cybersavvy

Cyber Insurance Checklist

Are you considering cyber insurance for your business? One of the steps will be to fill-in an application that insurers can use to assess the risks to your organization and appropriately price your policy.

When completing the form, it is important for you to communicate the good risk management strategies you already have in place for your business. You should also consider what other risk mitigation plans you can implement to improve your organization's risk profile.

To help you prepare, below is a checklist of questions you could be asked when applying for cyber insurance.

How would you describe your business?

1. How would you describe the operation(s) of the organization?
2. How many employees/contractors do you have working for the organization(s)? List the employee count per division.
3. Who is your customer? Consumers (B2C), government or other businesses (B2B).
4. What is the breakdown of revenue between the various divisions, type of consumer (B2C, B2B, etc.), and between revenue from Canada, USA and foreign/international?

What information does your business collect and do you need to collect this information?

1. Specifically, how many records from the list below do you retain in your organization?
    - credit and debit card account numbers
    - chequing, banking and clearing house information

- financial data for others
- government issued identification (driver's license, passports, social insurance numbers)
- personal information: Name, address and contact details for individuals
- medical or health information for individuals
- any information on children that use your services, do you get parental permission?
- trade secrets or intellectual property
- other organizations corporate information

- **TIP:** Consider reducing the information collected to reduce your exposure to privacy loss and breach.

What cyber security plans and protocols does your business currently have in place?

1. Do you have a dedicated Chief Privacy Officer or Chief Information Officer? In not, who is responsible for this role and what qualifications do they have? If this is the Presidents/CEO responsibility – what have you done to become qualified as a CPO or CIO?
2. Have you developed a written information/privacy security plan for the organization? Does this plan comply with existing handling and disclosure of information regulation?
3. When was the last security and/or privacy audit performed and were all recommendations completed? If any recommendations were not completed, why were they not completed?
4. Are you providing security/privacy training for all staff?

What cyber security controls do you have in place to help reduce your business' cyber risk?

1. What physical controls are used to prevent access to the facility/office(s)?
2. What are the current security measures used to prevent access to systems and servers?
3. What technology is used for encryption, authentication, anti-virus, and firewall?
4. What is the annual budget for all cyber protection controls?
5. What physical controls, security measures and technology will be updated in the next 6 months to improve cyber protection? For example:
    - regular backup of computer systems and data

- regular software updates
- use of anti-virus software, firewall security or spam filtering
- document/email retention and destruction policies
- protected access for all wireless networks
- access control and authentication procedures (e.g., multi-factor authentication)
- encryption of all sensitive and confidential information
- electronic device inventory
- controlled use of foreign applications on workplace equipment.

Are you a business owner with general questions about how you can reduce your cyber risk or about getting a cyber insurance policy? Insurance Bureau of Canada (IBC) can help. Contact IBC's free Consumer Information Centre by calling 1-844-2ask-IBC (1-844-227-5422) or visit us at IBC.ca.

Disclaimer: *Insurance Bureau of Canada's Cyber Insurance Assessment provides general information about cyber risk for your convenience only. This information should not be construed as providing specific cyber security advice.*