THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Insider threats - when the risk is already inside

Not every insider is malicious - most insider incidents are caused by negligence. We distinguish deliberate, negligent, and compromised insiders and show how cultural and technical measures work together.

min read: 7 min **Updated:** 14 March 2026 **Risk:** Medium risk
Source: awareness-as-a-service.com/en/resources/threats/insider-threats

What are insider threats?

Insider threats arise from people who have legitimate access to systems, data, or buildings - and who use that access in an abusive way, whether deliberately or not. The term covers three fundamentally different profiles:

Deliberate insiders act with malicious intent: they steal customer data before moving to a competitor, sabotage systems out of frustration, or sell access credentials to external attackers. These cases are dramatic but comparatively rare.

Negligent insiders are statistically more common: employees who send sensitive data to the wrong email address, lose a USB stick, use shadow IT services without checking them, or fall for a phishing email. There is no malicious intent - but the damage is real.

Compromised insiders often do not know they have become a tool: their credentials were stolen, their device infected with malware, or they were manipulated through social engineering into unwitting cooperation.

At a glance

01

Negligence is the dominant cause

In most insider incidents there is no criminal intent. Inadequate training, process gaps, and time pressure are more common causes than malice.

02

Insiders bypass the technical perimeter

An employee who is legitimately allowed to download data triggers no alert rules - even if they copy mass quantities shortly before resigning.

03

Early indicators are often cultural

Unusual behavior, social withdrawal, expressed frustration, or noticeable loyalty shifts often precede insider incidents by weeks.

How to recognise insider threats

Unusual data download
Mass downloads of customer data, contract documents, or IP - especially outside working hours or shortly before resignation or departure.

Access outside own role
A sales employee accesses development repositories; a support worker opens HR files. Unusual access patterns are early warning signals.

New privilege escalation
Accounts that suddenly acquire higher rights or submit access requests outside normal processes.

"Covering" for a colleague
Other employees helping someone explain or conceal their behavior - can indicate deliberate collusion or social pressure.

Abrupt loyalty shifts
Suddenly negative attitude towards the organization, mention of competitor offers, conspicuously new interest in sensitive areas.

USB use on locked-down systems
Attempts to move data through unauthorised routes (USB, personal cloud accounts, screenshots).

How to protect yourself

For employees

- **Report unusual behavior** - even when it concerns a trusted colleague. Speak-up channels exist precisely for situations like this.
- **Do not share credentials**, even within the team. Every employee should use their own account.
- **Use data only for legitimate purposes:** Customer or product data should be handed back - not taken - at the end of a project or upon departure.
- **Report shadow IT tools** rather than simply using them. IT departments can often provide fast solutions once the need is known.

For administrators

- **Apply least privilege consistently:** Restrict access rights to the minimum required for the role; conduct regular recertification.
- **Sharpen the offboarding process:** Revoke access on the last working day (not after), collect equipment, deactivate cloud accounts.
- **User and Entity Behaviour Analytics (UEBA):** Detect deviations from baselines (mass download, night-time access, unusual devices).
- **Data Loss Prevention (DLP):** Configure rules for the exfiltration of sensitive data via email, USB, and cloud uploads.
- **Establish a whistleblowing system:** A low-threshold, anonymous reporting channel for colleague behavior - compliant with applicable whistleblower protection law.

Real cases

CASE 01 · SOFTWARE COMPANY · DE · Q2/2025

A developer who felt passed over for a promotion systematically copied source code and customer configurations to personal cloud storage during his final two weeks. He joined a competitor and used the material for a competing product.

Damage: trade secret loss, litigation · **Detection:** UEBA alert on mass download three days after resignation notice · **Lesson:** DLP rules and UEBA could have stopped the exfiltration before it was complete.

CASE 02 · HOSPITAL · CH · Q4/2025

An administrative employee used the patient-data access of a retired colleague whose account had accidentally remained active for months. She sold patient profiles to a marketing company.

Damage: breach of medical confidentiality, fine, patient litigation · **Detection:** access log analysis by an external auditor · **Lesson:** The offboarding process should have deactivated the account on the last working day. Access reviews would have been a further safety net.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Revoke the affected account's access immediately** - do not wait for consultation; act at once.
2. **No confrontation without HR and legal:** Insider incidents carry employment law consequences that wrong procedure can make expensive.
3. **Forensic preservation** before device access: secure log data, event logs, and storage contents before the device is wiped.
4. **Determine the scope of access:** What was downloaded, when, and where did it go? This determines reporting obligations.
5. **Check GDPR/DSG notification requirements:** For data protection breaches, notification to the supervisory authority may be required within 72 hours.
6. **Consider a criminal complaint** - especially in cases of deliberate trade secret theft.

Frequently asked questions

Is monitoring employees legal?

Within limits and with restrictions. In Germany, the BDSG applies and the works council has co-determination rights. In Switzerland, the DSG applies. Behaviour-based anomaly detection (UEBA) is assessed differently under data protection law than continuous keystroke logging. A works agreement or staff regulations should provide the legal basis.

What is the difference between a deliberate and a negligent insider?

Deliberate: conscious intent to harm or self-enrich. Negligent: inattentiveness, process circumvention for convenience, poor judgement without malicious intent. Legally and interpersonally the difference is significant - but the technical countermeasures overlap considerably.

How do I address insider threats in a small team?

Through processes (dual control, access minimisation, offboarding checklists) and culture (open communication, psychological safety). Technology alone rarely works at small scale - trust and clear expectations matter more.

Related topics

Insider threats overlap with ransomware (compromised insiders as an entry point), data leaks through shadow IT, and social engineering (an external actor using an internal employee as a tool).