WeirFoulds LLP

National Cyber Security Awareness Month: 10 Tips For Businesses

September 30, 2016

By Ralph Kroman

In a world that is more connected and accessible than ever, the declaration of October as national Cyber Security Awareness Month by governments and business leaders in several countries including Canada, the United States and Australia, is a strong statement that cybersecurity is an international safety concern.

The campaign aims to bring awareness to the wide scope of concerns that the term cybersecurity covers, including internet security, privacy, mobile safety, distributed denial-of-service (DDoS) attacks, botnets, hacking, data breaches, malware, pharming and phishing to name a few.

Now is a good time for businesses to review their cybersecurity practices. It is tempting to think that "it can't happen to me", but in the wake of Yahoo's recent admission that personal data was hacked, it is clear that this can happen to anyone.

Of course, technological safeguards are critical to security, however operations and policy play a crucial role as well. The steps outlined below focus on tips that involve measures that go beyond technology.

1. **Plan on a Prudent Response**. In a 2015 study commissioned by the Office of the Privacy Commissioner of Canada, only 41% of surveyed companies stated that they had policies or procedures in place that dealt with data breaches where there was a compromise of customer personal information. If an Incident Response Plan is made ahead of time in order to deal with a cybersecurity breach, a company will be in a position to respond quickly in a manner that mitigates harm to the business and to third parties (such as customers). Companies who do not make such a Plan are often caught flat-footed and fumble through an incident, and increase the risk of complaints to regulators and class action or other lawsuits.
2. **Build an Effective and Safe Cybersecurity Workforce**. Robust recruitment processes that properly vet candidates will help ensure that the hiring of problematic employees is avoided. Unfortunately, many attacks come from inside an organization. Background checks are an important tool in the screening process. Employees play a key role in helping to prevent cybersecurity incidents. Proper training is key, and will enable employees to spot suspicious activities and events, and report them to the appropriate personnel. Employees are the single most important group of people who can help to reduce unintentional errors and technological vulnerabilities.
3. **Make Continuing Education a Practice**. It was recently reported in the news that the World Anti-Doping Agency was hacked by a Russian cyber group known as "Fancy Bear". The group accessed confidential medical data of athletes because a password was obtained through spear phishing (generally an e-mail that appears to be from someone the recipient knows and trusts – such as someone in a position of authority in the recipient's company). News reports about incidents like this should be shared and discussed with employees as they provide an opportunity for companies to educate and share information with personnel about cyber risks.

4. **Create an Incident Response Team**. If a cybersecurity breach occurs, a business must act quickly. The establishment of an Incident Response Team will make the business nimble and mitigate harm. Key stakeholders to be included on the Team may include executive leaders/decision makers, IT and security, marketing and business development (media and other third-party notifications), legal (breach and notification obligations and protection from potential litigation), privacy and human resources.
5. **Have a Lead Person**. The Incident Response Team needs a lead who is primarily responsible for dealing with an incident and whose duties include (i) conducting an initial immediate assessment of an incident, (ii) determining the extent to which the information, system or network is impaired, (iii) reaching out to the Incident Response Team (and other appropriate personnel) depending upon the initial assessment, and (iv) being the main point of contact.
6. **Create Relationships with Third Party Service Providers**. It is best to retain third-party contacts for the purpose of a cyberbreach response before the incident occurs. Common sense dictates that it will be less expensive and more efficient if third-party engagements are considered by a company and finalized before (as opposed to after) a cyberbreach. Potential service providers include legal (assess and deal with breach notification obligations to third parties), public relations firms (deal with reputation management) and forensics. In-house IT resources are useful to take the machines/system offline and preserve evidence – but third-party forensics may be required to investigate and remediate the incident to get the organization back in business.
7. **Consider Cyber Insurance**. Traditional insurance coverage may help deal with risks and potential losses posed by cyber risks to a certain extent, but cyber insurance policies extend coverage. Cyber insurance may be purchased separately or may run parallel with existing insurance at an increased premium. Both first-party coverage and third-party coverage are available. First-party coverage insures the policyholder from a loss resulting from a cybersecurity incident and third-party coverage covers the policyholder regarding liabilities to outside entities as a result of an incident. Third-party coverage may help with crisis management including public relations expenses related to dealing with a response to the incident. First-party coverage may also extend to payments to cyber extortionists who threaten to disclose sensitive confidential information unless their demands are met.
8. **Be Careful About What You Say Today**. Sometimes online privacy policies and other publications of a company make statements about security such as the company has "implemented reasonable and appropriate means to protect personal information against unauthorized access." In a US case, a court held that the foregoing statement was deceptive in light of the company's actual cybersecurity practices. A company risks liability if it makes statements to the public about cybersecurity that are not readily justified by the facts. Be wary about merely copying and pasting text into privacy policies and other publications.
9. **Be Prepared – Identify Disclosure Obligations**. It is best to keep abreast of privacy breach notifications and obligations imposed by legislation in each jurisdiction where a company does business. The rules are not uniform, and some preparation will help a company to respond to an incident efficiently. The legal landscape is changing. Canada's Digital Privacy Act passed in June, 2015 will require an organization to notify the Privacy Commissioner and affected individuals of any "breach of security safeguards involving personal information under the organization's control, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual". It is anticipated that these data breach disclosure obligations will come into force when final regulations are passed.
10. **Work on "Operational Security" (OPSEC)**. OPSEC is a term originating in the military. In the context of cybersecurity, it involves (i) identifying the information that is most critical to successful business operations (such as customer lists and other contact information), (ii) analysis of the likely cyber criminals who may attempt to obtain critical information, (iii) identification of the potential vulnerabilities regarding the protection of critical information (such as poorly secured mobile devices that have access to the critical information), (iv) investigation of measures to mitigate each vulnerability, and (v) implementation of measures based upon the cost of implementing each measure against the harmful effects of a cybersecurity breach.

For more information or inquiries:

Ralph Kroman

Toronto
416.947.5026

Email:
rkroman@weirfoulds.com

Ralph Kroman brings broad experience and high-level expertise to his business law practice with an emphasis upon contract negotiations, intellectual property, information technology and commercial transactions.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035