Cybersecurity Readiness for In-House Counsel

Authors: Jeffrey Kowall

published 07/11/2024

As threat actors ramp up efforts, organizations need to be prepared for a cybersecurity incident. With first-hand knowledge of an organization's operations, in-house counsel can serve as a valuable resource to ensure that the organization has cybersecurity readiness policies and procedures that comply with the organization's legal obligations and best practices.

As part of a cybersecurity readiness team, in-house counsel should:

- identify statutory and other regulatory requirements applicable to the data that the organization collects, including those of a **foreign jurisdiction** in which the organization operates.
- identify the statutory or other regulatory notice requirements triggered by a **cybersecurity breach** and implement procedures to ensure that the required notices are provided to regulators and affected individuals.
- ensure that the organization's data retention policies comply with applicable statutory and operational requirements and that procedures are in place to make sure that data no longer required to be retained is being deleted.
- ensure that the organization's privacy policies comply with statutory requirements and accurately reflect how the organization collects, uses, stores, shares and deletes personal information and other sensitive data.
- establish procedures to ensure that any confidential or other sensitive data collected under contract with a third party is used, stored and deleted in accordance with contractual requirements and identify the contractual obligations triggered by a cybersecurity incident.
- ensure that the organization vets potential third-party suppliers to assess the suitability of their cybersecurity readiness policies and procedures and that a contract with a third-party supplier contains appropriate cybersecurity readiness obligations and breach notification procedures.
- assist in preparing an information security policy to ensure that internal data security and access policies and procedures reflect applicable legal requirements and best practices.
- assist in preparing an incident response plan that provides a roadmap for the organization to follow in the event of a cybersecurity breach, ensuring compliance with legal requirements and other damage mitigation measures.
- assist in developing internal staff training programs relating to cybersecurity risks.
- assist senior management with cybersecurity risk oversight efforts and ensure that cybersecurity risk assessment is part of all new organization initiatives.
- establish protocols for engaging external counsel to provide advice and assist in managing a response to a cybersecurity incident and to preserve solicitor-client privilege over incident response documentation and information whenever possible.
- assist in periodic reviews of cybersecurity policies and procedures to ensure they remain compliant

with legal obligations.
- Assist with evaluating **cyber insurance** policies to ensure that the organization understands the scope of the risks covered and the procedures to be followed in the event of a cybersecurity incident.

Cybersecurity threat actors continue to develop new and increasingly sophisticated methods to infiltrate an organization's systems. It is no longer a matter of whether an organization will be the target of a cybersecurity threat but when. In-house counsel should take an active role in safeguarding the organization against a cybersecurity threat by having cybersecurity and data protection checklists and robust policies in place which comply with applicable legal and contractual obligations and best practices.

This article is presented for informational purposes only. The content does not constitute legal advice or solicitation and does not create a solicitor-client relationship. The views expressed are solely the author's and should not be attributed to any other party, including Thompson Dorfman Sweatman LLP (TDS), its affiliate companies or its clients. The author makes no guarantees regarding the accuracy or adequacy of the information contained herein. The author is not able to provide free legal advice. If you are seeking advice on specific matters, please contact Keith LaBossiere, CEO and Managing Partner, at ***kdl@tdslaw.com*** *or (204) 934-2587. Please be aware that any unsolicited information sent to the author is not solicitor-client privileged.*

Are you interested in booking a 30-minute consultation? If so, please contact Jeffrey Kowall at **jkowall@tdslaw.com**, and somebody will contact you shortly.

---

would be pleased to provide you with our assistance on any of the issues raised in these articles.

