

Insider Threat

An 'insider' is a person who exploits, or has the intention to exploit, their legitimate access to an organization's assets or operations for unauthorized purposes.

An insider could be a full-time or part-time employee, a contractor or a business partner. They could deliberately seek to join an organization to conduct an insider act, or may be triggered to act at some point during their employment. Employees may inadvertently trigger security breaches through ignorance of rules, or deliberate non-compliance.

COMPONENT

OWNERSHIP & GOVERNANCE

THREAT

Positive and visible management support for protective security is vital to demonstrate to staff the value placed on security policies and procedures:

- · It will deter employees who may wish to harm an organization by creating an open and transparent organizational framework
- · Active promotion of the security related responsibility of all staff
- A proportionate, multi-disciplinary approach to countering insider threats

COMPONENT



Types of insider

- Exploited/recruited insider: individuals who are identified by a threat actor as having desirable access or information and who are likely to be influenced or persuaded
- Volunteer/self-initiated insider: individuals who are motivated to exploit their access to company information for their benefit. The nature of this motivation can be varied
- Deliberate insider (infiltrator): individuals who are engaged by a threat actor prior to their joining of a target organization
- Accidental insider: employees who inadvertently trigger security breaches through ignorance of rules, or deliberate non-compliance

Motivations of insiders

Motivations can be complicated and contradictory. Several categories can be identified:

- Ideology and desire for recognition: individuals may be motivated by issues relating to political, nationalistic or religious views
- Financial gain: individuals may be motivated by monetary benefits
- **Disgruntlement (revenge)**: individuals may have become unhappy with the organization they work for and seek to damage it as a reprisal or to improve their circumstances
- Coercion: insiders may also be unwilling individuals who are being coerced into cooperation with a threat actor
- Unwitting insiders: not all individuals are deliberately motivated to assist threat actors. Threat actors may pretend to be someone they are not to deceive an individual into assisting them

RISK ASSESSMENT

COMPONENT



Potential insider activity

Five main types of activity:

- Unauthorized disclosure of information Process corruption
- Facilitation of third parties access to an organization assets and information
- Physical or IT system sabotage

There is a clear link between an insider threat and exploitable weaknesses in an organization security and management processes:

- Poor management practices
- Poor use of auditing functions
- Lack of protective security controls
- Poor security culture

Vulnerabilities

- Lack of adequate role based personnel security risk assessment
- Poor pre-employment screening
- Poor communication between business areas
- Lack of awareness of people risk at a senior level
- Inadequate corporate governance

Understanding what security risks an organization faces is essential for

developing adequate security mitigation measures:

- Identification of critical assets
- Identification of threat
- · Assessment of the impact
- Assessment of the likelihood
- Adequacy of existing counter measures
- · Assessment of the residual risk
- Addition of new measures to mitigate the risk

COMPONENT



RISK MANAGEMENT

Insider threat risk management should be a system of policies and procedures which aim to:

- Reduce the risk of recruiting staff who are likely to present a security concern
- Minimise the likelihood of existing employees becoming a security concern Reduce the risk of insider activity, protect the organization's assets
- Carry out investigations to resolve suspicions or provide evidence for disciplinary procedures
- Implement security measures in a way that are proportionate to the risk

COMPONENT



MONITORING & ASSESSMENT

Monitoring and assessment is an essential element of managing the insider threat. Effective line management is essential in both detecting and

COMPONENT



Governance and Leadership

Positive and visible top down leadership is a critical element for success

Insider Risk Assessment

There is a clear link between and individual with opportunity and an exploitable weakness

Pre-Employment Screening

Comprises the procedures involved in deciding an individual's suitability to hold employment. It is not limited to 'new joiners', but also individuals who are moving between jobs within an organization.

A suitable level of screening should be applied to all individuals who are provided access to critical information.

Monitoring and Assessment of Employees

IMPLEMENTATION

Effective leadership and good line management is an essential in preventing, managing and detecting disgruntled personnel

Investigation and Disciplinary Practices (Response)

The primary duty for an investigator is to establish the true facts, whilst adhering to appropriate HR policy and employment laws by:

- Identifying and analyzing the root cause of the incident
- Identifying the appropriate disciplinary actions or interventions that are needed
- Assessment of the effectiveness of current control measures
- Identifying gaps in current practices • Developing more effective control measures
- reduced by encouraging employees to think and to act in a more security conscious ways
 - Employees are more likely to report behaviours and activities of concern

The risk of security incidents and breaches is

Security Culture and Behaviour Change

component of a functioning security management system and helps to mitigate against insider

An effective security culture is an essential

• Employees are engaged with, and take

• Level of compliance with protective security

responsibility for, security issues

measures is high

threats: