Courtesy of
Crendon Insurance Brokers Ltd

CYBERRISKS&LIABILITIES_

Policies to Manage Cyber Risk

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputations and discouraging inappropriate behaviour by employees.

Many companies already have these types of policies in place, but they may need to be tailored to reflect the increasing impact of cyber risks on everyday transactions, both professional and personal. 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 reviewed regularly to ensure that they stay pertinent as your business' needs change.

Establish security roles and responsibilities.
One of the most effective and least expensive means of preventing serious cyber security incidents is to establish a policy that clearly defines the separation of roles and responsibilities with regard to 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 clearly identify company data ownership and employee roles for security oversight and their inherent privileges, including:

- Necessary 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 role before access rights must be reviewed
- If employees may hold multiple roles, the circumstances defining when to adopt one role 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 sole manager for customers' private information. The manager 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 handling of personal information.

Develop a privacy policy.
Privacy is important for your business and your customers. Continued trust in your business practices, products and secure handling of your clients' unique information impacts your profitability. Your privacy policy is a pledge to your customers that you will use and protect their information in ways that they expect and that adhere to your legal obligations.

Your policy should start with a simple, clear statement describing the information you collect about your customers (physical addresses, email addresses, browsing history, etc.), and what you do with it. There are a growing number of regulations protecting customer and employee privacy, such as the Data Protection Act, which often carry costly penalties for privacy breaches.

That's why it's important to create your privacy policy with care and post it clearly on your website. It's also important to share your privacy policies, rules and expectations with all employees and partners who may come into contact with that information. Your employees need to be familiar with your privacy policy and what it means for their daily work routines.

Establish an employee Internet usage policy.
The limits on employee Internet usage in the workplace vary widely from business to business. Your guidelines should allow employees the maximum degree of freedom they require to be productive (for

Crendon Insurance Brokers

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact a legal or insurance professional for appropriate advice.

example, short breaks to surf the Web or perform personal tasks online have been shown to increase productivity). At the same time, rules of behaviour are necessary to ensure that all employees are aware of boundaries, both to keep themselves safe and to keep your company successful. Some guidelines to consider:

- Personal breaks to surf the Web should be limited to a reasonable amount of time and to certain types of activities.
- If you use a Web filtering system, employees should have clear knowledge of how and why their Web activities will be monitored, and what types of sites are deemed unacceptable by your policy.
- Workplace rules of behaviour should be clear, concise and easy to follow. Employees should feel comfortable performing both personal and professional tasks online without making judgement calls as to what may or may not be deemed appropriate. Businesses may want to include a splash warning upon network sign-on that advises employees about the company’s Internet usage policy so that all employees are on notice.

Establish a social media policy.
Social networking applications present a number of risks that are difficult to address using technical or procedural solutions. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. At a minimum, a social media policy should clearly include the following:

- Specific guidance on when to disclose company activities using social media, and what kinds of details can be discussed in a public forum
- Additional rules of behaviour for employees using personal social networking accounts to make clear what kinds of discussion topics or posts could cause risk for the company
- Guidance on the acceptability of using a company email address to register for, or get notices from, social media sites
- Guidance on selecting strong passwords for social networking accounts

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. Taking the time to educate your employees on the potential pitfalls of social media use may be the most beneficial social networking security practice of all.

Identify potential reputation risks.
All organisations should take the time to identify potential risks to their reputations and develop a strategy to mitigate those risks with policies or other measures as available. Specific types of reputation risks include:

- Being impersonated online by a criminal organisation (such as 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 sites

All businesses should set a policy for managing these types of risks and plan to address such incidents if and when they occur. Such a policy should cover a regular process for identifying potential risks to the company’s reputation in cyber space, practical measures to prevent those risks from materialising and plans to respond to and recover from incidents as soon as they occur.

Crendon Insurance Brokers Ltd has numerous sample policies available to our clients upon request. These policies are a great starting point for your policy-creation efforts and can be modified to fit the unique needs of your business.