HARVARD WESTERN INSURANCE

Cyber
RISKS & LIABILITIES

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputations and discouraging inappropriate employee behaviour. Many companies already have these policies in place, but they may need to be tailored to reflect the increasing impact of cyber risk on everyday, professional and personal transactions.

Policies to Manage Cyber Risk

As with any other business document, cyber security policies should follow good design and governance practices—not so long that they become unusable, not so vague that they become meaningless, and regularly reviewed to ensure that they stay pertinent as your business' needs change.

Establish Security Roles & Responsibilities

One of the most effective and least expensive means of preventing serious cyber security incidents is establishing a policy that clearly defines the separation of roles and responsibilities concerning systems and the information they contain. Many systems are designed to provide for strong role-based access control (RBAC), but this tool is of little use without well-defined procedures and policies to govern the assignment of roles and their associated constraints.

At a minimum, such policies need to identify company data

data ownership and employee roles for security oversight and their inherent privileges, including:

- **Vital roles and the privileges and constraints accorded to those roles.**
- **The types of employees who should be allowed to assume the various roles**
- **How long an employee may hold a position before access rights must be reviewed**
- **If employees may have multiple roles, the conditions defining when to adopt one position over another**

Depending on the types of data regularly handled by your business, it may also make sense to create separate policies governing who is responsible for certain types of data. For example, a business that handles large volumes of personal information

from its customers may benefit from identifying a chief steward for customers' privacy information. The steward could serve not only as a subject matter expert on all matters of privacy but also as the champion for process and technical improvements to the handling of personally identifiable information (PII).

Develop a Privacy Policy

Privacy is vital for your business and your customers. Continued trust in your business practices and products and secure handling of your client's unique information impact your profitability. Your privacy policy is a pledge to your customers that you will use and protect their information in ways they expect, and that adhere to your legal obligations. To have a successful Privacy policy, consider the following:

- **Policies need to be simple, with a clear statement outlining the information being collected from customers and how that information will be used**
- **Ensure privacy policies, rules, and expectations of employees and partners are clearly expressed**

Establish an Employee Internet Usage Policy

The limits on employee Internet usage in the workplace vary widely from business to business. Rules for behaviour are necessary to ensure that all employees are aware of boundaries to keep themselves safe and your company successful. Some guidelines to consider:

- Personal Breaks: **Limit to a reasonable time period and specific activities**
- Web Filtering Systems: **Employees should know how/why their web activities are monitored and what sites are deemed unacceptable**
- Workplace Behavior: **Rules should be clear, concise and easy to follow. Reduces the risk of an employee making a judgment call which may be deemed inappropriate**

Establish a Social Media Policy

A solid social media policy is crucial for any business that uses social networking to promote its activities and communicate with its customers. At a minimum, a social media policy should include:

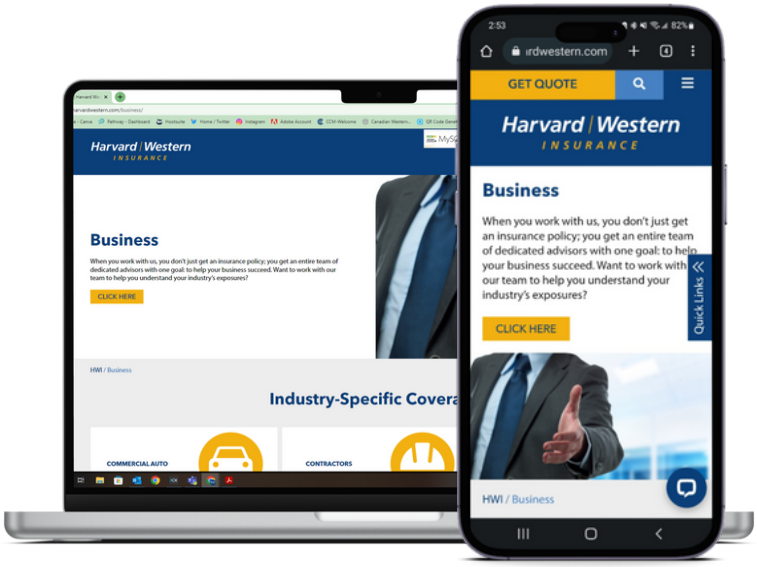
- Disclosure of Company Activities: **Specific guidelines should be enforced on what can be discussed in a public format**
- Employee Behavior: **Additional rules for using personal social networking accounts to identify what kinds of discussion topics or posts could cause risk for the company**
- Company Email Usage: **Guide use of the company email address to register for/get notices from social media sites**
- Password Strength: **Lengthy passwords with unique symbols should be used. Very few social media sites enforce strong authentication policies for users**

All users of social media need to be aware of the risks associated with social networking tools and the types of data that can be automatically disclosed online when using social media. Educate your employees on the potential pitfalls of social media use, especially sites with geo-location services.

Identify Potential Reputation Risks

All organizations should take the time to identify potential risks to their reputations and develop strategies to mitigate them with policies or other measures. Specific types of reputation risks include:

- **Online impersonation by a criminal organization (e.g., an illegitimate website spoofing your business name and copying your site design, then attempting to defraud potential customers via phishing scams or other methods)**
- **Having sensitive company or customer information leaked to the public via the Web**
- **Having sensitive or inappropriate employee actions made public via the Web or social media**



All businesses should set a policy for managing these risks and should cover their process for identifying potential threats to the company's reputation in cyberspace, practical measures to prevent those risks from materializing, and plans to respond and recover from incidents as soon as they occur.

Contact our Team today to learn more about your industry's exposures and cyber security policy options to help you protect what matters most.

Harvard | Western INSURANCE

harvardwestern.com