Insider abuse can take in the following forms:

1. Unapproved hardware/software.
2. Remote **access** to sensitive data.
3. Data leakage through USB devices.
4. Unauthorized deletion of data.
5. Hijacking or **abuse** of admin accounts.
6. Unauthorized application usage.
7. Unauthorized **access** to shared folders.

Data breaches resulting from human error often result from the following scenarios:

- Weak passwords
- Falling for phishing scams while at work (clicking on unsafe attachments, visiting suspicious websites, etc.)
- Sending sensitive info to the wrong recipients
- Use of personal smartphone or laptop using the organization's network
- Accidentally publishing private information to the Internet
- Improper disposal of documents
- Failure to use encryption
- System misconfiguration
- Leaving computers unlocked
- Poor patch management

What You Can Do to Guard Against Human Error and Insider Abuse

Fortunately, you can implement the following straightforward tactics to reduce insider abuse threats and human error in your small business or across your entire enterprise.

1. Start by setting strong password requirements.
2. Assess your existing system configurations and perform firewall audits. During these audits, look for security loopholes and set up access controls.
3. Set up a network analyzer or content-based filtering to monitor data that's shuffling back and forth on your network. Take note that this may not work for encrypted data.
4. Secure internal wireless networks through proper encryption and authentication.
5. Monitor employees who are about to leave the organization and potentially take data with them. Implement a strict employee exit strategy.

6. Audit activities of employees who have access to sensitive data. Also, be careful about providing access privileges.
7. Identify portable devices and require registrations for BYODs (Bring Your Own Device).
8. Set up a rigorous process on how to dispose of trash.
9. Perform background checks and screenings of your employees. Evaluate contractors and third-party vendors.
10. Set up financial assistance programs for employees to ward them off from insider abuse for financial gain.
11. Educate employees about security. Send regular emails on best practices to avoid data breaches and encourage other employees to report suspicious activities.
12. Establish checks and balances for access to confidential info.
13. Install continuous file integrity monitoring (FIM) software to detect malicious or unusual insider activity.

Best-of-Class FIM for Insider Abuse Detection

When choosing an FIM tool to safeguard your network from insider abuse and human error, ensure that it performs better than the average FIM software out there. The key word here is **average.**

While most solutions can detect changes in your files and operating systems, the average FIM tool cannot detect administrative user actions. In a nutshell, it is best to opt for an FIM tool that will allow you to detect changes in the software itself and adjust settings where you can disable admin users from altering features in the FIM who can potentially cover up insider abuse.

CimTrak is one of the few FIMs available today with an audit trail that cannot be altered by users. With real-time monitoring of admin and privileged user actions, insiders will not be able to hide malicious activities and internal threats are reduced significantly. Possible human errors are also tracked.

To start protecting your assets from insider threats and human errors, get your free demo of CimTrak today.

What is system penetration?

According to the Committee on National Security **Systems**, **penetration** testing is "Security testing in which evaluators attempt to circumvent the security features of a **system** based on their understanding of the **system** design and implementation." Servers that hold critical information should be **penetration** tested.

What is meant by penetration testing?

Penetration testing, also called **pen testing** or ethical hacking, is the practice of **testing** a computer system, network or web application to find **security** vulnerabilities that an attacker could exploit. ... The main objective of **penetration testing** is to identify **security** weaknesses.

How is penetration testing done?

Penetration testing in simple terms is a simulation of a process a hacker would use to launch an attack on a business network, attached devices, network applications, or a business website. The purpose of the simulation is to identify security issues before hackers can locate them and **perform** an exploit.

What are the different types of Pen Test?

- External network penetration test. An external network penetration test is typically what most people think of when talking about pen testing. ...
- Internal network penetration test. ...
- Web application penetration test. ...
- Social Engineering.
  What is the goal of penetration testing?
  The purpose of a **penetration test** is to explore your business from the perspective of an attacker and, most importantly; to discover and understand the various weaknesses that may be in your environment and how to protect your business from them.
  What is penetration testing with example?
  A Complete **Penetration Testing** Guide with **Sample Test** Cases. It's the process to identify security vulnerabilities in an application by evaluating the system or network with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack.

The Top Pen Testing Tools Today

- The Network Mapper (also known as “NMAP”)
- Metasploit.
- Wireshark
- The Web Application Attack and Audit Framework (also known as the “W3AF”)
- John the Ripper.