

Insider Threats

AnnexVault LLC

Groundhog Research Group™

Original publication: April 2025

Revised: 26 October 2026

A background brief for evidence review

Overview

Insider threats are risks posed by people who have or previously had authorized access to an organization, including employees, contractors and business partners. Harm can be intentional or accidental and can affect information, systems and operations. [1, 2]

This brief focuses on digital access and information handling. Its central recommendation is to distinguish deliberate misuse, mistakes and compromised accounts before attributing intent. Account activity is evidence to investigate, not a complete explanation of who acted or why.

Why this matters to AnnexVault

This report shows why access, behavior, and organizational context must be reviewed carefully. Insider risk cannot be understood from one event or one indicator alone.

Three situations to distinguish

Intentional misuse

A person knowingly abuses access or organizational knowledge to cause harm. Deliberate unauthorized removal of protected data is one possible example. Intent requires supporting evidence. [1, 2]

Accidental exposure

A mistake can expose information without an intention to cause harm. Examples include sending a file to the wrong recipient or granting an inappropriate permission. [2]

Compromised accounts

An external attacker may act through stolen credentials. Some insider incident studies include this category, but the account owner should not be assumed to be the actor. [5]

Intended readers

Security, insider risk and investigation teams, together with leaders responsible for access governance and accountable review.

Review evidence before attributing intent

The review sequence below is a practical synthesis for this brief. It is not a validated scoring system or a test of an individual. CISA recommends corroboration, contextual assessment and attention to mitigating information. [1]

A practical review sequence

Record the observation

Describe the specific event, affected asset, time and source. Separate a log entry, a witness report and an analyst interpretation.

Preserve provenance

Keep the original record, collection context and known gaps. Note whether clocks, identifiers and account records can be reliably matched.

Establish the access context

Check the person's role, permissions, task and approval history. Consider shared accounts, service accounts and possible credential compromise.

Test other explanations

Ask whether a scheduled job, approved transfer, changed duties, configuration error or mistaken destination could explain the event.

Corroborate the concern

Compare independent records where available. Document both supporting and conflicting evidence, along with what remains unknown.

Choose a proportionate response

Use established incident and personnel processes. Record the decision, responsible reviewer and reason for any escalation or access restriction.

An illustrative review example

A large file transfer outside usual working hours may warrant review. Possible explanations include an approved backup, a legitimate task in another time zone, an error, or unauthorized extraction. The observation alone does not establish an explanation. This is a hypothetical example, not a reported incident.

Responsible review

Limit review to relevant, lawfully obtained information and authorized roles. Protect privacy, civil rights and civil liberties. Give mitigating evidence a place in the record. Avoid demographic profiling or conclusions based on appearance, emotion or a presumed psychological condition.

[1]

Reduce exposure and prepare to respond

Use a combination of access governance, clear working practices and incident preparation. Select controls for the organization's systems and obligations rather than treating any single tool as a complete solution.

Practical safeguards

Manage the access lifecycle

Review and update accounts when responsibilities change or employment ends. Remove access that is no longer required. [3]

Apply least privilege

Give users and processes only the access their assigned tasks require. Review privileged permissions deliberately. [3]

Review relevant audit records

Define what to log, who reviews it and how findings are escalated. Treat unusual activity as a prompt for analysis, not a verdict. [3]

Make safe work practical

Explain approved ways to handle information and report mistakes. Tailor training to actual duties and common failure points. [2]

Prepare incident handling

Define responsibilities for detection, analysis, containment and recovery. Preserve evidence and use lessons from incidents to improve the process. [3]

A documented historical case

In March 2019, a remote login system was used to shut down a Kansas water treatment plant and turn off a filter. The U.S. Department of Justice reported that investigators linked the intrusion to the phone of a former employee who had resigned that January. DOJ announced his guilty plea in October 2021. [4]

The case illustrates why former access relationships and remote access deserve scrutiny. The public release does not establish a specific account removal failure, water contamination or physical injury. An access lifecycle review is a practical lesson drawn here, not a finding attributed to DOJ.

Keep the operational priority specific

Identify the information or service at risk, the relevant access path and the action that reduces exposure while preserving evidence and fair review.

Read the evidence within its limits

A cost figure with the correct scope

The 2022 Ponemon study, sponsored by Proofpoint, reported about US\$15.4 million in average annual organizational costs associated with insider incidents. It did not report that amount as the average cost of one incident. The sample contained 278 organizations that had experienced material insider incidents. [5, 6]

This is a historical benchmark from a selected sample, not a current estimate for every organization or a measure of any one sector. Its definition includes credential theft. Do not treat it as a universal breach rate or compare it directly with a differently defined breach dataset.

Scope and method

This revision synthesizes public government guidance, a primary case account and an identified industry study. It contains no original dataset, interviews or empirical evaluation. The operational guidance is editorial synthesis rather than a tested assessment method. Historical evidence is dated explicitly; this is not a comprehensive review of current threat activity or a product performance evaluation.

PDF revision prepared on 26 October 2026 from the updated web report. The original report page was dated 1 April 2025.

References

- [1] [Insider Threat Mitigation Guide](#)
- [2] [How to protect your organization from insider threats](#)
- [3] [Security and Privacy Controls for Information Systems and Organizations](#)
- [4] [Kansas Man Pleads Guilty to Water Facility Tampering](#)
- [5] [2022 Cost of Insider Threats Global Report](#)
- [6] [Global Cybersecurity Study on the Cost of Insider Threats](#)