Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

Fundamentals of Cyber Security for Canada's Critical Infrastructure Community

1ST EDITION 2016

Canada

Page left blank

Table of Contents

Executive Summary

Canada's national security relies on the uninterrupted functioning of its critical infrastructure, disruptions of which can have a serious impact on lives, the safety of communities and the economy. Critical Infrastructure organizations use the vast array of interdependent networks and systems, including information technology (IT) and industrial control systems (ICS), to support their operations and ensure that Canadians have access to essential products and services. However, these systems are vulnerable to accidental disruption and intentional exploitation, both of which can create devastating consequences.

This document offers action-oriented guidance and mitigation measures to raise awareness and begin working towards achieving a minimum baseline level of cyber security; however, it is not a definitive guide on all aspects of cyber security. This document should be read in conjunction with other documents, such as industry specific guidelines, international standards and other Government of Canada documents, as appropriate. Organizations should also consider consulting cyber security experts to address their specific needs and circumstances.

This document was developed by a National Cross Sector Forum on Critical Infrastructure working group to recommend an appropriate response to the evolving cyber threat. The guidelines were developed to address the need for action-oriented advice to increase cyber security.

Building true resiliency usually requires active engagement from a number of different players. Canada's national cyber security incident response team, the Canadian Cyber Incident Response Centre (CCIRC) operates at the convergence of the private and public sectors to strengthen the cyber systems that underpin our national security, and it welcomes partnerships with Canadian owners and operators of critical infrastructure. In addition, Public Safety Canada endorses the NIST Framework, developed by the United States' Department of Homeland Security with the National Institute for Standards and Technology (NIST), and acknowledges the relevance and applicability of the NIST Framework in the Canadian context.

Given the evolving nature of the cyber threat environment, it is important for critical infrastructure sectors, and the partners that support them, to regularly review and analyze their state of readiness with regards to cyber security and measure progress against actions taken. This document outlines several measurement instruments, both reactive and proactive, that can be used to assess the progress of an organization's resilience to cyber threats at both the national and organizational level.

Cyber Security: A Cornerstone of Canada's Digital Economy

The Canadian cyber landscape is rapidly growing and becoming more complex each day[1].

[1] *Digital Canada 150*, Canada's digital economy strategy, identified cyber security as one of its key components. For further information, see: http://www.ic.gc.ca/eic/site/028.nsf/eng/home.

Greater integration and dependence on technology, coupled with an increase in threat vectors and security vulnerabilities, is causing both government and citizens to realize the importance of cyber security, and to take the necessary steps to protect themselves from compromise and exploitation.

Information is often an organization's most valuable asset; consequently, cyber security—the protection of this valuable asset—must be integrated into core operational and business processes. Critical infrastructure sectors are interconnected and dependent upon secure cyber systems, and cyber disruptions to critical infrastructure can have significant economic implications – creating the potential of extensive losses for businesses and negatively affecting local, national and global economies.

Value Proposition

As well, the indirect cost of a cyber-attack can lead to lost production, sales disruption, and damage to consumer confidence. Indirect economic costs such as these can be just as significant as damage to equipment and infrastructure, with potentially far reaching and long term consequences for employment, innovation, and economic growth.

Cyber systems have become indispensable to almost all economic sectors. Many industries, including manufacturing, shipping and natural resource exploitation, have been revolutionized by the use of information technology and electronic systems. Even in industries where cyber system use is less obvious, a successful cyber-attack could disrupt operations or compromise sensitive information.

Scope

This document offers adaptable, action-oriented guidance to critical infrastructure sectors that will enable organizations to achieve a minimum baseline level of cyber security with little investment. Ultimately, by asking a few simple questions and adopting a strategic approach to addressing gaps, organizations will be able to improve their overall cyber security posture, thus contributing to stronger and more resilient infrastructure and improving quality of life for Canadians.

Current Threat Environment

Cloud storage, mobile computing, and increasing automation and internet connectivity of corporate and process control systems have all increased the potential vulnerabilities of critical infrastructure organizations to cyber threats. Research studies involving interviews with hundreds of owners and operators of critical infrastructure have highlighted several areas of growing risk. In fact, studies and reports suggest that, among others, the prevalence of cybercrime, costs associated with compromise, risks to Industrial Control Systems, and sophistication of attacks are all growing.

Many cyber-attacks share the following characteristics:

- **Inexpensive** – Many attack tools can be purchased for a modest price or downloaded for free;
- **Effective** – Even minor attacks can cause extensive damage; and
- **Low risk** – Attackers can evade detection and prosecution by hiding their tracks through a complex web of computers and exploiting gaps in domestic and international legal regimes.

The threat actors responsible for the majority of cyber based incidents in today's digital economy normally fall into the following categories:

- **Industrial Espionage** – Individuals or organization who seek classified and proprietary information, including market and pricing strategies, corporate financials, client information, product designs or formulas, research data and corporate vulnerabilities.
- **State-Sponsored Cyber Espionage –** Persons who are well-funded and supported by national programs with sophisticated capabilities to compromise and exploit vulnerable systems.
- **Criminals** – Persons who seek any data that can be sold or used for a profit.
- **Hacktivist/Recreational Hackers** – Hackers, both experienced and inexperienced, who operate using the latest techniques and tools to perform a network attack, sometimes for personal gain or as part of an organized group.
- **The Insider Threat** – Individuals already operating within organizations—legitimately or otherwise—can also pose a serious hazard.

Administrative Systems Security

Like all businesses, critical infrastructure owners/operators use IT systems to manage the administrative aspects of their business. Common operations such as customer relationship management, human resources, finance, billing, and research and development are performed on these systems.

The personal and financial data on administrative systems can be attractive targets for malicious actors, as is the even more valuable intellectual property that is often maintained on these systems. The administrative infrastructure can be a particularly attractive target for criminal groups seeking to gain financial advantage.

Critical infrastructure owner/operators use IT assets throughout their business, both for administrative activities and their operations. While these domains were traditionally separately managed, they are becoming increasingly interconnected. As a result,

owner/operators should ensure robust controls across their business and pay close attention to any interconnection points.

Industrial Control Systems Security

IT systems have been added to improve the management of industrial control systems (ICS) that perform essential mechanical functions and the Supervisory and Control and Data Acquisition (SCADA) systems that monitor and control them. These systems are used in a variety of critical applications and industries including energy and utilities, transportation, health, manufacturing, food and water. This has led to improved service, lower costs and technological advancements such as Smart Grids. However, these IT developments can also expose critical infrastructure to software vulnerabilities. More connectivity means additional access points, and potentially increased exposure to cyber threats.

Fundamentals of Cyber Security

Institutionalizing cyber security is everyone's responsibility. Following a few key fundamentals can greatly increase the resiliency of an organization:

1) Raising Security Awareness

Even the most sophisticated security technologies can be rendered ineffective if people don't use them properly. Increasingly, the hacker community is reverting to tricking employees to gain illegal access to corporate assets. A strong security awareness program is key to keeping up with the ever changing cyber security battleground. Starting with basic training for staff, such a program should later expand to include reminders on policies, best practices, and information on the latest way hackers try to trick employees (see Annex 1 for useful resources). Your security awareness plan can also include a regular, scheduled review to update existing security measures, including adopting new means of protection as needed.

2) Defining Roles and Responsibilities

While cyber security is everyone's responsibility, accountability starts at the top of an organization.

Heads of organizations have a crucial role to play with key responsibilities. They are uniquely placed to promote a culture of awareness and prevention, and ensure that vulnerabilities are assessed, cyber security plans are established and accountability measures are put in place.

Every organization should have at least one cyber security point of contact with the following responsibilities:

- Learning about threats, trends and security options.
  - Membership in a cyber-security association can help organizations stay informed about the latest developments – see annex 1 for examples.
- Planning, acquiring and implementing security safeguards.
- Helping other personnel understand cyber security best practices and policies.
- Enforcing cyber security best practices and policies with management support.
- Maintaining and updating the security safeguards used by your business.

Managers should have cyber security as part of their accountabilities and be responsible for the following:

- Providing guidance to employees on the importance of cyber security as part of operations, including policies to outline accountability for cyber security.
- Supporting and monitoring cyber security projects.
- Consulting with experts, such as legal counsel, for any external obligations such as provincial or federal law.

3) Developing Policies and Standards

A security ***policy*** is a document that explains what employees may or may not do with respect to cyber security; for example whether they're allowed to access the Internet or social media on corporate networks. Cyber security policies are essential in helping employees understand their roles and responsibilities.

An acceptable use policy might state, for example:

- *Employees **may not** connect a personal computer or personal mobile device to the business network; or*
- *When accessing the business network from home, you **must** use approved security tools.*

A ***standard***, on the other hand, is a document that explains how a specific task should be done. In the cyber domain, standards most often apply to setting up and using technical systems. For example, a password standard would describe exactly what an acceptable password can or cannot include, how long it should be and how often it should be changed.
The following should be considered when developing and using cyber security policies and standards:

1) Begin with a simple, comprehensive policy to clearly lay out principles and rules.

2) Identify and adapt existing standards to deal with specific cyber security issues or technologies in the business, or write your own.

3) Explain policies and standards to personnel so they will understand the rationale for rules, to whom they apply, and any consequences for not following the policy.

4) After the initial cyber security policy and associated standards are in use, revisit them and add more detailed, specific information as needed.

4) Establishing a Cyber Security Plan

Developing a cyber-security plan should be a priority for any business. A cyber security plan will identify those baseline cyber security controls that form the foundation for every organization. It will further detail those assets that need additional safeguarding, specific threats and risks to the business, and which safeguards to implement. Remember that you can always revisit and expand your plan over time. In addition, the Canadian Cyber Incident Response Centre (CCIRC) has resources available to help organizations with their cyber security planning. Once an organization's plan has been established, it should be approved by an organization's senior management, reviewed periodically, and budgeted for. Cyber security plans may contain sensitive information and should be marked, handled, stored, transmitted, and destroyed with security in mind.

5) Budgeting for Cyber Security

Security controls are most effective when considered at the earliest stages of an undertaking and then continuously throughout the lifetime of the undertaking. As a result, organizations should include security as an integral aspect of their budgeting exercises. Cyber security activities should be accounted for when drawing up annual business plans and budgets. Some policies or internal documents can be developed in-house at minimal cost. However, other security measures will have to be purchased, and may also involve annual subscription fees. For example, unlike software, which typically involves a one-time fee, renewals for anti-malware software might need to be purchased annually. Investments in mitigation and preparedness activities can yield significant returns. Cyber security budgets should also take into account the value of the assets being protected. Similarly to taking out an insurance policy, investing in cyber security is such that measures are put in place hoping that the organization will not have to make use of them – as homeowners take out a flooding insurance hoping their house never gets flooded. It is recommended that organizations allocate resources across the following five areas:

1) Fixed costs for security tools;
2) Ongoing/annual resource (e.g.: software) updating fees;
3) Support, consulting and training costs;
4) Audit/verification; and
5) Contingencies.

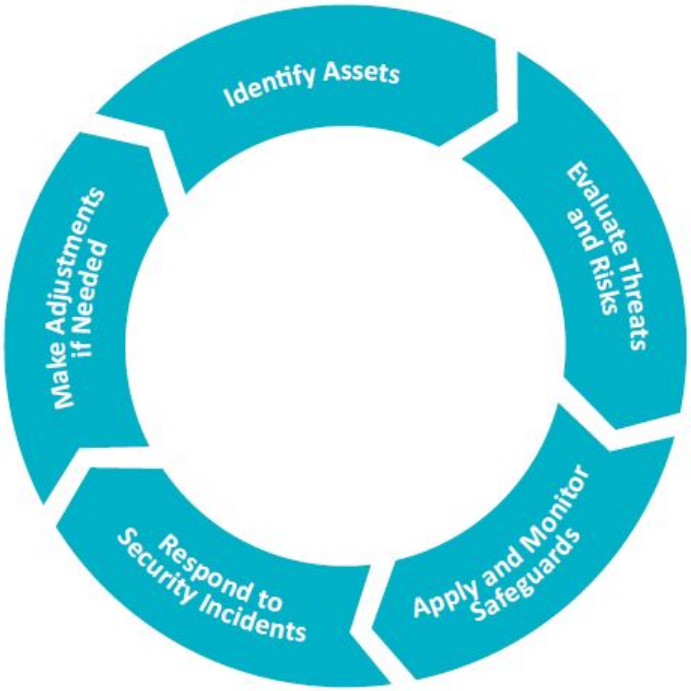
Contingency funds are important to deal with unforeseen emergencies (such as malware infection). In some cases, your insurance may cover losses due to a cyber-security incident. It is important to discuss this with your insurance provider in advance.

Cyber Security: Basic Questions

Many public and private sector organizations have crisis management structures in place to facilitate a coordinated internal response to emergencies, regardless of the cause or nature of the emergency. Such mechanisms also ensure their management is apprised in an appropriate and coordinated fashion. It is important to ensure that these mechanisms are also well suited to dealing with cyber incidents.

While all assets require a baseline level of assurance, specific assets may require additional protective measures. Even with these measures in place, organizations still need to be ready to respond to security incidents as they occur and adjust safeguards in response to changes in assets, threats, and risks.

Figure 1 – Cyber Security Fundamentals



Organizations can take the following steps to define and prioritize assets, evaluate threats and identify when to apply appropriate augmented safeguards (see Figure 1).

1. **Identify Assets –** Which assets require enhanced or specialized safeguards? *Maintain an inventory of all assets essential to your operations.*

2. **Evaluate Threats and Risks –** What *threats* and *risks* could affect those assets or business operations? What safeguards should be in place to mitigate risks and secure assets?

3. **Apply and Monitor Safeguards –** Monitor safeguards and assets to prevent or manage security breaches.

4. **Respond to Security Incidents –** Respond to cyber security issues as they occur.

5. **Make Adjustments When Needed –** Update and adjust safeguards in response to changes in assets, risks and threats.

Top Four Safeguards

Implementing cyber security controls can seem daunting for owners and operators, especially given the lengthy checklists of controls and domain-specific lexicon. There is a variety of

industry- and government-recognized listings of cyber controls that can provide baseline controls across organizations. The Australian Signals Directorate (ASD) Strategies to Mitigate Targeted Cyber Intrusions (Top 4/35) and other similar lists provide meaningful direction for organizations of all types.

It has been found that the following four safeguards would prevent the vast majority of exploits:

1) **Application whitelisting** - Identifying specific programs that are permitted to execute on a given system and enforcing a policy so that only those identified components can operate.

2) **Use modern operating systems and applications** - Install current systems/programs and establish a life-cycle approach to migrate to newer versions.

3) **Patch operating systems and applications** - Patch within a two-day timeframe of a high risk vulnerability being made public.

4) **Restrict administrative privileges** - Minimize the number of users with domain or local administrative access to a system or device.

Government of Canada Resources

The federal government offers a number of products and services to support the strengthening of critical infrastructure in Canada, including the cyber systems which support it, some of which are outlined below. See Annex 1 for additional resources. The table below lists the 10 critical infrastructure sectors in Canada and their associated federal government departments and agencies also known as “lead-departments”. In the event of an incident, the lead department identified is responsible for coordinating the federal government response.

Sector	Sector-specific federal department/agency
Energy and utilities	Natural Resources Canada
Information and communication technology	Innovation, Science and Economic Development Canada
Finance	Finance Canada
Health	Public Health Agency of Canada
Food	Agriculture and Agri-Food Canada
Water	Environment and Climate Change Canada
Transportation	Transport Canada
Safety	Public Safety Canada
Government	Public Safety Canada
Manufacturing	Innovation, Science and Economic Development Canada / National Defence and the Canadian Armed Forces

Government of Canada Resources cont'

✓ Emergency Management Act

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, for example, 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 to ensure that the consequences of the incident were effectively managed. The concept of cyber security introduces complications to existing emergency management structures as cyberspace is independent of physical and geographical boundaries.

✓ Cyber Incident Management Framework (CIMF)

To address some of the boundary-crossing elements of cyber security, Public Safety Canada developed the *Cyber Incident Management Framework (CIMF)*. The CIMF is a guidance document involving provincial and territorial governments, critical infrastructure owners and operators, and other public and private sector partners. The CIMF was 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.

✓ The National Strategy and Action Plan for Critical Infrastructure

The goal of the National Strategy for Critical Infrastructure is to build a safer, more secure and more resilient Canada. To this end, the National Strategy advances coherent and complementary actions among federal, provincial and territorial initiatives and among the ten critical infrastructure sectors.

The fundamental concepts and principles outlined in this National Strategy flow from the *Emergency Management Framework for Canada*, which sets out a collaborative approach for federal, provincial and territorial emergency management initiatives. Consistent with this Framework, and recognizing the interconnected nature of critical infrastructure, the National Strategy fosters the development of partnerships among federal, provincial and territorial governments and critical infrastructure sectors, advances an all-hazards risk management approach, and sets out measures to improve information sharing and protection.

To keep pace with the rapidly evolving risk environment, a key element of the national approach is an Action Plan that builds on the central themes of the National Strategy:

- sustainable partnerships with federal, provincial and territorial governments and critical infrastructure sectors;
- improved information sharing and protection; and
- a commitment to all-hazards risk management.

This Action Plan is updated regularly to enable partners to anticipate and address new risks.

✓ The Canadian Cyber Resiliency Review

If you are an owner and/or operator who requires assistance in assessing your organization, Public Safety Canada offers the Canadian Cyber Resiliency Review (CCRR). The CCRR is a one day, on-site facilitated workshop designed to assess an organization's overall approach to cyber security practices and procedures. For more information on the CCRR, organizations are encouraged to contact the following email address: rrap_perr@ps-sp.gc.ca.

✓ Canadian Cyber Incident Response Centre

The Canadian Cyber Incident Response Centre (CCIRC) provides a range of guidance documents, security bulletins, and technical reports related to cyber security issues as well as timely and actionable information in response to cyber events.

Community Portal: In 2012, CCIRC launched a secure Community Portal for its partners in the public and private sectors in order to enhance incident reporting, links to useful tools and sector discussions. The portal provides the CI community with a collaborative platform to foster information sharing. It also offers a series of sub-sites organized by sector or community of interest.

The Community Portal includes an archive of all of CCIRC's executive and technical products, including those not posted to our public website. Partners are encouraged to request a Community Portal account.

Operational Reports: The purpose of this suite of professional products is to raise critical infrastructure executives' awareness of the noteworthy incidents and trends observed by CCIRC, and to highlight case studies and security best practices. The reporting period of these products are based on a monthly, quarterly, and annual publication. In addition, CCIRC publishes an episodic report called "Spotlight On…" which is a series that highlights ongoing or emerging cyber security issues.

Technical Product Suite: CCIRC provides a full suite of technical products for its partners in the public and private sectors, which contain time-sensitive threat detection and mitigation information for immediate security issues. In addition, CCIRC regularly posts a range of security publications to its website, such as **Information Notes, Technical Reports, Alerts, and Advisories**.

CCIRC regularly issues **Cyber Flashes** to notify its public and private sector partners of potential, imminent or actual cyber threats. Additionally, CCIRC produces a **Weekly Technical Report** for its trusted partners that include a summary of incidents and their associated indicators of compromise, and noteworthy news items. Both of these products are posted to CCIRC's secure Community Portal.

Incident Coordination: Provision of incident response coordination for ongoing cyber based incidents 24/7.

Mitigation Advice: Provision of advice intended to improve a client's cyber security posture.

Technical Analysis: Technical analysis and reporting on malware samples, digital media analysis and forensics.

Victim Notifications: CCIRC's National Cyber Threat Notification System leverages an in-house malware laboratory to provide stakeholders with tailored malware notifications.

CONTACT CCIRC:
For more information on the CCIRC community portal and the products available, please contact CCIRC at cyber-incident@ps-sp.gc.ca

The CCIRC Cyber Duty Officer is the point of contact for members of the critical infrastructure community to report incidents to CCIRC and to receive assistance in managing incidents.

✓ Canadian Critical Infrastructure Information Gateway

The *Critical Infrastructure Gateway* is a forum for CI owners and operators for promoting timely information sharing and collaboration across critical infrastructure sectors. Users can access documents, links, RSS feeds, geospatial material and contact information from every CI sector quickly and efficiently. Users can also recommend and submit potential content to be shared with the CI Gateway community. E-mail: cigateway@ps-sp.gc.ca

✓ Industrial Control Systems (ICS) Security Workshops and Training

Public Safety Canada's Industrial Control Systems (ICS) Security workshops bring together recognized experts along with representatives from the federal Government to provide briefs on the latest threats and steps that can be taken to increase the security of industrial control systems.

Public Safety Canada's Industrial Control Systems (ICS) Security training is focused on the development of basic incident handler skills for the ICS environment. The training is hands-on using real tools and targets.

Monitoring and Measuring Progress

Measuring the effectiveness of cyber security remains a challenge. The absence of an adverse event does not necessarily indicate that an organization has a well-functioning cyber security program. The effectiveness of a cyber-security program should consider both the adverse, reactive activities as well as the positive proactive activities.

Public Safety Canada recommends adopting a multi-dimensional approach to monitoring and measuring progress towards a clearly identified outcome of strengthening the resilience of critical cyber infrastructure. By collecting indicators at the organizational and national levels, organizations should be able to track progress on enhancing resilience at both a detailed and macro level perspective. The organizational indicators listed below may be adapted for organizations to measure their own performance.

Measurement Indicators	
Reactive Measures	**Source**
Relative malware rates in Canada	National Metrics – Microsoft Security Intelligence Report: Worldwide Threat Assessment
Canada's rank within top countries hosting Phishing URLs	National Metrics – McAfee Labs: McAfee Labs Threats Report
Percentage of global bots population in Canada/National standings in bot ranking	National Metrics – Symantec Corporation: Internet Security Threat Report
Canada's annual encounter and infection rates	National Metrics – Microsoft Security Intelligence Report: Regional Threat Assessment
Restoral rates[2]	Organizational Metrics – Collected for internal use by organizations
Proactive Measures	**Source**
Top recommended mitigation actions (CCIRC) implementation rate	Organizational Metrics – Collected for internal use by organizations
Public Safety Canada Canadian Cyber Resilience Review (CCRR) aggregate scores	National and Organizational Metrics
Network Traffic ratios[3]	Organizational Metrics – Collected for internal use by organizations
Software recency rates[4]	Organizational Metrics – Collected for internal use by organizations

[2] Length of time for critical services to be back on line after an exploit, followed by secondary services and finally all services.
[3] Legitimate network traffic vs. botnet traffic (spam).
[4] Measure of how quickly an organization can implement updates or new versions of software.

Conclusion

The advice provided in this document is not meant to be an exhaustive list of how an organization can improve its cyber security. It is meant to complement, enhance, and in many cases, begin your organization's approach to the dynamic, complex, and always evolving field of cyber security.

Early investment in prevention and protective cyber security measures can help mitigate costly response and recovery services.

A national collaborative approach to the challenges of cyber security is crucial, as with increasingly integrated and interconnected systems and networks, the effects of a cyber-incident against one stakeholder has the potential to affect all stakeholders. Collectively, government, business partners, and citizens have a greater expectation that the organizations and institutions with which they do business are resilient enough to withstand cyber incidents and avoid cascading impacts within and across sectors. *Cyber Security is everyone's responsibility.*

The more we do today to collectively advance the cyber security of critical infrastructure, the more ready we'll be to meet the challenges of both the present and the future.

Annex 1: Additional Resources

Government of Canada Resources

Canada's Anti-Spam Legislation

- www.fightspam.gc.ca/eic/site/030.nsf/eng/h_00241.html

Canadian Anti-Fraud Centre for fraud prevention and reporting (including cyber crime)

- Toll Free: **1-888-495-8501** or email: info@antifraudcentre.ca
- Website: http://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Canadian Cyber Incident Response Centre (CCIRC)

- Advanced Persistent Threat Guide: www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-eng.aspx
- Cyber Security Technical Advice/Guidance/Training: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-eng.aspx
- DDOS Mitigation Guide: www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-001-eng.aspx
- Get Cyber Safe Guide for Small and Medium Businesses http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-eng.aspx
- Malware Removal Guide: www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-001-eng.aspx
- SCADA / ICS Guide: www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-eng.aspx

Canadian Radio-television and Telecommunications Commission (CRTC) scam reporting site:

- www.crtc.gc.ca/eng/INFO_SHT/G9.htm

Communications Security Establishment (CSE)

- Architecture guides ITSGs: https://www.cse-cst.gc.ca/en/publication/list
- Threat and Risk Assessment (TRA): https://www.cse-cst.gc.ca/en/publication/tra-1

***Digital Canada 150* Strategy**

- https://www.ic.gc.ca/eic/site/028.nsf/eng/h_00569.html

Get Cyber Safe provides news and guidance on cyber security for individuals and business. www.getcybersafe.gc.ca

Office of the Privacy Commissioner of Canada:

- Getting Accountability Right with a Privacy Management Program: www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp
- Securing Personal Information Self-Assessment Tool: www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

Resources from International Partners

Australia

- **Australian Signals Directorate (ASD) Strategies to Mitigate Targeted Cyber Intrusions (Top 4/35):** http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm
- *The Australian Government Information Security Manual*

UK

- *10 Steps: Executive Companion*
- Cyber Essentials Guidance

U.S.

- Department of homeland Security - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Recommended practices: https://ics-cert.us-cert.gov/Introduction-Recommended-Practices
- US National Vulnerability Database Version 2.2: http://nvd.nist.gov/
- National Institute for Standards and Technology (NIST) Cybersecurity Framework Framework for Improving Critical Infrastructure Cybersecurity

NZ

- Cyber security & risk management - An Executive level consideration http://www.ncsc.govt.nz/assets/cyber-security-risk-management-Executive.pdf
- The National Cyber Security Centre Voluntary Cyber Security Standards for Industrial Control Systems http://www.ncsc.govt.nz/assets/NCSC20voluntary20cyber20security20standards20for20ICD20v.1.0.pdf

Other resources (Associations, Standards, Reports, etc.)

A wide variety of organizations publish useful information on cyber threats – examples include:

Canadian Cyber Threat Exchange (CCTX)

- An independent, not-for-profit organization, to help Canadian businesses and consumers guard against cyber-attacks: https://cctx.ca/

Cyber Security Member Associations in Canada

- American Society for Industrial Security (ASIS): www.asis-canada.org/
- High Technology Crime Investigation Association (HTCIA): www.htcia.org/
- Information Systems Audit and Control Association (ISACA): www.isaca.org/Membership/Local-Chapter-Information/Browse-by-List/Pages/North-America-Chapters.aspx
- Information Systems Security Certification Consortium, Inc. (ISC2) https://www.isc2.org/chapters/Default.aspx
- Information Systems Security Association (ISSA): https://www.issa.org/?page=ChaptersContact

International Organization for Standardization – Information security management standard:

- http://www.iso27001security.com/html/27032.html

Microsoft Security Intelligence Report:

- https://www.microsoft.com/security/sir/default.aspx

McAfee publications:

- http://www.mcafee.com/ca/apps/view-all/publications.aspx

Kaspersky Internet Security Center:

- http://www.kaspersky.com/internet-security-center

FireEye Annual Threat Report:

- https://www.fireeye.com/current-threats/annual-threat-report.html

Symantec Security Response Publications:

- https://www.symantec.com/security_response/publications/

SANS Institute Critical Security Controls (Top 20):

- https://www.sans.org/critical-security-controls/

The supporting standards shown in the table below can assist with effective cyber security management, planning and decision making:

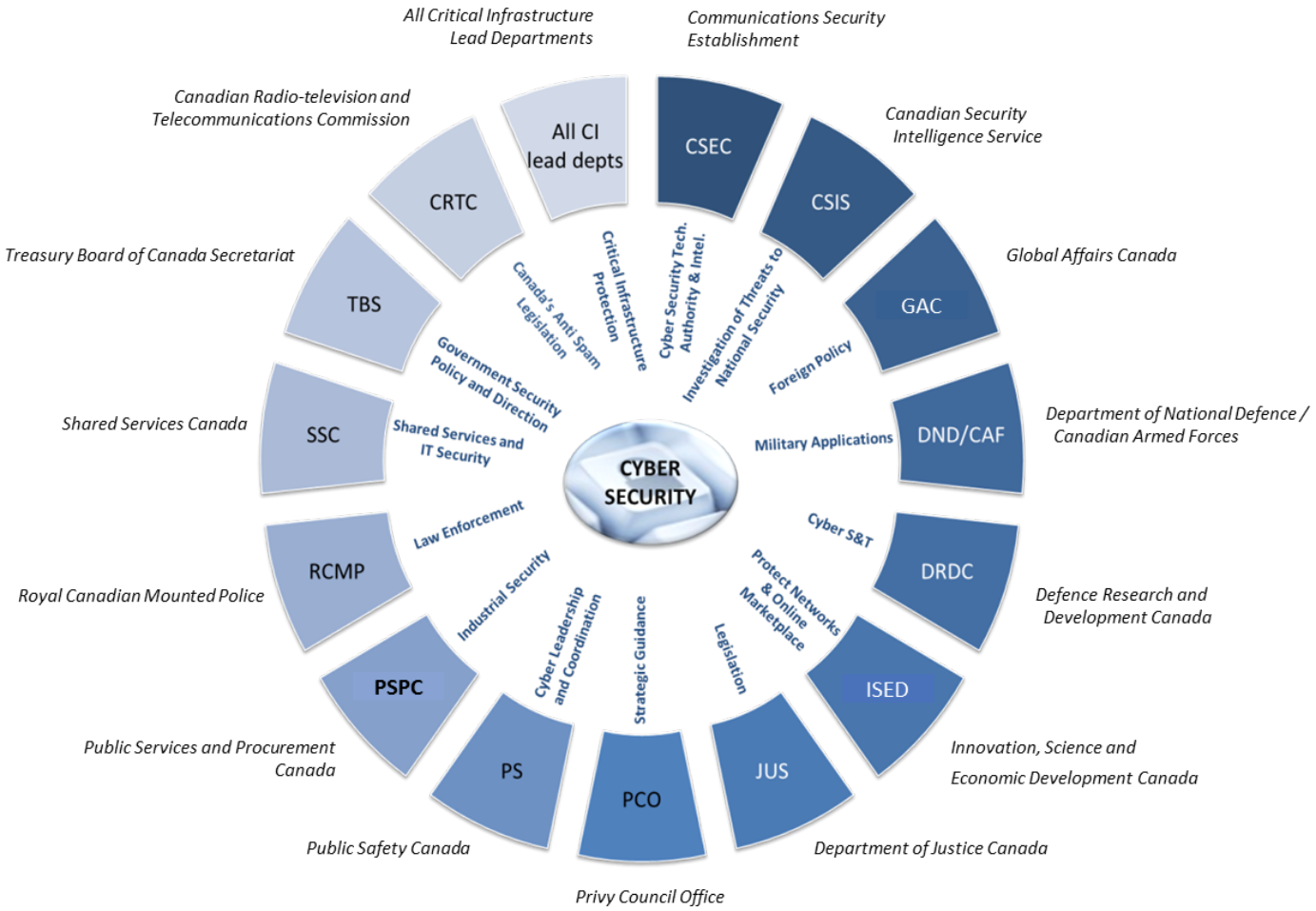
Supporting Standards and Guidance *(hyperlinks)*
Framework for Improving Critical Infrastructure Cybersecurity (National Institute for Standards and Technology)
Partnering for Cyber Resilience (World Economic Forum)
Cybersecurity Best Practices Guide For IIROC Dealer Members (Investment Industry Regulatory Organization of Canada)
Cyber Incident Management Planning Guide For IIROC Dealer Members (Investment Industry Regulatory Organization of Canada)
Strategies to Mitigate Targeted Cyber Intrusions (Australian Signals Directorate)
Information security management standard (International Organization for Standardization)
Risk and Responsibility in a Hyper connected World Pathways to Global Cyber Resilience (World Economic Forum)

Annex 2: Government of Canada Departments and Agencies Roles and Responsibilities for Cyber Security

While the vast majority of the nation's cyber infrastructure resides in private hands, the national and economic security risks associated with these assets demand close partnerships among government and the private sector, and coordination action to protect and defend them. Released in 2010, *Canada's Cyber Security Strategy* (Cyber Strategy) represents the Government of Canada's plan to help guard against attacks to vital cyber systems, protect government networks and keep Canadians safe from cyber-facilitated crime.

It is recommended that critical infrastructure sectors understand the roles and responsibilities of federal departments and agencies under the Cyber Strategy (see Figure 1), and establish linkages with the appropriate partners to effectively manage the evolving cyber risks.

Figure 1 – Government of Canada departments and agencies involved in security



Public Safety Canada has an important and unique role in the cyber security arena. The Department is responsible for coordinating and implementing the Cyber Strategy. This includes working with critical infrastructure sectors to raise awareness of cyber threats, identify vulnerabilities and develop mitigation strategies.

The Canadian Cyber Incident Response Center (CCIRC) operates within Public Safety Canada. As Canada's computer security incident response team, CCIRC is responsible for monitoring and providing mitigation advice on cyber threats, as well as coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. With this in mind, owners and operators have access to the following products and services:

Public Safety Canada also recently launched the Cyber Security Cooperation Program (CSCP) as a means to improve the security of Canada's vital cyber systems. The program provides grants and contributions to owners and operators of vital cyber systems, along with other stakeholders, to support projects that increase the resilience of Canada's cyber systems. For more information on the CSCP, or to apply for funding, please refer to the program website.

Below is a list of other government departments with a summary of their cyber security roles/responsibilities:

Canadian Radio-television and Telecommunications Commission (CRTC)

- Ensures that Canadians have access to a world class communications system, while protecting Canadians from unsolicited communications and contributing to a more secure online environment for consumers and businesses.

Canadian Security Intelligence Service (CSIS)

- Conducts national security investigations. Reports to and advises the Government of activities constituting a threat to the security of Canada as defined in the CSIS Act.
- Provides analysis to assist the Government of Canada in understanding cyber threats, and the intentions and capabilities of cyber actors operating in Canada and abroad who pose a threat to the security of Canada.
- This intelligence enables the Government of Canada to improve its overall situational awareness, better identify cyber vulnerabilities, prevent cyber espionage or other cyber threat activity, and take action to secure critical infrastructure.

Communications Security Establishment (CSE)

- Monitors and defends Government of Canada networks by detecting, discovering and responding to cyber threats, and provides mitigation and recovery advice, guidance, and services to federal institutions and critical infrastructure owners/operators.
- Government of Canada’s cryptologic agency responsible for the collection of cyber foreign intelligence and Canada’s interface with the Five Eyes cryptologic community.
- Undertakes research and development for cyber security.
- Provides assurance programs for commercial technologies.
- Partners with Shared Services Canada and Industry Canada to ensure the integrity of the

cyber supply chain for Government of Canada equipment and services.
- Shares cyber threat and vulnerability information with CCIRC for distribution to critical infrastructure owners/operators.

Defence Research and Development Canada (DRDC)
- Leads the development of military cyber security S&T in support of Canadian Forces.
- Leads domestic Public Safety Canada cyber security S&T efforts not specifically assigned to another department or agency through the Centre for Security Science and with domestic security partners in the Public Security Technical Program. This is delivered in partnership between Government, industry, academia and allies.

Global Affairs Canada
- Supports international bodies in mitigating cyber threats and assisting foreign governments in improving their cyber security profile and capabilities.
- Contributes to diplomatic engagement in order to help shape the multilateral regulatory space that is emerging with respect to cyber security. Enables the Government to better position Canada on the international stage to defend and promote its foreign policy and cyber security-related interests.

Department of Justice Canada
- Supports initiatives of client departments and agencies through the provision of legal advice on matters relating to cyber policy and law.
- In respect of certain matters, especially those relating to criminal law policy and information sharing, Justice plays a leading role. Departmental Legal Services within the Communications Security Establishment Canada had been designated as the centre of excellence on cyber-related legislation.

Department of National Defence / Canadian Forces (DND/CF)
- Responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process.
- Contributes to Government situational awareness during the monitoring and analysis, mitigation, and response phases of the GC IT IMP by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

Innovation, Science and Economic Development Canada (ISED)
- Responsible for spectrum management and for fostering a robust and reliable telecommunications system. Develops policies to ensure a safe and secure online marketplace. Helps to ensure continuity of telecommunications during emergencies.

Privy Council Office (PCO)
- Houses and provides support to the National Security Advisor to the Prime Minister.
- Coordinates activities among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to national security.

Public Services and Procurement Canada

- Provider of shared and common services. As part of its Industrial Security Program activity, ensures security in contracts awarded by the Department or when requested by other Government departments.
- Ensures the protection of foreign and NATO classified information within the private sector in Canada.
- The Industrial Security Sector maintains relationships with allies and negotiates Memoranda of Understanding on industrial security matters, including cyber security, in contracting.

Royal Canadian Mounted Police (RCMP)

- Leads the criminal investigative response to suspected criminal cyber incidents involving critical information infrastructure (i.e., unauthorized use of computer and mischief in relation to data). Leads the investigative response to suspected criminal national security cyber incidents.
- Advises and guides domestic and international partners on cyber crime threats.

Shared Services Canada (SSC)

- Streamlines and consolidates information and communications technologies in the areas of email, data centres and networks, and ensures the confidentiality, integrity and availability of common information technology (IT) services provided to departments.
- Provides IT security services and other solutions to enable departments to exchange information with citizens, businesses and employees.
- Gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to the common IT services and Government IT critical infrastructure they manage, and communicates the information to the Canadian Cyber Incident Response Centre and, as authorized, to departments and cyber security partners.

Annex 3: Glossary and Acronyms

Glossary

Assets: Any items belonging to or held by the business, with some value (including information, in all forms and computer systems).
Attack: An attempt to gain unauthorized access to business or personal information, computer systems or networks for (normally) criminal purposes. A successful attack may result in a security *breach* or it may be generically classified as an "incident."
Authentication: A security practice implemented (usually through software controls) to confirm the identity of an individual before granting them access to business services, computers or information.
Backup: The process of copying files to a secondary storage solution, so that those copies will be available if needed for a later restoration (e.g., following a computer crash).
Breach: A security breach is a gap in security that arises through negligence or deliberate attack. It may be counter to policy or the law, and it is often exploited to foster further harmful or criminal action.
Cyber: Relating to computers, software, communications systems and services used to access and interact with the Internet.
Encryption: Converting information into a code that can only be read by authorized persons who have been provided with the necessary (and usually unique) "key" and special software so that they can reverse the process (e.g., decryption) and use the information.
Firewall: A type of security barrier placed between network environments. It may be a dedicated device or a composite of several components and techniques. Only authorized traffic, as defined by the local security policy, is allowed to pass.
Identity Theft: Copying another person's personally identifying information (such as their name and Social Insurance Number) and then impersonating that person to perpetrate fraud or other criminal activity.
Malware: Software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software. Malware should not be confused with defective software, that is, software which has a legitimate purpose but contains harmful bugs.
Password: A secret word or combination of characters that is used for authentication of the person that holds it.
Patch: An update to or repair for any form of software that is applied without replacing the entire original program. Many patches are provided by software developers to address identified security vulnerabilities.
Phishing: An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Risk: Exposure to a negative outcome if a *threat* is realized.
Safeguard: A security process, physical mechanism or technical tool intended to counter specific threats. This is also referred to as a "control".
Server: A computer on a network that acts as a shared resource for other network-attached processors (storing and "serving" data and applications).
Spam: Junk or unsolicited e-mail sent by a third party. An annoyance to users and administrators, spam is also a serious security concern as it can be used to deliver Trojans, viruses, and phishing attempts. It could also cause a loss of service or degradation in the performance of network resources and e-mail gateways.
Threat: Any potential event or action (deliberate or accidental) that represents a danger to the security of the business.
Vulnerability: A weakness in software, hardware, physical security or human practices that can be exploited to further a security attack.
Wi-Fi: A local area network (LAN) that uses radio signals to transmit and receive data over distances of a few hundred feet.

Acronyms

CCIRC: Canadian Cyber Incident Response Centre
CCRR: Canadian Cyber Resilience Review
CSCP: Cyber Security Cooperation Program
CSE: Communications Security Establishment
DDOS: Distributed denial-of-service
ICS: Industrial Control System
IT: Information Technology
ITSG: Information Technology Security Guidance
HTTPS: Hypertext Transfer Protocol Secure
NCSF: National Cross Sector Forum
NIST: National Institute for Standards and Technology
OS: Operating System
OTP: One-Time Password
POS: Point of Sale
RRAP: Regional Resilience Assessment Program
SCADA: Supervisory Control and Data Acquisition
TRA: Threat and Risk Assessment
URL: Uniform Resource Locator
VPN: Virtual Private Network