CSNP
CYBERSECURITY NON-PROFIT

Insider Threat Prevention Guide

A comprehensive framework for protecting your organization from internal security risks through awareness, prevention, and response.

CYBERSECURITY NON-PROFIT

Understanding Insider Threats

What Are Insider Threats?

Insider threats occur when individuals with authorized access to organizational resources intentionally or unintentionally compromise security, data, or operations.

These threats are particularly dangerous because insiders already have trusted access to sensitive systems and information, making detection more challenging than external attacks.

Why They Matter

Studies show that insider incidents account for a significant portion of security breaches and can be more costly than external attacks.

The average cost of an insider threat incident has risen to over $15 million per year for affected organizations, including investigation, containment, and recovery costs.

Types of Insider Threats

Malicious Insiders

Employees who intentionally steal data, sabotage systems, or harm the organization for personal gain or revenge.

Negligent Insiders

Well-meaning employees who accidentally cause security incidents through carelessness, lack of training, or poor security hygiene.

Compromised Insiders

Employees whose credentials have been stolen by external attackers, unknowingly facilitating unauthorized access.

Each type requires different prevention and detection strategies. Understanding these categories helps organizations tailor their security approaches effectively.

Warning Signs to Watch For

Behavioral Changes

- Sudden disgruntlement or conflicts with management
- Working unusual hours without clear business need
- Excessive interest in matters outside their role
- Financial difficulties or lifestyle changes

Access Pattern Anomalies

- Accessing files or systems unrelated to job duties
- Downloading large amounts of data
- Using unauthorized devices or storage media
- Attempting to bypass security controls

Policy Violations

- Repeated security policy breaches
- Unauthorized sharing of credentials
- Disregard for data handling procedures
- Resistance to security training or compliance

Core Prevention Strategies

01

Build a Security-Aware Culture

Regular training, clear policies, and leadership commitment create an environment where security is everyone's responsibility.

02

Implement Least Privilege Access

Grant employees only the minimum access needed for their roles, reducing potential damage from compromised accounts.

03

Establish Clear Policies

Document acceptable use, data handling, and security procedures that all employees must acknowledge and follow.

04

Foster Open Communication

Encourage reporting of suspicious activities and create channels for employees to raise security concerns safely.

Access Control Measures

Multi-Factor Authentication

Require additional verification beyond passwords for accessing sensitive systems and data.

Role-Based Access Control

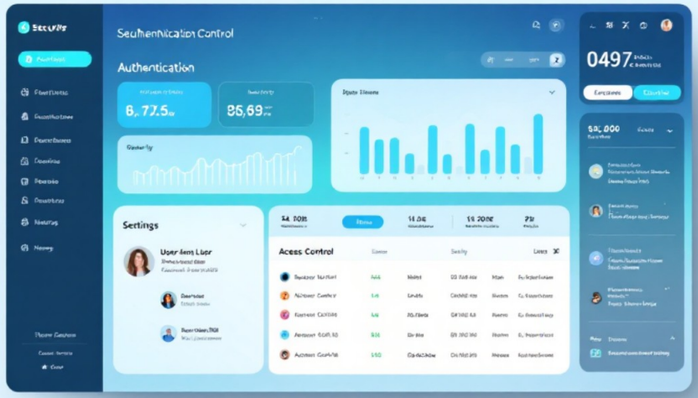
Assign permissions based on job functions with regular reviews and updates as roles change.

Privileged Access Management

Strictly control and monitor accounts with elevated permissions through secure vaults and session recording.

Regular Access Reviews

Quarterly audits ensure permissions remain appropriate and remove unnecessary access promptly.



Pro Tip: Implement automated access reviews that flag dormant accounts and excessive permissions for immediate attention.

Monitoring and Detection

User Activity Monitoring

Track file access, system logins, and data transfers to identify unusual patterns that may indicate threats.

Behavioral Analytics

Use AI-powered tools to establish baseline behaviors and alert on deviations that suggest malicious activity.

Audit Logging

Maintain comprehensive logs of security events for investigation and compliance, with tamper-proof storage.

Effective monitoring balances security needs with employee privacy. Ensure transparency about what is monitored and why, and comply with all applicable privacy laws and regulations.

Secure Termination Procedures

1

Pre-Termination Planning

Document all access rights and assets assigned to the employee. Coordinate with IT and security teams.

2

Immediate Access Revocation

Disable accounts, collect devices, and revoke physical access simultaneously during termination meeting.

3

Asset Recovery

Retrieve all company property including devices, badges, keys, and ensure data is properly secured.

4

Exit Monitoring

Monitor for unusual activity in the weeks before and after departure, especially data downloads.

Incident Response and Prevention Checklist

When an Incident Occurs

- **Contain the threat**

  Immediately isolate affected systems and revoke suspect access

- **Preserve evidence**

  Document all activities and maintain forensic copies of relevant data

- **Investigate thoroughly**

  Determine scope, impact, and root cause of the incident

- **Communicate appropriately**

  Notify stakeholders, legal, and potentially law enforcement

- **Remediate and improve**

  Fix vulnerabilities and update policies based on lessons learned

Essential Prevention Checklist

- Comprehensive security awareness training program
- Written and acknowledged security policies
- Multi-factor authentication on all systems
- Regular access reviews and privilege audits
- User activity monitoring and behavioral analytics
- Data loss prevention tools deployed
- Secure offboarding procedures established
- Incident response plan tested and documented
- Anonymous reporting channel for concerns
- Regular security risk assessments

About Cybersecurity Non-Profit

> Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety
- Senior Digital Safety
- Women's Security
- Parents & Educators

100% Free Resources

All our educational materials, training programs, and security resources are completely free and accessible to everyone in our community.

Visit us: csnp.org

Resources: csnp.org/resources