Key Measures for Preventing and Mitigating Cyber Attacks and Ransomware

In light of recent events, HIROC has prepared this one-pager to re-iterate key measures that healthcare entities and providers are advised to take to facilitate the prevention of a cyber-attack and the immediate steps to be taken to mitigate harm should a cyber-attack occur.

1 Prevention

- ✓ Patch operating system/software on a regular basis
- ✓ Carry out Social Engineering/Phishing training awareness and testing
- ✓ Carry out daily backup strategy and store the backup files securely offline
- ✓ Install antivirus and malware protection; and update it regularly
- ✓ Provide users with rights which are limited to what is required to do their job. Least required privilege access rights
- ✓ Allow only those with "administrator privileges" to install or modify the systems/applications. Administrators to use regular user account to do non-administrator tasks
- ✓ White list applications necessary for the daily business operations and DENY execution of application not approved.

2 Monitoring

- ✓ Filter incoming traffic for suspicious files and automatically block downloads from the web and strip attachments from emails, apply alerts and notifications
- ✓ Install Web URL filtering and email firewall to detect phishing URLs
- ✓ Install a SIEM for historical reporting and forensics
- ✓ Install IDS monitoring to trigger on anomalous behaviour

3 Incident response

- ✓ Disconnect the infected networks from the internet
- ✓ Disconnect infected machines from the network and lock down shared network drives
- ✓ Notify key healthcare partners, insurer and legal counsel
- ✓ Get expert help if needed to achieve the following:
  - Analysis – identify specific variant of ransomware, determine how it entered the network (i.e. unsolicited email, web browser vulnerabilities)
  - Containment – remove infected computer from all access (network and wireless)
  - Eradication – remove ransomware from infected system(s). If ransomware came in through email, search and purge all existing messages or isolate the email(s). If ransomware came in through web browser, block the site first. Change all passwords for affected users
  - Recover data from last good backup (remember that ransomware can reside for periods of time before being detected)
  - Conduct a post-attack retrospective – lessons learned, identify vulnerabilities and security controls that may not have been in place

For more information of cyber risk management please see the following guides:

- HIROC's Cyber Risk Management Guide
- Deloitte's Taking data hostage: The rise of ransomware https://www2.deloitte.com/ca/en/pages/risk/articles/ransomware.html