CANADIAN CENTRE FOR CYBER SECURITY

Transitioning to a cyber resilience approach

May 2024

ITSAP.10.190

Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions and compromises on systems that use or are enabled by cyber resources.

A cyber resilience approach considers security from a system of systems perspective and recognizes this complexity in planning and response. Collaboration between the elements of a system, like computing platforms, networks, business applications, people, and processes are fundamental to this approach.

The Cyber Centre focuses on cyber resilience as an approach that can help the owners and operators of IT systems that support business operations mitigate the potential impacts of cyber events. Operational technology (OT) and industrial control systems (ICS) are also increasingly being connected to the Internet and becoming reliant on IT systems to function. A cyber resilience approach can help critical infrastructure (CI) owners and operators secure their OT and ICS.

How to transition to a cyber resilience approach

The following elements can assist your organization in transitioning to a cyber resilience approach:

1. **Collaboration and governance:** Put in place appropriate engagement and governance mechanisms with clear roles and responsibilities. Ensure participation from the key stakeholders by agreeing on objectives and working towards a common vision. Involve non-traditional partners, such as experts in OT, business continuity planning, disaster recovery, civil society organizations, and broader communities (such as rural, remote, and Indigenous communities).

2. **Understanding the risk:** Identify your critical functions, systems, assets, and their dependencies. Understand your existing capabilities to protect these elements, reduce the likelihood of compromise, and prioritize ways to minimize the potential impact of a cyber event. Increase information sharing amongst stakeholders to enhance the broader understanding of the threat landscape in your sector.

3. **Prevention and mitigation:** Identify, develop, and implement initiatives and solutions to adapt to or reduce cyber security risks by increasing the level of robustness, redundancy, resourcefulness, and rapid recovery of your systems.

4. **Incident preparedness, detection, and response:** Implement the capabilities required to detect cyber incidents on your systems. Ensure effective training, recovery plans, and resources are in place to respond to incidents and minimize their impact.

5. **Forward-looking recovery:** Learn from cyber incidents and share these lessons with other stakeholders to foster a proactive threat information sharing culture. Use cyber incidents as an opportunity to address underlying issues and reduce vulnerabilities to enhance resilience after the event.

AWARENESS SERIES

D97-1/10-190-2024E-PDF
978-0-660-71815-6

Canada

Why cyber resilience is important to your organization

The interconnectedness and dependencies across sectors, such as energy, finance, telecommunications, and transportation, create the potential for greater and cascading impacts when an incident occurs. IT and physical systems have converged in ways that challenge traditional approaches to security in both domains, which introduces greater complexity. A cyber resilience approach considers the greater connections and dependencies between systems and can assist in mitigating the risks of cascading cross-sector impacts and evolving threats and changes in the environment.

CI underpins many of the services Canadians use every day. As noted in the National Cyber Threat Assessment, the cyber resilience of CI systems is important and is increasingly at risk from cyber threat actors. Any disruption to the confidentiality, integrity, or availability of critical systems will cause significant impacts on industrial processes, the customers they serve, and the economy.

Threat actors and state-sponsored actors target CI for financial gain, to cause disruption, and to collect information through espionage. They will preposition themselves by injecting malicious implants into CI systems. Some implants are intended for espionage to exfiltrate information. Others can lie dormant as a capability they can leverage to cause disruption in the future.

Benefits of cyber resilience

- Increased understanding of threats and the risk posed to CI systems enables more effective investment in cyber defence.
- Proactive measures to restore and recover critical functions reduces downtime, cost, and impact of a disruption.
- Increased cyber defence capabilities makes CI systems more difficult to disrupt.
- Coordinated response, preparedness, and communications improve public trust when a cyber incident occurs.
- Cyber resilient CI systems improve national security by minimizing the risk of cascading impacts across CI sectors.

The U.S. National Institute of Standards and Technology (NIST) has also published guidance on a systems security engineering approach to developing cyber resilient systems. This approach has similar goals to the Cyber Centre's resilience guidance and links to relevant security controls.

For more information on cyber resilience approaches and security controls, see NIST SP 800-160 Vol.2 Rev.1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach and the International Organization for Standardization's Security and resilience: Organizational resilience - Principles and attributes (ISO 22316:2017).

Learn more

- ITSG-33: IT security risk management: A lifecycle approach
- An Emergency Management Framework for Canada
- Emergency Management Strategy for Canada: Toward a Resilient 2030
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- Security considerations for critical infrastructure (ITSAP.10.100)
- Protect your operational technology (ITSAP.00.051)