THE CYBER THREAT LANDSCAPE IS EXPANDING ARE YOUR STAFF PREPARED AND IS YOUR BUSINESS SECURE?

Viruses, Malware, Ransomware, Phishing; the cyber threats that businesses of all sizes face are evolving and are becoming more frequent. According to Beazley plc (Beazley), a leading provider of data breach response insurance, small businesses continue to be a main target for cyber criminals (reference). This is largely due to the type of information collected from clients. The report also highlights that "…businesses also cannot ignore the all too prevalent accidental disclosures and human error risks."

For example, did you know that all three scenarios below are considered privacy breaches?

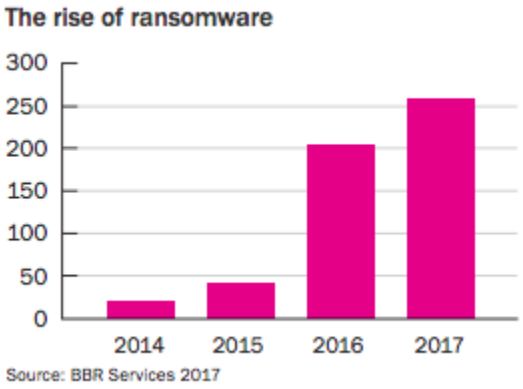
1. A virus is sent via a fake promotional email to staff, which is accidentally opened allowing access to stored customer information.

2. An employee is walking to their car and a folder of files containing customer information is blown away in a gust of wind and unable to be recovered.

3. An employee accesses customer files that they do not have authority to look at.

While many of us believe privacy breaches only stem from sophisticated attacks by elusive hackers, simply misplacing or losing documents is still considered a breach. From November 1, 2018 it will become mandatory across Canada to notify of certain privacy breaches. Businesses subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) will have to do this as soon as feasible following a breach and can face regulatory fines of up to $100,000 if they don't comply.

Ransomware also continues to be one of the largest threats to small businesses. The Beazley Breach Response team defines Ransomware as, "A type of malware used in cyber extortion that encrypts data on an endpoint or network so that the data is unusable unless the victim pays a ransom for the decryption key."



Another commonly used tactic is Email Phishing. This is carried out via email, where someone is encouraged to click on a link or proceed to provide information that subsequently downloads a virus. The emails are made to look like they're coming from the person's employer or a credible source and can be hard to differentiate from authentic correspondence.

Some tips to protecting your organization against Email Phishing:

- ✓ Establish clear procedures for how any legitimate request for financial information or fund transfer will be handled, and train relevant employees annually on the procedures. If possible, establish a policy that no requests for transfer of funds will be made or responded to by email.

- ✓ Train all employees, especially those with employee payroll or benefits information, to beware of phishing attempts.

- ✓ Configure your email system to highlight emails coming from outside the network. Phishing emails are often masked to look like they are from within the company.

Cyber attacks and privacy breaches can be costly, particularly for small and medium sized businesses. They can occur quickly and when you least expect.

The Canadian Government's "Get Cyber Safe" has a range of general tips for businesses to help mitigate the risk of a cyber attack, including:

- ✓ Educate employees to not click on pop-ups when on the internet and encourage caution when opening certain emails containing links or inconsistent branding.
- ✓ Keep software and operating systems up-to-date
- ✓ Regularly back up important data
- ✓ Encrypt computers, laptops and USBs
- ✓ Appoint an administrator and ensure the main password is changed regularly and only known to that employee

For more information, videos and additional resources to share with staff, visit the Get Cyber Safe link below.

Even after implementing multiple measures to protect your business, cyber attacks can still occur. As a Paddle Canada member, you have access to comprehensive Cyber Security & Privacy Liability Insurance coverage. This product is available for individuals or businesses of almost any size.

What protection does this offer?
The Cyber Security & Privacy Liability policy is designed to help manage the risk of holding increasingly large quantities of personally identifiable data of clients, employees, and others.

This policy includes coverage for the following:

- Payment of damages to a third party, including coverage for your legal expenses;

- Costs associated with investigation into the cause of the breach;

- Costs involved to notify individuals affected by the breach;

- Coverage for regulatory defence costs and penalties resulting from a violation of a Privacy Law;

- Coverage for ransomware and more.

For more information or if you have any questions about Cyber Security & Privacy Liability Insurance, contact a broker at BMS on 1-855-318-6558 or at paddlecanada@bmsgroup.com.

References:
https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtct-smlbsn/dctn-mpls-en.aspx
https://www.beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf