Securitas

Risk Intelligence Center

Insider Threat Awareness Month – What is Insider Threat?

1 September 2023

Intelligence@securitas.com

This report is subject to GDPR and data retention policies in line with such regulations.

Securitas provides the intelligence reports for the recipient's business internal use. Securitas accepts no responsibility for any decisions taken by the recipient on the basis of the analysis offered in this report. Use of Securitas' name, brand names, logos, taglines, slogans, or other trademarks without written permission is strictly prohibited. Disclosing, copying, distributing or use of any part of the reports electronically or otherwise other than for the strict purpose for which it has been provided is strictly prohibited. Securitas Security Services (UK) Limited is a limited company registered in England & Wales. Registered number: 01146486. Registered Office: 24 Old Queen Street, London, SW1H 9HP

Contents

Priority Intelligence

- **An insider threat is an individual or entity that uses their access, knowing or unknowingly, to facilitate unauthorized access to an industry / organization or its data, and can materialize through various means including negligence, malicious intent, or third parties.**
- **Insider threats are difficult vulnerabilities to detect and deter and are likely to pose a substantial risk to organizations. Organizations are coming under increasing pressure to implement and adhere to insider threat mitigation measures to protect their operations, security, and brand and reputation.**
- **Insider threats often feature a combination of pre-existing and enabling factors which allow insiders to become threats and undertake hostile actions, including personality traits, stressors, and organizational vulnerabilities. However, these factors can also be used to identify behaviors and vulnerabilities associated with increased insider threat, which can help organizations detect and mitigate the impacts.**
- **Malicious insider threats can be influenced by factors including financial gain, ideological motivations, influence from third parties, or general dissatisfaction toward the organization, its people, partners, or the wider industry.**
- **The insider threat landscape is complex and challenging and is influenced by factors including technological advances, geopolitical tensions, economic concerns, and industry competition. Changes within these factors are likely to impact the insider threat landscape, highlighting the importance of maintaining awareness of trends and understanding current threats.**
- **The Risk Intelligence Center (RIC) assesses that insider threat will continue to pose a substantial challenge for organizations in the immediate term, with both accidental and malicious threat actors presenting significant security, operational, and brand and reputational risks. Insider threats are highly likely to continue to be motivated by diverse and wide-ranging factors and will continue to exploit existing vulnerabilities whilst also seeking and developing new methods with which to target organizations, highlighting the importance of implementing and maintaining effective insider threat programs and security protocols.**

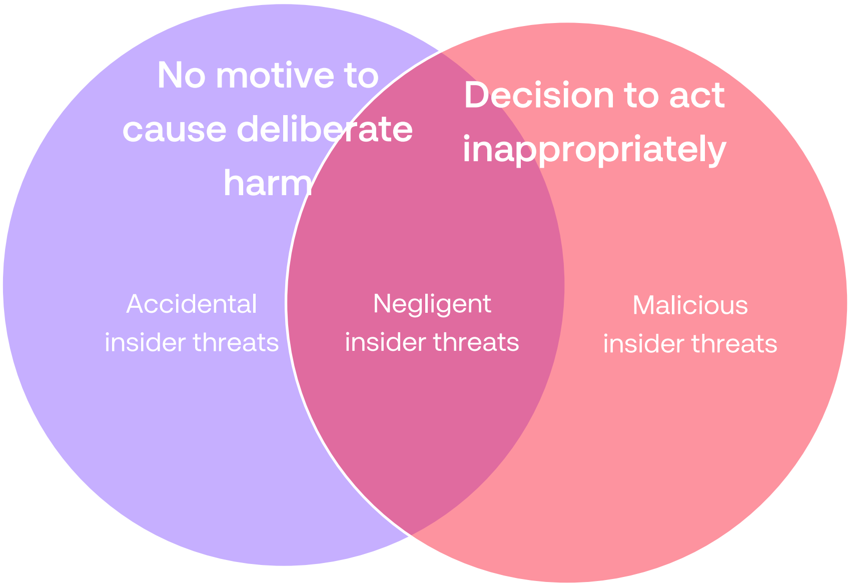
What is Insider Threat?

An insider threat is an individual or entity that uses their access, knowing or unknowingly, to facilitate unauthorized access to an industry / organization or its data. Insider threats can materialize through various means including negligence, malicious intent, and external pressures such as financial hardship or blackmail. Insider threats pose a significant threat to businesses as the perpetrators are often aware of and / or have more direct access to the organization's vulnerabilities, increasing the likelihood of further successful exploitation of the organization for information, technological, or economic gains. Insider threats are assessed as being one of the most difficult vulnerabilities to detect and deter within an organization and are likely to pose a substantial risk. No security system is immune to an individual with legitimate access who chooses to use it to compromise or otherwise circumvent those systems.

Negligent or accidental insider threats

Negligent or accidental insider threats include individuals who engage in poor security practices such as re-using passwords, removing confidential data from restricted areas, or otherwise failing to follow security protocols, as well as well-meaning individuals who are duped through tactics such as social engineering. For example, a laptop bag containing documents left on a train, or an email sent to the wrong addressee list – once the information is outside of the organization, it becomes impossible to guarantee it will not fall into the hands of hostile threat actors and therefore weaponized.

Negligent or accidental insider threats can arise from an individual's lack of awareness of security protocols or procedures and can be further exacerbated by organizational vulnerabilities. Whilst negligent or accidental insider threats can be difficult to identify and therefore prevent, the threat can be mitigated through comprehensive training and awareness programs for employees, effective and up-to-date security protocols, and procedures to prevent physical and virtual threats, as well as adopting an effective insider threat detection program / system.


No motive to cause deliberate harm
Decision to act inappropriately
Accidental insider threats
Negligent insider threats
Malicious insider threats

Malicious insider threats

Many insider threats stem from disgruntled current or former employees and exploitable leftover credentials, in addition to identity-related compromise, as businesses increasingly move towards digitalization and remote working. An insider's knowledge of an organization's operations, security procedures, or IT systems is highly likely to aid their efforts to engage in successful hostile actions and can lead to extremely disruptive or damaging attacks as known vulnerabilities, access rights or credentials can be targeted to maximize the impact on an organization.

The reasons for an employee choosing to engage in the deliberate leaking of confidential or damaging information can be broad – a disaffected individual seeking to damage a company as revenge for perceived poor treatment, an activist seeking to further their cause at the expense of their employer, or even an individual who is seeking to damage an organization for personal profit. Malicious insider threats can also be influenced by third parties, such as hostile states or criminal gangs seeking to target an organization, industry, or country.

Types of insider threats

The potential for embarrassment and negative brand and reputational impact resulting from a confirmed insider threat incident may discourage organizations from reporting or pursuing potential incidents formally, however, previous examples of insider threats highlight how they can manifest and impact organizations in several ways including through:

Sabotage	Espionage	Theft	Violence	Cyber
Physical Deliberate acts that disrupt or destroy an organization's people, property, or physical assets.	**Economic** Acquisition of economic intelligence (technical secrets, intellectual property, etc.) for strategic gain or to influence a rival's economic security.	**Financial crime** Exploiting an organization's money or financial assets with the intent to benefit from it.	**Workplace violence** Insider violence includes criminal or destructive threats that damage infrastructure or threaten / harm people or assets.	**Unintentional threats** Exposure of an organization's IT infrastructure, systems, and data that causes unintended harm.
Virtual Using technical or cyber means to damage or disrupt an organization's virtual infrastructure.	**Government** Covert intelligence-gathering activities by governments or government-linked threat actors to obtain an advantage.	**Intellectual property (IP)** The theft of organizations' ideas, inventions, or creative expressions to gain an advantage.	**Terrorism** Insiders can use their knowledge of an organization's structure, security, or systems to carry out terror attacks for an ideological or political cause.	**Intentional threats** Malicious actions performed by hostile insiders using technical means to disrupt or cease an organization's operations.

Influential factors behind malicious insider threats

Disgruntled employee - Factors including deteriorating performance, pay / promotion disputes, confrontation with colleagues / management, lack of recognition, in some cases can cause an employee to become disgruntled and lead to them becoming an insider threat.

Financial gain - Insider threats can steal and sell data, IP, proprietary information, or trade secrets and steal money using their legitimate and authorized access to an organization's people, property, or assets, to hostile state actors, other organizations, or criminal gangs for personal gains.

Third party influence - Employees may be subject to blackmail, honey trapping or social engineering campaigns which may lead them to steal data / money, or grant unauthorized access to a site / an organization's systems, to benefit a third party.

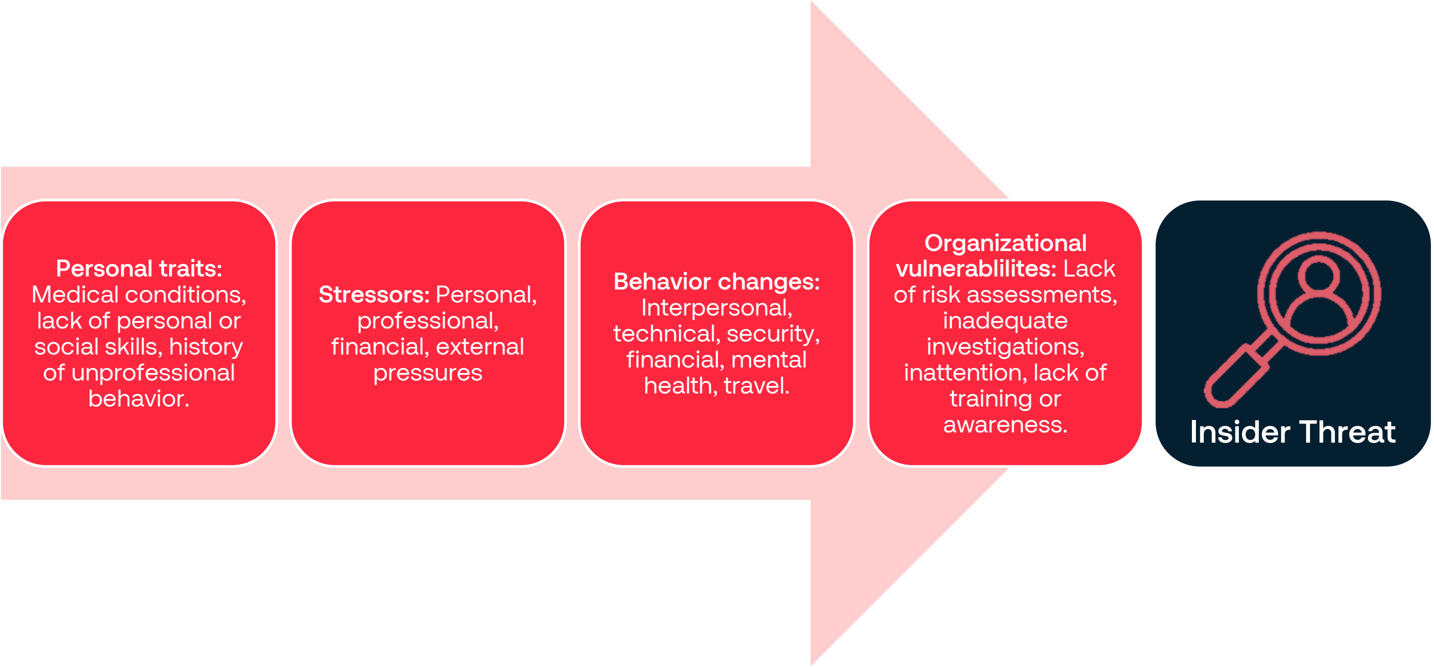
Ideological - An individual with a strong ideology may seek to disrupt or cease an organization's operations; in extreme cases an individual may join a specific organization due to their intent to exploit it due to their ideology, or an individual may gain a strong ideology once they have joined an organization.

Notoriety - An individual may be fueled by the desire for notoriety, or to gain fame, by causing disruption to an organization's operations or causing brand and reputational damage.

Identifying insider threats

Insider threats do not always follow a single path, and multiple pathways and factors can contribute to a potential insider threat developing. For an insider to become a threat to an organization there are often personal factors, stress influencers, and organizational vulnerabilities which can combine to enable an insider to exploit the organization's people, property, and assets, in turn posing a threat to its operations, security, and brand and reputation.

Although identifying any type of insider threat can be highly challenging, monitoring for unusual behavior, such as activity at unusual times (well outside of working hours, for example), transferring unusual files, accessing atypical resources, or asking probing / unnecessary questions may all be signs of a potential malicious insider threat.



Personal traits: Medical conditions, lack of personal or social skills, history of unprofessional behavior.

Stressors: Personal, professional, financial, external pressures

Behavior changes: Interpersonal, technical, security, financial, mental health, travel.

Organizational vulnerablilites: Lack of risk assessments, inadequate investigations, inattention, lack of training or awareness.

Insider Threat

Intelligence assessment

Insider threats within an organization (Loss of data / theft, security breach, financial loss, operational impact)				
Threat type:	Security	Operations	Brand & reputation	THREAT LEVEL
Severity:	4 – HIGH	4 – HIGH	4 – HIGH	4 – HIGH

The Risk Intelligence Center (RIC) assesses that insider threat will continue to pose a substantial challenge for organizations in the immediate term, with both accidental and malicious threat actors presenting significant security, operational, and brand, and reputational risks. Insider threats are highly likely to continue to be motivated by diverse and wide-ranging factors and will continue to exploit existing vulnerabilities whilst also seeking and developing new methods with which to target organizations, highlighting the importance of implementing and maintaining effective insider threat programs and security protocols.

A 2023 report from US cybersecurity firm Cybersecurity Insiders suggests that 74% of organizations are vulnerable to insider threats, with events such as the COVID-19 pandemic being central factors behind increased organizational vulnerabilities and individual circumstances that may result in insider threats.

- Publicly available data on incidents involving insider threats, especially regarding incidents targeting private organizations, is likely to be limited due to the risks it could present to the organizations' security, operations, and brand and reputation, indicating that many insider threats are likely to go unreported and the true scale of the insider threat landscape is likely to be unclear.

The current insider threat landscape is driven by several factors that can influence an insider to become a threat and / or enable them to exploit an organizational vulnerability to undertake intentional or unintentional hostile actions.

- Global financial concerns, including rising inflation, can act as a motivating factor behind insider threats, potentially enticing insider threats into stealing data / IP to sell to other organizations, as well as making them more susceptible to monetary offers from third parties to disrupt or damage an organizations operations, or leading to higher levels of disgruntled employees due to concerns over salaries leading to hostile actions.
- Competitiveness between organizations continues to increase as markets and access to resources become more strained, with a heightened likelihood of corporate espionage deployed by insider threats either for financial gains or ideological / notoriety motivations.

Geopolitical tensions can heighten the likelihood of third-party influence on insider threats, as they can be a successful way for hostile actors to disrupt key elements of a country's infrastructure through private organizations. Third parties, including nation-state level actors, may deploy individuals to gain legitimate access to an organization, either directly or through the supply chain with the intent to either undertake hostile actions or approach individuals already in those positions.

- Organizations with affiliations to Governments or within sensitive sectors such as defense, technology, and financial services are common targets for third-party influence, however, any organization within any industry is susceptible to insider threats.

Technological advances are a significant contributor to the insider threat landscape as they present more opportunities for social engineering or cyberattacks to cause unknowing individuals to become insider threats by granting access to an organization's systems without knowledge.

- Threat actors including hostile nation-states are deploying increasingly complex cyberattacks and social engineering campaigns aimed at insiders to cause them to unknowingly become an insider threat.
- Social engineering specifically seeks to cause and / or exploit human error, and even a hypothetical, 100% failproof system can be overridden, ignored, or switched off by an operator who believes they are doing the right thing.
- Organizations with outdated security protocols, including weak password requirements, increase their susceptibility to both malicious and accidental insider threats. Access to an organization's systems can present significant operational and security threats creating risks to an organization’s people, property, and assets likely through financial losses and brand and reputational damage.

Supply chains, although less likely to be considered as a direct vulnerability, can be vulnerable to insider threats, due to their position as an asset to organizations.

- Insider threats within the organization can pose risks to other organizations or elements within the supply chain, potentially damaging business or customer relations or leading to legal challenges and financial losses.
- If insider threats arise within an element of an organization's supply chain this can directly affect the organization through potential stolen data / IP theft, risks to employees, and prolonged financial impact.

Advisory

Insider threats pose a significant threat to organizations across all sectors and of all sizes – not only is there considerable operational and financial risk, but the reputational damage that can be caused by a successful insider threat exploitation – particularly one in which the organization is assessed as being negligent – can be significant and long-lasting. Organizations should:

- Organizations are strongly advised to develop and implement effective insider threat identification and detection programs, including a focus on behavioral indicators / exploitable traits, repeated security violations, and unnecessary attempts to become involved in sensitive or restricted areas, combining human resources and technology.
- Carry out an assessment of the most likely threat actors for their sector and organization – rival organizations, hostile state actors, dissatisfied employees, etc. Different threat actors will have different motivations and may utilize specific tactics, techniques, and procedures (TTPs). Identifying possible threats can help to detect vulnerabilities in security procedures.
- Organizations should maintain situational awareness to pre-emptively identify issues or trends that may see an increase in insider threats, whether targeting the organization specifically, its partners, or supply chain.
- Educate staff on the potential risks and sources of espionage, including the dangers of social engineering. Establish clear and detailed processes for reporting concerns or suspicious behavior, including instances of suspicious contact on social media and via emails.
- Organizations should carry out appropriate levels of vetting for prospective employees and contractors, as well as establish and maintain an effective insider threat program.
- Ensure that robust security processes and systems are in place – both for physical and remote access to restricted or high-value data and / or objects.
- Develop and implement a comprehensive incident response plan (IRP) – this describes who should do what when responding to a detected incident to minimize damage, helping to protect the business's reputation and relationships with customers. Ensure that the IRP is reviewed regularly and – where appropriate – tested through tabletop and 'live' exercises.
- Develop and utilize intelligence services to monitor for active, developing, or potential insider threats.

ASSESSED THREAT LEVELS	
5 – EXTREME	Very high / extreme threat of disruption. Review and respond if required.
4 – HIGH	High / major threat of disruption. Consider taking appropriate action.
3 – MODERATE	Moderate threat of disruption. Maintain awareness, consider precautions.
2 – LOW	Low / limited threat of disruption. Be advised.
1 – VERY LOW	Very low / insignificant threat of disruption. For awareness.

LANGUAGE OF PROBABILITY							
Term:	Remote	Highly unlikely	Unlikely	Realistic / Possible	Likely / Probable	Highly likely	Almost certain
Probability:	0-4%	10-20%	25-35%	40-50%	55-75%	80-90%	95-99%

Intelligence Cut Off Date (ICOD):	1700hrs, 31 August 2023