Organizational Strategies to Address Ransomware Threats

Alberta Netcare Security Bulletin No. 2019-001 (August 2019)
Issued by Alberta Health Privacy & Security Team

Impacts to Healthcare Providers

The ever-increasing reliance for communications and services to move online corresponds with an increase in potential vulnerabilities for ransomware to exploit. The lack of adequate protections against vulnerabilities can result in ransomware impacting healthcare providers by limiting the ability to provide clinical care, a loss of patient privacy, financial penalties under the *Health Information Act* (HIA), and a loss to organizational reputation.

The Alberta *Health Information Act* (HIA) lays out a number of requirements for the protection of health information. Under section 60 of the HIA, a custodian must take reasonable steps to maintain administrative, technical and physical safeguards for information and protect against reasonably anticipated threats or hazards to the security or integrity of health information.

This guide provides an overview for organizational management to identify the critical components of their information security operations. It provides preventative advice specific to reduce the likelihood of ransomware attacks, as well as how to limit the impact of an attack. Technical and implementation guidance concerning ransomware are provided in the reference section at the end of this document.

Preventive Measures

1. **Training and Awareness**
    - **Increase employee awareness** – Employees must understand how their online actions can contribute to an increased risk of ransomware attacks, as well how they can detect and what to do if they suspect an infection. Providing ransomware security awareness training can be an effective way to protect your organization against a ransomware attack.

2. **Email Security**
    - **Deploy email filtering** – Ransomware is commonly delivered through email and phishing attacks. Configuring email servers to prevent phishing messages and malicious attachments from reaching employees helps reduce the threat of ransomware.

3. **Network Security**
    - **Segregate networks** – Ransomware can spread rapidly through an organization's network. Segregating networks and data (physically and logically) into different organizational units (e.g. finance, human resources, medical delivery services, etc.) can restrict ransomware impacts to specific business functions rather than the entire organization. Deploying firewalls at network boundaries to filter traffic can help in preventing or containing a ransomware attacks.
    - **Harden operating systems** – Ransomware is known to gain access by exploiting commonly used services (such as remote desktop and server message block protocols) and unpatched vulnerabilities. Hardening operating systems by disabling or limiting unused services and applying timely security updates/patches reduces the effectiveness of ransomware attacks.

- **Follow privilege/administrator user account management practices** – Ransomware often requires access to privileged/admin accounts in order to execute and spread to other systems. It is important that the use of privileged/admin accounts is based on the principle of least privilege required, that their use be restricted to those individuals and times required to conduct privileged or administrative tasks.

4. **End Point Security**

- **Deploy anti-malware and anti-virus to all systems, workstations and servers** – Known ransomware strains can be detected by anti-virus and anti-malware software. Consider deploying centrally managed anti-virus solutions that include automated deployment of current signatures and automated alerting to IT personnel allowing threat to be addressed in a timely manner and prevent further infection.
- **Ensure only trusted applications are used in the environment** – Ransomware can masquerade as useful applications ("Trojans"), or exploit vulnerabilities in legitimate software. It is important that applications be obtained from trusted sources (physical or download), and that known vulnerabilities are patched and tested with the latest versions before being deployed. Reduce unnecessary risk by disabling social media integration features available in software if they are not required.

5. **Mitigating Impact : Business Continuity, Disaster Recovery and Incident Response**

- **Plan and test your organizations business continuity** – Ransomware attacks can take time to resolve and have an impact on patient care or other critical business services. Having a planned and rehearsed incident response to implement business continuity processes (i.e. developing manual and/or paper-based processes) can help minimize impacts during system restoration.
- **Prepare disaster recovery procedures for restoring from backup** – Having a data backup can eliminate the need to pay a ransom to recover data. It is important that data is regularly backed up, securely stored/segregated to prevent access from attackers, and that restoration processes and data integrity are tested.

What to do if your organization is a victim of ransomware attack?

Should Preventive Measures Fail

Organizations are advised to implement their incident response process that may invoke other processes such as business continuity and disaster recovery.

Informing Law Enforcement

The RCMP requests victims reach out to their local RCMP office to file a compliant. Providing details such as those below will help their investigations and future prevention:

- Date of infection
- How the infection is believed to have occurred (link in e-mail, browsing the Internet, etc.)
- Ransomware variant if known (identified on the ransom page or by the encrypted file extension)
- Organization/company impact statement including losses, industry type, business size, etc.
- Requested ransom amount and attacker's bitcoin wallet address

Paying the Ransom?

A victim organization may grapple with the decision to pay a ransom in hopes of regaining access to their encrypted data or systems. This decision requires the evaluation of options to protect shareholders, employees, and customers. Organizations will want to evaluate the technical feasibility, timeliness, and cost of restoring systems from backup. On a more practical level, paying a ransom requires an organization to "trust the attacker". The attacker may increase ransom demands, fail to provide the promised decryption key needed to regain access to the encrypted data or systems, or put you on their paying customers list in hopes of a successful repeat engagement in the future. Paying the ransom also comes with the unfortunate consequence of encouraging this type of criminal activity.

Technical Guidance and Glossary of Terms

Technical Guidance and Resource Links	
Publications and Guidance	*NIST Special Publication 1800-11 - Data Integrity Recovering from Ransomware and Other Destructive Events* https://www.nccoe.nist.gov/publication/1800-11/ *The CIS Critical Security Controls for Effective Cyber Defense* https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense *NIST National Checklist Program Repository* https://nvd.nist.gov/ncp/repository
Ransomware Research	https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/ https://go.kaspersky.com/rs/802-IJN-240/images/Healthcare-Survey-Report.pdf
Ransomware attacks on Canadian Healthcare	https://www.cbc.ca/news/technology/carepartners-data-breach-ransom-patients-medical-records-1.4749515 https://www.scmagazine.com/home/security-news/true-crime-samsam-ransomware-i-am/ https://ehrintelligence.com/news/canada-hospital-enters-ehr-downtime-after-discovering-computer-virus https://www.itworldcanada.com/article/ryuk-ransomware-strikes-at-least-four-organizations-in-canada/409893
Ransomware Variants	https://en.wikipedia.org/wiki/Ransomware#Notable_examples

Glossary of Terms	
Anti-malware or anti-virus (AV)	Software designed to prevent or remove malicious software from a computer system or network.
Malware	Software designed to infect and cause malicious damage to systems. *Malware* refers to code, scripts, or content that is distributed through a

	variety of methods including computer viruses, worms, trojan horses, adware, etc.
Phishing, Spear-phishing	Phishing refers to the fraudulent activity to lure individuals to provide sensitive information (e.g. usernames, passwords, and credit card details) by disguising email, phone, or text requests to appear as though they were sent by a trusted entity. The sensitive information is used to obtain access to information and financial assets resulting in losses, fines, or identity theft. Spear-phishing refers to phishing attempts directed at a specific individual or department, and typically uses messages with customized content that appear to be sent from an organization's management.
Ransomware	Malware that prevents victims from accessing their data, or that threatens to inappropriately share or publish a stolen copy of their data. Attackers request a ransom payment via bitcoin or other crypto-currency in exchange for the promise to restore access to data or to stop release of the stolen data.
Spam	Unsolicited or undesired email, voice, or text messages commonly used to distribute advertising messages or to hide malware content or links.
Trojan	A type of malware that is disguised as or within legitimate software. Attackers attempt to trick users into loading and executing Trojans on systems. Once installed or activated, Trojans allows attackers to observe systems and copy or steal data.
Email Filtering	The automated processing of email using specified criteria to detect unsolicited messages and malicious payloads.
Firewall	An IT infrastructure or network device that allows or blocks network traffic based on a defined set of rules.
Hardening	The protection of a computing system (and associated risk) by limiting its available entry points, removing unnecessary code or features, and eliminating unnecessary services. Organizations are encouraged to use recommended hardening configurations for systems (available online through security organizations such as NIST) as a starting point configuration for system default settings, passwords, users, network ports, encryption, services/software, logging, etc.
Patch	A software fix used to correct a problem or "bug" within a system. Security patches are used to correct security vulnerabilities.
Privileged or Administrator accounts	Accounts with access to perform tasks not normally accessible to user accounts. These accounts (e.g. "admin", "root", "SYS", etc.) are valued by attackers as they can be used to install malware and ransomware, or to obtain access to restricted infrastructure or financial systems.
Business Continuity Planning (BCP)	An organization's planning and preparation response to support the continuance of normal or reduced business operations during an incident.
Disaster Recovery Planning (DRP)	An organization's planning and preparation response to support the protection and/or restoration of infrastructure and assets (information and financial) when continuity of business operations is not possible, such as during a serious incident or disaster.
Incident Response Planning (IRP)	An organization's planning and preparation to help IT staff detect, respond, and recover from network security incidents. Incident response addresses issues such as cyber attacks, data loss, and service outages that threaten business operations. Incident response plans may invoke an organization's disaster recovery or business continuity plan.