CISRO / OCRA

Canadian Insurance Services Regulatory Organizations

Cybersecurity readiness when using generative artificial intelligence

Preamble

Regulated insurance intermediaries (“intermediaries”) have access to and rely on a variety of technological solutions for the purpose of selling or servicing insurance products. Some of those solutions are powered by generative artificial intelligence (“generative AI”).

Generative AI refers to the use of artificial intelligence to create new content, such as writing or translating text. Intermediaries have access to various programs, platforms, or applications that use generative AI.

Intermediaries using technological solutions powered by generative AI (“AI solutions”) in the course of business activities should review their cybersecurity practices and ensure that appropriate measures are in place to prevent cyber incidents that could compromise or lead to the theft of customer information.

This publication provides general information for intermediaries on the importance of adapting their cybersecurity strategy to the risks specific to the use of AI solutions. This information is complementary to the cyber security practices proposed in the Cyber Security Readiness reference document, which intermediaries are invited to refer to.

Types of AI solutions

Intermediaries have access to various AI solutions that are available online or may be integrated into an organization’s IT systems or networks.

Public and open solutions are available online and accessible to everyone. The information shared through these solutions is transmitted and processed on servers that are not controlled by the organization. It is then analyzed and may be redistributed to the public. The organization cannot exercise any control over the information shared with a public and open solution.
e.g. a chatbot available for free or a translation tool accessed via a paid subscription.

Private and closed network solutions are integrated into the organization’s network. The information inputted into the organization’s computer systems is transmitted and processed on servers controlled by the organization or a third-party service provider. It is then analyzed and redistributed only to users authorized by the organization. The organization can determine the cybersecurity measures they need to implement to prevent or mitigate the cyber risks associated with these solutions.
e.g. a virtual assistant integrated into a software or cloud services.

Enterprise AI are developed by the organization or in partnership with a third-party service provider to meet their specific needs. The information is shared into the organization’s computer systems and processed on servers controlled by the organization. The organization can determine the cybersecurity measures they need to implement to prevent or mitigate the cyber risks associated with these solutions.

Questions for organizations to consider when using generative AI

1. Is your organization using generative AI or is considering using it?

The organization should ensure that the person overseeing cybersecurity risks and members of the organization are able to recognize whether the technological solutions they use or intend to use are powered by generative AI.

The organization should know which programs, platforms and applications used in the course of business activities are AI solutions and know what information is being shared with them.

The organization should consider the assistance of a cybersecurity professional to understand and assess the risks associated with each type of AI solution when using them or considering doing so.

2. Do you know the risks of using generative AI?

The organization should also ensure that appropriate cybersecurity measures are implemented. These measures should be tailored to the risks specific to each type of AI solution.

For example, since information shared with a public and open solution is processed on servers that are not controlled by the organization, no confidential information should be shared with this type of AI solution.

As the organization is responsible for the services it outsources to third-party service providers, it should identify the risks associated with the use of a third-party service provider's AI solution and assess its cybersecurity practices before integrating it into the organization's computer systems and networks.

3. Are your cybersecurity policies and procedures adapted to the use of AI solutions?

The organization should review its cybersecurity policies and procedures to ensure that members of the organization are following cybersecurity practices adapted to the use of AI solutions.

For example, the organization should inform its members of AI solutions they are allowed to use, prohibit sharing confidential information in a public and open solution, and review the control over access to data inputted in a private and closed solution or in a custom solution.

The organization should update its cyber incident response plan accordingly.

4. Do members of your organization know how to use generative AI in accordance with cybersecurity best practices?

The organization should continuously train and raise awareness among its members on cybersecurity best practices specific to the use of AI solutions so they :

- Are aware of the risks associated with their use;
- Recognize the related cyber threats;
- Follow the policies and practices established by the organization.

5. Have you assessed the consequences of the use of generative AI on your liability?

The organization should understand the consequences of using AI solutions on its liability, especially in the event of an error in the content generated by an AI solution. When necessary, the organization should consult with legal counsel.

The organization should establish controls that evolve based on the use of AI solutions, including raising awareness among its members on the importance of verifying the content being generated before using or disclosing it.

Questions for individuals to consider when using generative AI

1. Does your organization govern the use of generative AI?

Check with your organization to find out if the use of AI solutions is permitted.

Review the organization's policies and procedures on this subject and follow the practices established therein.

2. Do you know how to use generative AI?

Participate in training that helps you understand how to use AI solutions and the risks of using them.

3. Do you know which AI solution to use?

Use only AI solutions that are authorized by your organization.

Check with your organization before using a public and open solution as it may not allow it's use or have put in place cybersecurity measures that you are required to follow in order to use it.

4. Do you know what information you may share with an AI solution?

Comply with your organization's policies and procedures regarding the collection, use, and storage of confidential information when using AI solutions.

Don't share confidential information in public and open solutions.

5. Can the content generated by an AI solution be trusted?

Content generated by an AI solution may be error-prone or generate false information.

Systematically check the content generated in this way before communicating it to another person, such as a client, and, if necessary, make the appropriate corrections.