# Insider Threats: Balancing Trust and Security in Organizations

**TechRounder PDF Edition**

Live article: https://www.techrounder.com/business/insider-threats-balancing-trust-and-security-in-organizations/

By Vipin PG | Published November 21, 2023 | Updated January 4, 2026 | Format: Article | 4 min read

## In brief

Today, organizations face a delicate balancing act when it comes to insider threats. On one hand, they need to foster an environment of trust, empowering employees to collaborate and innovate.

Today, organizations face a delicate balancing act when it comes to insider threats. On one hand, they need to foster an environment of trust, empowering employees to collaborate and innovate. But on the other, they need robust security measures to protect critical systems and data from both intentional and unintentional insider risks.

It’s a complex issue with no easy solutions, requiring a layered approach that combines security awareness and technology.

## The Growing Threat of Insiders

Insider threats are on the rise. A recent report found that 90% of organizations feel vulnerable to insider attacks, which are becoming more frequent and damaging. The financial impact can be severe. According to the research, the average cost of an insider incident is $11.45 million.

What’s driving this upward trend? Some factors include:

Increased access to sensitive data: Remote work, bring your own device policies, and cloud storage give insiders greater access to company assets. Growth in third parties: Contractors, vendors, partners all pose risks that are difficult to control. Digital transformation: As companies digitize operations, more entry points emerge for insiders to exploit.

Clearly organizations must take insider threats seriously. But doing so raises difficult questions. How can companies protect critical assets while maintaining openness, collaboration and agility? Where should they draw the line between security and employee privacy?

## Striking a Balance

Organizations don’t have to choose between an authoritarian security regime and a free-for-all. With care, it’s possible to strike a balance - gaining visibility and control over insider risk without damaging company culture. Elements of a balanced approach include:

## Security Awareness Training

One of the most powerful tools is in-depth security training for all employees. Training should take a positive tone, avoiding fear-mongering. It should aim to foster a company-wide culture of shared responsibility towards security. Topics should cover:

- Social engineering red flags
- Safe internet usage
- Strong password practices

- Identifying and reporting suspicious activity
- Protecting sensitive data

Regular training keeps security top of mind, and empowers staff to be part of the solution. Gamification makes sessions engaging. And the human element enhances cyber resilience.

## Least Privilege Access

Limiting employee access to only what they absolutely need to do their jobs ("least privilege") is a foundation of insider threat mitigation. However, although most agree in principle, few put it into practice. In reality, overprovisioned access is commonplace.

How come? Partly due to the effort involved in defining and enforcing granular roles. And partly because it seems to conflict with the broader goal of empowering workers. But with modern identity access management (IAM) tools, least privilege access is easier to achieve. And rather than disempowering staff, it liberates them from dealing with unnecessary distractions.

## Multiple Layers of Protection

Preventing insider threats requires layers upon layers of overlapping protection. This includes:

Encryption: Making data unusable to unauthorized parties Data loss prevention: Monitoring and controlling data flows Access controls: Limiting access to apps, folders and files Privileged access management: Strict approvals for admin accounts Endpoint monitoring: Tracking detailed user activity

No one layer is impregnable. But combined, they greatly shrink the attack surface, drive up attacker cost and maximize the chance of early detection.

## Monitoring with Care

Some degree of user monitoring is essential to combat insider threats. But it’s important to implement monitoring ethically, with both transparency and privacy in mind.

Staff should be clearly informed if workplace systems are being monitored, and what is captured. Policies should focus monitoring only on protecting key assets, avoiding unnecessary privacy invasion. And data collection should always comply with local regulations.

Following such principles keeps monitoring targeted on security, not overbearing blanket surveillance. Wise use of AI can further enhance precision. Overall the aim is gain visibility where needed to combat real risks, while maintaining a trusting, empowering culture.

## Promoting Wellbeing

Among the most damaging insider attacks are those by disgruntled employees. Research shows that issues like stress, overwork and feeling undervalued can motivate sabotage.

Promoting staff wellbeing and fulfillment is therefore a key part of insider threat mitigation. Tactics like employee engagement programs, mental health support, flexible work options and diversity & inclusion initiatives help keep employees happy, healthy and invested in the company’s success.

When people feel treated with fairness and respect, they’re far less likely to do harm. Healthy security balances caring for employees with protecting from them.

## An Ongoing Challenge

There are no quick fixes for insider threats. They require an integrated strategy spanning technology, training and corporate culture. Security teams must partner with HR, IT and leadership to implement appropriate policies.

With care, organizations can both promote fulfillment and purpose for employees, and achieve robust protection for critical assets. But it takes an ongoing commitment. Insider risk management should be a regular boardroom agenda item, not a one-off exercise.

The inside threat landscape will keep evolving. As emerging risks like cloud misconfigurations arise, programs must be updated continuously. Through strong governance and executive buy-in, companies can maintain productive trust, collaboration and creativity, while keeping valuable data secure.

With some forethought, even small organizations can get the balance right. For instance, someone who often use a VPN for Omegle to access private chats securely says "We implemented common sense solutions like security training, 2FA, and limited share drives early on.

It let us stay nimble and innovative, without fear of insider attacks derailing our mission. If you build security in from the start, it becomes a natural part of operations, not a drag." There are always new threats, but with the right mindset and controls, companies can thrive while keeping risk in check.

## Final Thoughts

Insider threats present a growing danger, but with care, organizations can strike an effective balance between trust and security. Through layered controls, security awareness, promoting fulfillment, and governance, it’s possible to empower employees while protecting assets. There are challenges, but also huge opportunities to embed security thinking into company culture. With wisdom and foresight, business leaders can make their organizations both open and secure against evolving insider threats.

### References

1. cybersecurity-insiders.com - ninety-percent-organizations-vulnerable-insider-threats-according-new-cybersecurity-report - https://www.cybersecurity-insiders.com/ninety-percent-organizations-vulnerable-insider-threats-according-new-cybersecurity-report/#:~:text=Ninety%20percent%20of%20organizations%20feel,of%20information%20technology%20(35%25).

2. proofpoint.com - sites / default - https://www.proofpoint.com/sites/default/files/observeit/2020/02/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

3. safetydetectives.com - blog / best-vpns-for-omegle - https://www.safetydetectives.com/blog/best-vpns-for-omegle/