ALBERTA MEDICAL ASSOCIATION

INVESTIGATION AND FORENSIC AUDIT OF AMA DATA BREACH

The Alberta Medical Association (AMA) engaged the services of the Cyber Security Team of PricewaterhouseCoopers (PwC) to investigate the breach of AMA member and staff data reported on May 16, 2017. PwC has recently completed their Digital Forensics and Incident Response investigation. The purpose of this report is to summarize the findings of the forensic investigation and communicate next steps.

Introduction

The AMA contracts with a records and document management vendor to digitize paper records that the AMA is required to retain for regulatory and other reasons.

The AMA was notified by the vendor on May 11 that a virus had been discovered on their secure server used for transferring data between the vendor and the AMA. In response, an internal investigation was launched to assess impact, consult the Office of the Information and Privacy Commissioner of Alberta and to engage the services of PwC's Cyber Security Team to investigate the breach.

As part of the investigation, PwC has: been able to interview the vendor; had access to the virus for analysis; and analyzed the infected server.

Objective

The Cyber Security Team was tasked with investigating and determining:

(i) Whether any AMA data was accessed by the cyber-attacker
(ii) Whether there was any evidence of unauthorized removal of AMA data from the server

Findings

Through their investigative actions, PwC found:

(i) There was no evidence of unauthorized access of AMA data
(ii) There was no evidence of unauthorized offloading of AMA data

Evidence and process

On May 16, PwC began their investigation of the incident. The following is a flow of events related to the breach and the findings based on all available information and expertise of the Cyber Security Team.

- May 9, 8:38 AM (MST): Breach Occurred.
    - Evidence suggests the virus (malware) was introduced to the server through a well-publicized cyber-attack method ("Eternal Blue") released in January 2017 affecting all Microsoft systems.
- May 9, 9:59 AM (MST): A system failure occurred on the server
    - Evidence points to the malware as the cause of the failure.
    - This led to the discovery of the virus.
- May 10: AMA files were removed from server by vendor
    - In response to the malware discovery, the vendor removed all customer files from the server.
- May 15: Server was taken offline.

The Cyber Security team identified two unique pieces of malware on the infected server:

(1) A virus ("Crypto-Miner") whose purpose is to steal computing power to generate cryptocurrency such as Bitcoin (in this case it was a currency called Monero), was tying up the resources of the computer but not extracting data. (Cryptocurrency is a digital currency that uses cryptography to verify and reward users for verifying transactions.)

(2) A virus that grants the attacker remote access to the server.

The viruses were part of a botnet which began infecting computers globally in early May. (A botnet is a network of private computers, infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send SPAM messages.)

Once infected, the first virus began monopolizing computer resources to generate crypto coins for the attacker. The purpose of the virus is not to discover or steal data. Despite the presence of a second virus, there is no evidence of access by a remote attacker within the server holding AMA data. This finding is bolstered by the fact that, globally, this botnet has only been observed to hijack systems for mining cryptocurrency.

Next Steps

The AMA will undertake a comprehensive review of our processes and policies to identify areas of improvement within our data protection strategy. Findings and recommendations will be reviewed by the AMA's Committee on Financial Audit.

[1] This document does not constitute a formal report. The results of the investigation were based upon information available at the time of the review, and are provided for the use of the AMA. PwC and/or the AMA are not liable or responsible for any losses or costs to any third party who may rely or act upon the information herein.