~~Advisory~~

~~Category: Supervisory~~

~~Subject:~~ Technology and Cyber Security Incident Reporting

Type of Publication: Advisory
Category: Supervisory
Date: ~~January 2019~~ August 2021
Effective Date: ~~March 31, 2019~~August 13, 2021

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, ~~federally regulated financial institutions (FRFIs) must~~FRFIs have a responsibility to address technology and cyber security incidents in a timely and effective manner. ~~A FRFI's policies and procedures for dealing with such~~FRFIs are required to provide timely notification to OSFI when incidents relating to their operations occur. This requirement should ~~include timely notification of OSFI~~be reflected in FRFIs' policies and procedures for dealing with technology and cyber security incidents.

~~The~~Incident reporting ~~of incidents~~ can help ~~to~~ identify areas where ~~a FRFI~~FRFIs or the industry at large can take steps to proactively prevent such incidents or ~~to~~ improve their resiliency ~~in cases where~~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 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~~priority and severity levels within in their incident management framework. When in doubt about whether to report an incident~~ materiality~~, FRFIs should consult their Lead Supervisor.

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

- ~~Significant operational impact to key/critical information systems or data;~~
- ~~Material impact to FRFI operational or customer data~~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 ~~such~~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;
- ~~Significant operational~~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 ~~is material~~poses an impact to external 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~~ negative reputational impact is imminent (e.g., public~~/~~ and/or media disclosure);
- ~~Material impact to critical deadlines/obligations in financial market settlement or payment systems (e.g., Financial Market Infrastructure);~~
- ~~Significant impact~~Impact to a third party ~~deemed material to~~affecting the FRFI;
- ~~Material consequences to other FRFIs or the Canadian financial system;~~
- A ~~FRFI~~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~~ or~~;
  - another federal government department (e.g., the Canadian Center for Cyber Security);
  - other local~~/~~ or foreign supervisory or regulatory ~~authorities~~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

~~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~~Under the ~~incident characteristics in this~~ Advisory~~.~~

, FRFIs ~~are expected~~ must report a technology or cyber security incident to ~~notify their Lead Supervisor~~ OSFI's Technology Risk Division as well as ~~TRD@osfi-bsif.gc.ca.~~ their Lead Supervisor at OSFI **within 24 hours, or sooner if possible**.

When reporting a ~~Technology~~technology or ~~Cyber Security Incident~~cyber security incident to OSFI, a FRFI must notify OSFI's Technology Risk Division (at TRD@osfi-bsif.gc.ca) as well as their Lead Supervisor and **must do so in writing** (Electronic~~/Paper).~~[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 ~~should~~must indicate 'information not yet available.' In such cases, the FRFI ~~should~~must 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~~ their expectations of ~~business or regions, including any third party involved;~~
  - ~~whether incident originated at a third party, or has impact on third party services, and~~

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

  - ~~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~~when additional information ~~for the FRFI incident executive lead and liaison with OSFI~~will be available.

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~~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.

~~Appendix~~

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.

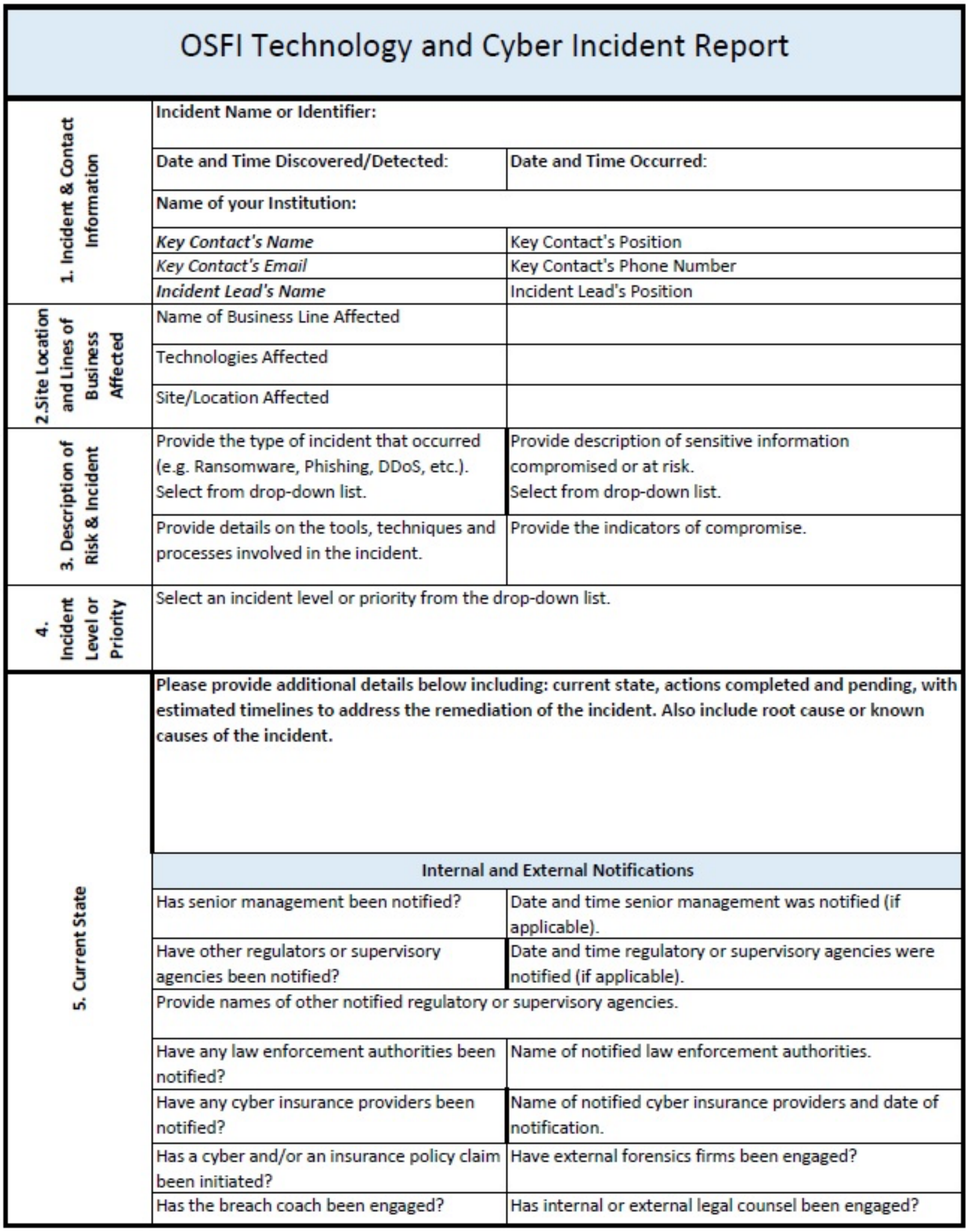
APPENDIX I – EXAMPLES OF REPORTABLE INCIDENTS

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 ~~defences~~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 ~~accounts have~~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 ~~Material impact~~Impact to FRFI data is possible
Extortion Threat	FRFI has received an extortion message threatening to perpetrate a ~~Cyber~~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@osfi-bsif.gc.ca as well as their Lead Supervisor using the template below.



OSFI Technology and Cyber Incident Report

1. Incident & Contact Information	**Incident Name or Identifier:**	
	Date and Time Discovered/Detected:	**Date and Time Occurred:**
	Name of your Institution:	
	Key Contact's Name	Key Contact's Position
	Key Contact's Email	Key Contact's Phone Number
	Incident Lead's Name	Incident Lead's Position
2.Site Location and Lines of Business Affected	Name of Business Line Affected	
	Technologies Affected	
	Site/Location Affected	
3. Description of Risk & Incident	Provide the type of incident that occurred (e.g. Ransomware, Phishing, DDoS, etc.). Select from drop-down list.	Provide description of sensitive information compromised or at risk. Select from drop-down list.
	Provide details on the tools, techniques and processes involved in the incident.	Provide the indicators of compromise.
4. Incident Level or Priority	Select an incident level or priority from the drop-down list.	
5. Current State	**Please provide additional details below including: current state, actions completed and pending, with estimated timelines to address the remediation of the incident. Also include root cause or known causes of the incident.**	
	Internal and External Notifications	
	Has senior management been notified?	Date and time senior management was notified (if applicable).
	Have other regulators or supervisory agencies been notified?	Date and time regulatory or supervisory agencies were notified (if applicable).
	Provide names of other notified regulatory or supervisory agencies.	
	Have any law enforcement authorities been notified?	Name of notified law enforcement authorities.
	Have any cyber insurance providers been notified?	Name of notified cyber insurance providers and date of notification.
	Has a cyber and/or an insurance policy claim been initiated?	Have external forensics firms been engaged?
	Has the breach coach been engaged?	Has internal or external legal counsel been engaged?

A screenshot of the OSFI Technology and Cyber Incident Report. Please refer to the Excel spreadsheet.