Security Incident Response Standard for Canadian Telecommunications Service Providers (CTSPs)

V1.1 January 20, 2020

Authored by: Canadian Telecommunications Cyber Protection (CTCP) working group
for
Presentation by: Canadian Security Telecommunications Advisory Committee (CSTAC)

Contents

Revision History

The following table highlights edit changes to the document.

Editor	Date	Notes
CTCP Response committee	June 1, 2020	Content created
Kevin Miller, SaskTel	Sept 17, 2019	Draft started
Marc Kneppers, TELUS	Jan 20, 2020	Minor update based on stakeholder feedback

The following table highlights major content or policy changes to the document.

Section	Contribution	Date

1. Security Incident Response Standards

1.1 Incident Response Capabilities

Canadian Telecommunications Service Providers (CTSPs) should have the capability to:

1. Implement a governance structure for their cyber security incident management program.
2. Manage cyber security incidents via a defined, tested, and repeatable program.
3. Respond to operational security incidents occurring during normal and off-hour times.
4. Engage with defined contacts for reporting abusive behaviour, which is monitored and responded to appropriately.
5. Implement a process for reporting breach of sensitive information to customers, employees, or reporting agencies.

1.2 Response Procedures for Issues Affecting Customers

1.2.1 Incidents Involving Customers' Information Technology (IT) or Home Computers

CTSPs should have the capability to:

1. To indicate when customer notifications are required and what methods will be used for notification
2. Track customer notifications, including methods and frequency of notifications issued.
3. Validate third party incident information before acting on it.
4. Protect the information source in customer notifications when the source is a confidential third party.
5. Identify and respond to known breaches or potential loss situations affecting customers.

1.2.2 Breach of Customer Information

CTSPs should have the capability to:

1. Define notification procedures that can be implemented in a timely manner.
2. Document and communicate a communication plan, including who is responsible

for notification of affected customers and/or to the Privacy Commissioner.
3. Establish a trusted method for communicating breach information with customers.
4. Establish mechanisms to ensure that customers can authenticate communications from the CTSP.

1.3 Remediation and Mitigation of Malicious or Inappropriate Traffic

CTSPs should have the capability to:

1. Determine what categories of malicious traffic the TSP would be willing to throttle, filter, or block, and ensure that they have the capability to take these actions.
2. Implement security controls which will accurately detect problem network traffic.
3. Identify the conditions under which throttle, filter, or blocking actions will be taken on malicious traffic.
4. Implement strategies which will permit traffic throttling, filtering or blocking to be effective against problem traffic while minimizing the likelihood of impact on legitimate traffic.
5. Publish policies on malicious traffic remediation and mitigation within the TSP's customer Service Level Agreements (SLAs) and Acceptable Use Policy (AUP).