FIVE QUESTIONS TO CONSIDER IN DEVELOPING YOUR INCIDENT RESPONSE PLAN

The following questions will help you in developing and maintaining your incident response plan.

1. What are your threats and risks?

- Leverage your threat and risk assessment and cyber threat scenarios to identify what type of response actions may be required
- Ensure you've considered likely deliberate, accidental incidents as well as natural hazards
- Understand who and how incidents will be detected and reported to initiate organizational response actions

2. What resources do you need to support your response actions?

- Determine what people, processes and technologies you need to support incident response
- If you have several employees and your own infrastructure, you may wish to assign an incident response coordinator
- Consider the talent you have within the organization – they don't necessarily need to be IT experts
- If you don't have the expertise, consider third party support
- Ensure you have a contact list of important resources (Senior management, IT support, internal or third-party computer Incident Response team support, media contacts, law enforcement, mandatory reporting [e.g. to pprovincial privacy officials], etc.)

3. How are you going to coordinate your responses?

- Identify roles and responsibilities within an incident response plan including decision-making authorities
- Cover preparation, detection and analysis, mitigation, recovery and post-incident analysis phases
- Ensure that the plan considers alternate roles and can adapt to different scenarios
- Define internal and external communications channels

4. How do you know your plan will work?

- Train those in specialized roles
- Test your plan regularly – at least annually
- Communicate your plan to everyone in your organization

5. How do you know your plan will continue to work?

- Monitor your business, technical and threat context
- Update your plan to address any significant changes
- Measure the effectiveness of your plan during tests and exercises – think continuous improvement!

These questions will help guide your development. Several employees may be involved, and you may assign an incident response coordinator to manage the process. However, don't forget that effective cybersecurity incident response should be based on business priorities, so it relies on your leadership and support throughout.