THOMPSON DORFMAN SWEATMAN

Privacy and Cyber Safe Questions

Authors: Doug Tait

published 11/17/2020

Reducing unnecessary legal spend

When it comes to legal services, an ounce of prevention really is a pound of care. While our litigators make a living litigating, they all advise their clients to be proactive in order to avoid disputes, because the cost of going to court is so high.

Cybersecurity and data protection is no different. In fact, the 2019 total average cost (both direct and indirect) of a data breach in the U.S. was 8.2 million. While the Canadian figures are not likely as high as in the U.S., the total average cost of a data breach in Canada still exceeds $1,000,000.

So how can businesses, crown corporations, municipalities, and other organizations reduce unnecessary legal spending? By proactively developing plans and policies related to cybersecurity, data protection, and privacy law. The costs (legal, IT, and others) associated with developing these plans and policies should be viewed as an investment and not an expense. The reason being, the potential return on investment from avoiding significant government fines, class action lawsuits, and crippling brand damage, easily covers the costs of preventing a breach in the first place. For organizations doing business in the European Union (EU) and/or the United States (U.S.), the potential risks and costs are of course higher, due to GDPR in the EU and **CCPA in the U.S.**

Organizations that are concerned with cybersecurity risks and want to reduce unnecessary legal spend, can take a proactive first step, by completing the checklists below.

Is your organization privacy compliant and cyber safe?

1. Has your organization conducted assessments to identify, quantify, and prioritize its current privacy, data protection, and cybersecurity risks?
2. Can your organization identify its privacy, data protection and cybersecurity compliance obligations?
3. Is your organization aware of the relevant domestic and international privacy laws (e.g. PIPEDA,

GDPR, CCPA) that may govern your organization?
4. Does your organization have the appropriate policies, procedures and processes in place to address its privacy, data protection and cybersecurity risks and compliance obligations?
5. Does your organization know all the types of data it holds, where it holds the data, how the data is protected, and who has access to the data?
6. Does your organization apply security safeguards, both technological (such as firewalls, anti-malware and intrusion detection system) and physical (such as locked doors, access cards and security cameras), appropriate to the sensitivity of the data it holds?
7. Does your organization's employees have the appropriate degree of awareness, knowledge, skill and training to effectively deal with the sensitivity of the data it holds and address the applicable privacy, data protection and cybersecurity risks?
8. Does your organization have a formal incident response plan to deal with a breach of security safeguards that it regularly tests and updates?
9. Does your organization evaluate and manage privacy, data protection and cybersecurity risks arising from its contractual obligations with third-party contractors or service providers?
10. Does your organization have Cyber Insurance? If so, do you fully understand what is covered? Do you fully understand what is not covered (i.e. the policy exclusions and other limitations)? Are you fully satisfied that the policy adequately addresses the specific needs of your organization?

If you answered NO or I DON'T KNOW to any of these questions, your organization could be at risk of being non-compliant with its privacy and data protection obligations, or in the event of a security incident. We can help you protect and defend your organization.

Acronym terms:

Personal Information Protection and Electronic Documents Act (PIPEDA)

General Data Protection Regulation (GDPR)

California Consumer Privacy Act (CCPA)

204.934.2587. Please be aware that any unsolicited information sent to the author(s) cannot be considered to be solicitor-client privileged.

While care is taken to ensure the accuracy for the purposes stated, before relying upon these articles, you should seek and be guided by legal advice based on your specific circumstances. We would be pleased to provide you with our assistance on any of the issues raised in these articles.

