Government of Canada Gouvernement du Canada

Cyber Incident Management Framework for Canada

August 2013

Table of Contents

Introduction

Canadians – individuals, industry and governments – are embracing the many advantages that cyberspace offers, and our economy and quality of life are better for it. But our increasing reliance on cyber technologies makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and public safety.

Cyber threats and the risks of cyber attacks have become harsh realities that affect us all. Governments, industry and Canadians have a responsibility to protect their own portion of cyberspace. However, effective cyber security cannot be achieved in isolation. It is only through partnerships and information sharing that the cyber security posture of all our networks will improve. Organizations must have the ability to respond to cyber incidents in a well-coordinated manner, working with partners, at the local, provincial and federal levels.

Emergency management in Canada is well defined and documented with most emergencies local in nature and managed by municipalities or provincial/territorial governments. The federal, provincial and territorial (FPT) governments created in 2007 *An Emergency Management Framework for Canada* (EMF) to unify FPT emergency management initiatives. It recognizes that each FPT government has a responsibility for emergency management and public safety in Canada. The National Emergency Response System (NERS) incorporates and operationalizes the principles for emergency management as set out in the EMF. The NERS harmonizes federal, provincial and territorial response to emergencies and facilitates coordination between all levels of government, the private sector, non-governmental organizations and international stakeholders.

Emergency management in Canada is based on an all-hazards approach designed to encompass all emergencies independent of their underlying cause. This well-established approach would be enacted when a cyber incident causes consequences in the physical domain (for example, a cyber attack causing a water treatment plant serving a large city to cease operations) and would help ensure that the consequences of the incident were effectively managed. This all-hazards approach depends on the expert communities that deal with the broad spectrum of possible emergencies – natural hazards, transportation incidents, public health emergencies, infrastructure failures, etc. – having mechanisms and processes in place to handle the incident specific aspects of the emergency.

The concept of cyber security, in particular how to manage or respond to significant cyber security incidents, introduces complications to existing emergency management structures as cyberspace is independent of physical and geographical boundaries. Cyberspace is engineered, regulated, maintained, operated, owned, and secured by various levels of government and private industry. The existing EMF and NERS provide overarching guidance to respond to the physical consequences of a significant cyber incident; however, a framework specifically for cyber incidents is required that complements existing emergency management policies, frameworks, procedures and plans.

Canada is fortunate to have a talented cyber security expert community, but to date the means by which it coordinates its activities have been informal and undocumented, in part due to the complexity of cyberspace itself. There are numerous stakeholders across federal, provincial and territorial governments and the public and private sectors. This is complicated by the fact that cyber threats and attacks can originate from amateur hackers, hacktivists, criminal organizations and nation states, which traditionally are dealt with using differing authorities. Furthermore, the emergency management and cyber security communities are not uniformly connected across Canadian jurisdictions.

There are increasing numbers of bilateral and community based arrangements that provide the building blocks for a cyber-specific framework. Public Safety Canada has established partnerships with numerous partners, and many organizations are participating in regional, sector based, or professional associations. These maturing structures provide a useful toolkit (reporting criteria, thresholds, communications mechanisms and impact severity) to serve as a baseline for the Canadian cyber security community.

The Cyber Incident Management Framework (CIMF) is a guidance document involving provincial and territorial governments, critical infrastructure owners and operators, and other public and private sector partners. The CIMF is designed to complement and tie into existing federal, provincial, and territorial emergency management frameworks and plans as well as emergency plans from the critical infrastructure owners and operators.

Public Safety Canada has developed the CIMF using a collaborative approach, soliciting input from Canada's cyber security community and leveraging existing FPT and industry committees and structures. It is intended to be an evolving document that is amended as required to meet the needs of this community as it responds to and learns from handling cyber security incidents. Participation in the CIMF is voluntary, but in keeping with international best practises, all stakeholders are encouraged to adopt it for the management of cyber incidents and sharing of information. The success of the CIMF is dependent upon buy-in from cyber security stakeholders in provincial and territorial governments and the private sector.

Scope of the Cyber Incident Management Framework

The purpose of the CIMF is to provide a consolidated whole of nation approach to the management and coordination of potential or occurring cyber threats or incidents. It sets out the roles and responsibilities of all levels of government, critical infrastructure owners and operators and other public and private sector partners, in the coordinated prevention and mitigation of, preparedness for, response to and recovery from incidents affecting Canada's portion of cyberspace. The CIMF is intended to enable each organization to fully and effectively participate in a coordinated national cyber incident response.

The CIMF documents the previously informal arrangements that connect the lower-level operational relationships between partners and the over-arching emergency management constructs for three purposes:

1. To clarify roles, responsibilities, authorities and capabilities of stakeholders in the cyber security community;
2. To set expectations of all stakeholders on what they should be prepared to do, and what assistance they might obtain; and
3. To serve as a vehicle for improving the management of cyber incidents and promoting coordination.

Roles and Responsibilities of Stakeholders

Cyber Security Capabilities

In addition to any central role pertaining to the CIMF, all organizations are responsible for their own internal cyber security. It is envisioned that organizations will already have established a robust and effective cyber security capability, proportionate to their risk posture and informed by industry best practices. Many sectors have in place, or are developing, standards and regulations for information protection, operational resilience, and security that must also be followed, and which can provide guidance even if not mandatory. Appropriate measures may include incident response plans and capabilities, secure configurations for hardware and software, secure configurations for network devices, monitoring and analysis of security audit logs, disaster recovery plans, escalation procedures to senior management, linkages to governmental regulating bodies and provincial/territorial emergency management organizations and communications/public affairs plans.

While it is recognized that cyber security capability varies from organization to organization, experience has shown that outside help arriving at a time of crisis is far less effective than robust internal capacity.

Federal Government

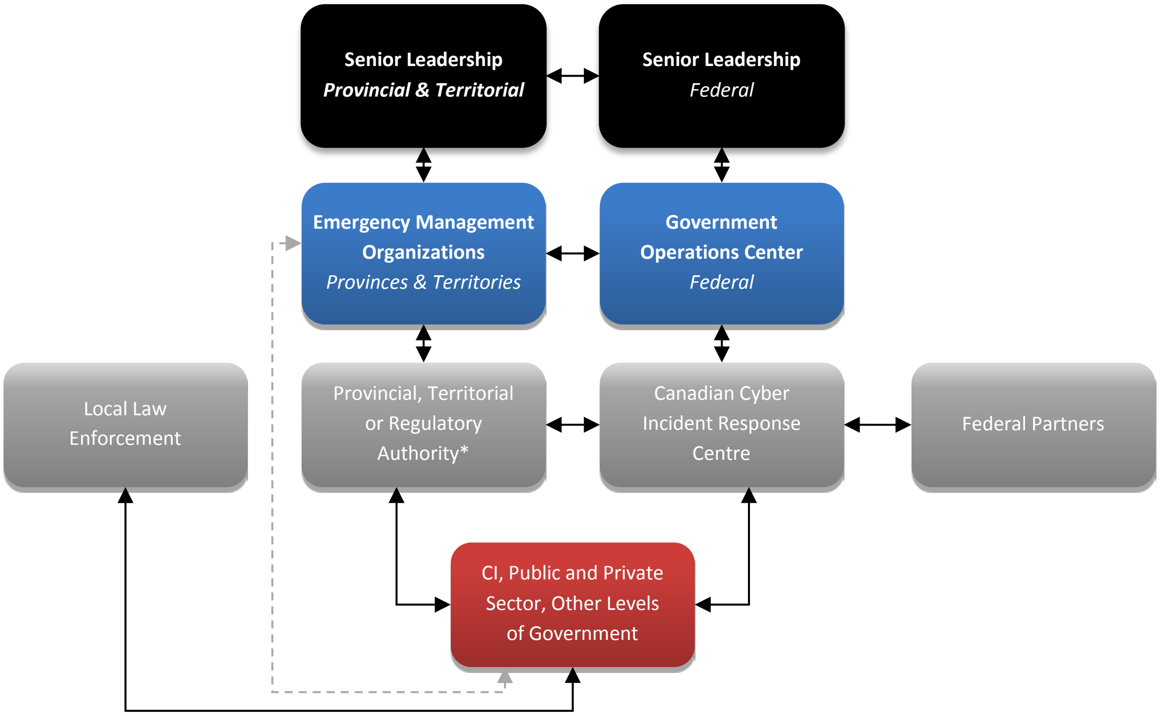
There are numerous federal government departments that play an active role in coordinating a response to cyber incidents. Departments and agencies such as Public Safety Canada (PS), the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment Canada (CSEC), and the Royal Canadian Mounted Police (RCMP) have clearly defined roles and mandates pertaining to cyber incident response. The federal government is continually working to improve internal coordination to ensure a cohesive response; much of that coordination is achieved through the Canadian Cyber Incident Response Centre (CCIRC).

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to and recovery from cyber incidents. In most cases, an affected organization's first contact with the federal government and the resources that it can bring to bear in response to a cyber incident will be via CCIRC. CCIRC, as part of Public Safety Canada, has established working relationships at the federal level with the RCMP, CSIS, CSEC, and other federal agencies. CCIRC works closely with Canada's key allies, in particular the national Computer Security Incident Response Teams (CSIRTs) of the United States, the United Kingdom, Australia and New Zealand, as well as national CSIRTs representing countries from around the world. CCIRC also has established relationships with provincial and territorial government information protection centres, critical infrastructure owners and operators and other public and private sector organizations' cyber security staffs. As a result of these relationships, CCIRC is well positioned to provide alerts and mitigation advice, and to disseminate information that will benefit all stakeholders in improving the cyber security posture of their computer systems and the information contained therein.

More information about CCIRC and instructions on how to engage can be found at the Public Safety Canada website at www.publicsafety.gc.ca.

In cases where the affected organization believes that a crime has been committed, they should contact local law enforcement authorities. In cases where the affected organization believes that there is a threat to national security, they should contact the Canadian Security Intelligence Service. It may not always be possible to know if an incident has criminal or national security implications. If required, CCIRC can review the incident and provide advice on whether to contact law enforcement or national security authorities.

Should a significant cyber incident result in physical consequences (for example, a cyber attack on an electric utility results in blackouts), the Government Operations Centre (GOC) would likely take over the lead role in coordinating consequence management. At this point, various emergency management arrangements may be invoked, including linkages to provincial and territorial emergency management organizations, as outlined below in Figure 1.


Senior Leadership
Provincial & Territorial
Senior Leadership
Federal
Emergency Management Organizations
Provinces & Territories
Government Operations Center
Federal
Local Law Enforcement
Provincial, Territorial or Regulatory Authority*
Canadian Cyber Incident Response Centre
Federal Partners
CI, Public and Private Sector, Other Levels of Government

*There may be instances where an organization has no oversight reporting requirements.

Figure 1: Notional Reporting of Cyber Incident with Non-cyber Consequences

Provinces, Territories and Other Levels of Government

Provinces, territories and other levels of government are responsible for protecting their own computer systems. They also have regulatory or oversight responsibilities for numerous industries, and will incorporate cyber security matters into regulations and guidelines as appropriate. Provincial and territorial governments have established relationships with federal and municipal emergency management counterparts and other stakeholders to coordinate the response to emergencies, and some of these arrangements include measures specific to cyber incidents. It is envisioned that organizations will already have established a robust and effective cyber security capability, as detailed above in Cyber Security Capabilities .

Critical Infrastructure Owners and Operators, and Other Public and Private Sector Organizations

Critical infrastructure owners and operators, as with all public and private sector organizations, are responsible for protecting their own computer systems. In some instances, they may have existing relationships with various levels of government to coordinate the response to cyber incidents. It is envisioned that organizations will already have established a robust and effective cyber security capability, as detailed above in Cyber Security Capabilities .

Organizations that are part of a regulated industry (e.g., telecommunications, power, oil, and gas) can expect to see increased attention to cyber security and resilience issues in the regulations and standards that apply to them. Such organizations will have existing relationships with the government department responsible for regulating their sector (either federal or provincial), as well as their provincial emergency management organization. Just as those connections would be leveraged to manage an emergency in the physical domain, they would be used for information sharing and response coordination during a cyber incident. Affected organizations are also expected to maintain contact with CCIRC for the purposes of sharing and receiving information and guidance specific to the cyber aspects of the incident. At present, it is not realistic for any organization subject to a regulatory regime to plan on engaging with only a single entity (e.g., a provincial organization or CCIRC) in a serious cyber incident. Organizations will require the internal management processes necessary to coordinate these multiple contacts.

Many public and private sector organizations have crisis management structures in place within their organization to facilitate a coordinated internal response to emergencies, regardless of the cause or nature of the emergency. Such mechanisms also ensure their Executive is apprised in an appropriate and coordinated fashion. It is important that all organizations ensure that such mechanisms are well suited to dealing with cyber incidents as well. Executive management should establish relationships with their counterparts at the appropriate levels of government, including both regulatory and emergency management organizations, to facilitate effective communication and coordination during a crisis situation.

Local Law Enforcement

Local law enforcement agencies are responsible for enforcing laws and maintaining peace, order and security. Should an affected organization believe that they are the victim of a cyber related crime, they should immediately report it to their local law enforcement agency.

Cyber Incident Management Framework Landscape

As identified above, the purpose of the CIMF is to outline the roles and responsibilities of all levels of government and critical infrastructure owners and operators in the coordinated response to cyber incidents affecting Canada’s portion of cyberspace. As such, the CIMF defines the strategic framework for coordinated response and mitigation efforts, while other documents will provide more detailed plans and procedures. The envisioned CIMF landscape, showing all the document types required for robust response to cyber incidents, is shown below in Figure 2.

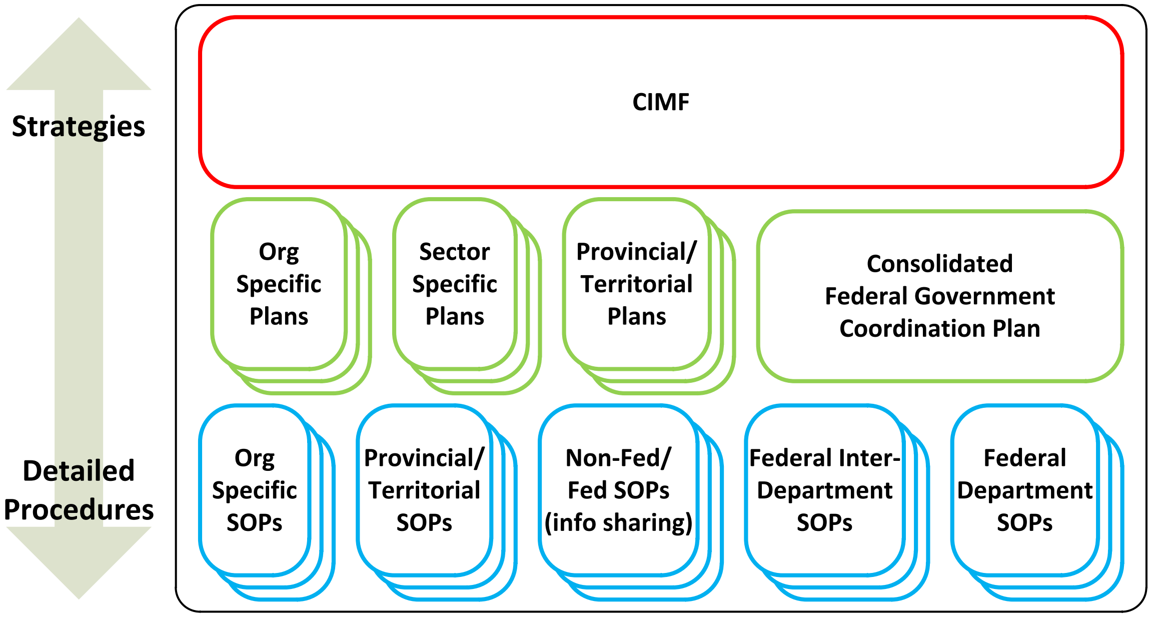

Strategies
Detailed Procedures
CIMF
Org Specific Plans
Sector Specific Plans
Provincial/ Territorial Plans
Consolidated Federal Government Coordination Plan
Org Specific SOPs
Provincial/ Territorial SOPs
Non-Fed/ Fed SOPs (info sharing)
Federal Inter-Department SOPs
Federal Department SOPs

Figure 2: Ontology of Cyber Incident Response Frameworks, Plans, and Standard Operating Procedures

Each organization should have plans in place to address the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents. Plans should also be utilized by provincial and territorial governments and critical infrastructure sectors, as required, to ensure efficient coordination and collaboration. Many of these plans already exist at various stages of maturity. For its part, the federal government is continuously working to ensure its internal coordination mechanisms are efficient and responsive.

Detailed standard operational procedures (SOPs) are also required within each participant organization to cover the daily activities of technical staff, such as reporting and information sharing, and other operational concerns. Some SOPs will be internal to each participant organization covered by the CIMF, and others will detail the sharing of information between participant organizations, including with the federal government.

Concept of Operations

The CIMF is based on the guiding principle that the people best positioned to respond to cyber incidents on an organization's network are members of that organization, as they are ultimately responsible for the operation of their network and the protection of their assets. Even in a widespread attack affecting many networks, each organization is ultimately responsible for its own defence. It must be understood that due to the complexity and uniqueness of individual networks, it is difficult for any external agency to assimilate a network's particulars quickly enough to mount a robust defence. Therefore, no organization should assume that it can rely solely on external assistance in the event of a cyber incident. Experience has shown that the best outcomes result from a sophisticated and well-prepared cyber security capability internal to the organization working collaboratively with external expert partners such as CCIRC. Organizations that are able to articulate precisely what information and advice they require are more likely to receive meaningful assistance.

CCIRC has established an Impact Severity Matrix (see Annex) to categorize cyber incidents based on several factors, including information disclosure, economic well-being, health and safety, public confidence, and essential services. This structure provides the basis for the organization of the CIMF concept of operations. While the thresholds shown may not be appropriate in all cases, each organization is encouraged to adapt a similar tiered structure to guide their internal processes and to facilitate coordination with the broader community. The matrix contains five distinct severity levels, which range from very low to very high.

The initial classification of the severity level for any given incident will be performed by the reporting client; CCIRC will evaluate all incoming incidents and, where required, work with the reporting client to determine the potential impact an incident may have. The determined level of impact will guide the actions of the reporting client, CCIRC, and partners.

In most cases, the response to a specific cyber incident will be led by the affected organization, with assistance from external partners as requested. Incidents that meet identified thresholds may require the coordinating assistance and/or response of the broader national cyber security community. In addition, a cyber security incident may trigger second or third order effects (this could be in the physical realm such as impact to water treatment plants). These incidents would require consequence management and would fall under existing emergency management policies, frameworks and arrangements.

Normal Cyber Security Operations

Maintaining cyber security is a continuous business process that should be treated as an ongoing, everyday operation. Simplistic and automated cyber attacks occur at a high rate (many times per second on a large network), and all organizations are expected to protect their computer systems and networks from these attacks, as detailed above in Cyber Security Capabilities .

All organizations participating in the CIMF are expected to report cyber incidents, regardless of impact severity level, to CCIRC. It is only through consistent and comprehensive reporting that a complete picture of cyber security incidents in Canada can be maintained. Organizations making the commitment to share cyber incident information with CCIRC and, by extension, with the Canadian cyber community, contribute to shared cyber awareness for the benefit of themselves, other organizations, and all Canadians. Reporting a cyber incident to CCIRC does not replace reporting requirements through pre-existing agreements or arrangements.

Organizations are also advised to contact CCIRC if there is any uncertainty whether or not a cyber incident has criminal or national security implications, and where an organization requires mitigation assistance.

CCIRC is committed to protecting the confidentially and anonymity of the reporting organization. Wherever possible, information shared with the Canadian cyber community will be sanitized to remove any identifying characteristics and/or reported in the aggregate.

Very Low Impact Incidents

As identified in the Impact Severity matrix, incidents with very low impact typically affect a very small number of individuals and do not result in the loss of any essential services or any significant economic impact. Such incidents are common, and most organizations are well positioned to address them without external assistance or coordination. However, the lack of any direct impact to the organization that notices the incident does not mean that some other organization has not been severely impacted. For cyber incidents involving the theft of data, for instance, it is possible that the incident will go undetected for some time by many organizations. It is for this reason that reporting incidents to CCIRC is so important, as it allows the community to benefit from the collective diligence of all members.

Expected Actions by the Affected Organization: The affected organization is expected to report these incidents to CCIRC for information purposes and trend analysis only. Sectoral associations and other communities may also wish to be informed of such incidents.

Potential Actions by the Community: Very low impact incidents do not normally require the involvement of any partner outside the affected organization. CCIRC will monitor very low impact incidents and collate reports from the community to determine if an incident initially deemed to be very low impact is part of a larger campaign affecting multiple organizations, in which case the incident severity level may be increased. Based on the nature of the incident, CCIRC may also provide mitigation advice or other recommendations.

Low Impact Incidents

Low impact incidents would be those types of incidents that are perceived to affect a small group or small community for a limited period of time (where “limited period of time” can vary widely, depending on the nature of the organization). In a low impact incident it is anticipated that there would be little to no effect on critical services for individuals.

Expected Actions by the Affected Organization: The affected organization would perform standard incident response activities to address the incident. The organization is also expected to report these incidents to CCIRC, to enable advice and observations to be shared with the broader community without attribution.

Potential Actions by the Community: Based on the details of the incident, CCIRC may prepare notifications and advise partners of the situation. As with very low impact incidents, CCIRC will monitor low impact incidents and collate reports from their client base to determine if an incident initially deemed to be low impact is part of a larger campaign affecting multiple clients, in which case the incident severity level may be increased. Organizations receiving notifications of incidents from an affected organization, a sectoral association, or CCIRC should check their own systems for similar incidents, adjust their risk posture, and share relevant information back as appropriate. CCIRC will manage a low impact cyber incident in accordance with its SOPs, including the possible provision of mitigation advice or other recommendations. CCIRC may issue a notification to other partners advising them of the situation, but will not typically escalate the incident to any other response mechanisms.

Medium Impact Incidents

Medium impact incidents are those incidents that are perceived to affect a medium sized group or community and for which there would an extended loss of service. Financial losses would be significant, and there would likely be the potential for the loss of some critical services, but there would be no anticipation of serious injury or loss of life.

Expected Actions by the Affected Organization: The affected organization would perform standard incident response activities to address the incident, and would likely inform internal management. The organization is also expected to report these incidents to CCIRC, and to other regulatory bodies and emergency management agencies at municipal and/or provincial levels, as appropriate. At this severity level, it is likely that public affairs will become involved, with the need to communicate effects and mitigation actions to the public, shareholders, clients and suppliers.

Potential Actions by the Community: A medium impact incident would almost certainly prompt substantial information sharing across the cyber security community, with CCIRC playing a coordinating role. The GOC would likely initiate planning to ensure they are prepared to assist with a coordinated emergency management response to the situation, should that become necessary. CCIRC would advise other federal partners of the situation and would brief other cyber officials in government on the situation and the potential impacts. In parallel, local and regional emergency management agencies may be contacting affected organizations to address impacts. Depending on the nature of the event, Internet Service Providers, telecommunications companies, and other expert vendors may become involved.

High Impact/Very High Impact Incidents

For high and very high impact severity levels, consequences are expected to be more severe and include the potential for loss of life and/or large financial impacts. The incident would no longer be categorized solely as a cyber incident, as the real world consequences would dictate the activation of emergency response procedures. As such, high impact and very high impact incidents would be coordinated by the emergency management agency of jurisdiction. At the federal level, this would be the GOC with support from CCIRC.

Expected Actions by the Affected Organization: An event of this severity would receive significant attention from media, the public, and regulatory officials. Many officials within the affected organization would be engaged, regardless of the fact that a cyber incident was the origin of the effects, and leadership of the response would likely no longer rest with cyber experts. Therefore, it is essential that cyber security experts be able to communicate cyber concepts to non-expert personnel who may be leading the overall response efforts. International interest would likely be present and coordination with international partners may be required, and there would be a strong need for public affairs. Although other emergency management agencies will likely be leading response efforts, the affected organization should still report these incidents to CCIRC, which would serve as the coordination point for handling the cyber specific aspects of these issues.

Potential Actions by the Community: At the federal level, response activities would be coordinated by the GOC in accordance with the NERS. At the same time, CCIRC would continue to coordinate the cyber-related aspects of the response in support of the GOC, and involve other federal partners and cyber officials as appropriate.

Other Possible Actions

Depending on the details of a particular cyber incident, other actions may occur at any impact severity level, including:

1. A national security investigation;
2. A law enforcement investigation; and
3. The sharing of the cyber incident information with other stakeholders, based upon agreed terms for the use of the information between CCIRC and the submitting/reporting organization, to improve awareness and management of cyber incidents.

These activities often occur in parallel with efforts to manage an incident and mitigate its impacts.

Closing

As stated previously, the CIMF has been developed using a collaborative approach involving Canada's cyber security community. Public Safety Canada welcomes further contributions to the CIMF as we all work together to improve the cyber resiliency of Canada.

ANNEX – CCIRC IMPACT SEVERITY MATRIX

This matrix is provided for reference purposes only; each organization is encouraged to establish their own impact severity matrix, using thresholds appropriate for the size, complexity, and nature of the organization.

Impact Severity Matrix

Impact	Info Disclosure	Life or Injury	Economic	Health and Safety	Essential Services	Public Confidence / Media
Very low *negligible effect*	Publicly available info = Unclassified	Minor discomfort for some	Small impact on SME / medium effect for individual Damages < $1K	F/P/T/M and CI able to provide for Canadians' welfare	Small group = temp loss(< 24 hrs.)	Negligible effect
Low *Minor effect*	Low sensitivity info = Protected A	Moderate to serious discomfort for some	Small effect on Canada's economic sector Large impact for SME $1K < Damages < $100K	Lead response agency requires surge resources to contain a problem / Other H+S services are not significantly impacted	Small group / small city = medium (between 24 and 72 hrs.) / temp loss	Letters to the editor / Phone complaints / Local news coverage
Medium *Major effect*	Medium sensitivity info or injury to the national Interest = Protected B / Confidential	Serious discomfort / injury / illness for many	Medium effect on Canada's economic sector Very large impact for SME $100K < Damages < $10M	Lead response agency requires surge resources to contain a problem / Other H+S services are adversely impacted	Small group / small city / large city = Long (>72 hrs.) / medium / temp loss	Media editorials / National media coverage / Focussed debate in Parliament
High *Significant effect*	High sensitivity info or serious injury to the national interest = Protected C or Secret	Potential loss of life / permanent disability	Canada's economy / strategic economic objectives damaged $10M < Damages < $1B	Lead response agency approaching capacity to contain a problem / Other H+S services becomes ineffective	Large group / large city / P/T = Long / medium / temp loss	Gov. policy challenged / Extensive international media coverage / Acts of civil disobedience
Very High *Catastrophic effect*	Exceptionally grave injury to the national interest = Top Secret	Potential for widespread loss of life	Extensive damage to Canada's economy / strategic economic objectives Damages > $1B	Lead response agency's capacity to contain a problem is exceeded / Other H+S services are halted	Large City / P/T = long / medium loss	Disruption of Gov. Services / Violent demonstrations / Focused international media coverage / Canadians severely impacted