CANADIAN CENTRE FOR CYBER SECURITY

Security considerations for research and development organizations

April 2024 ITSAP.00.130

As a research and development (R&D) organization, you are continuously innovating and making new discoveries. This means, however, that your data and intellectual property are high-value targets. Cyber threat actors may try to access your servers and information for malicious reasons. A successful cyber attack can prevent you from continuing your work and can jeopardize your data. To protect your research environment and intellectual property, your organization should understand common cyber security threats and implement some basic security measures.

Why research and development organizations are high-value targets

R&D is integral to Canada's economic growth, prosperity, and security. Canadian businesses rely on your work to provide them with a competitive edge in the market. For example, the healthcare system depends on R&D to improve medical equipment and patient care across the world.

Threat actors may carry out cyber attacks to disrupt R&D activities, steal data to sell, or give advantages to competitors. This is a loss to both the organization and Canada's economic and infrastructure growth.

Common cyber threats

Cyber threat actors can use different methods to tamper with or steal your research data and intellectual property., and compromise your organization. The following are a few examples of the many threats that can leave your systems vulnerable.

Phishing: A threat actor may call, text, email, or use social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information. Phishing attacks may allow threat actors to steal credentials that can be used to log in to research portals and work-related accounts, or to freeze networks and delay operations.

Insider threat: Anyone who has access to your organization's infrastructure and data can intentionally or unintentionally cause harm. Whether an insider threat is intentional or unintentional, the effects can impede progress or put information at risk.

- Intentional insider threat: A member of your organization gains access to research databases to steal data
- Unintentional insider threat: A researcher or colleague may lose a portable storage device that contains sensitive data (for example, a USB)

Ransomware: Phishing and Insider threats most commonly lead to ransomware attacks in R&D organizations. Ransomware is a type of malware that restricts access to a device or network, making your data inaccessible until a ransom is paid. For example, a threat actor may send a phishing email with a link that will lock systems and encrypt all files until a payment is made.

Cyber security best practices

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.

AWARENESS SERIES

Cat. No. D97-1/00-180-2024E-PDF
ISBN 978-0-660-70811-9

Train your employees

Train your employees on cyber security topics and best practices to help them understand their roles in protecting your organization against cyber threats. Your cyber security training should include topics like:

- spotting suspicious emails
- using the Internet safely
- implementing good password habits

You may also want to address expected behaviours and any security requirements, such as:

- encrypting information,
- locking devices when not in use
- reporting incidents to an identified point of contact

Use multi-factor authentication (MFA)

MFA is a process that uses two or more different methods of verifying your identity, known as 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).

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 users only have the necessary amount of privileges and access for their specific job. Granting excessive privileges to members puts your organization at a higher risk of data or privacy breaches and cyber attacks.

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, like ransomware, from infecting your primary systems. 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. Your data should be stored in Canada under Canadian privacy laws.

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 Canadian Internet Registration Authority (CIRA) Canadian Shield to further protect your systems from cyber 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.

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, like 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 like software bugs. Patching and updating software frequently will reduce the risks of cyber threats that can damage your organization's systems and data.

Learn More

- Baseline Cyber Security Controls for Small and Medium Organizations
- ITSAP.00.005 Common Employee Cyber Security Challenges
- ITSAP.00.057 Protect Your Organization from Malware
- ITSAP.00.087 Mobile Devices and Business Travellers
- ITSAP.00.099 Ransomware: How to Prevent and Recover
- ITSAP.00.101 Don't take the bait: Recognize and avoid phishing attacks.
- ITSAP.10.003 How to Protect Your Organization from Insider Threats.
- ITSAP.10.096 How Updates Secure Your Device
- ITSAP.30.030 Secure Your Accounts and Devices with Multi-Factor Authentication
- ITSAP.80.101 Virtual Private Networks
- 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**