SECURITY CONSIDERATIONS FOR RESEARCH AND DEVELOPMENT

SEPTEMBER 2020 ITSAP.00.130

As a research organization, you rely on your ability to continuously innovate, develop, and improve. Your research data and intellectual property are high-value targets for cyber threat actors, and a successful cyber attack can prevent you from carrying out your work and jeopardize your data. To protect your research environment and data, your organization should understand common cyber security threats and implement some basic security measures.

R&D ORGANIZATIONS ARE HIGH-VALUE TARGETS

Your research may focus on improving the functionality of a product or service or advancing knowledge in a specific area. As such, research and development (R&D) is integral to Canada's economic growth, prosperity, and security. Canadian businesses rely on your research to provide them with a competitive edge in the market. For example, the healthcare system depends on R&D to improve patient care across the world.

Not only do R&D organizations need to keep up with consumer needs, but they are competing to increase their shareholder value. R&D organizations need to receive financial support to contribute to Canada's economic and infrastructure growth.

Cyber threat actors may carry out attacks to disrupt R&D activities, steal data to sell, or give advantages to competitors. Cyber security measures protect your data and help you maintain a competitive edge. If you don't have security measures in place, you should implement the best practices in this document as a starting point. Effective security controls help protect your organization from potential threats that could impact the outcome of your R&D efforts.

COMMON CYBER THREATS

Cyber threat actors can use different methods to tamper with or steal your research data and intellectual property. The threats below are just two examples, but these attacks can leave your systems vulnerable to other threats.

Phishing: A threat actor calls, texts, emails, or uses social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information. Phishing attacks may allow a threat actor to steal passwords that can be used to log in to a research portal or work-related accounts.

For more information, see *ITSAP.00.101 Don't take the bait: Recognize and avoid phishing attacks*.

Insider threat: Anyone who has access to your organization's infrastructure and data can intentionally or unintentionally cause harm. As an example of an intentional insider threat, a member of your organization may gain access to research databases to steal data. Whereas, in an example of unintentional insider threat, a researcher or colleague may lose a portable storage device (e.g. a USB) that contains sensitive data. Whether an insider threat is intentional or unintentional, the effects can impede progress or put information at risk.

For more information, refer to *ITSAP.10.003 How to Protect Your Organization from Insider Threats*.

These two cyber threats most commonly lead to **ransomware** attacks in R&D organizations. Ransomware is a type of malware that will make your data inaccessible (e.g. locking systems and encrypting all files) until a ransom is paid.

For more information, see *ITSAP.00.099 Ransomware: How to Prevent and Recover*.

AWARENESS SERIES

GET STARTED WITH THESE CYBER SECURITY PRACTICES

Cyber security might be a new priority for you, but there are actions you can take to reduce the risks associated with cyber threats and vulnerabilities. These actions are only a starting point. For more guidance, see our *Baseline Cyber Security Controls for Small and Medium Organizations*.

TRAIN YOUR ORGANIZATION'S MEMBERS

Train your employees, researchers, students, and contractors on cyber security topics and best practices to help them understand their roles in protecting your organization against cyber threats. You may want to include topics such as creating passphrases, spotting suspicious and malicious emails, and browsing the Internet safely. You may also want to address expected behaviours and any security requirements, such as encrypting information, locking devices and computers when not in use, or reporting incidents to an identified point of contact.

USE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is a process that uses two or more different methods of verifying your identity (called *authentication factors)*. There are three types of authentication factors: something you know, something you have, and something you are. You may already use some forms of MFA, such as requiring that you swipe a badge (something you have), entering a code (something you know) to enter a research facility, and using your fingerprint to unlock your phone (something you are).

INSTALL SECURITY SOFTWARE AND TOOLS

There are security tools that you can install on your systems and devices, such as firewalls and anti-virus software, that help protect your systems and networks from malware. We recommend using the Canadian Internet Registration Authority (CIRA) Canadian Shield as an additional step to protect your systems against phishing and malware attacks.

If your employees work remotely, use a virtual private network (VPN). A VPN creates a secure, encrypted tunnel through which employees can send information. For more information, see *ITSAP.80.101 Virtual Private Networks*.

You should also consider using a managed service provider (MSP) to manage the necessary security tools to protect your secure data. Having your MSP set up endpoint device security helps your organization monitor where data is accessed and by whom (e.g. securing data handled by organizations outside of Canada). Verify that your MSP follows Canadian privacy laws.

UPDATE AND PATCH DEVICES AND SOFTWARE

Update and patch your devices and software to ensure systems are protected from security vulnerabilities (e.g. software bugs). Patching and updating software frequently will reduce the risks of cyber threats that can damage your organization's systems and data.

IMPLEMENT ACCESS CONTROLS

Not all members of your organization need to be able to access the same information. Your organization should practice the principle of least privilege to ensure that members only have the necessary amount of privileges for their specific job. Granting excessive privileges to members puts your organization at a higher risk of data or privacy breaches.

All members should have individual log-in credentials rather than using shared credentials for multiple people. Additionally, when members change projects or leave the organization, be sure to revoke their privileges.

BACK UP YOUR DATA

Backing up your organization's data helps you restore information systems after an attack, outage, or natural disaster. Ensure backups are stored on a device that is not directly connected to your primary network. This protects the backups from potential cyber attacks on your primary systems (e.g. ransomware), remaining a path to restore if necessary. You should also test your backups regularly.

Cloud services are common and convenient for storing data backups. Ensure the service provider offers MFA to access information and encryption for data in transit and at rest, and store the data in Canada (i.e. protected by Canada's privacy laws).

LEARN MORE

Refer to some of our related publications for more cyber security best practices:

- *ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication*
- *ITSAP.00.057 Protect Your Organization from Malware*
- *ITSAP.10.096 How Updates Secure Your Device*
- *ITSAP.00.087 Mobile Devices and Business Travellers*
- *ITSE.50.060 Benefits and Risks of Adopting Cloud-Based Services in Your Organization*
- *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information*

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 (Cyber Centre) at **cyber.gc.ca**