A REFERENCE FOR INTEGRITY MANAGEMENT AND INSIDER-THREAT PREVENTION

Preventing insider fraud

What the researchers recommend, based on an analysis of 36 insider fraud cases in US organizations.

The researchers analyzed 36 documented cases and 401 behavioural events, drawn from court documents, US Department of Justice releases and media reports. They found no uniform profile of the perpetrator, and almost half of the perpetrators held leadership positions. The fraud developed as a process in which human and technical behaviours were linked, and in some cases the perpetrators disclosed information about their activity before misusing systems or gaining unauthorized access.[1]

36
Fraud cases examined

401
Behavioural events

17/36
In leadership and management roles

The researchers base their recommendations on Situational Crime Prevention theory, which focuses on changing the conditions that make the offence possible.[1]

Recommendations for organizations

1. **Combine technical detection and reporting.** According to the researchers, detection may improve through automatic digital detection and also through reporting by people.
2. **Access control.** Limit employees to the privileges their role requires, to reduce opportunities.
3. **Technical monitoring.** Stricter monitoring of unauthorized system access. Automatic detection needs to go beyond identifying misuse of access privileges.
4. **Reporting culture.** Co-workers whom an insider tells about an intent to defraud need a safe space to report it.
5. **Communication analysis.** Monitor electronic communication for revelations of an offence. Natural language processing (NLP) to identify leakage of offending or of intent to offend could be part of the toolkit. Its effectiveness was not tested in the study.
6. **Contact with competitors.** Policies that restrict employee meetings with competitors, or detect secret meetings.
7. **Accountability of those who help.** Accountability should also extend to those who aid insiders, for example by sharing passwords or keeping them visible.
8. **Organizational transparency.** Appropriate announcements that insiders have approached certain organizations may encourage greater vigilance.
9. **Intervention points.** Further examination of the transitions between behaviours may help organizations identify points where they can intervene before damage is done.

The most frequent indicators in the cases examined

- False statements or reports: **77**
- Misuse of organizational systems: **20**
- Concealed conflict of interest: **10**
- Overseas travel: **9**
- Communications relating to the fraud: **50**
- Unauthorized access to data and systems: **15**
- Sold data or assets: **9**
- Problematic workplace behaviour: **9**

Number of occurrences, not number of employees. The same behaviour can occur several times in one case.[1]

The caveat

According to the researchers, the recommendations are derived from retrospective patterns and require evaluation before their effectiveness can be established.[1] The study is based on 36 publicly detected and documented cases from the United States, and it is not a predictive model. Financial difficulty, overseas travel, an external business relationship or a change in behaviour is not in itself evidence of malicious intent. Any monitoring or collection of information must be lawful and proportionate, protect employees' privacy and include human review of the findings.

The full review in the Knowledge Hub: **profcheck.co/knowledge/insider-fraud-behavioural-pathways**

Source

1. Whitty, M.T., Ruddy, C., Keatley, D. & Jamil, H. (2026). Insider threat detection: a socio-technical analysis of behavioural pathways in malicious insider fraud. Journal of Financial Crime, 1-19. CC BY 4.0. doi.org/10.1108/JFC-04-2026-0185