CYBERSECURITY

Insider Threats

What is Insider Threats?

- An insider threat is a security risk that originates from within the targeted organization
- Disgruntled and/or former employee who gains access to sensitive information with the network and misuses that access

TYPES OF INSIDER THREATS

Intentional threat – someone who takes action to harm an organization for personal benefit or out of malicious intent

Unintentional threat – someone who unintentionally or accidentally exposes the organization to threats

A mole – someone from the outside who has gained access to a privileged network by posing as a trusted employee

How to Protect Against Insider Attacks

Conduct regular risk assessments to understand the potential impact of insider attacks

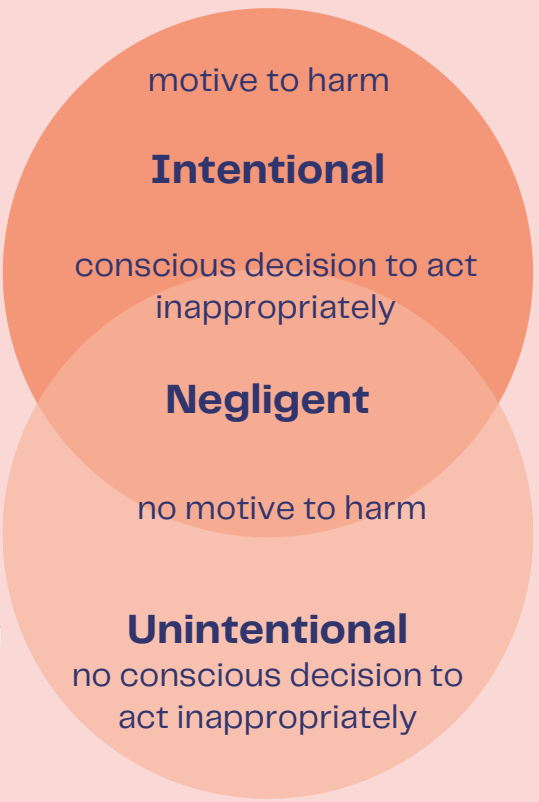
Provide regular security awareness training for all staff

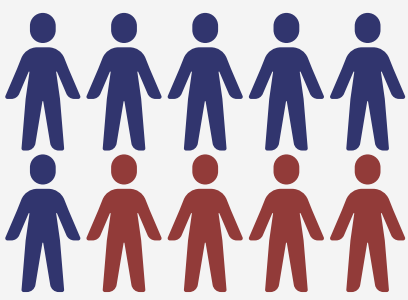
Closely manage the accounts and privileges of all employees and contractors

Perform penetration testing at least annually to help identify security improvements

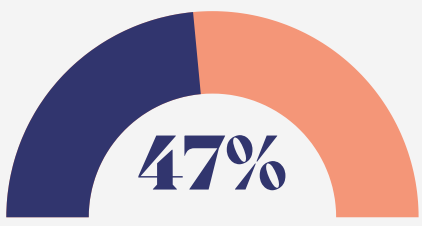
Commission a simulated phishing assessment

Implement 24/7 network and endpoint monitoring to detect anomalous behavior

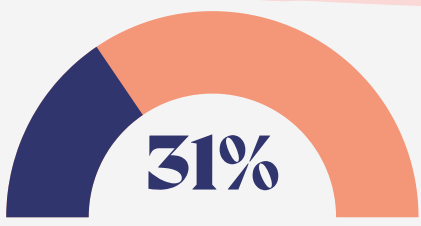




60 PERCENT OF DATA BREACHES ARE CAUSED BY INSIDER THREATS



SINCE 2018, THE NUMBER OF INSIDER SECURITY INCIDENTS HAS RISEN BY 47 PERCENT



SINCE 2018, THE COST OF INSIDER THREATS HAS RISEN 31 PERCENT

References CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY; U.S. DEPARTMENT OF HOMELAND SECURITY; SECURITY INTELLIGENCE