Insider Threats

Introduction: Description of what constitutes an insider threat

Depending on the way an insider could constitute a risk for an organization, numerous definitions of insider threats exist. The most important point is that the definition of insider threat is contextual. Determining the internal threat is a best practice for each organization because it allows it to address the specifics of its working environment, beliefs, and resources that it believes are most vulnerable.
Nevertheless, insider threats are typically defined as cybersecurity risks arising from authorized users (e.g., contractors, business partners) who either purposefully or inadvertently abuse their permitted access or have their accounts compromised by cybercriminals.
The potential for an insider to exploit their permitted access or unique knowledge of an organization constitutes an insider threat.

Type of Insider Threats:

- **Unintentional Threat**

Negligent – This kind of insider carelessly exposes an organization to danger. Negligent insiders put the organization at risk when they choose to disregard security and/or IT policies, even though they are usually aware of them. Examples include losing or misplacing a portable storage device that holds sensitive data, letting someone "piggyback" via a secure entry point, and disobeying prompts to install security patches and new upgrades.
Accidental – This kind of insider inadvertently exposes an organization to risk. Examples include unintentionally sending a confidential company document to a competitor; clicking on a hyperlink by mistake; or accessing a malicious attachment in a phishing email.

- **Intentional Threats**

The term "malicious insider" is frequently used interchangeably to refer to a purposeful insider. Ambition, financial demands, or dissatisfaction over a perceived grievance are some of the reasons behind purposeful insider trading. Some people could put themselves in risk or reveal private information to gain attention and recognition. In their minds, they might even be serving the public interest. In the delusion that doing so will advance their careers, they may engage in violent acts, harass colleagues, sabotage machinery, leak confidential information, or steal intellectual property.

- **Other Threats**

Collusive Threats – Collusive threats are a subclass of malicious insider threats in which one or more insiders work with an external threat actor to compromise an organization. In many of these cases, insiders are recruited by cybercriminals to facilitate fraud, intellectual property theft, espionage, or a mix of the three.
Third-Party Threats – Furthermore, third-party risks are usually vendors or contractors who are not employees of a company but who have been given access to people, systems, networks, and facilities to carry out their business.

Identification: Indicators of potential insider threats within an organization

There are six common insider threat indicators:

1. Unusual data movement

An insider threat may be indicated by unusual spikes in data downloads, transmitting significant volumes of data outside the organization, or transferring information using Airdrop.

2. Use of unsanctioned software and hardware

Negligent and malicious insiders might install unauthorized software to expedite tasks or make data exfiltration easier. Shadow IT may be a sign of an insider threat regardless of intent because data security is compromised by unapproved hardware and software.

3. Increased requests for escalated privileges or permissions

It is common for contractors, vendors, and employees to require authorization to view sensitive data. When more people want access to it, there are more potential hazards to sensitive data, which is why it becomes a concern. Insider threats increase with the number of individuals having access to confidential information.

4. Access to information that’s not relevant to their job

Accessing information that is irrelevant to their position is another indicator that someone may be an insider threat. When combined with additional clues, these circumstances can assist security teams in identifying insider threats.

5. Renamed files where the file extension doesn’t match the content

Renaming files is one-way malicious insiders may try to hide their data exfiltration. The concerning activity could also include the conversion of zip files to JPEG extensions. You can identify potentially suspicious activity with the aid of a data security tool that can locate these mismatched files and extensions.

6. Departing employees

Insider threat activity can arise from both voluntary and involuntary employee departures from a company. To gain an advantage in their next position, workers may forward strategic plans to personal devices. More malicious individuals might steal information and provide it to rival businesses.

Strategies to prevent insider threats

It's critical to identify insider threats as soon as they appear to prevent expensive fines and reputational harm from data breaches.

The following tactics can be used to identify insider threat indicators and lessen the likelihood of a data leak:

- Use a zero-trust approach while implementing access restrictions.
- Employee training and awareness
- Keep an eye on and safeguard all your data—not just the ones you've designated as "important."

- Establish a baseline of reliable conduct. When there is a benchmark, it becomes simpler to discern between unsafe and normal behavior.
- Launch a program to fight insider threats.
- Use AI and behavior analytics to spot threats.
- Improve security using multifactor authentication (MFA).

Immediate Actions: What to do when you've spot an insider threat

Reporting an insider threat is a serious matter that typically involves the security or human resources departments within an organization. If you believe you have identified an insider threat, follow these general steps:

Use the Internal Reporting Channels:

- Contact your organization's IT or security department: They are usually equipped to handle security incidents and potential insider threats.
- Human Resources (HR): If the threat involves employee misconduct, HR may need to be involved to address any personnel issues.

Follow Company Policies:

Refer to your organization's policies and procedures: Many companies have specific guidelines on how to report security incidents or concerns. This information may be available on the company intranet, or through other internal resources.

Anonymous Reporting:

If you are concerned about anonymity, some organizations have anonymous reporting mechanisms in place. This could include a hotline, an online reporting system, or other confidential channels. Check with your company to see if such options are available.

Security Incident Response Team (SIRT):

Some organizations have a dedicated Security Incident Response Team. If your company has one, report the incident to them as they are trained to handle security-related issues.

Legal and Compliance Teams:

Depending on the nature of the threat, it may be appropriate to involve legal or compliance teams within the organization.

Law Enforcement:

In certain cases, such as when the insider threat involves criminal activity, you may need to involve law enforcement. Consult with your organization's legal department before taking this step.

Document the Details:

Before reporting, document as much information as possible about the insider threat. This may include specific incidents, individuals involved, dates, times, and any other relevant details.

The specific process for reporting insider threats can vary from one organization to another. It's essential to follow the company's established procedures and protocols. If you are unsure about how to proceed, reach out to your supervisor, HR representative, or IT/security contact for guidance.

Reporting Protocols: Who and how to report the incident to authorities or internal IT departments

The establishment of reporting pathways is essential to thwarting insider threats. There is no way to mitigate unknown threats. Together with organizational policies that structure and implement reporting processes, the governance group in each organization should create confidential reporting pathways that are simple to find, understand, and use. The governance group should prioritize assisting individuals and highlighting the benefits of reporting while carrying out this work.

Establishing a culture of shared responsibility and informing people that the program is confidential and intended to support both them and the potential insider are important steps in establishing a system that encourages reporting within an organization.

An insider threat mitigation program should steer the organization toward positive change by motivating its members to report suspicious activity and hold their peers and organization accountable.

The following are some ideas for creating a culture of reporting:

- Enabling anonymous and online reporting systems
- Investing in training and awareness of the staff members
- Responding to threats reported by staff members to let them know that such reports are taken seriously.
- Accepting reports from friends, family, and other non-organization sources
- Creating a mercy policy to eliminate any doubts or anxieties about reporting.
- Promoting an inclusive culture and fostering upward communication
- Taking reporting accessibility and availability into consideration
- Shielding those who come forward from possible reprisals.
- If someone thinks they have seen illegal activity, they can report it to external law enforcement or the organization's Insider Threat Program.

The Insider Threat Mitigation Plan will define the ways and contacts to whom the employees should report an Insider Threat.

This project was funded by the European Union's Internal Security Fund - Police Programme under Grant Agreement No 101038738