What We Can Learn about Canadian Privacy Laws from Casino Rama's Pending Lawsuit

By: PROLINK—Canada's Insurance Connection

In October 2016 Casino Rama suffered a massive breach exposing data on at least 10,990 people: patrons, employees, and even individuals who self-identified as having a gambling dependency.

Although Casino Rama claims to have had sufficient and reasonable security safeguards in place at the time of the breach, a recent report published by Ontario's Information and Privacy Commissioner found the measures to be inadequate in protecting the privacy of Casino Rama's patrons. **A pending $60M class action lawsuit against Casino Rama, CHC Casinos Canada Ltd., and OLG has been further fueled by the Privacy Commissioner's report and awaits approval by the courts in early May.**

The suit could involve up to 200,000 plaintiffs thanks to privacy breach notification requirements as set out by the government—even though the actual number affected is close to 11,000. The suit alleges negligence, an intrusion of privacy, emotional distress, embarrassment, and reputational damage, all resulting from the data breach.

Negligence, as defined by Canadian Privacy Laws:

The unclear language surrounding what is considered to be a ***"reasonable"*** response time to investigate a breach and to notify clients, as well as the definition of implementing ***"reasonable"*** security safeguards **leaves a large grey area for subjective interpretation.**

Pre-breach: Casino Rama's Security Measures

OLG and CHC Canada:

- Had a broad IT Security Procedures document;
- Restricted data on a need-to-know basis;
- Asked employees to sign Computer Use Agreements;
- Used web and email applications to filter malicious content;
- Educated employees on phishing;
- Used up-to-date anti-virus software;
- And more.

By all general accounts, the above appears to represent sufficient measures. So what happened? How did their safeguards fail?

The Breach:

- A computer hacker sends a **spear phishing e-mail** to the company email addresses of 11 Casino Rama employees. The email is ostensibly from a Casino Rama manager and contains a link to a supposed Holiday Work Schedule for Employees.
    - The email successfully bypasses Casino Rama's phishing and email filtering software and arrives undetected. The targeted employees, while not part of the IT department, required local administrator privileges for no other reason than to access legacy software important to the business operations. They likely lacked the training and awareness of administrators with broad security enforcement responsibilities.
        - Those of the 11 who clicked on the malicious link, thought it was broken when it didn't take them to any page. They did not pursue it any further.
        - Others approached their manager about the email. The manager identified it as fraudulent and promptly notified the IT department.
        - Casino Rama then sent out reminder communications that outlined how employees can recognize a spear phishing attack and advised that employees should delete the email and avoid clicking on any unknown links in the future.

- **Several days after the incident:** a Casino Rama employee notifies the IT department that a remote connection to her desktop prevented her from logging in at her workstation. In response, Casino Rama's IT team launches a small-scale investigation but ultimately classifies the event as a low-severity incident.
    - Approximately three days after, the IT department changed all administrator, server, and firewall passwords.
    - Eight days following the remote connection incident IT conducted a thorough scan of the employee's workstation. That's when they determined a Russian IP address was attempting to communicate with the computer. Casino Rama blocked the IP address and considered the issue resolved.

- **In November 2016, the OLG notified the Information and Privacy Commissioner of a potential data breach at Casino Rama, and a few weeks later, the hacker released 4.49 gigabytes of sensitive information on the internet.**

Where Casino Rama Fell Short: the Privacy Commissioner's Perspective

The main errors highlighted in the Privacy Commissioner's Report were as follows:

- **Error #1:** Granting administrator access to employees who do not need it to perform essential duties and who do not understand the security risk. The legacy software, with lackluster security measures, acted as an easy gateway to the organization's server.
- **Error #2:** Launching communications that did not instruct employees to report to their IT department if they had already clicked the link. Casino Rama believed that it had sufficient measures in place to handle any unforeseen consequences. This helped mask the size and scope of the attack.

- **Error #3:** Failing to investigate quickly and appropriately. Eight days may seem like a short amount of time, but Ontario's Privacy Commissioner firmly states that every minute counts when dealing with privacy breaches.

How Privacy Breach Insurance Can Help:

Privacy Breach Insurance can obviously help offset some of the potential financial liability related to legal costs and damages. The insurance also includes:

- Access to a forensic investigations team to help you determine the size and scope of the breach;
- A breach coach who will guide you through the legal process of navigating a breach under attorney-client privilege. The coach will tell you what to report and when;
- Funds to set up credit monitoring and notification for affected parties; and
- A team of consultants to help manage your organization's reputation.

Need guidance? PROLINK will help you plan and protect. We can share what steps others in your industry are taking and advise you based on your unique operations.

Contact Peter McCabe at 416 644 7730 or PeterM@prolink.insure for more information today!