October 9, 2018 | Issue 9

BRITISH COLUMBIA

OCIO

Office of the Chief Information Officer

TOPIC: Incident Management and Incident Response

While the occurrence of most incidents cannot be determined, they can be contained through an effective incident management process. Managing an incident starts with a policy –an incident management policy should be in place within the organization to direct staff on steps to take when an incident occurs. It is advised to map out the incident management process so that it is easy to follow, and all staff within the organization should be aware of the incident management process.

Organizations should have the mindset "when we get breached" not "if we get breached" as the occurrence of most incidents cannot be determined, and a plan should be in place to ensure a coordinated effort of response activities. An incident response (IR) plan should contain roles and responsibilities and should list members (and alternatives) of a Security Incident Response Team (SIRT). Additionally, IR playbooks should be in place for various incident types. Incident handling should follow industry standard (i.e. Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned (PICERL)).

As mentioned in the last newsletter, policies set the tone at the top. An Incident Management policy should be in place within an organization, which should outline the process to report an incident. The policy must be followed, reviewed and updated regularly.

In relation to IR, the defensible security objective states that at a hygiene level, a plan should be in place which outlines roles and responsibilities as well as communication methods. To be proactive, playbooks for various known attack types should also be in place. Steps outlined in the playbook should be high-level and easy to follow along. Both the IR plan and playbooks are leaving documents and should be reviewed and updated regularly. Please visit our website for resources.

KEY EVENTS

- **Monthly Defensible Security Conference Call:**
  - **October 10, 2018**
  At the next conference call, we will discuss Asset Management and Change Management control areas of the DefSec framework.
  - **October 31, 2018**
  On the call, we will discuss Business Continuity and Disaster Recovery Planning.

- **BC Security Day: Nov 7, 2018**
  The Province organizes and hosts two "Security Day" events each year (Spring and Fall), free of charge. Representatives from the broader public sector, school districts, post secondary institutions, municipalities, and crown corporations are encouraged to attend. Visit the Security Day website for more information.

- **20th Privacy and Security Conference: Feb 2019**
  Anyone working in the information privacy and security fields will benefit from the speakers, discussions, and networking at the conference. The conference draws an international audience of some 1,000 delegates with an interest in cutting edge policy, programs, law, research, and technologies aimed at the protection of privacy and security.