Click Thinking Spotlight

Insider Threats

Insider threats are a serious concern for any business that can cause financial harm, tarnish brand reputations and erode customer and shareholder trust. So, it's important to understand these potential risks.

- Insider threats come from people within or associated with a company, such as current and former employees, contractors and business associates.
- These individuals have access to systems and information that make running the business possible. While most use this access responsibly, some don't. Although their motivations may differ, any insider threats can cripple your business.
- Careless users bypass security procedures for reasons of convenience or laziness. To them, protocols are a hassle or a waste of time. Examples include employees who fail to lock their devices when not at their desks. Or those who leave written passwords on hand because memorizing them takes too much effort.
- Compromised users are typically victims of spear phishing attacks or social engineering attempts. More often than not, they don't realize they've been compromised until after the damage is done. Examples include the employee who clicks a link in a phishing email that triggers a ransomware attack. Or the accounts payable associate who's tricked into wiring money to a fake account.
- Malicious users may be motivated by greed, a desire for revenge, ideology or any number of other reasons. Because they're highly motivated and can cover their tracks while they work, malicious users have the potential to do significant harm to a company over an extended time period. Examples are the foreign national who takes a contracting position and sends proprietary information back to homeland operatives. Or the IT manager who profits by selling customer account information to criminals.
- While it's impossible to eliminate all insider threats, there are things a company can do to mitigate them, including training or penalties for careless use resulting in a breach. Technology such as firewalls and anti-phishing software can flag harmful emails that might otherwise compromise users.
- Although malicious users are harder to detect, there are signs that indicate they may be at work. These include large data transfers, unexpected or incorrect access requests, multiple failed logins, service account abuse, new activity on dormant accounts, off-hour network traffic and interactions with unfamiliar users or locations. Unexpected financial gains indicating an employee may be selling company secrets is also a sign.

For the Insider Threats module, see your manager or information security contact.