PROTECT INFORMATION AT THE ENTERPRISE LEVEL

AUGUST 2022

ITSAP.10.097

Cyber threats (e.g. malware, phishing, ransomware) continue to change and develop with the continuous growth in technology. Your organization needs to constantly adapt to protect its networks, systems, IT assets, and information from changing technology and threats. For example, Internet-connected devices are becoming increasingly popular in the workplace and are being used for business purposes. While these devices introduce efficiencies and convenience, they can also increase your organization's security risks. In response, your organization needs to take measures to protect information at the enterprise level.

ASSESS YOUR INFORMATION

When you identify the information you have and the sensitivity of that information, you can ensure that you are taking the proper measures to protect it.

When assessing your organization's information, consider the types of information, such as business critical information (e.g. sales information, emergency response plans), sensitive information that needs to be kept confidential (e.g. financial or personal information, intellectual property), or records and evidence that need to be protected from unauthorized modification (e.g. contracts).

You can determine the value of information by assessing the possible harm that could result if compromised. Assigning a value to your information can help you prioritize your protection efforts.

MANAGE YOUR INFORMATION

Your organization is responsible for managing and protecting information throughout its lifecycle (i.e. from its creation to its destruction). Information management includes activities to ensure that information is handled, stored, and destroyed properly. When information has met the end of its lifecycle and is no longer required for business purposes, you should ensure that it is properly destroyed.

Using data loss prevention (DLP) software will also help in preventing data from leaving your organization's control. DLP uses alerts, encryption, and other protective actions to restrict end users from sharing sensitive data.

You should ensure that information management is covered in your awareness and training activities so that employees, contractors, and service providers understand their roles and responsibilities. You may want to consider addressing the following topics:

- Handling physical and digital information appropriately
- Keeping information for the necessary retention period
- Destroying information properly
- Sanitizing media
- Tracking information systems and components through inventories
- Backing up information

AWARENESS SERIES

Cat. No. D97-1/10-097-2022E-PDF
ISBN 978-0-660-44896-1

SECURE YOUR DATA EXTERNALLY

Your organization's information management practices must be considered when using mobile devices, service providers, and other external information systems (e.g. portable storage media). To protect your organization's information externally, you need to verify that any of the external systems that you use have security controls that align with your organization's security policies. To ensure your organization's information is protected when using external information systems, consider the following recommendations:

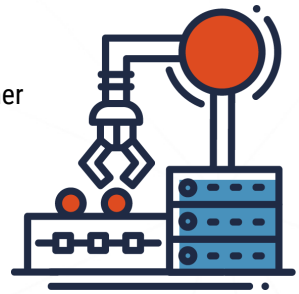
- Implement security controls on devices before connecting to organizational systems.
- Limit device access to certain types of information, services, or applications.
- Use a virtualized environment to limit your system's other components from affecting your organization's data.
- Ensure all users and partners agree to your organization's terms and conditions (e.g. document agreements).
- Monitor all endpoint devices continuously.
- Audit external information systems for suspected compromises (e.g. abnormal updates, changes, authentication attempts).

PROTECT DATA USING SERVICE PROVIDERS

Data stored outside of Canada is subject to different privacy, security, and data ownership laws and regulations. If you use a cloud service provider (CSP) or a managed service provider (MSP) outside of Canada, review applicable laws and possible impacts to the privacy of your data and evaluate the level of sensitivity with the data being handled.

PROTECT YOUR SUPPLY CHAIN

Your organization may rely on systems and services that are provided by other organizations. You should identify potential risks and agree on security policies to ensure that your information is protected appropriately. When working with service providers, you should use a service-level agreement (SLA) to establish your service expectations. Your SLA should also indicate which security measures are used and define roles and responsibilities with regards to auditing and incident response.



For more details on protecting your organization when working with other suppliers, refer to *ITSAP.00.070 Supply Chain Security for Small and Medium Organizations*.

CHOOSE A MOBILE DEVICE MODEL

Mobile devices can increase efficient remote work for your organization, but it also raises risks to your organization's information. If a mobile device is compromised, threat actors can access your organization's networks, systems, and information. The four enterprise mobility models are included in the following:

- Corporately owned for business only (COBO)
- Corporately owned and personally enabled (COPE)
- Choose your own device (CYOD)
- Bring your own device (BYOD)

These mobility models differentiate in the level of ownership your organization has over the device. The level of ownership and personal use should be considered under the threat and risk assessment when deciding which mobility model is best suited for your organization (e.g. level of control over the information on the device).

For more details on the enterprise mobility models, refer to *ITSAP.70.002 Security Considerations for Mobile Device Deployments*.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**