PCnet
total IT management

INSIDER THREATS:
SPOTTING THE COMMON WARNING SIGNS

According to Verizon, **around 33% of all data breach incidents can be attributed to insider threats.** To protect your business from insider attacks, it is critical that your entire organization understands what these threats are and learn how to spot or identify the common indicators and warning signs before it's too late.

WHO POSES AN INSIDER THREAT?

Anyone with privileged access to or inside knowledge of your company's data or information assets, infrastructure and operational strategies could pose a potential security threat.

COMPROMISED OR EXPLOITED INSIDERS

A user whose authorized or privileged credentials were captured via a phishing email or any other breach and used to gain access.

Around *50%* of breaches are caused by credential theft and social engineering.[2]

MALICIOUS AND CRIMINAL INSIDERS

Insiders using authorized access to steal/expose sensitive data or deliberately damage/destroy critical systems to intentionally harm the business or for personal gain.

NEGLIGENT OR CARELESS INSIDERS

A user with no aim to steal or jeopardize the business but who unintentionally exposes the company to security risks for the sake of productivity or efficiency.

80% of organizations report sensitive data being put at risk due to the wrong recipient being added on an outbound email.[5]

EXTERNAL OR THIRD-PARTY INSIDERS

Independent or third-party partners, vendors and contractors with access to internal systems and data assets or those who have 'inside' knowledge or information.

MOTIVATIONS BEHIND INSIDER ATTACKS

FINANCIAL/GREED

Around 65% of breaches are financially motivated.[2]

ESPIONAGE/COMPETITIVE ADVANTAGE

A departing Google engineer once stole approximately 14,000 confidential files, some of which included proprietary trade secrets. He then created a startup of his own that was later purchased by Uber.[3]

REVENGE/DISGRUNTLED EMPLOYEE

A former Cisco employee purposely deleted virtual machines that caused $1.4 million in damages and disruptions.[4]

IDEOLOGICAL/POLITICAL OBJECTIVES

We can't forget Edward Snowden, The Panama Papers or the DNC Email Exposures.

PRIMARY BUSINESS ASSETS AT RISK

CONSEQUENCES & COSTS

- Exposed Customer Data/Lost Trust
- Brand and Reputation Damage
- Financial Losses/Costs
- Regulatory Compliance Fines & Penalties
- Disclosure of Corporate IP or Trade Secrets

38% of organizations experienced a loss of critical data or operational disruptions/outages; *24%* suffered brand damage; *24%* faced legal or non-compliance liabilities; *18%* suffered direct loss in revenues.[6]

SPOTTING THE WARNING SIGNS & INDICATORS

While insider threats are often the hardest to detect, there are some common digital and behavioral indicators you should be monitoring for:

BEHAVIORAL INDICATORS:

- Repeated attempts to bypass security controls or hide or camouflage activities
- Working or logging in frequently during 'off-hours' or the middle of the night
- Displaying disgruntled behavior often or for a long period of time
- Acting odd, withdrawn or anxious with colleagues or management

DIGITAL INDICATORS:

- Obtaining or hoarding large amounts of data
- Searching for and saving sensitive or protected data
- Accessing or requesting access to data assets not associated with their job functions
- Using personal or unauthorized portable storage devices (USB, SD Cards)

PROACTIVE DEFENSE:
SECURITY & RISK MANAGEMENT PROGRAM

Securing your IT environment from insider threats starts with securing your critical assets, enforcing clear IT security policies, increasing your IT visibility and promoting a culture of change. This is the only way to mitigate and prevent insider threat incidents.

Our team has the specialized tools and experience in IT, Cybersecurity and Data Protection that can bring you peace of mind by securing your IT environment from both insider threats, unintentional or otherwise, and growing external threats.

Contact Us Today to Protect Your Business from Insider Threats!

Sources:
Verizon 2020 Data Breach Investigations Report | Google's Insider Threat Pleads Guilty | Ex-Cisco Engineer Pleads Guilty in Insider Threat Case | 2020 Outbound Email Data Breach Report (Egress) | Bitglass 2020 Insider Threat Report

PCnet
total IT management
sales@pcnetinc.com
417-831-1700
2026 E Phelps St.
Springfield, MO 65802