Advisory

Title	Technology and Cyber Security Incident Reporting
Category	Supervisory Advisories
Date	August 13, 2021
Sector	Banks Foreign Bank Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies
Effective Date	August 13, 2021

Table of Contents

Purpose

Scope and definition

Criteria for reporting

Initial notification requirements

Subsequent reporting requirements

Failure to report

Appendix I – Examples of reportable incidents

Appendix II – OSFI incident reporting and resolution form

Purpose

The Technology and Cyber Security Incident Reporting Advisory supports a coordinated and integrated approach to OSFI's awareness of, and response to, technology and cyber security incidents at Federally Regulated Financial Institutions (FRFIs). This Advisory replaces the current Technology and Cyber Security Incident Reporting Advisory, which was published in January 2019 and came into effect in March 2019.

As members of a sector critical to the Canadian economy, FRFIs have a responsibility to address technology and cyber security incidents in a timely and effective manner. FRFIs are required to provide timely notification to OSFI when incidents relating to their operations occur. This requirement should be reflected in FRFIs' policies and procedures for dealing with technology and cyber security incidents.

Incident reporting can help identify areas where FRFIs or the industry at large can take steps to proactively prevent such incidents or improve their resiliency after 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 the purpose of this Advisory, a technology or cyber security incident is defined as an incident that has an impact, or the potential to have an impact on the operations of a FRFI, including its confidentiality, integrity or the availability of its systems and information.

Criteria for reporting

FRFIs should define priority and severity levels within in their incident management framework. When in doubt about whether to report an incident, FRFIs should consult their Lead Supervisor.

A reportable incident may have **any one or more** of the following characteristics:

- Impact has potential consequences to other FRFIs or the Canadian financial system;
- Impact to FRFI systems affecting financial market settlement, confirmations or payments (e.g., Financial Market Infrastructure), or impact to payment services;
- Impact to FRFI operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity or availability of customer information;
- Disruptions to business systems and/or operations, including but not limited to utility or data centre outages or loss or degradation of connectivity;

- Operational impact to key/critical systems, infrastructure or data;
- Disaster recovery teams or plans have been activated or a disaster declaration has been made by a third party vendor that impacts the FRFI;
- Operational impact to internal users, and that poses an impact to external customers or business operations;
- Number of external customers impacted is growing; negative reputational impact is imminent (e.g., public and/or media disclosure);
- Impact to a third party affecting the FRFI;
- A FRFI's technology or cyber incident management team or protocols have been activated;
- An incident that has been reported to the Board of Directors or Senior/Executive Management;
- A FRFI incident has been reported to:
    - the Office of the Privacy Commissioner;
    - another federal government department (e.g., the Canadian Center for Cyber Security);
    - other local or foreign supervisory or regulatory organizations or agencies;
    - any law enforcement agencies;
    - has invoked internal or external counsel
- A FRFI incident for which a Cyber insurance claim has been initiated;
- An incident assessed by a FRFI to be of a high or critical severity, level or ranked Priority/Severity/Tier 1 or 2 based on the FRFI's internal assessment; or
- Technology or cyber security incidents that breach internal risk appetite or thresholds.
- For incidents that do not align with or contain the specific criteria listed above, or when a FRFI is uncertain, notification to OSFI is encouraged as a precaution.

Initial notification requirements

Under the Advisory, FRFIs must report a technology or cyber security incident to OSFI's Technology Risk Division as well as their Lead Supervisor at OSFI **within 24 hours, or sooner if possible**.

When reporting a technology or cyber security incident to OSFI, a FRFI must notify OSFI's Technology Risk Division (at TRD-DRT@osfi-bsif.gc.ca) as well as their Lead Supervisor and **must do so in writing** (Electronic[1]) as set out in

the Incident Reporting and Resolution Form (see Appendix II). Where specific details are unavailable at the time of the initial report, the FRFI must indicate 'information not yet available.' In such cases, the FRFI must provide best estimates and all other details available at the time including their expectations of when additional information will be available.

Subsequent reporting requirements

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

Depending on the severity, impact and velocity of the incident, OSFI 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.

Failure to report

Failure to report incidents as outlined above may result in increased supervisory oversight including but not limited to enhanced monitoring activities, watch-listing or staging of the FRFI.

Appendix I – Examples of reportable incidents

The following table provides some examples of the types 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 defenses 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 customer account(s) or information has 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 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

Appendix II – OSFI incident reporting and resolution form

FRFIs are required to report incidents to the Technology Risk Division at TRD-DRT@osfi-bsif.gc.ca as well as their Lead Supervisor using the OSFI Technology and Cyber Incident Reporting Form.

Footnotes

1 If electronic means of notification are not available, notification by telephone followed by a paper submission is acceptable.