Cyber security guidance for heightened threat levels

CANADIAN CENTRE FOR CYBER SECURITY

JULY 2022 | ITSAP.10.101

The threat level your organization faces is fluid and often changes with factors like global events and cyber crime prevalence. By following the guidance below, in addition to basic cyber security hygiene practices, your organization can ramp up your cyber security posture, enhance your resiliency, and better protect your organization during heightened threat levels.

Understand the risk

It is imperative you understand your baseline cyber security risk versus the risk your organization faces in an environment with known heightened threat levels. Your organization should conduct an assessment to determine your baseline risk, as well as an additional assessment to identify and mitigate risks during an heightened threat level. You should also develop an action plan that provides detailed instructions to your team on how to move quickly when your organization is facing heightened threat levels. Understanding your risks will enable you to better protect your networks, systems, data, clients, and business operations.

Find the balance

When your organization needs to ramp up its cyber security posture in response to a heightened threat level, it can be hard to strike a balance between enhanced security and operational requirements. You also need to consider the cost of ramping up your cyber security posture and the implications increased spending can have on your organization's ability to perform core business functions.

Take action

When the cyber threat to your organization is higher than normal, it's important to have an action plan in place that can seamlessly move your organization into a heightened alert status. Your action plan should:

- prioritize the security actions that need to be taken immediately
- detail how existing defences will be strengthened
- provide timelines or targets for each item to be implemented

Your plan should be endorsed by the highest level of authority in your organization to ensure the approval process is not a deterrent in activating your plan and moving your organization into a heightened defensive posture. The second page of this publication will provide you with a checklist of security actions to take during a heightened threat level.

Cyber threat actors and motivations

Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. Cyber threat actors can be categorized by their motivations and, to a degree, by their sophistication. Threat actors value access to devices, processing power, computing resources, and information for different reasons. In general, each type of cyber threat actor has a primary motivation.

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
INSIDER THREATS	DISCONTENT

Communications Security Establishment | Centre de la sécurité des télécommunications

© Government of Canada | This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE. Cat. No. D97-1/10-101-2022E-PDF ISBN 978-0-660-44404-8

Canada

How to respond to heightened threat levels

CANADIAN CENTRE FOR CYBER SECURITY
JULY 2022 | ITSAP.10.101

Security actions under heightened threat

The following actions will enhance your organization's cyber security posture when facing a heightened threat environment:

- ☐ Review existing monitoring, logging, and detection systems to ensure they are functioning properly
- ☐ Enhance network monitoring where necessary (e.g. endpoints)
- ☐ Prioritize the review of critical network services and internet-exposed system logs
- ☐ Change passwords across your networks and ask users to change their passwords
- ☐ Postpone system changes or implementations if possible until the threat level is lowered
- ☐ Run exercises to test your incident response and business continuity plans to ensure you can respond and recover quickly and effectively if a cyber incident occurs
- ☐ Report incidents to the Cyber Centre via the My Cyber Portal
- ☐ Disable all non-essential ports and services
- ☐ Take critical systems offline if possible to prevent threat actors' ability to access them
- ☐ Monitor, inspect, and isolate traffic from areas of known geopolitical unrest
- ☐ Enhance insider threat monitoring and implement a "two-person" rule when performing critical administrative functions to guard against social engineering tactics by highly sophisticated threat actors
- ☐ Review all privileged access accounts and redefine levels of access or remove entirely
- ☐ Enforce MFA for all remote access to your organization's network
- ☐ Deploy a host-based intrusion prevention system (HIPS) to protect your organization's systems against both known and unknown malicious attacks

Report cyber incidents

A primary component of your incident response should include reporting cybercrimes to law enforcement, the Canadian Anti-Fraud Centre, and online via the Cyber Centre's My Cyber Portal.

Critical Infrastructure (CI) and high value targets

- ☐ Isolate CI components and services from the internet when under imminent threat
- ☐ Use Privileged Access Workstations (PAWs) to separate sensitive tasks and accounts
- ☐ Implement network security zones to control and restrict access and data communication flows to certain components and users
- ☐ Test manual controls to ensure critical functions remain operable if your network is unavailable or untrusted
- ☐ Identify, separate, and monitor your information technology (IT) and operational technology (OT) networks
- ☐ Test industrial control systems (ICS) and OT to ensure critical functions remain operational during an outage

Cyber Centre tools

The Canadian Centre for Cyber Security has a suite of tools and services available to assist CI sectors in enhancing their cyber security posture. CI sectors can request access to these tools and services from the Contact Centre and will be required to complete an onboarding process. The following services are available:

- Threat Intelligence
- Alerts about cyber threats and vulnerabilities (with mitigations)
  - Weekly incident summaries
  - Regular threat briefings
  - Vulnerability notifications
- Access to our malware analysis platform
- Access to real-time threat feed of Indicators of compromise
- Access to cybersecurity assessments and templates
- Dedicated Cyber Centre point of contact

Non CI organizations can sign up for cyber security alerts, flashes, reports, and assessments by reaching out to the Contact Centre.

Communications Security Establishment | Centre de la sécurité des télécommunications

© Government of Canada | This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE. Cat. No. D97-1/10-101-2022E-PDF ISBN 978-0-660-44404-8

Canada