Deloitte.

Insider Threat Mitigation: A holistic & risk-based program

2022

Introduction

The term 'insider threat' is a less heard term, as some organisations might be more accustomed to threats from the outside. Hence, all the efforts are directed towards controlling these external threats. With the onset of the pandemic and organisational perimeters expanding, enterprises are getting accustomed to the reality of threats from within, which is known as 'insider threat'.

> Per the **2022** *Cost of insider threats* report by Ponemon Institute, insider threat incidents have risen by **44** percent over the past two years, with costs per incident up by more than a third to **US$15.38** million.

In certain industries such as finance and health care, the frequency of insider incidents is comparatively higher.

Additionally, incidents that involve stolen credentials tend to cause the highest financial damage. Insider threats can originate from sources, such as complacent or careless internal users or a malicious insider.

> Per Gartner, **60** percent of the reported insider threat incidents resulted due to careless employees or contractors, **23** percent were caused by malicious insiders, and only **14** percent involved cybercriminals stealing credentials.

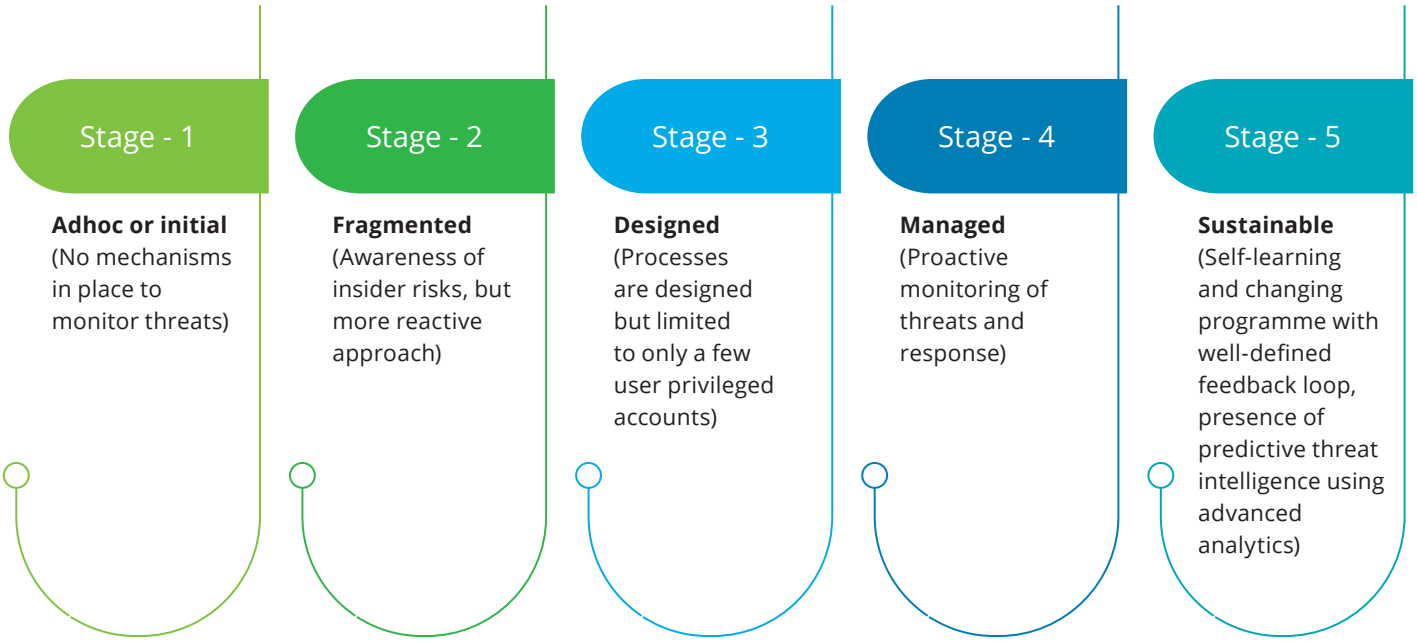
How to manage insider threats

As the first step, organisations must completely dissect the term 'insider' to understand who all fall under this very generic term. It could be full-time employees, contractors, or a third-party vendor who commits a malicious or ignorant act using their trusted access, which will bypass all perimeter controls. Next, organisations need to monitor critical assets or crown jewels, for any changes caused by an increased threat surface by insiders.

As the last step, organisations need to factor in otherwise unfamiliar insider risks while zeroing in on an insider risk management programme. This programme must consider the new types of behavioural, technical, and operational risks that surfaced due to COVID-19. Potential behavioural risks involve situations where employees could be stressed, which eventually leads to impulsive decisions. On the technical side, employees use their own devices and home networks, which may give rise to technological risks. Operationally, when organisations try to stand on their feet after the pandemic, they could drop their guard leading to fraudulent transactions going unnoticed.

While creating an insider risk management programme, organisations can perform a current state assessment to identify their maturity level. The results can be categorised per the five maturity stages listed below.

Maturity model for insider risk management programme



Once the current maturity stage is identified, organisations will have a time-bound road map to reach their target stage by clearly defining their priorities.

Insider risk management: A holistic approach

Though insider risk management forms a part of an organisation's cyber strategy, organisations have realised the need for a broader insider threat mitigation process rather than only looking at it through a technical lens. Along with the technical solutions, a people-centric approach needs to be taken with participation from various functions such as IT, HR, finance, and operations. It is also important to implement business level controls across the management of the entire employee lifecycle. A comprehensive, proactive risk-based insider threat management programme should be devised by organisations to outplay the insider's tactics and protect their assets.

This programme should address all the categories under insider risk, such as information theft, security risk due to privilege escalation and malware, violation of code of conduct, intentional destruction of equipment and IT infrastructure, supplier risks, and even work-place violence that affects the safety of the organisation itself.

Components of an insider risk management programme

Any insider risk management programme for an organisation should have the following three components:

- Insider risk specific incident response plan across the complete employee life cycle, including background checks, etc.
- Formal policies, procedures, and training programmes to communicate behavioural expectations
- Continuous monitoring by implementation of security and privacy controls

Organisations must look at developing their capabilities on the above three components based on the inputs from various functions such as HR, finance, legal and the physical security team. It is very important for them to catch red flags using the above methods as early as possible and act upon it, to limit
the damage.

An indicative list of red flags for potential insider threats (not limited to) include the following:

Disgruntled employees consistently showing disagreement with peers and reporting managers, potentially due to poor appraisals

Working hours consistently outside the normal working hours and unusual travel itineraries

Excessive leaves or absenteeism and irresponsible social media behaviour

Disengagement with the organisation in terms of consistent policy breaches and voicing disagreement with company policies

Financial distress or a sudden or unexplained financial gain

Abnormal download of sensitive data and heavy use of content sharing platforms, or sharing a large amount of data via emails

Attempt to access privileged accounts using default passwords or multiple wrong passwords for these accounts

Installation of unauthorised applications, plugins, or changing the approved configured settings on systems

Usually, organisations deploy techniques such as analytics on different data sets to catch these red flags early. These organisations need to also have a filtering mechanism to filter out the false positives and then take the required actions on the remaining ones.

Controlling insider risk

Implementation of anomaly detection, privilege access management, Data Loss Prevention (DLP), multi-factor authentications, segregation of duties, physical security controls, User and Entity Behavior Analytics (UEBA), and other prevention capabilities to detect risky behaviour and policy violations.

Conclusion

Per Gartner's predictions, 60 percent of large organisations will have well defined incident response scenarios for insider threats by 2023, which is around 20 percent today.

With hybrid and remote working models becoming the norm after COVID-19, organisations are witnessing increased risk from insiders. The need of the hour is to have a self-evolving insider risk management programme customised to organisational needs, and a business model that can auto-learn from feedback mechanisms under the sponsorship of the executive leadership. A well designed insider risk management plan should be capable of preventing, detecting, mitigating, and even deterring the insider threat, thereby driving trust in an organisation.

Connect with us

Rohit Mahajan
President, Risk Advisory
Deloitte India
rmahajan@deloitte.com

Gaurav Shukla
Partner and Leader - Cyber,
Risk Advisory, Deloitte India
shuklagaurav@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
Deloitte India
deseshadri@deloitte.com

Contributor

David George

Deloitte.