F12-01-MS: Summary of the Office of the Information and Privacy Commissioner's (OIPC) Investigation of the breach of personal information at the British Columbia Institute of Technology

Introduction

In June, 2012 during an audit of its information systems, the British Columbia Institute of Technology (BCIT) discovered an anomaly on one of its servers. Further investigation revealed that the server had been accessed by an unknown intruder in the early months of 2012. The server stored and processed information related to the Student Health Services Medical Clinic.

BCIT reported the breach to the OIPC on June 27, 2012.

Investigation

The purpose of the investigation was to determine whether BCIT had responded to the breach adequately including containing the breach, evaluating the risks associated with the breach, notifying affected individuals about the breach and mitigating the risks associated with the breach.

Key steps in responding to privacy breach

Breach containment

Upon discovering the breach, the BCIT Information technology services team contacted the department responsible for the server and took the server offline to contain the breach and prepare the system for further investigation. Checks were then performed on other servers in the BCIT environment to determine whether the breach was limited to the one system or whether multiple systems were impacted and would also need to be taken offline. BCIT determined that the Student Health Services server was the only server affected by the attack.

Evaluate the risks associated with the breach

BCIT performed a computer forensic review of the affected system to determine, whether the server was compromised; the details of the compromise; and whether personal information was accessed during the

attack. BCIT also reviewed numerous other systems and system logs to ascertain the scope and impact of the breach.

The types of personal information on the server were reviewed and an assessment was done to determine the potential impacts to the 12,680 affected individuals. When the preliminary review was concluded, BCIT was unable to confirm with absolute certainty that no personal information was accessed on the server. However, given the nature of the intrusion it was unlikely the objective of the attack was to gather personal information.

Notification

On July 4, 2012, BCIT sent letters to all of the affected individuals advising them of the breach and providing contact information for individuals who had questions regarding the breach. A news release was issued on July 5, 2012 setting out the circumstances of the breach. BCIT launched a website which provided details about the breach, information on resources for affected individuals and a Q&A. Also on July 5, 2012, a notification email was sent to all of the affected individuals who had BCIT email addresses.

Prevention

BCIT identified a number of areas for improvement with respect to the compromised server including relocating the server on the network, system upgrades, increased monitoring and further restrictions on access to the system.

Conclusion

The Office of the Information and Privacy Commissioner found that BCIT responded to the breach in a timely and efficient manner and took immediate action to ensure that the causes of the breach were identified and addressed.