CANADIAN CENTRE FOR CYBER SECURITY

How to protect your organization from insider threats

May 2024 ITSAP.10.003

Insider threats can come from anyone who has or had access to or knowledge of your organization's networks, systems or data. These threats can be intentional, where the goal is to cause harm, or they can be unintentional, such as employee negligence and accidents. Insider threats can put your organization's employees, customers, assets, reputation and interests at risk. However, there are security procedures you can implement to reduce these risks.

Unintentional insider threat

It is possible for an employee to accidently cause harm to your organization's infrastructure or information. Some causes of unintentional insider threats include:

- misplacing a mobile device or removable media
- granting other employees access to sensitive information that they are not authorized to access
- mishandling sensitive information by leaving it out in the open or forgetting to apply the appropriate permissions

Malicious insider threat

A malicious insider threat occurs when someone knowingly uses your infrastructure and information to cause harm. They may gain unauthorized access or abuse access on general or privileged accounts. An individual may be motivated to gain unauthorized access or perform unauthorized actions for the following reasons:

- looking for revenge, due to a perceived slight or workplace issue
- being threatened or extorted
- hoping for some form of personal or financial gain

Anyone who has authorized access to your infrastructure or information can be an insider threat. This includes employees, contractors, and partners. These individuals may try to cover up their actions by altering detection programs or deleting audit records. Employees who have unnecessarily high access privileges can present serious threats to your organization. You should ensure that employees only have the access that they need to carry out their functions, this is called the **principle of least privilege**.

Possible impacts

After gaining unauthorized access, an individual could expose sensitive or personal information. Insiders can cause significant compromises to the confidentiality, integrity, and availability of your organizations business processes and information.

AWARENESS SERIES

Cat. No. D97-1/10-003-2024E-PDF
ISBN 978-0-660-71499-8

How to respond to an insider threat

If an insider threat successfully gains unauthorized access and-performs unauthorized actions, activate your incident response plan.

- Manage access controls and restrict administrative and privileged account access to reduce further damage
- Track and monitor all endpoint and mobile devices as an insider threat can act remotely
- Check audit logs to identify suspicious behaviour
- Inform third-party service providers as the malicious activity could spread to their systems, or it may have originated on their systems
- Use the experience to raise awareness and provide tailored training

Make sure you follow communications guidelines outlined in your plan to inform stakeholders. If you don't already have an incident response plan, consult Developing your incident response plan (ITSAP.40.003).

How to manage the risks of insider threats

Insider threats are difficult to identify. However, you can manage risks by implementing the following security controls: policies and procedures, access control, audits, and data loss prevention.

Policies and procedures

Implement policies and procedures to clearly define your organization's security requirements and the expected behaviour of all users when using organizational networks, systems, and information. To prevent insider threats, you should address the following topics in your policies:

- Employee screening
  - Perform initial and recurrent background checks and integrity assessments
  - Implement internal moves and departure plans such as performing employee exit interviews
- Mandatory cyber security training and awareness activities
  - Cover topics such as phishing, malware exposure, social media risks
  - Tailor training to address organization-specific threats and security controls and provide refresher training with security awareness activities
  - Provide refresher training with security awareness activities
- Security agreements with partners and third parties
  - Ensure your organization's data is located in Canada to fortify data protection under Canada's legal jurisdiction
  - Monitor and log actions by tracking who accesses the data and when
  - Determine reliability of partners and build long-term trusted relationships

Learn more:

- Top 10 IT security action: #6 provide tailored cyber security training (ITSM 10.093).
- Identity, credential, and access management (ICAM) (ITSAP.30.018)

Access control

Access control is the selective restriction of a user's access to networks, systems, and data through authentication and authorization methods. Employees should only have access they require to carry out their functions. Consider the following examples of access controls:

- Apply the **principle of least privilege** when assigning administrative privileges and account access
- Implement multi-factor authentication methods. Refer to Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Implement the **rule of two-person integrity (TPI)** to secure critical material or operations
  - TPI is a system in which two authorized persons are required for a task to be performed; prohibiting individual activity
- Revoke account access and administrative privileges when a user no longer requires them, such as when they move to a different team
- Ensure the concept of separation of roles between administrators and users in your organization's network is understood and practiced
- Establish allow lists and deny lists to protect information

Learn more:

- ITSM.10.094 Top IT security actions: #3 Manage and control administrative privileges
- ITSM.30.010 Securing access controls in a volunteer-based organization

Audits

With auditing actions, you can collect, analyze, and store records and logs that are associated with user actions on information systems. Some ways in which you can use audit logs to manage risks associated with insider threats include the following examples:

- Monitor and log detailed actions to detect when unusual behaviour is detected
- Log actions and events and label them with time and date stamps
- Regularly review administrative changes
- Track mobile devices that are corporately owned
- Implement Security information and event management strategies (SIEM)

For more information, refer to Network security auditing (ITSAP.80.086).

Data loss prevention

Data loss prevention (DLP) is a software that detects and prevents data from leaving your organization's control. DLP software uses alerts, encryption, and other protective actions to restrict end users from accidentally or maliciously sharing sensitive data.

Depending on your organization's cyber security budget, we recommend implementing a security control profile if your organization handles highly sensitive information. Refer to our Security control catalogue (ITSG-33) to learn more about selecting security controls to protect your information systems.