ZEROFOX Intelligence

Brief

The Malicious Insider Threat

B-2026-06-05a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Insider Threat, Threat Actor, Dark Web

June 5, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 11:00 AM (EDT) on June 3, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Malicious Insider Threat

| Key Points

- Intentional, or malicious, insider threats represent a significant attack vector in which likely disgruntled employees compromise organizations by misusing access to sensitive networks and data or abusing advantageous positioning to enact harm against the employer.
- An individual's likelihood of becoming an insider threat is often signaled by predisposing factors, such as their specific organizational positioning and access alongside various personal and professional vulnerabilities.
- Threat actors almost certainly monitor social media and dark web forums for disgruntled employees, whom they target to exploit as a means of gaining entry into specific corporate environments.
- Malicious insiders often execute highly structured operations that mirror external adversary tactics, utilizing their unique, high-level credentials and proprietary insights to facilitate their activities.
- Malicious insider threats will almost certainly continue to pose a significant risk—with detrimental effects that span beyond just a targeted organization—throughout 2026, as opportunities for insiders to “switch sides” are becoming increasingly accessible on social media and the dark web.

Intentional Insider Threats

Intentional, or malicious, insider threats represent a significant attack vector in which likely disgruntled employees compromise organizations by misusing access to sensitive networks and data or abusing advantageous positioning to enact harm against their employer. Unlike accidental insider threats, intentional insider threat actors take deliberate and overtly malicious action to harm, or otherwise negatively affect, the integrity, confidentiality, and availability of an organization, its data, personnel, or facilities.[1]

- According to Cogility's 2025 Insider Risk Report, 93 of their respondents reported insider threats are as difficult or more difficult to detect than external cyberattacks—and merely 23 percent of those respondents have high confidence in their ability to detect insider threats before harm occurs, underpinning a significant vulnerability many organizations face.[2]
- Reporting from 2025 demonstrated an increase of insider threat-related breaches. Successful malicious insider threats were found to be the most expensive incidents; the total cost for organizations, from detection to post-breach consequences, averaged USD 4.92 million per breach.[3][4]
- The Ponemon Institute's 2026 Cost of Insider Risks Global Report documented a steady rise in per-incident costs (only for responding to and containing the incident) from USD 701,500 in 2023 to USD 742,125 in 2025; this trend is consistent with a 20 percent increase in total insider risk costs over the same two-year period.[5] Costs are very likely to continuously rise, as the success and reporting of incidents are likely to increase proportionally.

Intentional insider-related security incidents differ greatly from accidental insider threats, which are unintentional and often a result of falling victim to social engineering or

[1] hXXps://www.cisa[.]gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
[2] hXXps://www.cybersecurity-insiders[.]com/wp-content/uploads/2025-Cogility-Insider-Risk-Report-by-CSI.pdf
[3] hXXps://arcticwolf[.]com/resources/blog/the-rise-of-insider-threats/
[4] hXXps://secureframe[.]com/blog/data-breach-statistics
[5] hXXps://ponemonsullivanreport[.]com/2026/05/2026-cost-of-insider-risks-global/

human error. Intentional insider threats very likely seek to maliciously harm an organization for personal benefit or due to personal/professional grievance.

- In May 2023, a prominent and widely known breach of a U.S.-based multinational electric vehicle company occurred when two former employees deliberately leaked thousands of personal identifiable information (PII) records and confidential company secrets to a foreign media outlet.[6]
- While the company took legal action against the former employees, it almost certainly experienced significant organizational and reputational harm.

Intentional insider-related threats are not always conducted by a lone individual; they can also manifest through collusive or third-party threats.

Collusive Threats. Collusive threats involve one or more insiders collaborating with an external threat actor to intentionally compromise an organization, often for financial gain negotiated with threat actors seeking the insider access. Advertisements for collusive insider threats appear on deep and dark web forums (DDW)—and more so through instant messaging platforms (Telegram) and social media sites (LinkedIn).[7][8]

- In 2025, reporting indicated there were at least 91,321 observed instances of recruiting, advertising, and threat actor discussions involving insider-related illicit activity, highlighting the efficiency of threat actors recruiting an insider to circumvent security barriers rather than developing a complex exploit from the outside.[9]
- In 2021, cybersecurity researchers reported that the DemonWare ransomware collective attempted to recruit insiders to act as accomplices by installing the group's ransomware on company devices in exchange for 40 percent of the presumed USD 2.5 million ransom.[10]

---

[6] hXXps://www.reuters[.]com/business/autos-transportation/tesla-says-two-ex-employees-behind-may-data-breach-2023-08-21/

[7] hXXps://blog.checkpoint[.]com/research/cyber-criminals-are-recruiting-insiders-in-banks-telecoms-and-tech/

[8] hXXps://www.airuniversity[.]af[.]edu/JIPA/Display/Article/3768503/covert-connections-the-linkedin-recruitment-ruse-targeting-defense-insiders/

[9] hXXps://www.helpnetsecurity[.]com/2026/03/12/agentic-attack-chains-infostealers-criminal-markets/

[10] hXXps://abnormal[.]ai/blog/nigerian-ransomware-soliciting-employees-demonware

Collusive threat operations were previously limited to singular exchanges, such as an employee sharing their password directly with a threat actor, enabling the threat actor to engage in an organization's system themselves. However, emerging tactics foster an enhanced collaborative relationship between actors and insiders in which insiders very likely function as continuous, on-demand operators directly providing active, sustained, and real-time operational support for an actor's illicit campaign.

Third-Party Threats. Third-party threats often originate from contractors or vendors who are not formal members of an organization but have been granted some level of access to facilities, systems, networks, or people to complete their work.

Collusive and Third-Party Threat Meets Espionage: The DPRK IT Worker Scheme

The Democratic People's Republic of Korea (DPRK) IT worker scheme is a well-documented example of collusive, third-party, and espionage insider threats. The scheme involves actors in North Korea utilizing AI and deepfake technology to masquerade as U.S.-based (and other countries) IT workers applying for remote jobs in the United States. Once the actors accept the role, they continue their masquerade as genuine employees of unsuspecting companies to abuse the access and information they gain—becoming malicious insider threats.

In 2025, U.S. federal investigations found that over 150 organizations were compromised by this insider threat scheme, and over half of those companies experienced data theft.[11] Reporting from 2025 also found a 220 percent year-over-year increase of incidents involving North Korean operatives gaining fraudulent employment as IT workers.[12]

Investigations into this scheme revealed that these actors use AI to create resumes and fabricate false identities, as well as use deep fakes to mask their identities in live video calls.[13]

[11] hXXps://www.techtarget[.]com/searchsecurity/feature/How-to-spot-and-expose-fraudulent-North-Korean-IT-workers
[12] hXXps://cyberscoop[.]com/crowdstrike-north-korean-operatives/
[13] *Ibid.*

Understanding the Malicious Insider

The fundamental human element of organizations cannot be overlooked in the context of cybersecurity risks, as employees naturally have the capacity to be susceptible to acting against an organization for personal, financial, or professional reasons. The inherent risk of malicious insider threats derives from predisposing factors and motivations that make an insider increasingly vulnerable to "switching sides."

Predisposing Factors

Personal and professional vulnerabilities and an individual's access and positioning are predisposing factors that may indicate a person's susceptibility to becoming an insider threat. Predisposing factors do not solely and directly determine whether an insider will become malicious; however, such factors—combined with triggering events—can present a pathway for an insider to turn against their organization.

Personal vulnerabilities. An individual's personality and psychological traits, in addition to their life circumstances, correlate with their potential willingness to become an insider threat. Research suggests that the psychological theory known as the "dark triad" of personality traits—narcissism, machiavellianism, and psychopathy—is one predisposing factor. In addition, of the "big five" personality traits, low agreeableness and low conscientiousness also align with those that are at an elevated risk.[14]

- The dark triad is a theory that describes personality traits in people who lack empathy, strategically manipulate others, and have a strong sense of entitlement or ego.[15]
- The big five or five-factor model is another personality theory that categorizes individuals on a spectrum of five traits. Lower agreeableness scores are associated with being analytical, detached, and skeptical of others, and low conscientiousness is associated with impulsivity, being laid-back, and easily sidetracked.[16]

[14] hXXps://pmc.ncbi.nlm.nih[.]gov/articles/PMC12951658/
[15] hXXps://cacm.acm[.]org/research/the-dark-triad-and-insider-threats-in-cyber-security/
[16] hXXps://pmc.ncbi.nlm.nih[.]gov/articles/PMC12951658/

Furthermore, individuals with mental health disorders, poor social skills, history of rule violations or complaints, and risky external or internal relationships are also vulnerable to increased risk.[17] These traits very likely increase an individual's susceptibility to rationalizing harmful and risky behaviors, especially in those that are professionally vulnerable with access and positioning in their organization.

Professional vulnerabilities. Workplace dissatisfaction, perceived injustice, and unmet expectations contribute to an individual's willingness to engage in insider threat activity. Work-related stressors, such as denied promotions, layoffs, and poor management of relationships/environments, can become factors that lead previously compliant employees toward harmful behavior—especially in those who are also personally vulnerable.

- Environmental factors and organizational responses contribute largely to triggering a state-of-crisis event, which may leave employees desperate or hopeless and increase their desire for retaliation.

Access and positioning. Employees with specialized access and advantageous positioning within an organization likely amplify the risk created by personal and/or professional vulnerabilities. Privileged users such as system administrators, finance personnel, and developers possess highly sensitive access that can lead to substantial consequences if misused or abused maliciously—presenting an increased and accessible opportunity for an organization's most-trusted employees to act for personal benefit or grievance.

Motivations

The primary motivation for insiders with personal and/or professional vulnerabilities and sensitive access opting to target their organization is very likely personal benefit; reporting from 2025 found that 89 percent of all privilege misuse/abuse malicious insider threat incidents were directly tied to financial gain.[18]

[17] hXXps://blog.signpostsix[.]com/signpost-six-blog/what-is-the-critical-pathway-to-insider-risk-cpir
[18] hXXps://www.syteca[.]com/en/blog/insider-threat-statistics-facts-and-figures

- Layoffs and the cost-of-living crisis are likely driving motivational factors that lead employees to seek personal financial benefit—which is an increasingly accessible opportunity due to the proliferation of insider threat recruitment ads on social media and the dark web offering insiders financial incentive.

Personal grievance is likely another significant motivator and encompasses revenge, reputational damage, and ideology. Predisposed employees—whether driven by personal benefit or grievance—are at risk of transitioning into conducting active harm as a result of negative professional action.

- Work-related triggering events typically include the denial of a promotion, the failure to receive a requisite salary adjustment or performance bonus, a reduction in compensation, formal disciplinary censure, or termination.[19]

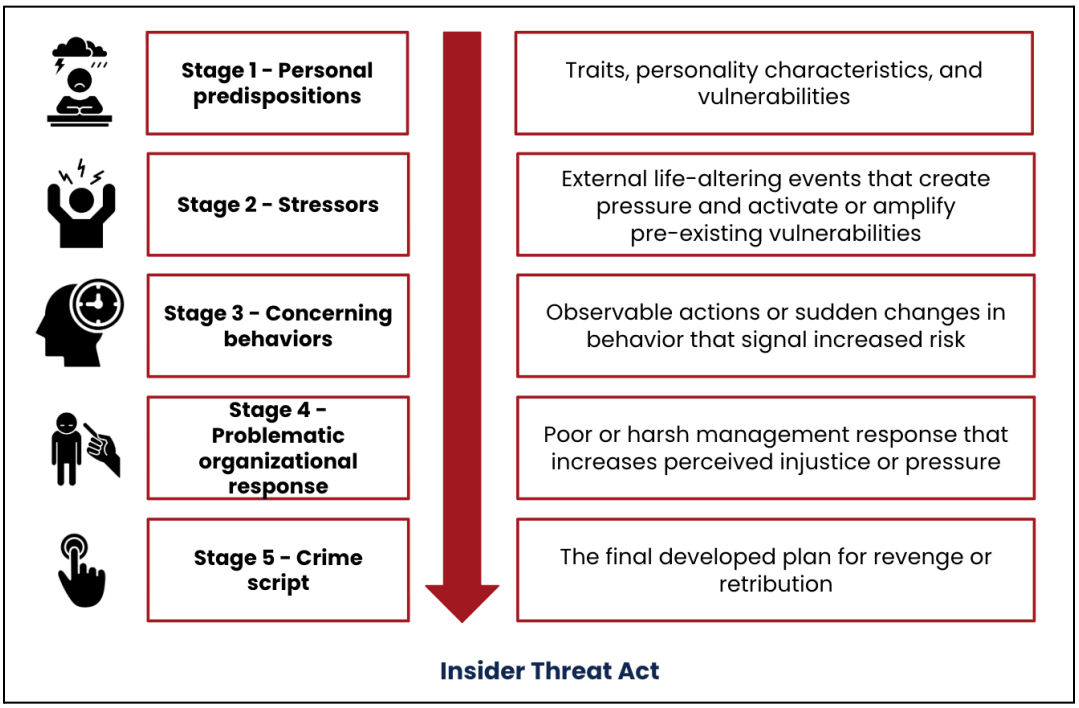
Coercion-motivated insider threat incidents represent a smaller vector and involve an insider being pressured or blackmailed into acting against their organization. These cases can also be a result of social engineering attacks or data breaches originating from an employee, whose data can then be used against them.

Espionage-motivated incidents increased at least 163 percent since 2025, likely indicating a significant surge in state-sponsored or ideologically compelled insider operations.[20] The North Korean IT worker campaign serves as a notable instance of large-scale, state-directed insider activity.

Indicators

The Critical Pathway to Insider Risk (CPIR) framework was developed to map the progression of insider threats and is used by threat analysts to identify indicators across its five stages: personal predispositions, stressors, concerning behaviors, problematic organizational response, and crime script.[21] Notably, the model suggests that risk increases with the accumulation of factors; while many insiders likely possess factors, very few take action.

[19] hXXps://www.sei.cmu[.]edu/news/insider-threats-in-the-time-of-covid-19/
[20] hXXps://www.verizon[.]com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf
[21] hXXps://blog.signpostsix[.]com/signpost-six-blog/what-is-the-critical-pathway-to-insider-risk-cpir



The CPIR model

Source: ZeroFox Intelligence

Professional, personal, and financial stressors have the potential to activate or amplify latent vulnerabilities, which initiates movement along the pathway. Insiders with pre-existing predispositions are more likely to become a threat when a cataclysmic event drives them to a turning point.

- Stressors are life-alerting events or conditions that are overwhelmingly stressful to an individual. These may include, but are not limited to, divorce, legal problems, family crises, debt or bankruptcy, demotion, negative performance reviews, and termination.

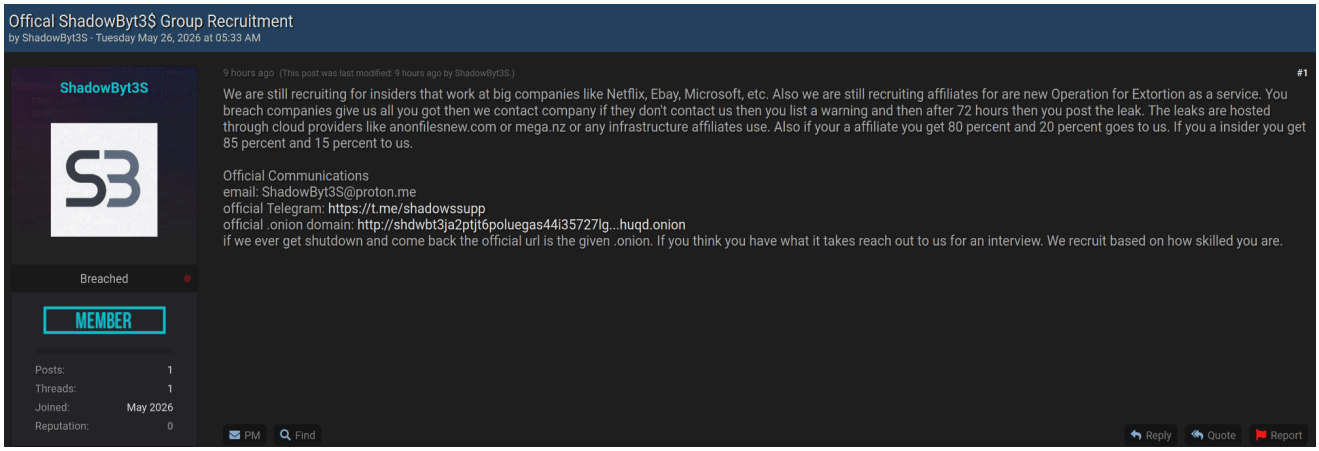
Observable behavioral shifts following a professional triggering event—particularly those rooted in workplace grievances—frequently manifest as recurrent articulation of concerns or overt dissatisfaction with management and colleagues. Collateral personal stressors such as financial instability, substance abuse, gambling, and engagement in illicit activities are also often drivers of sudden behavioral changes.

Other behavior indicators include, but are not limited to, the emergence of stress-related symptoms such as professional burnout, heightened frustration, paranoia, secrecy, blame directed at others, work during non-standard hours, access requests that exceed operational requirements, expression of extremist ideologies, and a decline in job performance, all of which serve as critical indicators of potential risk.

Unusual network activity such as atypical remote access to systems outside of assigned tasks, large file transfers or downloads, copying or unauthorized storage (such as USBs or external storage) of proprietary or classified materials, and privilege escalation are behaviors that may indicate an employee's planning or execution stage. In addition, emailing large volumes of sensitive data to personal or external accounts or installing unapproved software/utilizing unauthorized hardware are also indicators of exfiltration.

The Dark Web Business of Recruiting Insider Threats

Vulnerable insiders are targeted by threat actors trawling dark web forums and social media sites, seeking to exploit an insiders' disgruntlement to acquire initial access to targeted organizations. Insiders are likely to be identified by actors based on indicative online activity, such as online posts denouncing a workplace, comments expressing dissatisfaction or frustration, or posts seeking financial relief related to personal emergencies.



ShadowByt3S' insider threat recruitment post on BreachForums
Source: ZeroFox Intelligence

Once trust is established, a motivated and vulnerable insider is more likely to be swayed toward active harm—particularly where poor organizational responses to grievances leave an opening for a threat actor to step in as an empathetic and solution-oriented alternative. This signifies a moment where an already vulnerable insider can begin to rationalize resorting to extreme and risky behaviors—and is facilitated by threat actors.

- The dark web business of recruiting insider threats relies on the engineered manipulation and exploitation of vulnerable employees and provides malevolent insiders the marketplace to sell access or datasets themselves.

Other methods of insider recruitment on the dark web involve threat actors seeking intermediaries or brokers with access to insiders. In these cases, an insider is recruited by a broker or other third-party, who then advertises any information gained (via their insider) to other threat actors on the dark web.

Recruited and/or compromised insiders are very likely leveraged by threat actors to enable various illicit operations, such as obtaining and selling initial access, ransomware and malware deployment, data exfiltration, SIM swapping, account takeover and social engineering campaigns, credential harvesting, and other types of sabotage or harm.

Attack Lifecycle

An intentional insider threat attack involves the misuse or abuse of privileged access to an organization's systems, networks, and proprietary information to compromise the integrity, confidentiality, and availability of an organization, its data, personnel, or facilities. Insiders conduct a deliberate and sequenced operation that is similar to external threat actor tradecraft but benefits from insider-exclusive privileged knowledge and access.

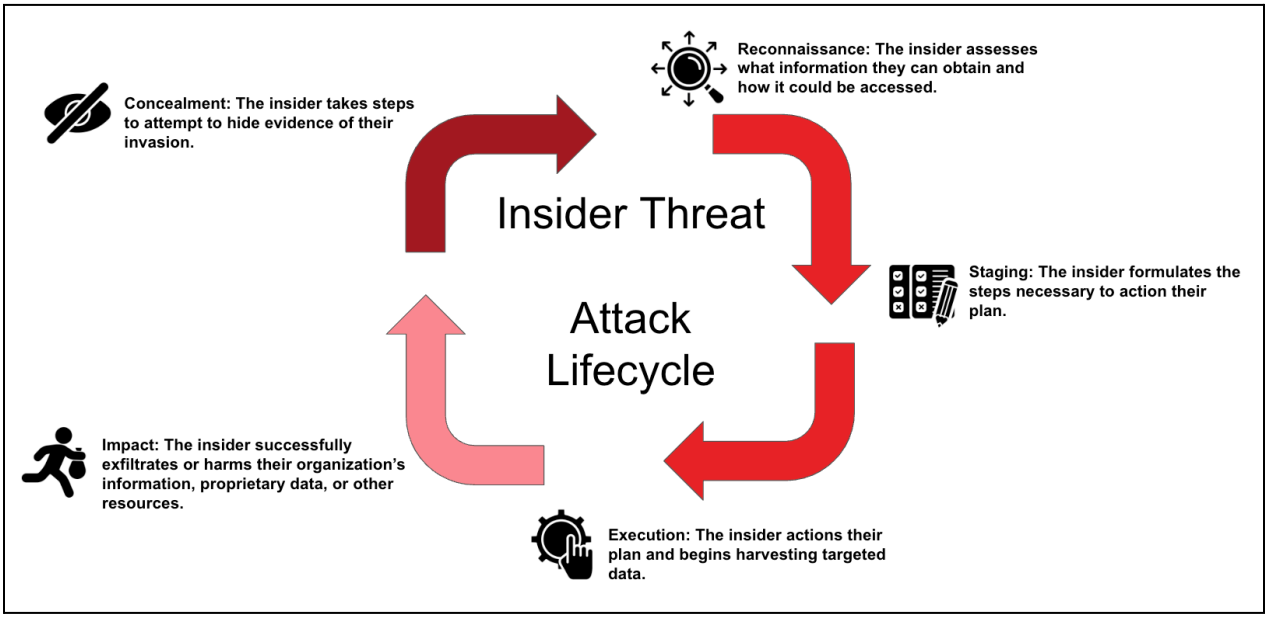
Reconnaissance: Once a grievance transitions into actionable intent, the malicious insider initiates a deliberate reconnaissance phase to prepare for the strike. During this stage, the individual identifies high-value target data and evaluates methodologies to circumvent security controls and detection mechanisms.

Staging: An insider gathers the necessary credentials, elevates permissions, or uses their existing access to prepare the technical environment for the impending strike—actions that frequently include the installation of malware or other unauthorized utilities.

Execution: An insider launches their attack, often over an extended period of time to avoid detection; this can include stealing intellectual property, altering data, or crashing systems.

Exfiltration or impact: At this stage, the victim organization's data is exfiltrated outside of its network; it is often downloaded, emailed, or stored in personal clouds or devices. In some instances, information is physically stolen from an organization's facilities.

Concealment: Technically sophisticated insiders may attempt to conceal their nefarious activity within an organization's network or delete data, logs, or other records in an attempt to cover up their actions and delay discovery.



The malicious insider threat attack lifecycle
Source: ZeroFox Intelligence

Methods of Compromise

Malicious insider threats manifest in several ways within the following categories:

- Data and information compromise
- Operational and technical harm
- Financial and administrative abuse
- Physical safety threats

At the start of the insider threat attack cycle, an insider will begin reconnaissance to assess which threat category will either be the most personally lucrative or have the highest level of impact.

Data and information compromise: This category typically comprises unauthorized disclosure, theft, and espionage. Unauthorized disclosure occurs when an insider intentionally leaks, exposes, or shares sensitive organizational data to unauthorized receivers, which may include competitors, foreign entities, the public, or the press. Theft specifically refers to an insider removing, copying, or extracting an organization's data, assets, or property (ideas, inventions, creative expressions, trade secrets, and proprietary products); notably, theft deprives an organization from controlling its assets. Espionage involves an insider gathering and transmitting sensitive information for a competitor or adversarial nation-state government; distinctly, espionage attacks manifest through covert and longer-term operations.

- **Nation-state operations:** Operations conducted by nation-state actors and nation-state sponsored entities; this activity is linked to covert adversarial governments that engage in advanced persistent threat (APT) activities. APTs are sophisticated and well-resourced malicious cyber threat collectives aimed towards prolonged espionage operations, as well as other cyber threat activity.[22]
- **Corporate espionage/competitor-planted insiders:** Operations conducted or secretly sponsored by competitors who engage in illegal spying activities under false pretenses. This activity also includes the malicious transfer of trade secrets between organizations.[23]

[22] hXXps://www.cisa[.]gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
[23] hXXps://www.upguard[.]com/blog/corporate-espionage

Operational and technical harm: Sabotage and intentional degradation of resources or capabilities considerably overlap. Both target an organization's ability to function; however, sabotage usually refers to a broader destructive intent rather than specific targeting of a system or control to degrade.

- Both methods consist of the deliberate deletion, disruption, or destruction of an organization's systems, data, operations, equipment, facilities or reputation. These attacks are more likely to be deployed in cases of grievances rather than being financially motivated.

Financial and administrative abuse: This category encompasses corruption, fraud, and theft. These methods involve abusing access or authority within an organization for personal financial benefit, through financial crimes such as embezzlement, bribery, organized crime, or other illegal fraud. Methods involving theft can transpire through financial crimes—directly stealing funds from an organization for personal financial benefit.

- CISA specifically distinguishes financial crime—the unauthorized taking or illicit use of money or property through deception—as separate from theft and corruption.
- Financial crime and fraud are treated as distinct categories even within cybersecurity contexts. Financial crime covers money laundering, bribery, and tax evasion, while fraud is defined as crimes involving active deception of financial personnel or systems to commit theft, such as forgery, false invoicing, and credit scams.[24]

Physical safety threats: This category includes both the threat of and actual workplace violence or terrorism. Workplace threats encompass any action of physical harm that creates an intimidating, hostile, or abusive environment by a co-worker or associate that occurs in a person's place of employment or while a person is working.

[24] hXXps://www.cisa[.]gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

- Workplace violence is any action or threat of physical violence, harassment, sexual harassment, intimidation, bullying, offensive jokes, or other threatening behavior.
- Terrorism is violence associated with political, ideological, or social objectives that target members or facilities of an organization.[25]

Incident Response

Depending on the attack type, an insider threat incident can span weeks or be a months-long operation. In 2025, the average time to detect and contain an insider incident was roughly 81 days, and just 12 percent of incidents were contained in less than 31 days.[26] Initially detecting a malicious insider is typically difficult since—unlike external threat actors—insiders possess legitimate credentials, technical skills, and institutional knowledge that provides an unmatched ability to mask their malicious intent.

In response to this inherent risk, organizations utilize proactive incident response strategies and insider threat programs. An insider threat incident response framework consists of detection, containment, investigation, legal referral, and evidence preservation.

Detection increasingly relies on User and Entity Behavior Analytics (UEBA), which establishes behavioral baselines and flags anomalies such as unusual data access volumes, off-hours activity, and large file transfers—though only 44 percent of organizations currently deploy these tools.[27] Once an insider incident is confirmed, containment must occur quickly; incidents contained in under 31 days cost an average of USD 10.6 million, while the cost for those exceeding 91 days significantly increases to USD 18.7 million.[28]

- Containment actions include immediate account lockdowns, endpoint isolation, network segmentation, and credential revocation, with short-term evidence preservation a simultaneous priority in order to avoid destroying forensic data.

[25] *Ibid.*
[26] hXXps://www.syteca[.]com/en/blog/insider-threat-statistics-facts-and-figures
[27] hXXps://www.exabeam[.]com/explainers/ueba/what-ueba-stands-for-and-a-5-minute-ueba-primer/
[28] hXXps://www.brightdefense[.]com/resources/insider-threat-statistics/

Investigations typically involve human resources (HR), legal, and information technology (IT) security stakeholders and trace the attack to determine whether the incident was malicious, negligent, or accidental, as each outcome triggers a different escalation path. For confirmed malicious activity, legal referral decisions carry strategic weight, as premature action can compromise law enforcement or counterintelligence operations.

- Evidence preservation is the cornerstone of a legally sound insider threat case. Digital forensics teams follow strict chain-of-custody protocols; collect data from computers, mobile devices, cloud storage, and network infrastructure; and prioritize volatile data first in the order of collection.

Despite the average timeframes, costs, and consequences, many organizations lack the pre-defined playbooks, behavioral monitoring tools, and cross-functional coordination required to respond effectively to a malicious insider incident, underscoring the need for a structured, proactive approach to insider threat response.

Outlook

The consequences of malicious insider threats are often immediate and severe, with losses of private customer data, proprietary information, and sensitive internal communications. These losses can further manifest into market disadvantages and supply chain vulnerabilities, which can have long-term effects on both the organization and the broader industry.

Market disadvantages: Insider-caused breaches expose intellectual property or customer data, resulting in reputational harm, legal liability, and financial loss. The erosion of consumer trust and investor confidence can reduce an organization's market value and weaken its competitive position.

Supply chain vulnerabilities: Insider-caused breaches can lead to operational disruptions or expose third-party integrations. Delays in production, system downtimes, and security gaps ripple across the enterprise and can affect downstream partners. Resources are diverted to secure the organization, generating additional costs and decreasing productivity. In highly connected industries, such disruptions may cascade across entire sectors or international networks.

Legal and regulatory consequences: Malicious insider threats expose an organization to an array of criminal prosecution, civil litigation, and sector-specific regulatory penalties. A victim organization—and potentially some of its executives (CISOs and CSOs)—can also face independent criminal charges, regulatory enforcement actions, and civil fraud liability when they fail to adequately prevent, disclose, or respond to insider-related incidents.

Organizations impacted by insider-related incidents are likely to face civil lawsuits from affected parties, such as customers whose data was breached via an insider. Intentional insider incidents that result in data exposure also can trigger compliance failures across multiple regulatory entities, often compounding an organization's liability independent of the insider's own criminal culpability.

Malicious insider threats will almost certainly continue to pose a significant risk to organizations across industries globally throughout 2026. The opportunity for insiders to "switch sides" is increasingly accessible through the proliferation of offers and financial incentives available across social media platforms and the dark web. The risk of intentional insider threats is significant, with potentially detrimental effects that span beyond just a targeted organization. The implementation of insider threat programs is a crucial proactive and preventative measure to counter the risk of insider threats.

Recommendations

- Adopt a Zero-Trust cybersecurity architecture grounded in the principle of least privilege (PoLP), and enforce role-based access controls (RBAC) across all organizational systems.
- Conduct periodic privilege audits to eliminate "privilege creep"—the gradual accumulation of excessive access rights over time.
- Implement Privileged Access Management (PAM) solutions to enforce time-limited, task-specific access for sensitive operations, especially for remote or third-party users.
- Proactively monitor DDW forums for organizational mentions, stolen credentials, and evidence of insider recruitment.
- Establish a formal, automated offboarding protocol that immediately revokes all system access upon an employee's departure—including credentials, VPN access,

cloud storage, SaaS platforms, project management tools, and customer-facing systems.

- Implement a comprehensive data loss prevention (DLP) solution that monitors and enforces policy across endpoints, networks, email, and cloud environments to detect and block unauthorized data exfiltration attempts in real time.
- Integrate DLP with identity and access management (IAM), multi-factor authentication (MFA), and UEBA to create a layered, identity-centric enforcement framework that dynamically responds to both behavioral anomalies and policy violations.
- Establish a cross-functional Insider Threat Program (ITP) integrating personnel from HR, legal, IT security, and physical security that is aligned with established frameworks such as CISA's Insider Risk Mitigation Program Evaluation (IRMPE) and the National Insider Threat Task Force (NITTF) 19-element framework.
- Establish confidential, anonymous reporting channels that empower employees to report suspicious colleague behavior without fear of retaliation.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%