Advisory

Category: Supervisory

Subject: Technology and Cyber Security Incident Reporting

Date: January 2019 **Effective Date: March 31, 2019**

Purpose

As members of a sector critical to the Canadian economy, federally regulated financial institutions (FRFIs) must address technology and cyber security incidents in a timely and effective manner. A FRFI's policies and procedures for dealing with such incidents relating to their operations should include timely notification of OSFI.

The reporting of incidents can help to identify areas where a FRFI or the industry at large can take steps to proactively prevent such incidents or to improve their resiliency in cases where an incident has occurred.

Scope and Definition

This Advisory applies to all FRFIs and describes OSFI's incident reporting requirements. It does not include guidance on OSFI's expectations for an incident management framework. For such guidance, please refer to OSFI's Cyber Security Self-Assessment Guidance.

For the purpose of this Advisory, a technology or cyber security incident is defined to have the potential to, or has been assessed to, materially impact the normal operations of a FRFI, including confidentiality, integrity or availability of its systems and information.

Technology or Cyber Security Incidents assessed by a FRFI to be of a high or critical severity level should be reported to OSFI.

Criteria for Reporting

FRFIs should define incident materiality in their incident management framework. When in doubt about incident materiality, FRFIs should consult their Lead Supervisor.

A reportable incident may have any of the following characteristics:

- Significant operational impact to key/critical information systems or data;
- Material impact to FRFI operational or customer data, including confidentiality, integrity or availability of such data;
- Significant operational impact to internal users that is material to customers or business operations;
- Significant levels of system / service disruptions;
- Extended disruptions to critical business systems / operations;
- Number of external customers impacted is significant or growing;
- Negative reputational impact is imminent (e.g., public/media disclosure);
- Material impact to critical deadlines/obligations in financial market settlement or payment systems (e.g., Financial Market Infrastructure);
- Significant impact to a third party deemed material to the FRFI;
- Material consequences to other FRFIs or the Canadian financial system;
- A FRFI incident has been reported to the Office of the Privacy Commissioner or local/foreign regulatory authorities.

Initial Notification Requirements

A FRFI must notify its Lead Supervisor, **as promptly as possible, but no later than 72 hours** after determining a Technology or Cyber Security Incident meets the incident characteristics in this Advisory.

FRFIs are expected to notify their Lead Supervisor as well as TRD@osfi-bsif.gc.ca. When reporting a Technology or Cyber Security Incident to OSFI, a FRFI **must do so in writing** (Electronic/Paper). Where specific details are unavailable at the time of the initial report, the FRFI should indicate 'information not yet available.' In such cases, the FRFI should provide best known estimates and all other details available at the time.

Details to report include the following:

- Date and time the incident was assessed to be material;
- Date and time/period the incident took place;
- Incident severity;
- Incident type (e.g. DDoS, malware, data breach, extortion);

- Incident description, including:
    - known direct/indirect impacts (quantifiable and non-quantifiable) including privacy and financial;
    - known impact to one or more business segment, business unit, line of business or regions, including any third party involved;
    - whether incident originated at a third party, or has impact on third party services, and
    - the number of clients impacted.
- Primary method used to identify the incident;
- Current status of incident;
- Date for internal incident escalation to senior management or Board of Directors;
- Mitigation actions taken or planned;
- Known or suspected root cause;
- Name and contact information for the FRFI incident executive lead and liaison with OSFI.

Subsequent Reporting Requirements

OSFI expects FRFIs to provide regular updates (e.g. daily) as new information becomes available, and until all material details about the incident have been provided.

Depending on the severity, impact and velocity of the incident, the Lead Supervisor may request that a FRFI change the method and frequency of subsequent updates.

Until the incident is contained/resolved, OSFI expects FRFIs to provide situation updates, including any short term and long term remediation actions and plans.

Following incident containment, recovery and closure, the FRFI should report to OSFI on its post incident review and lessons learned.

Appendix

The following table provides some examples of reportable incidents, but should not be considered an exhaustive list.

Scenario Name	Scenario Description	Impact
Cyber Attack	Account takeover botnet campaign is targeting online services using new techniques, current defences are failing to prevent customer account compromise	High volume and velocity of attempts Current controls are failing to block attack Customers are locked out Indication that accounts have been compromised
Service Availability & Recovery	Technology failure at data center	Critical online service is down and alternate recovery option failed Extended disruption to critical business systems and operations
Third Party Breach	A material third party is breached, FRFI is notified that third party is investigating	Third party is designated as material to the FRFI Material impact to FRFI data is possible
Extortion Threat	FRFI has received an extortion message threatening to perpetrate a Cyber attack (e.g., DDoS for Bitcoin)	Threat is credible Probability of critical online service disruption