CANADIAN CENTRE FOR CYBER SECURITY

Protecting high-value information:
Tips for small and medium organizations

June 2024

ITSAP.40.001

Small and medium organizations have valuable information that needs to be protected to ensure business activities run smoothly. This includes sensitive business, employee, and client information. Small and medium organizations are likely targets of cyber attacks because they often lack resources to put towards cyber security. While it may not be possible to protect everything, knowing what information is valuable to your organization can help you protect what matters most.

Know the value of information

By knowing the value of your organization's information, you can prioritize what needs to be protected. Value can be expressed in terms of quantitative measures, such as a dollar amount, and qualitative measures, like your reputation and relationships with other companies.

When assessing value, consider the impact and the possible harm that could result from the inability to protect the confidentiality, integrity and availability of information.

- **Confidentiality**: Sensitive information is accessed by unauthorized individuals
- **Integrity**: Information is modified or deleted when it's not supposed to be
- **Availability**: Information cannot be accessed or is lost

When assigning value, consider the following types of information:

- business critical information that your organization relies on to run, such as payroll, sales information and emergency response plans
- sensitive information that needs to be kept confidential or only accessed by certain people, like financial or personal information, and intellectual property
- records and evidence that needs to be protected from unauthorized modification, for example, contracts and receipts

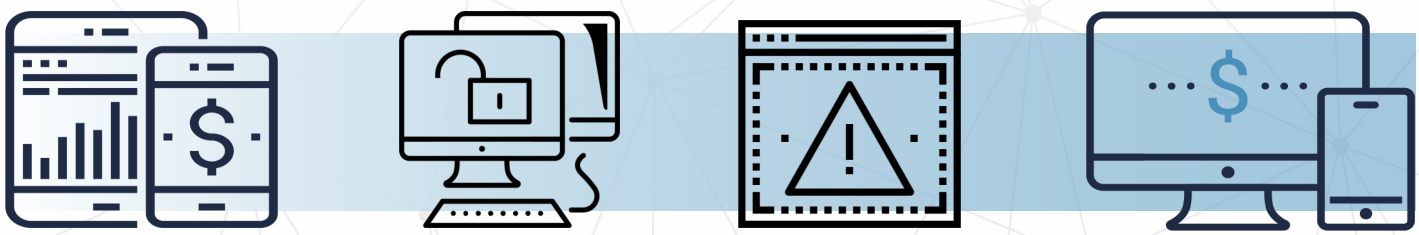
Identify threats and vulnerabilities

By identifying threats and vulnerabilities that are relevant to your organization, you can implement security measures that fit your environment and needs. A threat or vulnerability may affect your organization differently than another organization which may require you to adopt different security measures.

A **threat** is any potential cause of an incident, event or act that may harm your organization and its systems and information. Threats can be natural, such as fire and flood, or human in origin. Think about the types of threats that could affect your organization based on your activities and the type of information you have.

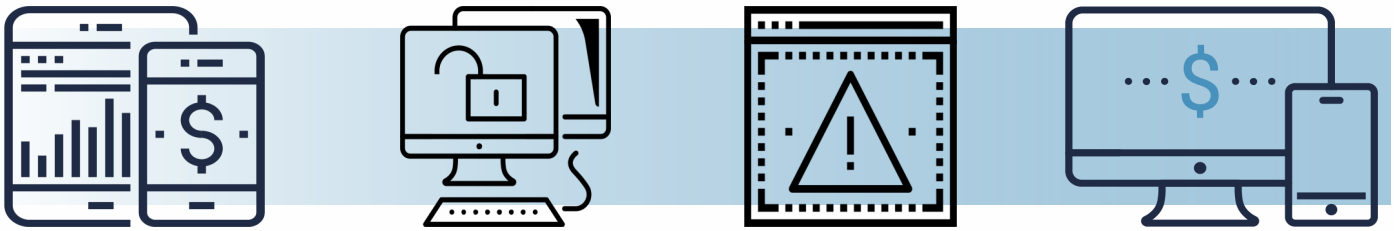
A **threat actor** is someone who initiates a threat, whether on purpose or not. Threat actors may target your organization for various reasons, including trying to gain a profit from stolen information, wreaking havoc, or taking revenge.

A **vulnerability** is a weakness or gap in your current security measures. Vulnerabilities may be caused by different factors, such as outdated software, unencrypted information, weak passwords or systems that have been infected by malware.



AWARENESS SERIES

Cat. No. D97-1/40-001-2024E-PDF
ISBN 978-0-660-69928-8



Make cyber security a part of your organization

Cyber security should be included in your business processes and plans so that you can protect your high-value information and your organization. Your customers expect that you'll keep their personal information safe. Additionally, the organizations you work with will want to know that you won't be putting their systems and information at risk.

There's no one-time, one-size-fits-all solution for security, and the threat landscape continues to change. To keep your organization safe, think of security as a continuous process of preventing, identifying and responding to threats.

Review our Baseline cyber security controls for small and medium organizations to identify the baseline security controls that you can implement. These security controls can protect your organization and your high-value information from cyber threats.

Learn more

Cyber security tips for remote work (ITSAP.10.116)

Protect your organization from malware (ITSAP.00.057)

Secure high-value information

Networks, systems and information that are properly secured are less likely to be compromised. Protect your high-value information with the following tips:

1. Identify
   - Know the value of your information
   - Know where high-value information is stored
   - Identify employees who have access to high-value information
   - Know how employees access high value information, such as from remote work locations
   - Identify vulnerabilities and possible threats
2. Protect
   - Limit access to sensitive systems and information
   - Encrypt sensitive systems and information
   - Install software updates and patches when available.
   - Use web and email filters
   - Keep devices that access high-value information in a secure location when not in use
   - Wipe all hardware before you dispose of it
3. Detect
   - Use anti-virus and anti-malware software
   - Activate, maintain and monitor activity logs to identify issues or incidents
4. Respond
   - Develop a response plan for incidents
   - Train employees on their roles and responsibilities
5. Recover
   - Back up information regularly
   - Consider if cyber insurance is right for you
6. Review
   - Review your needs and the systems in place and update accordingly to ensure your high value information stays secure