JULY 2024

CASE OF NOTE

PHIPA Decision 249

INTRODUCTION

Unfortunately, ransomware attacks are not an uncommon occurrence, especially in this era of rapidly advancing technologies. Bad actors use ransomware attacks to extract money and cause harm to others. As these types of attacks become increasingly common, health information custodians (HICs) should ensure that they have strong preventative measures in place to help minimize and prevent the risks of cybersecurity attacks.

BACKGROUND

Following detection of unusual activity on its systems in December 2022, a medical imaging clinic (the clinic) determined that it had been a victim of a ransomware attack. The clinic responded to the attack by immediately shutting off their servers and engaging breach counsel and a team of cybersecurity experts to assist with the containment, investigation, and remediation of the breach.

A week after the incident, the clinic notified the Office of the Information and Privacy Commissioner of Ontario (the IPC) that it was the victim of a ransomware attack. The clinic reported that affected files could have included up to 550,000 patient records and 1,600,000 case files.

The clinic's experts determined that the threat actor (a known hacking group) likely gained entry into the system through a dormant account, which had significant administrative privileges. The threat actor encrypted and exfiltrated files from the electronic medical records and file sharing servers, deleted the backups and demanded ransom payment. In this case, the clinic was not able to restore its systems using the relevant backups and had to temporarily close.

The clinic paid the ransom, after which the clinic was able to decrypt the information on the affected servers and recover all affected files. The clinic provided notice to the public of the breach both online and within its clinics.

The clinic explained to the IPC that it had security measures in place before the incident. However, the high level of activity during the attack caused logs to be overwritten before they could be reviewed. This meant that the clinic could not determine exactly how the intrusion occurred, or what tactics were used to gain access to the account credentials.

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

Since the incident, the clinic has taken remediation measures to strengthen its security by implementing several policies and practices aimed at preventing similar situations occurring in the future. For example, the clinic revised its Least Privilege Access Policy to limit domain access privileges to only two administrative staff and provide users only the minimum access necessary for their roles. It now has password strength and complexity requirements, monitors for and deletes dormant accounts, and conducts regular checks to ensure security patches are kept current.

The clinic has also segregated its networks and put up firewalls as needed. In terms of back ups, the clinic now keeps at least one viable copy of its backup offline that will remain unaffected in the event of another cyberattack so that the clinic will be able to resume operations. The clinic has improved its detection and response measures. It now uploads its VPN and firewall logs daily and stores them so that it can better investigate future cyber incidents with these logs in place.

FINDINGS

The IPC investigator determined that the clinic took sufficient efforts to determine the scope of the breach and provide the appropriate notice. The investigator found that the clinic responded adequately to the breach that occurred, especially considering the remediation steps that it took to address the matter. The investigator also determined that, as the clinic provided notice and put in place effective remedial measures, a review was not warranted.

KEY TAKEAWAYS

This case serves to alert HICs of the importance of having strong security procedures in place as a preventative measure against cybersecurity attacks, such as:

(a) giving privileged administrative access to only a very limited number of users

(b) reducing system access to the minimum amount necessary for each role and ensuring access is terminated when users leave or change roles

(c) monitoring for and deleting dormant accounts

(d) strong password policies

(e) anti-virus protection and spam filtering

(f) appropriate firewalls around the network, with external VPN connection

(g) multi-factor authentication

(h) regular checks to ensure security patches are kept current

(i) regular cybersecurity training to staff

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

(j) access logs with sufficient memory that can promptly detect unauthorized access to systems and assist in diagnosing what happened, when and how

(k) reliable backups in place, including at least one viable copy offline that remains unaffected in the event of a cyberattack so that the HICs are more readily able to resume operations

These are just some of the ways HICs can help prevent, or at least help mitigate, successful cybersecurity attacks. For more information on preventative measures HICs can take upfront, refer to IPC's fact sheet on ***How to Protect Against Ransomware***.

Once a breach has occurred it is imperative that the HICs take immediate action to contain the breach, including shutting off their servers, and engaging breach counsel and a team of cybersecurity experts. HICs should also consult the IPC guidance set out in ***Responding to a Health Privacy Breach: Guidelines for the Health Sector*** (the PHIPA Breach Guidelines) regarding appropriate steps to take once a breach has occurred.

Preventing a ransomware attack is no easy task. It takes time and resources. However, if proper and strong safety measures are put in place before an attack, then it is less likely that the threat actor will be successful. Taking measures to prevent a cyberattack is less costly than having to pay a ransom or rebuild a compromised system after the fact.