Ransomware and Your Obligations under *PHIPA*

David Weinkauf, Ph.D.
Senior Policy and Technology Advisor
Office of the Information and Privacy Commissioner of Ontario

Ontario Hospital Association Cyber Risk and Resilience Program
December 9, 2016

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Outline

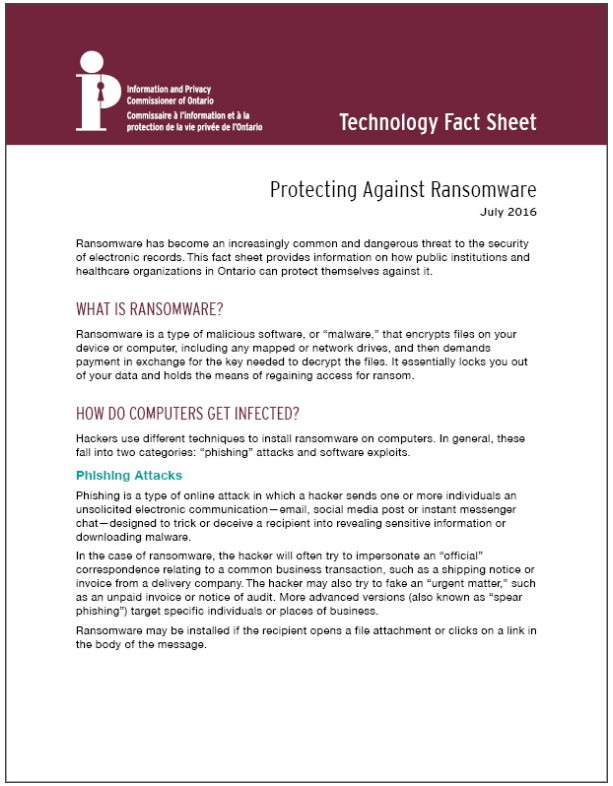
- About the IPC
- Protecting Against Ransomware Factsheet
- Security Obligations, s. 12(1) of *PHIPA*
- Notice Obligations, ss. 12(2) and 12(3) of *PHIPA*

About the IPC

- Information and Privacy Commissioner of Ontario (IPC) established in 1988
- Commissioner acts **independently** of government to uphold and promote **open government** and the protection of **personal privacy**
- IPC oversees three statutes:
  - Freedom of Information and Protection of Privacy Act (*FIPPA*) and its municipal counterpart (*MFIPPA*)
  - Personal Health Information Protection Act (*PHIPA*)
    - **Comprehensive** privacy protections for personal health information (PHI)

Protecting Against Ransomware

- IPC Fact Sheet released in July 2016
- What is ransomware?
- How do computers get infected?
  - Phishing attacks
  - Software exploits
- Protecting your organization
- Responding to incidents
- Available at www.ipc.on.ca



Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

Security Obligations, *PHIPA* s. 12(1)

- Requires health information custodians (HICs) to take steps that are **reasonable in the circumstances** to ensure PHI in their custody or control is protected against:
  - theft, loss and unauthorized use or disclosure
  - unauthorized copying, modification or disposal
- Depending on **level of risk**, measures **may** include:
  - Employee training
  - Antivirus software
  - Email quarantines
  - Limited active content
  - Data backups
  - Software updates
  - Minimal user privileges
  - Simulated attacks
- If a computer is compromised, HICs should take **immediate steps** to mitigate effects of attack

Notice Obligations, *PHIPA* s. 12(2)

- IPC has received **limited cases** of ransomware
- A ransomware infection **may** constitute a breach depending on factors such as:
  - whether any PHI was accessed by hackers
  - whether affected PHI was fully restored
- If breach has occurred, HICs must notify individuals at **first reasonable opportunity**
- *PHIPA* does not specify the **manner** of notification
- Best form of notification depends on **numerous factors**
- Contact IPC to discuss

Notice Obligations, *PHIPA* s. 12(3)

- Bill 119, *Health Information Protection Act, 2015*, introduced additional **breach notification** requirements into *PHIPA*
- If breach has occurred and meets the prescribed requirements, HICs must **notify IPC**
- However, **no requirements** have been prescribed yet
- Until then, HICs should **continue to notify** the IPC of privacy breaches as appropriate

How to Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
TDD/TTY: 416-325-7539
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca
Media: media@ipc.on.ca / 416-326-3965