2026 Corporate Crime and Risk Survey, Gallagher

"AI allows criminals to enhance deceptive actions. They can use these tools to generate fraudulent documentation or invoices, or fictitious vendor records to support their theft. It gives them more sophisticated technical skills to work with."

Cassandra Shivers
National Claims Advocacy Leader
Management Liability Policy & Cyber, Gallagher

AI in insurance claims fraud

AI is changing both sides of insurance fraud landscape. Criminals can use it to create or manipulate documents or photographs, making fraudulent claims harder to spot through manual review alone. According to Gallagher Bassett, one in two insurance carriers now experience AI-generated fraud.

Insurers, however, can use AI to fight back, scanning for inconsistencies and suspicious recurrent patterns.

Higher fraudulent payouts can increase claims costs and, ultimately, premiums. For business leaders, this makes fraud detection a financial and operational issue that depends on combining human expertise with technology that can analyze data at scale.

> “Many claims analysts are now armed with technology, whether AI-enabled or not, to spot patterns across multiple transactions. If five look the same and one looks different, it’s important to understand why. But the reverse can also be true: If five transactions look unusually similar, that may deserve attention too.”

Charlie Lamberta
EVP of Claims Operations — Liability, Gallagher Bassett



Insider fraud is a top exposure

While AI may enable new types of fraud, employee theft or dishonesty is reported as the most common crime (29%) in the past 12 months.

During periods of financial pressure, the incentives to commit commercial crimes may increase, while existing schemes can become harder to conceal as organizations face closer scrutiny and tighter financial constraints.

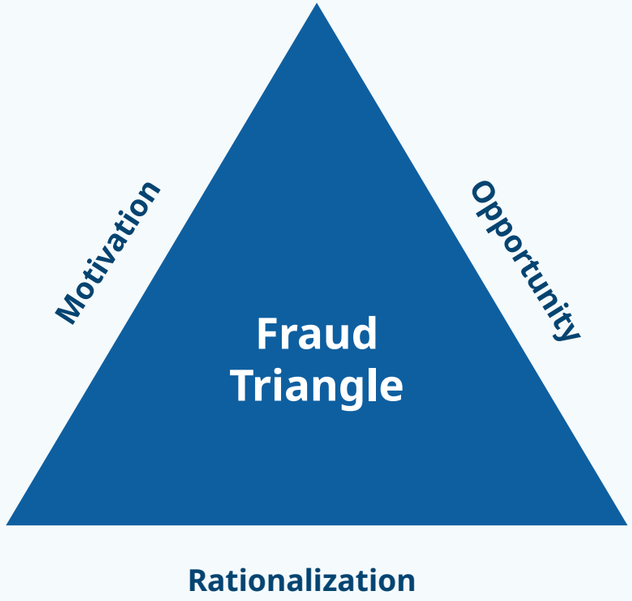
Physical goods become an attractive target as fraudsters turn to cargo theft

Through social engineering, criminals are not only diverting funds but also targeting physical inventory. By impersonating trusted vendors or business partners, they persuade employees to redirect inventory, raw materials and even product shipments.

These schemes rely on deception and can leverage compromised insiders. Attackers exploit trusted business processes within logistics networks and supply chains to gain control of valuable assets.

The trend is creating new insurance challenges. Historically, crime insurance focused on financial assets such as cash, funds and securities while property insurance dealt with accidental loss or damage.

As fraudulent diversion of physical goods becomes more commonplace, companies are challenged to upgrade their security posture to account for threats that are more digital in nature. There is growing demand for broader policy wordings and sublimits which encompass the evolving nature of the risk.



Fraud triangle

The driving factors behind a fraudulent act

The fraud triangle is a concept used in forensic accounting and fraud investigation to explain the factors contributing to criminal behavior. The term was coined by criminologist and sociologist Donald Cressey and consists of three elements: motivation, opportunity and rationalization.

Motivation

Motivation plays a crucial role in driving individuals to commit fraud. To identify motivations, antifraud professionals often look for financial incentives. When organizations or employees feel pressure to meet financial targets or beat their competitors, they may engage in dishonest activities.

Opportunity

Weak internal controls, lack of oversight or holding a position of trust within an organization can make it easier for fraudsters to cheat the system and get away with it. A lack of robust oversight enables wrongdoing. This is a common theme in many high-profile frauds.

Rationalization

Fraudsters often convince themselves that their dishonest actions were necessary and justifiable.

Source: The Next Wave of Workplace Fraud, Gallagher



The human layer and trust as the target

AI makes impersonation and social engineering attacks more convincing, but the central vulnerability is often not a technical flaw. Fraudsters exploit how organizations establish identity, confer authority and make decisions under pressure — turning trusted relationships and routine workflows into attack surfaces. “We have seen attackers manipulate employees into diverting funds, as well as redirecting inventory and product shipments,” says Miranda DesPain, Area Senior Vice President, Gallagher.

Urgency and apparent authority can compress thinking time and encourage people acting in good faith to bypass verification procedures. For example, an employee may be more inclined to authorize an urgent transfer if the instruction appears to come from a supervisor and is reinforced by a familiar voice, face or set of supporting documents.

In one example from May 2026, the Singapore government warned local businesses to be alert to a scheme involving impersonation of government officials after a victim was defrauded of approximately USD3.8 million.[3]

Building a “speak-up” culture in the workplace

There is no doubt that employee training remains an essential component of fraud prevention, but resilience depends on more than awareness. Organizations need employees who feel confident questioning unusual requests, challenging assumptions and raising concerns before a transaction is completed without fear of blame.

This places culture and governance at the center of fraud resilience. Creating a safe environment that fosters psychological safety and that feeds on ongoing communication can be just as important as developing formal training programs.

“Anytime employees start questioning, ‘Is this email from my boss real? Is this email from leadership legitimate? Is that voicemail truly from a colleague?’ — just having those doubts places a significant weight on employees and creates hesitation,” says Kathleen Schulz, Divisional Vice President, Global Innovation Leader, Organizational Wellbeing, Gallagher. “That hesitation is real, and it’s at this point that we start to see an impact on workplace culture.”

Leaders and managers play a critical role in maintaining a healthy work environment. As organizations introduce additional verification requirements and tighter controls, these should not undermine the trust they are trying to protect. Controls that create excessive friction or are poorly communicated can lead employees to feel scrutinized rather than supported.

According to our survey, 84% of leaders report having preventive risk-control frameworks in place. Security technology (49%), cyber risk management (47%) and employee training (43%) are common measures. In practice, ongoing training, such as simulated phishing exercises, helps staff better identify and escalate potential threats.

Employee awareness needs to keep pace with evolving fraud tactics. “Organizations need to understand what a deepfake is and the new ways that hackers are attacking,” says John Farley, Managing Director, Cyber Liability Practice, Gallagher, “and then equip their employees with the tools to recognize it and stop it, prevent it and mitigate it.”

Consistent accountability and visible consequences for misconduct also remain fundamental components of fraud prevention.

> “Creating an environment where people trust each other and have each other’s back takes a deliberate approach to workplace culture and communication. A clear, two-way communication strategy reduces stress and gives people the confidence to speak up if something raises a red flag. When you’re connected to your colleagues, you can recognize when something is wrong and intervene.”
>
> **Kathleen Schulz**
> **Divisional Vice President, Global Innovation Leader, Organizational Wellbeing, Gallagher**



Why corporate crime is a board-level resilience issue

When asked to select up to three of the most significant impacts commercial crime has had on their organization, a quarter of respondents chose direct financial losses, followed by investigation or response costs (22%), operational disruption (21%) and loss of customer or client trust (19%).

For boards, the exposure is twofold: Leaders can themselves be impersonated in more audacious crimes and they may later need to demonstrate that the organization had reasonable controls, clear accountability and a credible response plan.

Where losses are material, failures in oversight, disclosure or crisis handling may also lead to shareholder claims or D&O exposure.

Deepfakes move into the boardroom

Gallagher research among businesses in the UK and Ireland reflects growing concern about executive impersonation with deepfakes and voice cloning cited as respondents' leading concern.

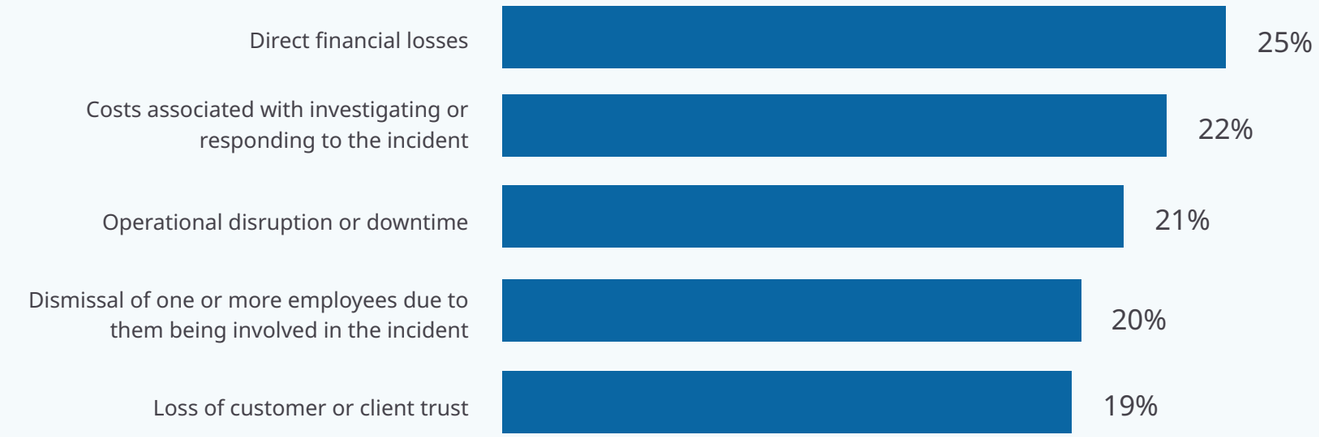
More than 50% of organizations reported at least one attempt to impersonate or deceive a senior executive.

Fraudsters can use information from company websites, LinkedIn, social media and executives' public appearances to make impersonation more convincing.

The financial consequences can be significant, with average incident costs exceeding USD600,000 according to the same research.

The costs of corporate crime extend well beyond direct financial losses.

Percentage of respondents selecting each impact among their three most significant impacts of commercial crime



Base: Respondents whose organizations experienced commercial crime in the past 12 months, n=861

Source: 2026 Corporate Crime and Risk Survey, Gallagher

> "While the immediate outcome of a breach might be financial, the reputational damage can be just as significant — if not more so. Rebuilding trust can take far longer than addressing the breach itself.

Lisanne Sison
Managing Director of Enterprise Risk Management, Gallagher



Regulatory expectations continue to rise

Under the UK's *Failure to Prevent Fraud offence*, effective from September 2025, large organizations may face criminal liability for fraud committed for their benefit unless they can demonstrate that reasonable prevention procedures were in place.[4]

According to Laura Parris, Executive Director, D&O, Gallagher, "Shareholders are likely to ask critical questions, such as what management knew, what actions the board took when challenged, how quickly the organization responded, and — most importantly — whether those decisions were properly documented."

A third of surveyed organizations detected their most recent fraud within 24 hours. The remaining took longer, including 25% that took more than a month. Such delays can make recovering funds significantly more difficult, particularly in wire transfers stemming from social engineering fraud, where money can move across accounts or digital wallets within minutes.

To reduce that delay, organizations need rehearsed escalation routes, rapid evidence preservation, coordination with banks, insurers and specialist investigators, and clear authority to act when an incident is suspected.

32%

detected their most recent fraud within 24 hours

25%

took more than one month

*Respondent base: 1,007; excludes those that selected "N/A does not apply to my organization"
Source: 2026 Corporate Crime and Risk Survey, Gallagher

Corporate crime calls for effective governance

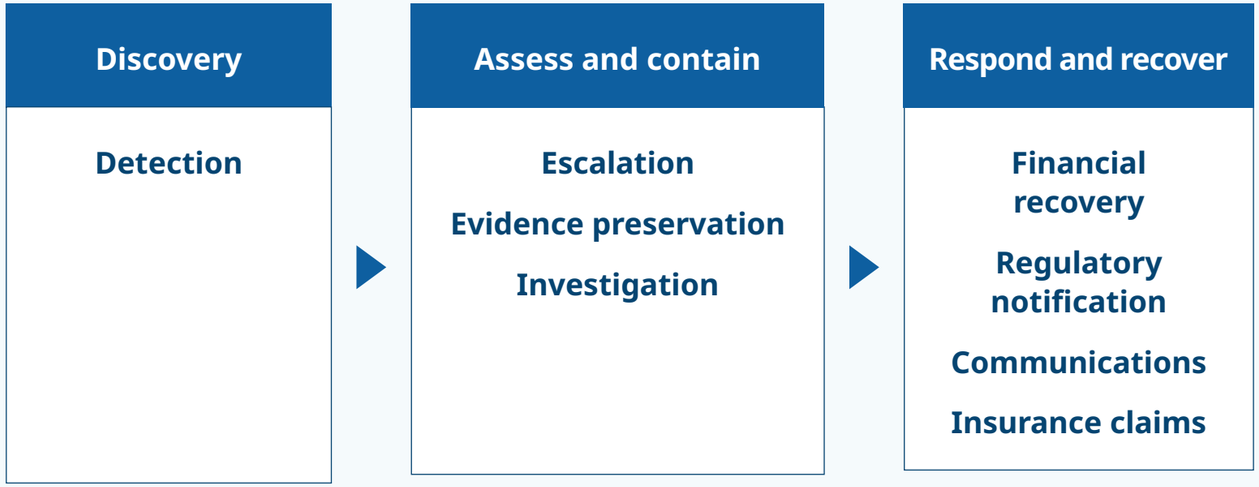
Leaders should plan for the full life cycle of an incident before it occurs: detection, escalation, evidence preservation, investigation, financial recovery, regulatory notification, communications and insurance claims.

Managing these consequences requires cross-functional teams to work together effectively:

- **Finance and Treasury:** Protects payment workflows and high-value transfers
- **Cybersecurity:** Investigates account compromises, identity theft and digital impersonation
- **HR:** Fosters psychological safety so employees can question unusual instructions without fear of criticism
- **Operations:** Handles third-party supplier security and logistics risks
- **Executive Management:** Ensures leadership accountability and clear crisis management steps
- **Legal and Communications:** Controls regulatory notifications, supervises public perception and watches over the brand

Insurance is a key part of an organization's response strategy. Even with strong controls in place, no organization is immune to commercial crime. When an incident occurs, one of the first questions leaders ask is: "Will it be covered?"

The crime incident pathway



Closing the fraud protection gap: Know the gray areas

Corporate crime events rarely follow a single, clearly defined path. One incident may trigger different policies due to losses that span crime, cyber, property loss, business interruption and management liability, leaving room for gaps in coverage. In fact, while 81% of respondents reported having relevant insurance in place, insurance covered an estimated 50% of commercial crime losses and costs over the past 12 months, on average, among insured organizations that experienced financial losses.

Additionally, although employee theft or dishonesty was the most commonly experienced commercial crime globally (29%), only a quarter of insured respondents reported having coverage specifically addressing that exposure.

Crime insurance may cover certain direct losses resulting from employee dishonesty or external fraud. Cyber insurance may be triggered by specified forensic, privacy and incident-response costs where a cybersecurity event has occurred. However, no two cyber policies are the same; each carrier writes its own wording and coverage can vary greatly from policy to policy.

More than half (52%) of respondents said they have at least two types of insurance that could respond to commercial crime, which makes coordination among different policies particularly important across the full event life cycle.



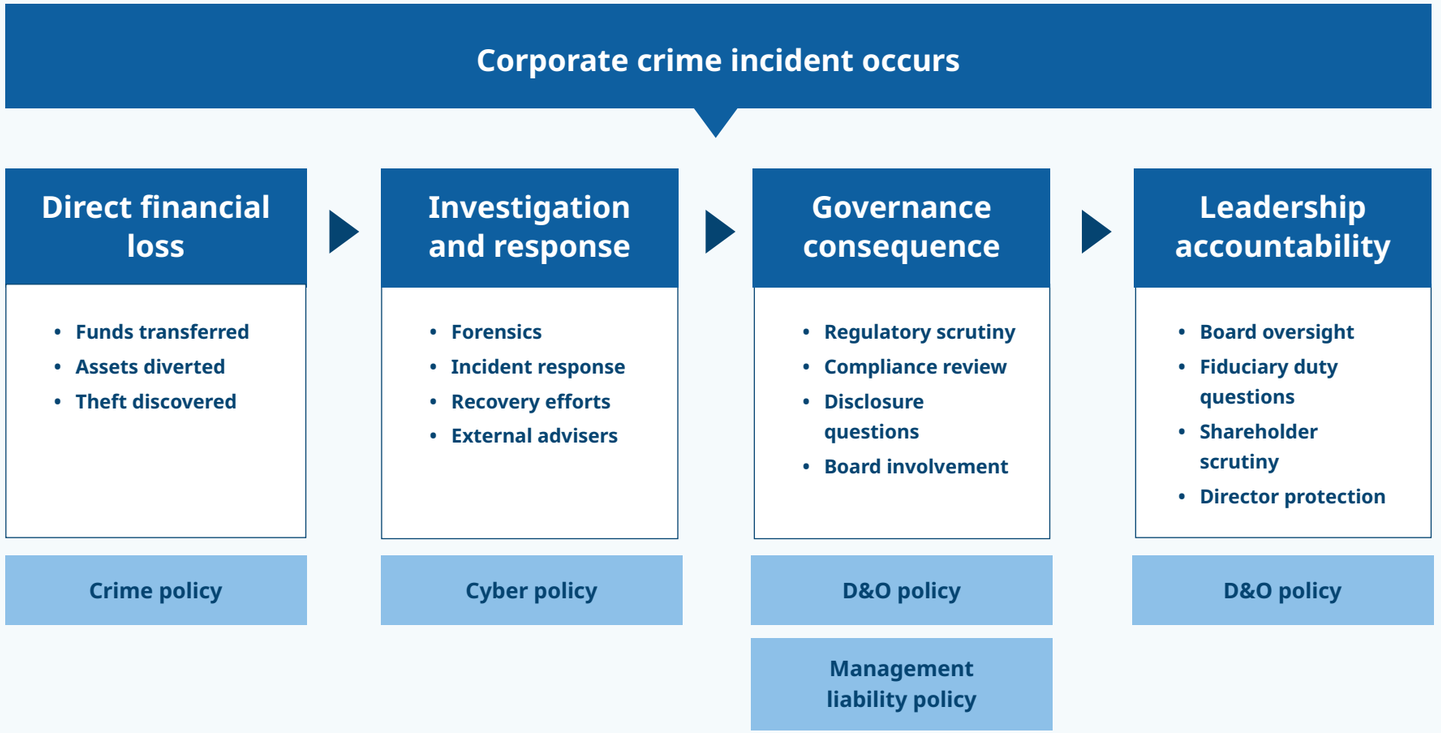
Even so, outcomes remain fact- and wording-specific. Social engineering coverage may be subject to sublimits, meaning lost funds may be capped at a much lower amount than the policy limit. Crime policies, on the other hand, may distinguish between unauthorized transfers and payments voluntarily approved after deception.

Additionally, cyber coverage may require unauthorized access or another defined trigger. Aware of the evolving nature of fraud, some carriers are already including affirmative language to add endorsements to clarify that social engineering losses may be covered by a cyber policy.

Exclusions, retentions, required controls and priority-of-cover wording can further affect recovery. For instance, both commercial crime and cyber policies might state that the coverage is "excess of any other valid and collectible insurance," potentially creating questions over which policy responds first.

> "Crime and cyber are absolutely intertwined — coverage needs to address both the loss suffered and the investigation required to stop the fraud from continuing."

Cassandra Shivers
National Claims Advocacy Leader, Management Liability Policy & Cyber, Gallagher

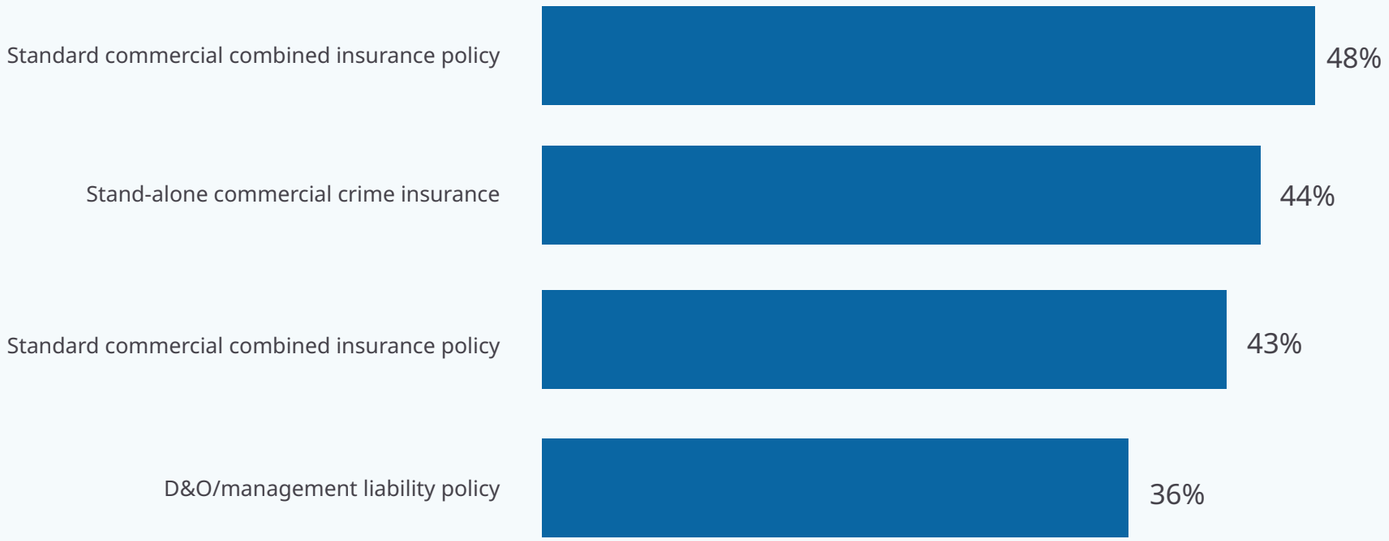


Coverage outcomes often depend on:

Policy triggers / Definitions / Exclusions / Sublimits / Retentions / Social-engineering Provisions / Voluntary-parting language Priority-of-cover provisions / Interaction between multiple policies

Organizations rely on multiple types of insurance to protect against corporate crime

Percentage of insured respondents selecting each type of coverage held for commercial crime losses



Base = 934 respondents who selected at least one type of policy

Source: 2026 Corporate Crime and Risk Survey, Gallagher

Brokers work to dovetail these coverages; ideally, one insurer agrees to act as primary, but "underwriters are not always willing to make that distinction," says Miranda DesPain. When that happens, brokers can compare retentions and limits across the policies and make sure clients know in advance that more than one policy will be involved.

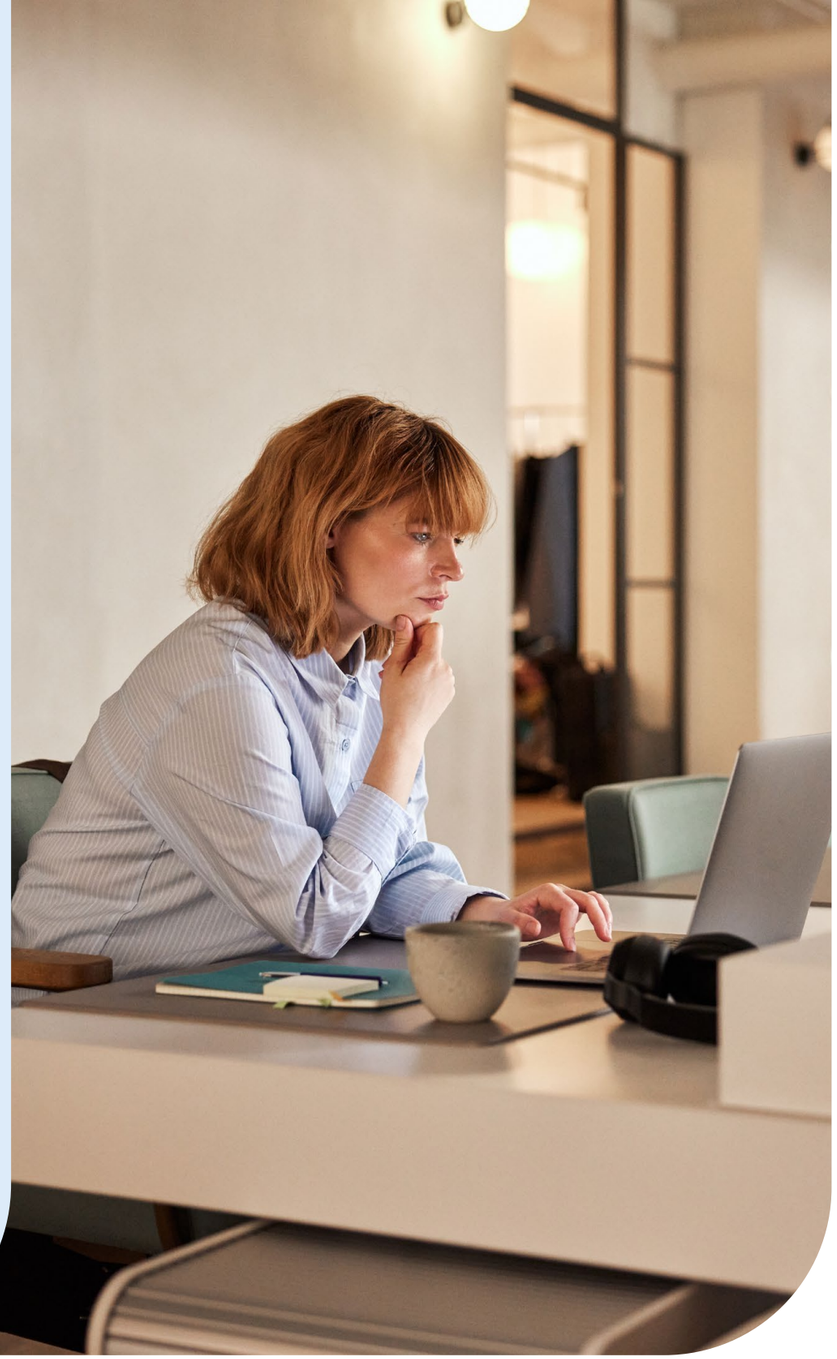
Understanding these interactions before a loss occurs and getting the right advice from a broker can help organizations reduce uncertainty and strengthen recovery efforts.

Businesses can work with their risk and insurance advisors to run scenario analysis and stress test their policies against different types of crime and fraud, so they can identify and address gaps in coverage early.

> "Social engineering losses can fall under both crime and cyber policies. The challenge is getting those policies to work together to establish which insurer responds first."
>
> **Miranda DesPain**
> **Area Senior Vice President, Gallagher**

> When fraud occurs, every delay can make recovery more difficult. Funds rarely stand still; they can be transferred, converted into cryptocurrency or used to purchase property and other assets. The earlier we start tracing that value, the better the chance of identifying where it has gone and preserving potential routes to recovery.

Marlon Pinto
Director of Investigations, Gallagher



Private investigations can support recovery efforts

An area that is often overlooked is the cost and complexity of investigating a fraud event. Whether the goal is to preserve evidence, understand how the incident occurred or trace stolen assets, some policies may include coverage for these activities. However, depending on the circumstances of the loss and the policies involved, organizations may need to fund some investigative work themselves.

Private investigations can also help address a growing resource gap. Law enforcement agencies often face competing priorities and limited capacity, which can delay investigations into fraud and enterprise crime. Private investigators can help gather evidence, work alongside legal counsel and support efforts to recover or freeze assets before they disappear. Acting quickly can improve the chances of recovery and prosecution.

Six pillars for building fraud resilience

1. Governance

Finance, cyber, HR, legal, procurement, risk, and communications teams should follow one process for raising concerns and agree on who makes key decisions. That clarity lets the organization show regulators, investors and insurers how it handled the risk. Regular review can help leaders assess the strength of prevention measures and the speed of response.

2. People and workplace culture

Technology supports fraud prevention, but people often determine whether a suspicious request is challenged. Regular training, practical verification tools and a healthy speak-up culture can help employees question authority, urgency and familiar workflows without fear of criticism.

3. High-risk processes

Payment changes, new bank details, vendor onboarding, shipment redirection and access to critical systems deserve stronger safeguards. Segregation of duties and independent channel checks avoid reliance on a single person.

4. Identity and access

Organizations that rely on face or voice biometrics for authorization should increase the robustness of this process rather than solely implementing specific deepfake detection systems. Common checks include requiring live video, not just audio, requiring random complicated acts on camera, e.g., move hands across the face. Multifactor authentication and regular reviews of privileged accounts add further protection and these controls should extend to third parties such as contractors, suppliers and logistics providers.

5. Detection and intelligence

Connected data can reveal a larger pattern. Integrating information from payments, cyber alerts, claims, vendors and employee reports can uncover repeated actors and recurring control failures. Monitoring emerging trends in commercial crime and near misses provides useful intelligence by revealing how attackers operate and where the next loss could occur.

6. Response and recovery

A response strategy should identify who preserves evidence, contacts banks, law enforcement and insurers, traces assets, and manages internal and external communications. Insurance should be tested against realistic scenarios, including policy triggers, exclusions, limits, sublimits and required controls.



Pivoting from reactive spending to proactive resilience

Organizations recognize that AI makes crime and fraud easier to scale and are investing in stronger controls, awareness programs and cybersecurity. Survey findings also suggest that lessons learned from previous events shape future prevention efforts.

Firms that have been hit by crime are far more likely to expect to spend more on prevention over the next year. Among those with three or more crimes in the past 12 months, 72% expect to increase spending. Among firms with no crime in that period, 40% expect to do so.

Strengthening resilience against fraud requires more than additional spending. As Lisanne Sison, Managing Director of Enterprise Risk Management at Gallagher notes, AI models have a tendency to agree with, flatter and validate users' viewpoints. Combined with the human psychological tendency to favor information that confirms preexisting beliefs, this builds a habit of accepting what is fed to us through AI.

That habit, she explains, "can actually make us more susceptible to crime, to fraud, to social engineering."

One of the best mitigation strategies against enterprise crime is encouraging critical thinking. "It's very important that organizations are value-centric and focus on their ethics, because these are the things that will anchor us when the technology exceeds our wildest imagination," says Sison. "It's the ethical underpinning of an organization that will function as those guardrails in the absence of regulation."

AI-enabled fraud is an interdisciplinary risk that requires a proactive approach rather than a reactive one. Resilience, therefore, depends on breaking down organizational silos and building an enterprisewide mindset that makes fraud harder to commit and reduces overall impact when it does occur.

Prevention investment is rising, but remains reactive

	Increased spending on prevention in the past year	Expected to increase spending on prevention in the next year
No crime experienced in past 12 months	35%	40%
One to two crimes	61%	58%
Three or more crimes	**74%**	**72%**

Base: All respondents, n=1,150

Source: 2026 Corporate Crime and Risk Survey, Gallagher

Four scenarios for stress testing coverage response

SCENARIO 1:
A compromised email leads to data loss

The event

An accounting employee receives what appears to be a legitimate email from a trusted vendor requesting updated payment details. Unknown to both organizations, the vendor's email account has been compromised.

Over several weeks, the attacker monitors communications, inserts fraudulent payment instructions and gains access to sensitive business information exchanged between the two companies. The organization eventually discovers the fraud when a payment is made to a fraudulent bank account by mistake.

Unlike an exclusively social engineering event, this incident combines fraud, cyber intrusion and potential privacy concerns. The financial loss may be only one part of a larger incident involving forensic investigations, legal obligations and stakeholder communications.

The response

A crime policy may be relevant to the direct financial loss resulting from fraudulent payments. A cyber policy may also activate if the incident includes unauthorized system access, email compromise, forensic investigations, legal advice, notification requirements or incident response costs.

The challenge is that modern fraud events rarely fit neatly into a single category. One common area of uncertainty is determining where a crime loss ends and a cyber event begins. Another involves the concept of voluntary parting. Many crime policies are designed to respond to unauthorized transfers of funds. However, if an employee willingly authorizes a payment based on fraudulent instructions, some policies may view the transfer as voluntary, even though it was induced by deception.

From the organization's perspective, the funds were stolen. From a coverage perspective, the question may be whether the money was taken without authorization or voluntarily transferred based on false information.

Organizations could benefit from understanding how multiple policies may respond to different aspects of the same event.



SCENARIO 2:
Fraud hidden in the supply chain

The event

A manufacturer discovers that a trusted supplier has been substituting approved materials with lower-quality alternatives. In a separate incident, a shipment of high-value goods disappears while in transit after fraudulent instructions redirect the delivery to an unauthorized location.

Customers begin reporting product issues, replacement costs increase, and questions emerge about supplier oversight and supply chain controls. What appears to be an operational issue ultimately reveals multiple forms of fraud affecting both product integrity and the movement of physical goods.

Organizations are encountering social engineering applied to property.

The response

Coverage may depend on the nature of the loss and the circumstances surrounding the event. Multiple forms of insurance may become relevant, including crime-related coverage, marine cargo protections, property-related coverage and policies addressing supply chain disruption.

Questions often arise around whether the loss resulted from theft, fraud, supplier misconduct or another covered cause. Recovery may also depend on how contracts, transportation arrangements and insurance responsibilities were structured before the event.

The social engineering of property introduces an additional layer of complexity. Traditionally, many crime policies used to focus on the loss of money, cash, securities and other financial assets rather than physical inventory or products. As a result, organizations may assume similar protections exist for diverted goods when that is not always the case.

The insurance market is evolving. Some insurers now offer extensions or supplemental coverage designed to address losses involving the fraudulent diversion of physical property.

SCENARIO 3:
A deepfake executive authorizes payment

The event

An employee joins what appears to be a routine video call with colleagues and a senior executive. During the meeting, the executive instructs the employee to facilitate a large payment to what appears to be a trusted business partner. The request follows established approval channels and the employee completes the transfer.

Only later does the organization discover that the executive, the meeting participants and the instructions were all part of a sophisticated AI-generated impersonation scheme. The funds were transferred to a criminal account and cannot be recovered immediately.

This scenario illustrates how fraud increasingly exploits trust rather than relying only on technical compromise. Social engineering identifies people with financial authority, while AI-generated voice, video and identity content manufactures credibility around a request.

The response

A crime policy may respond to direct financial loss resulting from the fraudulent transfer. However, coverage can depend on how the policy addresses social-engineering fraud, impersonation events and voluntary transfers of funds.

A cyber policy may be relevant if the incident involves unauthorized system access, compromised accounts or other cyber elements. In some circumstances, the policy may also support forensic investigations, incident response and related response costs.

The same incident can therefore raise questions about whether the loss is primarily a crime event, a cyber event or a combination of both. Social-engineering coverage may be available, but sublimits, if not properly assessed, may be lower than the loss itself.

SCENARIO 4:
Employee misconduct escalates into a governance issue

The event

A sales employee is found to have manipulated travel and expense claims over a period of several years. Following an internal review, investigators determine that numerous expenses were either inflated or entirely fictitious. Following the event, the employee alleges a wrongful termination case against the company.

While direct financial loss is material, the incident creates broader concerns about governance, oversight and internal controls. Shareholders question how the activity remained undetected for so long, and the board launches an investigation into management practices and reporting structures.

The response

A crime policy may potentially respond to aspects of the financial loss arising from the dishonest conduct of the employee. This policy may also cover the expenses from the employment practices liability (EPL) claim, including investigations and defense costs.

However, allegations related to oversight failures, governance practices or management decisions may fall under management liability or D&O policies. These policies are designed to provide coverage for those who act in good faith and are not involved in fraudulent activities.

Some solutions may also provide access to crisis response resources, including public relations and reputation management support, following a covered event.

[1]"FBI 2025 Internet Crime Complaint Center (IC3) Report," *IC3*, accessed 26 Oct 2026. PDF File.

[2]"The Report Fraud Annual Assessment FY 2025 26: Cyber Crime and Fraud," *Report Fraud City of London Police*, Sep 2026.

[3]"Police Advisory On Scams Involving the Impersonation Of Senior Government Officials, Including Secretary to the Cabinet," *Singapore Police Force*, 4 May 2026.

[4]"Economic Crime and Corporate Transparency Act: Failure to Prevent Fraud Offence," *UK Ministry of Justice (Gov.UK)*, 1 Mar 2024.

© 2026 Arthur J. Gallagher & Co. | CRPGLOB106949

Gallagher