Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

HOW TO PROTECT YOUR ORGANIZATION FROM INSIDER THREATS

FEBRUARY 2020 **ITSAP.10.003**

This document focuses on the IT-related concerns regarding insider threats. An insider threat is anyone who has knowledge of or access to your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm. 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 the risks.

INADVERTENT OR MALICIOUS INSIDER THREAT?

It is possible for an employee to inadvertently cause harm to your organization's infrastructure or information. Some causes of inadvertent insider threats include the following examples:

- 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

In the case of a malicious insider threat, someone knowingly uses your infrastructure or information to cause harm by gaining unauthorized access or abusing privileged accounts or general accounts. An individual may be motivated to gain unauthorized access or perform unauthorized actions for the following reasons:

- Looking for revenge (e.g. no job advancement, being laid off [former employee threat, depending on organization's exit plan])
- Being threatened or blackmailed
- Hoping for some form of personal or financial gain

Anyone who has trusted access to your infrastructure or information can be an insider threat (e.g. employees, contractors, third parties, partners). The individual 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 (i.e. principle of least privilege).

POSSIBLE IMPACTS

After gaining unauthorized access, an individual could expose sensitive or personal information. Data and privacy breaches can jeopardize your organization due to financial implications, a damaged reputation, and a loss in public trust.

WAYS TO RESPOND TO AN INSIDER THREAT

If an insider threat successfully gains unauthorized access to your organization's networks, systems, and information or performs unauthorized actions, you should take the following steps at a minimum:

- Manage access controls (i.e. restrict privileges to reduce further damage)
- Track and monitor all endpoint devices (e.g. an insider threat can threaten organizations remotely)
- Check audit logs to identify suspicious behaviour
- Inform third-party service providers if the insider threat activity could spread to their systems or if the threat originates from them
- Work with senior management to develop a communication plan for incident response
- Use the experience to raise awareness and provide tailored training

AWARENESS SERIES

WAYS TO PREVENT AND REDUCE HARM

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

POLICIES AND PROCEDURES

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

- Screening employees who handle sensitive information (e.g. background checks)
    - Implementing internal moves and departure plans (e.g. employee exit plans)
- Offering mandatory training and carrying out awareness activities
    - Covering topics such as phishing, malware exposure, social media risks
    - Tailoring training to address organization-specific threats and security controls
- Enforcing security agreements with partners and third parties
    - Ensuring your organization's data is located in Canada (i.e. keeping data protected under Canada's legal jurisdiction)
    - Monitoring and logging actions (i.e. tracking who accesses the data and when)
    - Building long-term, trusted relationships with partners (e.g. determine reliability)

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:

- Enforcing the principle of least privilege when assigning administrative privileges and account access
- Implementing two-factor or multi-factor authentication methods (e.g. password and hardware cryptographic tokens to access sensitive data)
- Implementing the rule of two-person integrity to secure critical material or operations
- Revoking account access and administrative privileges when a user no longer requires them (e.g. a user leaves the organization or moves to a different team)
- Ensuring the concept of separation of roles between administrators and users in your organization's network is understood and practiced

For more details on access control with administrative privileges, refer to *ITSM.10.094 Top IT Security Actions: #3 Manage and Control Administrative Privileges*, which is available on our website.

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:

- Monitoring and logging detailed actions to detect when unusual behaviour is detected (e.g. tracking system changes or unusual behavioural patterns)
- Logging actions and events and labelling them with time and date stamps
- Reviewing administrative changes (e.g. when accounts have been added and removed)
- Tracking mobile devices that are corporately owned (e.g. logging all actions taken on devices used to access organizational infrastructure and information remotely)

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. For details on security control profiles, refer to *ITSG-33 IT Security Risk Management: A Lifecycle Approach*, which is available on our website.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**