PROTECT YOUR MEDICAL RESEARCH EQUIPMENT FROM CYBER THREATS

February 2022 | ITSAP.00.134

Your medical research equipment is vital to your organization's operations. It collects data to fulfill your projects and critical needs within the medical field. Medical research environments are rich in data and the digital infrastructure it resides on, making them high value targets for cyber threat actors. As medical research labs become more connected, the risk of unauthorized access to your data increases. Threat actors can access unsecured connected devices (e.g. lab freezers) and use them to infiltrate your networks, systems, and data. By understanding your risks and the steps you can take to mitigate them, you can enhance your ability to protect your equipment and sensitive data.

THREAT EXAMPLES

The following examples demonstrate the types of cyber incidents that can impact connected medical research equipment.

Point-of-care analysis: By gaining access to your network through a point-of-care system (e.g. rapid testing machines), threat actors can exfiltrate your data. Phishing attacks are commonly used to trick users into clicking on a link or downloading a file that contains malware.

Data storage penetration: Threat actors find vulnerabilities in a point of entry to gain access to your data reserves. Data reserves contain high-value information (e.g. research findings, intellectual property, and personal health information [PHI]).

Laboratory automation exploitation: As research facilities connect to more automated systems, the risk of cyber attacks increases. Cyber threat actors target automated systems to exfiltrate data or gain access to networks.

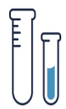
Insider threat: An insider threat is anyone who has knowledge of or access to your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm. The data produced by your research equipment could be vulnerable to insider threats. For more information on protecting your organization from insider threats, see *ITSAP.10.003 Protecting Your Organization from Insider Threats*.

HOW DO THREAT ACTORS TARGET MEDICAL RESEARCH EQUIPMENT?

Medical research equipment collects and analyzes sensitive information, such as PHI, study findings, and intellectual property. Threat actors seek to use connected equipment, such as mass spectrometers or particle sizers, to access your data with malicious intent.

Attacks are not limited to the threat examples provided. Points of attack are numerous and can also include the following:

- Exploiting your older systems or equipment that are no longer supported with patches and updates.
- Infecting your connected equipment and systems with malware (e.g. ransomware).
- Detecting vulnerabilities in your unprotected equipment and networks, such as a lack of encryption or firewalls, and exploiting them to access your data.



WHAT ARE THE IMPACTS FOR RESEARCHERS AND DATA?

Cyber attacks can target most connected medical research equipment, from an ultra-performance liquid chromatography (UPLC) to peripheral storage devices (e.g. USB sticks). Research, intellectual property, and PHI could be compromised if you are a victim of a cyber attack.

Since the onset of the pandemic, threat actors are increasingly targeting medical research facilities with ransomware and data exfiltration tactics. The cost to replace and recover compromised equipment and data could be devastating to your organization.

Educate your organization on the security measures needed to protect your medical research equipment. Create cyber security policies and guidelines for your staff and provide in-house training.

CANARIE NETWORK

Canadian research hospitals, universities, colleges, science facilities, and other academic and research centres can connect to the CANARIE Network through their provincial and territorial National Research and Education Network (NREN) partners. NREN connects these organizations together across Canada to other global research and education networks.

- CANARIE offers free network monitoring and maintenance tools.
- The Cybersecurity Initiatives Program (CIP) is funded by the Government of Canada and available to eligible members of NREN. The CIP provides you with firewall protection, an intrusion detection system, and a consolidated threat feed.

For more information on the CANARIE's CIP see Cyber Security Initiatives Program (CIP).

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

HOW CAN I PROTECT MY ORGANIZATION?

Securing your medical research equipment is vital in protecting your data. Any device that is running software and connected to your network is susceptible to cyber threats. Adhering to the cyber security tips below will enhance your environment and the protection of your research equipment, devices, and data.

Increase security: Secure your cyber environment to protect your labs, networks, connected devices, and information.

- Connect your devices through a virtual private network (VPN).
- Secure your accounts and your connected devices on lab equipment with multi-factor authentication (MFA) and use strong passwords or passphrases.
- Assign access rights and system privileges to users based on the tasks they need to complete.
- Deactivate accounts when users change roles or leave the organization.
- Replace older equipment that lacks a unique address, configurability, or event logs.
- Encrypt your device storage as well as communications between devices.
- Implement a security log monitoring solution that reviews logs from multiple devices and systems and alerts when anomalies are detected.
- Request your IT staff to segment your networks by dividing them into smaller zones to better control how traffic flows.
  - Segmentation also allows you to isolate and stop the spread of malware to different sections of your network, and control and restrict access to your information.
- Embed cyber security and data security standards into your service agreements with vendors.
- Verify that each vendor in your supply chain has robust cyber security controls in place.
- Examine your vendor's data management and security policies and identify where and how your data will be handled.

Value your information: High-value data needs to be secure and protected from threat actors.

- Encrypt your data stored on networks, in systems, or in the cloud.
- Back up your data regularly to an offsite storage location that is inaccessible by your networks or Internet connections.
- Implement a data classification methodology so your backup systems can easily differentiate high value data from the rest.

Manage your assets: Think of your medical equipment and data as corporate assets and protect them accordingly.

- Create a life-cycle management strategy to allow for plans and budgets of new research equipment and supporting software.
  - There will come a time where a piece of research equipment is no longer supported. Planning for their replacement will help to avoid security vulnerabilities after discontinuation occurs.
- Take stock of Internet-connected and enabled devices. Ensure you patch and update regularly to address vulnerabilities.

WHAT SHOULD I LOOK FOR WHEN PURCHASING EQUIPMENT?

The National Institute of Standards and Technology (NIST) Core Baseline recommends lab managers look for the following features or capabilities when purchasing network connected devices:

- **Identification:** The device should have its own unique address on computing networks.
- **Configurability:** The device's security software, firmware, and settings configuration should be accessible and easy to change by a lab manager.
- **Data protection:** Encryption should be embedded into the device to protect it from unauthorized access or modification.
- **Limited network interfaces:** The devices should require user authentication to access the device, which limits access to local and wide area networks.
- **Software and firmware updates:** A secure and configurable way to update the device's software and firmware should be available, whether automatic or manual.
- **Event logging:** The device should log cyber security events to alert lab managers to vulnerabilities and enable forensic analysis if hacked.

LEARN MORE

If you want to learn more about some of the key points identified, check out the following publications on our website (cyber.gc.ca).

- Security Considerations for Research and Development (ITSAP.00.130)
- Internet of Things Security for Small and Medium Organizations (ITSAP.00.012)
- Tips for Backing up Your Information (ITSAP.40.002)
- How Updates Secure Your Devices(ITSAP.10.096)
- Protecting High-Value Information: Tips for Small and Medium Organizations (ITSAP.40.001)
- Secure Your Accounts and Devices With Multi-Factor Authentication (ITSAP.30.030)
- Using Encryption to Keep Your Sensitive Data Secure (ITSAP.40.016)

Remote Work

Working remotely during the pandemic has opened the door for threat actors, providing an increasing threat surface. Cyber threats to research facilities have increased as threat actors can exploit personal devices and unsecured connections to gain access to your organization's networked systems, data, and equipment. By implementing the guidance listed above, in particular connecting devices through a VPN, applying updates and patches to your software, firmware, and operating systems, and using strong passwords or passphrases, you can enhance the security of your organization while employees are working remotely. For more information on working remotely securely, see Security Tips for Organizations With Remote Workers (ITSAP.10.016) and Cyber Security Tips for Remote Work (ITSAP.10.116).

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada