Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

UNCLASSIFIED

PROTECTING HIGH-VALUE INFORMATION: TIPS FOR SMALL AND MEDIUM ORGANIZATIONS

APRIL 2019

ITSAP.40.001

Small and medium organizations have valuable information (e.g. sensitive business, employee, and client information) that needs to be protected to ensure business activities run smoothly. Small and medium organizations are likely targets of cyber attacks because these organizations 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

Knowing the value of your organization's information will help you prioritize what needs to be protected. You can determine the value of information by assessing the possible harm that could result from the inability to protect the confidentiality, integrity, and availability of information, such as in the following examples:

- **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 (e.g. sales information, emergency response plans)
- **Sensitive information** that needs to be kept confidential or only accessed by certain people (e.g. financial or personal information, intellectual property)
- **Records and evidence** that needs to be protected from unauthorized modification (e.g. contracts, receipts)

IDENTIFY THREATS AND VULNERABILITIES

By identifying threats and vulnerabilities that are relevant to your organization, you can take security measures that fit your organization needs. A common threat or vulnerability may affect your organization differently than another organization.

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 (e.g. fire and flood) or human in origin. 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.

Think about the types of threats that could affect your organization based on your activities and the type of information you have.

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 system that has been infected with a virus.

AWARENESS SERIES

Canada

MAKE CYBER SECURITY A PART OF YOUR ORGANIZATION

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, and the other organizations with which you work 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.

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
   - Identify your organization's vulnerabilities and possible threats
2. **Protect**
   - Limit access to sensitive systems and information
   - Encrypt sensitive information
   - Install software updates and patches when available
   - Use web and email filters
   - Wipe all hardware before you dispose of it
3. **Detect**
   - Use anti-virus and anti-malware software
   - Enable, 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

Review our *Baseline Cyber Security Controls for Small and Medium Organizations* to identify the baseline security controls that you can implement to protect your organization and your high-value information from cyber threats.

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