PREPARING FOR INSIDER THREATS

WHAT IS AN INSIDER THREAT?

Someone who could intentionally or unintentionally harm the organization

Types of Insider Threats: Malicious, Negligent, Compromised

Frequency and cost of insider threats is increasing.

INDICATORS OF INSIDER THREATS

May be difficult to recognize because we want to trust people.

Behavior Indicators

Technical Indicators

PREVENTING INSIDER THREATS

Employee training and awareness programs

Implementing robust security & personnel policies

Implementing access control measures

Performing regular audits and monitoring

Adding Data Loss Protection strategies

Designing a thorough backup and recovery program

DETECTING INSIDER THREATS

Using technology to detect insider threats

Monitoring employee behavior

RECOVERING FROM INSIDER THREATS

Personnel, Technical, Legal & Regulatory

Remember: An insider threat is not simply a technical event.

BUILDING A CULTURE OF SECURITY

Encourage a security-first mindset

Promote open communication and reporting

Reward good security practices