INSIDER THREAT: MOTIVATION, MANIFESTATION AND MANAGEMENT IN AN ORGANISATION

Freedom C ONUOHA

Department of Political Science

University of Nigeria

Nsukka

freedom.onuoha@unn.edu.ng

chufreedom@yahoo.com

Paper presented at *3rd Annual Security Executives Converge*, workshop on "Organizational Security-A Panacea to Peacebuilding and National Development", Sheraton Hotels, Ikeja, Lagos, 21 -24 October 2019

Introduction

- The assurance of security is a fundamental pre-occupation of almost every entity – individual, organisation, group, community, and state
- The omnipresence of threats to security and integrity of people, assets and data exists in both the physical and virtual worlds.
- While organisations differ substantially, what they all have in common is people - all of whom have the potential to be an insider threat
- According to a 2018 report, “a malicious insider threat can cost an organization $2.8m per year, or an average of $604,092 per incident.”

Aim

Highlight the nature and forms insider threat may assume and the risk it poses to organization and national security

Scope of Presentation

- Introduction
- Conceptual Clarification
- Nature, Forms and Manifestation of Insider Threat
- Motivations behind Insider Threat in an Organisation
- Overview of Manifestation of Insider Threat in Nigeria
- Managing Insider Threat in an Organisation
- Some Best Practices in Managing Insider Threat
- Conclusion

Conceptual Clarification

❑ Insider

Someone who has been given a role within an organization and has access to premises and/or internal systems and information

Tagg, 2014:8

Attributes of an Insider

- Risk
- Skills
- Access
- Process
- Motivation
- Knowledge

Conceptual Clarification

❑ Threat

Threat as capability **X** intention. *Capability* refers to the ability of a threat agent to exploit the vulnerabilities in the system or environment in order to manifest certain intentions. *Intention* on the other hand is the underlying motive, goal, purpose, or aim of any action. *Vulnerabilities* are the opportunities, channels or means exploited by threats to harm or affect the entity

Cleary, 2006:38

- ❑ Individual
- ❑ Group
- ❑ Organisation
- ❑ state

Conceptual Clarification

❑ Insider Threat

The potential for an individual who has or had authorized access to an organization's assets to use their access, either *maliciously* or *unintentionally*, to act in a way that could negatively affect the organization or national security

Luckey, *et al.* 2019:9

Insider threats has the potential to undermine the integrity, survivability and security of data, information, technology, facilities and people

Nature of Insider Threat in an organisation

Nature of insider threat

- National security espionage
- Stealing sensitive information
- Sabotaging (data, systems, or networks)
- Causing physical harm in a workplace
- Cyber attack
- Fraud

Manifestation of Insider Threat in an Organisation

Two main domains an insider threat occurs

Offline

Online

Interaction

Physical World

Virtual World

Nature, Forms and Manifestation of Insider Threat

Three main categories of insider threat

Compromised

Threat actors who have stolen a legitimate employee's credentials pose as authorized users, utilizing their accounts to exfiltrate sensitive data. Employees often don't know they have been compromised.

Negligent

Employees without the proper security awareness training can inadvertently misuse or expose confidential data, often as a result of social engineering, lost/stolen devices or incorrectly sent emails/files.

Malicious

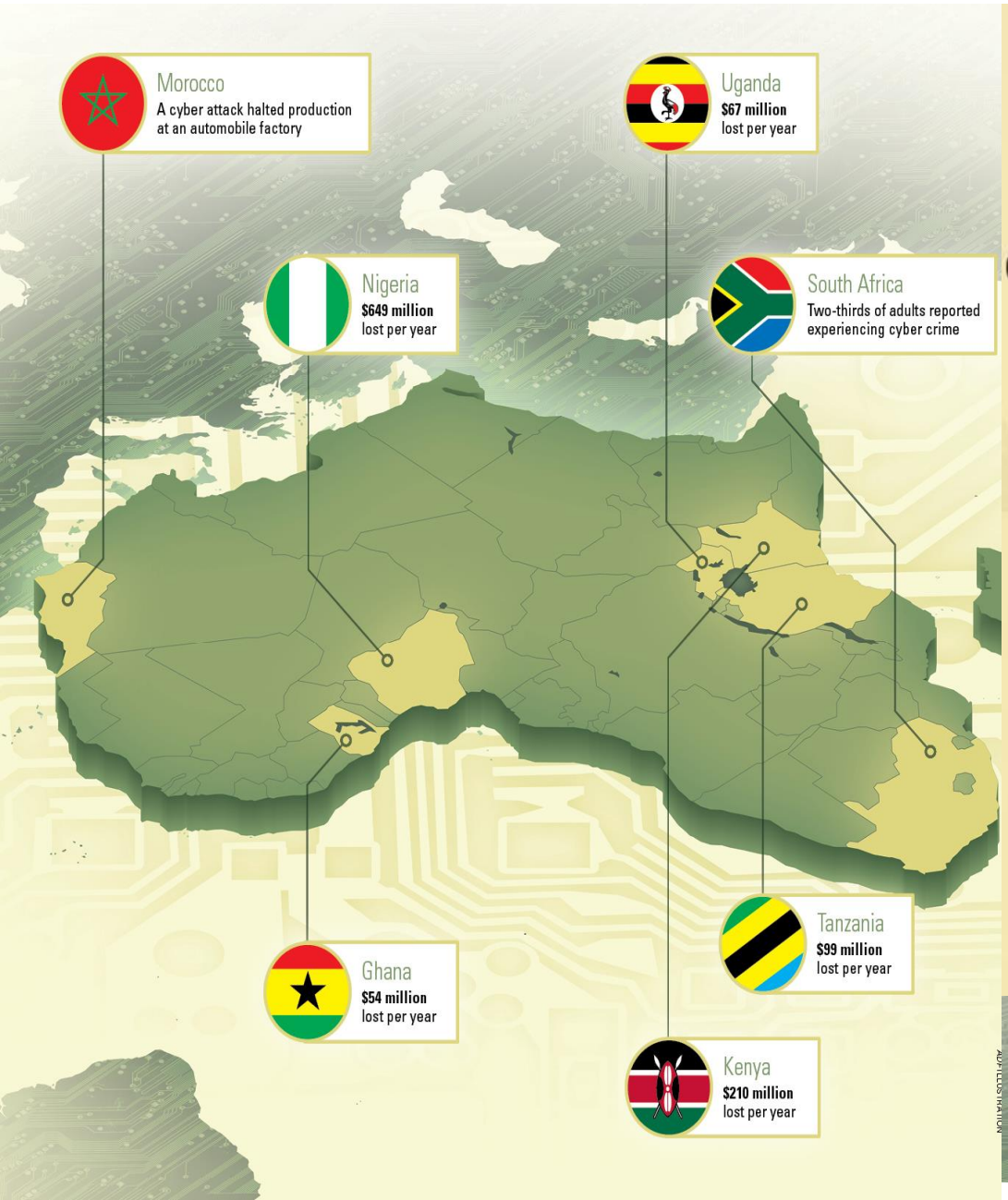
Bad actors—such as current or former employees, third parties or partners—use their privileged access to steal intellectual property or company data for fraud, sabotage, espionage, revenge or blackmail.

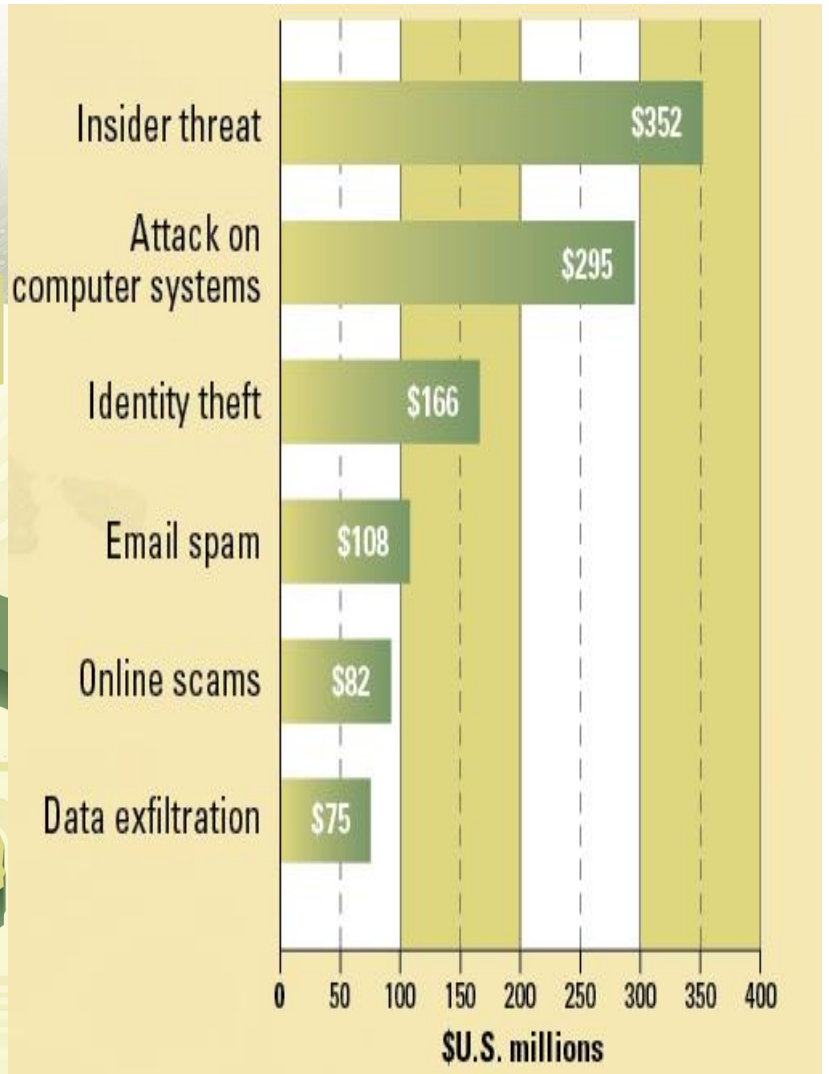
Motivations behind Insider Threat in an Organisation

Some known factors behind insider threat

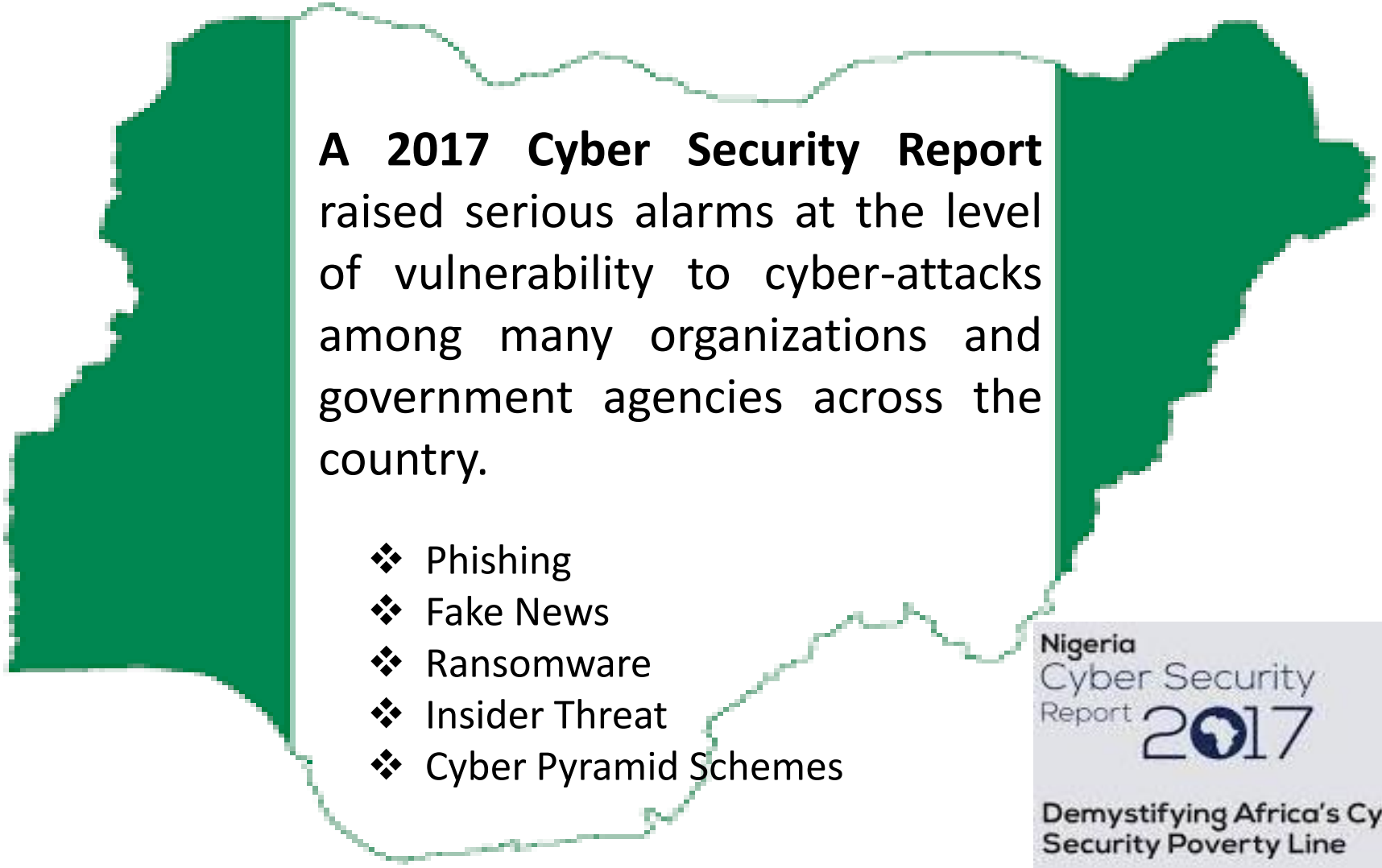
- Revenge
- Financial gain
- Political beliefs
- Response to blackmail
- Desire for recognition and power
- Loyalty to others in the organisation

The most Common Types of Attacks in Africa and Their Cost





Manifestation of Insider Threat in Nigeria



A 2017 Cyber Security Report raised serious alarms at the level of vulnerability to cyber-attacks among many organizations and government agencies across the country.

- Phishing
- Fake News
- Ransomware
- Insider Threat
- Cyber Pyramid Schemes

Nigeria Cyber Security Report 2017

Demystifying Africa's Cyber Security Poverty Line

It revealed that **insider threat** from workers and management of organisations tops the cost of cybercrimes in Nigeria.

Manifestation of Insider Threat in Nigeria

❑ Aviation Sector

Acts of terrorism, drugs and weapons smuggling, fraud, and sabotage are just a few of the types of incidents that can threaten aviation security

The fact that insiders are granted trusted access to aircraft, equipment, and critical airport infrastructure, coupled with the fact that insiders possess intimate knowledge of business operations, enables them to easily identify and exploit vulnerabilities to carry out malicious acts or criminal activity

Manifestation of Insider Threat in Nigeria

❑ Aviation Sector

Date	Description of Security Breach	Insiders	Remarks
24 December 2018	Planting of tramadol in a bag belonging in Zainab Aliyu's bag	Umar Shehu, Sanni Suleiman, Nuhu Adamu, Rhoda Adetunji, Udosen Itoro Henry and Sanni Hamisu	The six insiders are all workers at MAKIA
24 August 2015	Arrest of Chika Egwu Udensi, a senior flight attendant of Arik Air, with 20kg of cocaine at Heathrow Airport by the UK Border Force on arrival from Lagos	Ikechukwu Chibuzor Oliver (Arik Air employee)	Mr Oliver helped Mr Udensi get the cocaine of a potential street value of £2.46 million onto the flight. Mr. Udensi aile for 6 years
21 May 2013	Arrest of two Arik Air cabin crew staff at the Heathrow Airport, London, for being in possession of 6kg of cocaine and 60 packets of cigarettes.	Temitayo Olubunmi Daramola and Delita Abibimgbi	The arrest of the suspects made it the second time in 18 months that staff of the airline have been arrested in London for drugs-related offences.

Manifestation of Insider Threat in Nigeria

❑ Financial Sector

In March 2019, for instance, a marketing agent of a bank in Matori (Lagos State) was arrested by the police for allegedly diverting N3,441,000 from the savings of one of the bank's customers

A report of the NDIC revealed that bank workers in Nigeria committed 37,817 fraud cases in 2018 where they stole N26.182billion. Of the number, a total of 899 workers were involved in fraud and forgery cases in 2018 compared to 320 in 2017.

Manifestation of Insider Threats in Nigeria

❑ Security and Defence Sector

In November 2008, the Major and five other soldiers of the Nigerian Army involved in the arms deal were jailed for life by a court martial.

A Major, who is one of the officers in charge of the Central Ordinance Depot, Kaduna, had over N220 million in his account while a Colonel involved in the matter had about N100 million in his own account. Nine of the non-commissioned officers attached to the ordinance depot had various sums ranging from N50 million, N20 million to N10 million in their accounts

Manifestation of Insider Threat in Nigeria

❑ Household Sector

Kidnapping for Ransom

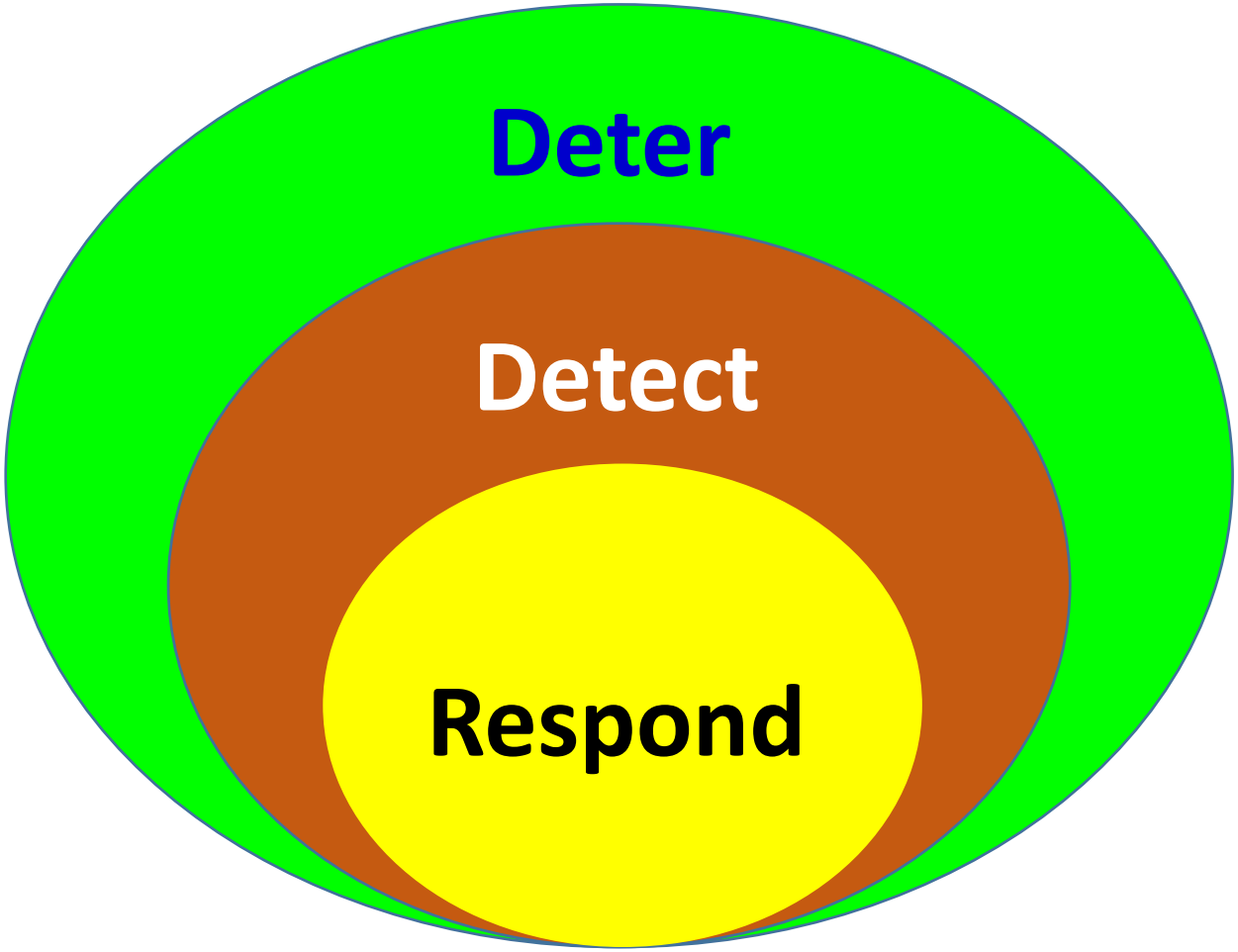
The kidnapping and eventual murder of Dr Edith Chinedu Aliyu, proprietress of Chelson Group of Schools and Chief Executive Officer of Grant Microfinance Bank

The insider threat involves a situation where someone who lives or is closely associated with the potential victim plays an active role by initiating, participating, directing or enabling the kidnapping of such targets. Such insider could be the relative, driver, cook, gatekeeper, nanny, business associate, confidant, or any other person who is reasonably in close contact with the potential target

Measuring the Cost of Insider Threat

- ❑ Loss or damage to life
- ❑ Loss or damage to data
- ❑ Loss or damage to finance
- ❑ Loss or damage to property
- ❑ Loss or damage to credibility
- ❑ Loss or damage to reputation

Managing Insider Threat in an Organisation



- **Deter:** Proactive security hygiene measures to prevent attacks
- **Detect**: Identification measures to timely uncover attacks
- **Respond:** Attentive measures to counter or contain attacks

Managing Insider Threat in an Organisation

❑ *Preventing Insider Threat*

- Deploying a robust employee screening
- Conducting regular mandatory employee training
- Executing vendor risk assessments and security protocol
- Maintaining controlled access points to only necessary personnel
- Ensuring sensitive/proprietary info is adequately protected
- Providing robust ways for employees to report concerns
- Proactively monitoring employee activity (signs of red flags)
- Regular monitoring and assessment of privileged functions

Managing Insider Threat in an Organisation

❑ *Detecting Insider Threat*

- ❖ Look out for unexplained financial gain
- ❖ Investigate all cases of abuse by service accounts.
- ❖ Investigate any case of multiple failed logins.
- ❖ Pay attention to large data or file transfers
- ❖ Review recorded past routines to check yellow and red flags

Managing Insider Threat in an Organisation

❑ *Responding to Insider Threat*

- ➢ Emplacing a process to investigate and document
- ➢ Commitment to responding based on evidence
- ➢ Maintaining a culture or rapid response - Act quickly.
- ➢ Be prepared to restore leveraging backup depository
- ➢ Deploy appropriate disciplinary measures

Best Practices and Lessons Learned

- ***Background Check***: Everyone has the potential to do harm, therefore conducting at least minimal background checks on employees helps to mitigate the risk of hiring persons who may likely turn out to be malicious insider.
- ***Continuous Evaluation****:* Continuous evaluation is a vetting process to review on an ongoing basis the background of an individual who has been determined eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility.
- ***Deploy Appropriate technology*****:** Some of the same tools used for detecting external attackers - including data loss prevention and user and entity behaviour analytics software - can also help sniff out insider threats.
- ***Adopt Enforceable and Realistic Compliance Policies***: Set enforceable and realistic security and compliance policies. People need to know what behaviours are acceptable or unacceptable.

Best Practices and Lessons Learned

- ***Routine Vulnerability Assessment:*** Another strategy of preventing and detecting insider threat is for an organisation to conduct comprehensive routine vulnerability and risk assessment of its facilities, networks, system and operations to possibly identify loopholes that insiders could exploit.
- ***Good Workforce Management and Supervision*** – Understanding the users who hold the potential for greatest damage is critical. Monitoring information technology administrators, top executives, key vendors, and at-risk employees with greater vigilance.
- ***Promote Security Awareness culture:*** The promotion of security situation awareness culture, both offline and online, is important in containing insider threat. Situational awareness will make them become more cognisant of the ever-evolving ecosystem of physical and cyber spaces

Conclusion

- The world is becoming increasingly complex and interdependent, with increased risks to both physical and online assets
- As the world becomes more globalised, the threat from insiders is likely to increase in the near term
- While insider threats in the physical domain will persist in the foreseeable future, it is the virtual or online space that would most likely witness heightened frequency and intensity of this evolving challenge
- It is possible that will may encounter a malicious insider threat online that will have cascading tragic or catastrophic impact offline
- Organisational leaders need to be familiar with these threats and how they can impact their business or operations


Your Biggest Risk Could Be
the People You Trust Most.

Thank You