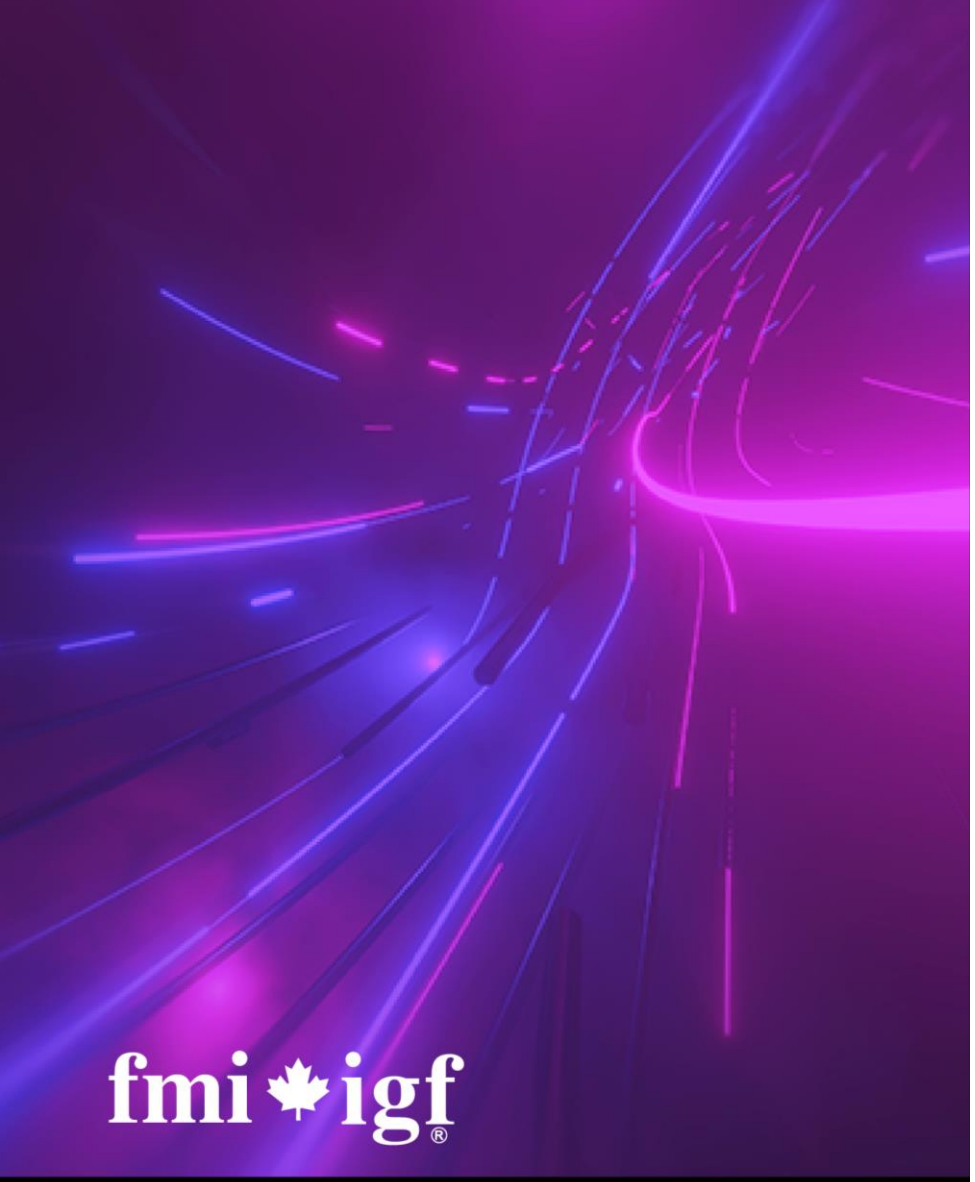


PD WEEK 2022

SEMAINE DE PP 2022

An Enterprise Approach to Cyber Security

SONY PERRON,

President, Shared Services Canada

In this presentation

A common understanding of cyber security risks.

An enterprise approach’s effect on cyber security posture.

The importance of personal responsibility.

How you can integrate cyber security into your plans.

Cyber risks

Cyber security is always top of mind for SSC.

Threats are constantly increasing.

Layered defence and the enterprise approach are key.

We must invest in talented people to stay ahead of threats.

The Information Technology Security Tripartite (ITST)

Roles and Responsibilities

Whole-of-Government Approach

Government security and the continuity of Government of Canada (GC) programs and services rely upon the ability of departments and agencies, as well as government as a whole, to manage cyber security events.

IDENTIFY • PROTECT • DETECT • RESPOND • RECOVER

Strategic Direction & Oversight
Treasury Board of Canada Secretariat

- Setting vision and strategic direction enterprise services, information, data, information technology (IT) and cyber security
- Decision making on management of cyber security risks on behalf of the GC
- Direct a deputy head to implement a specific response to cyber security events

Networks & Security Services
Shared Services Canada

- Providing certain services related to email, data centres, networks and end-user technology devices including IT security services
- Monitoring of departmental electronic networks and devices
- Identification and investigation of issues and implementation of corrective action in the event of unacceptable use

Cyber Defence
Canadian Centre for Cyber Security

- Leadership, advice and guidance for technical matters related to it SECURITY
- Protecting and monitoring of electronic information and infrastructure
- Threat identification, protection and mitigation against cyber events
- Leads the development of trusted sources of supply
- National authority for communications security (COMSEC)

Cyber Security Management
Departments and Agencies

- Departmental cyber security management function
- Develop and deliver client-centric service by design including security
- Protecting sensitive information under the department's control
- Report cyber security events and incidents
- Ensuring that appropriate and timely remedial action is taken

Perimeter Defence / Supply Chain Integrity

Controls and active monitoring of the GoC Network Environment.

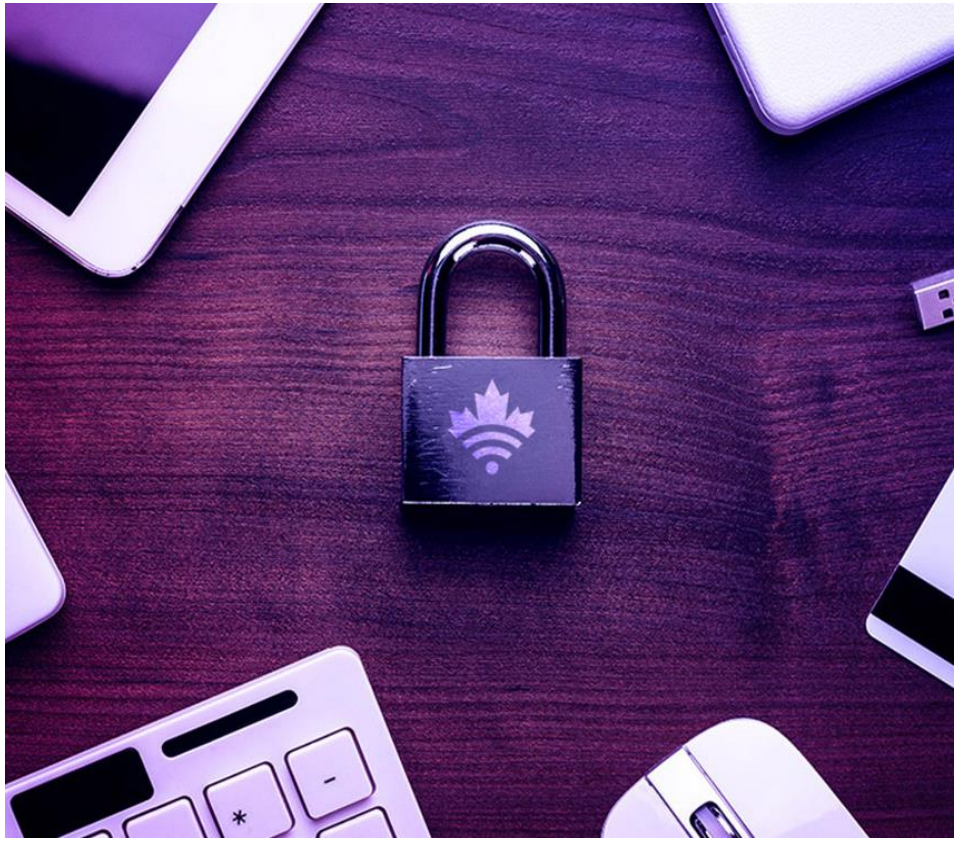
Services and Equipment Procurement subject to highest integrity standards.

Modernization of the GoC Data Center Infrastructure.

Secured Enablement of Public Cloud Utilization.

Outdated application and technology is a continued factor or risk.

Modernization



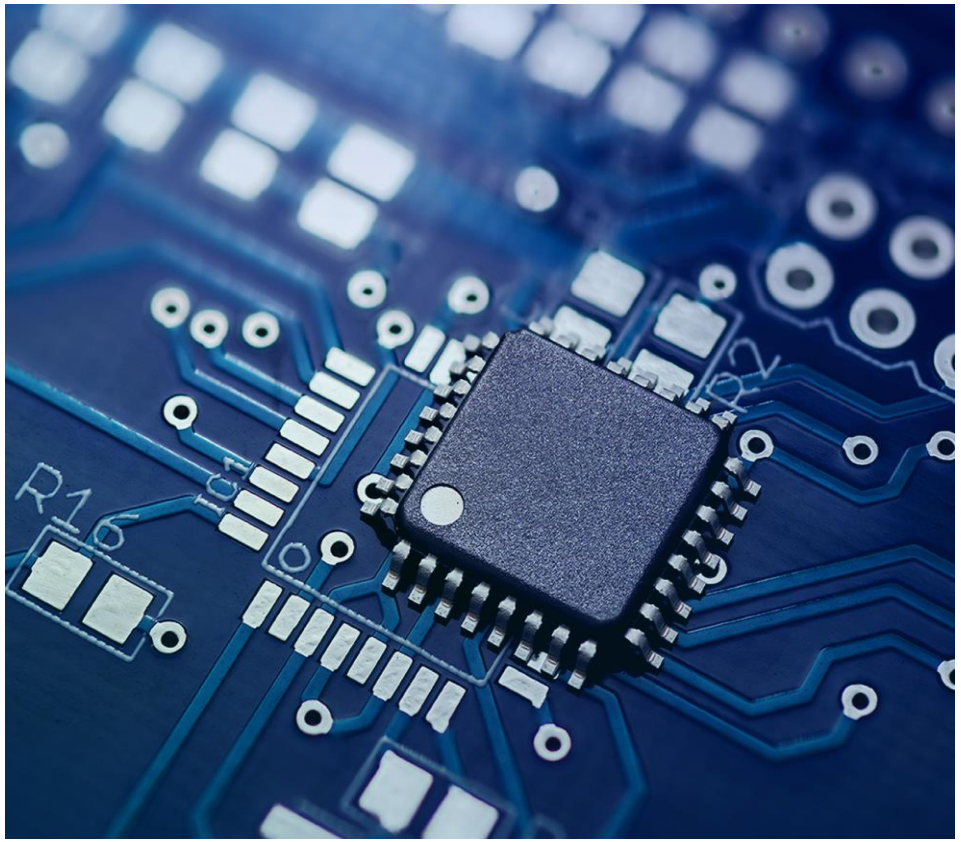
Standardization, Simplification, Visibility.

Designing a secure network from the ground up minimizes flaws that could compromise security.

A shared enterprise network improves reliability and stability, reducing the time and effort we spend on troubleshooting problems.

Enhance ability to respond to cyber event.

The Canadian Centre for Cyber Security



Created in 2018 as part of the Communications Security Establishment.

Most security systems are designed and managed by SSC.

The Cyber Centre uses complimentary solutions to supplement those systems (for example, host-based sensor for monitoring and protection of GoC endpoints).

Enterprise approach

Aims to reduce the many similar IT solutions across the Government of Canada that meet the most common IT needs.

Key to the success of a digital government.

Our response to the pandemic and has demonstrated the benefits of a government-wide enterprise approach to IT infrastructure services.

What financial managers should look for

Provision in budget and financial plan for cyber security.

Consider the cost if Digital Solution Failure due to a cyber attack occurs.

Leverage common solutions rather than department-specific measures.

Automation as protection

The Government of Canada has systems in place that use advanced machine learning algorithms to automatically and quickly prevent attacks.

Shared awareness is essential.

Information needs to be available to all concerned at the same time.

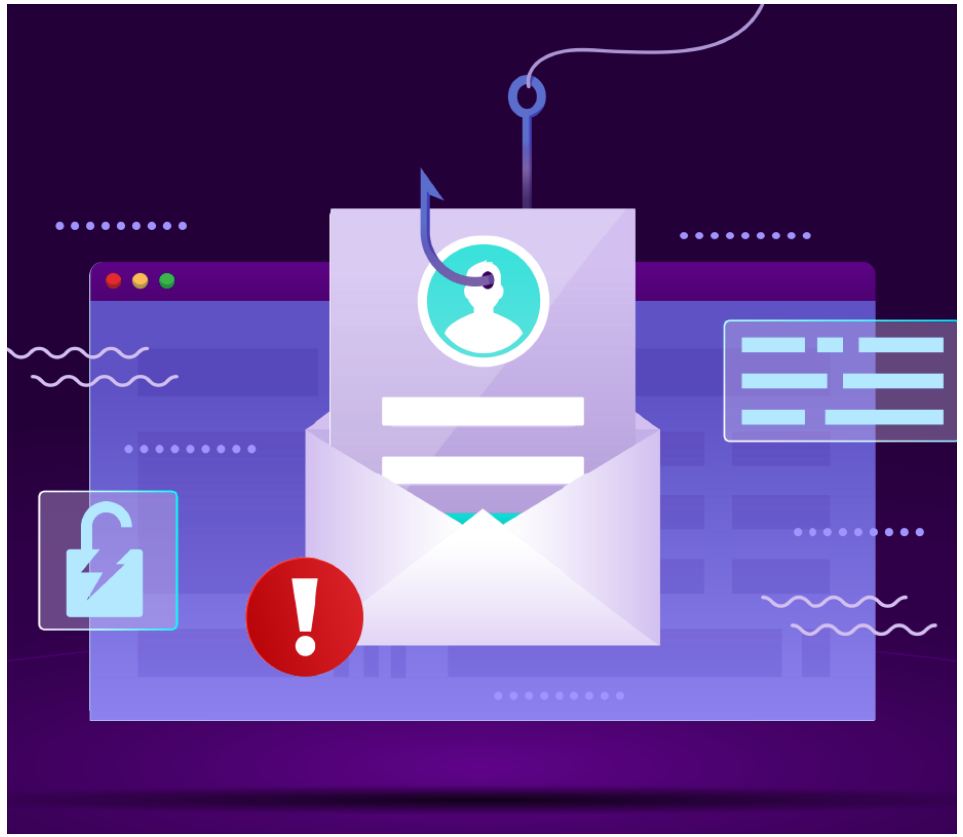
What financial managers should look for

Provision in budget and financial plan for cyber security.

Consider the cost if Digital Solution Failure due to a cyber attack occurs.

Leverage common solutions rather than department-specific measures.

Personal Responsibility

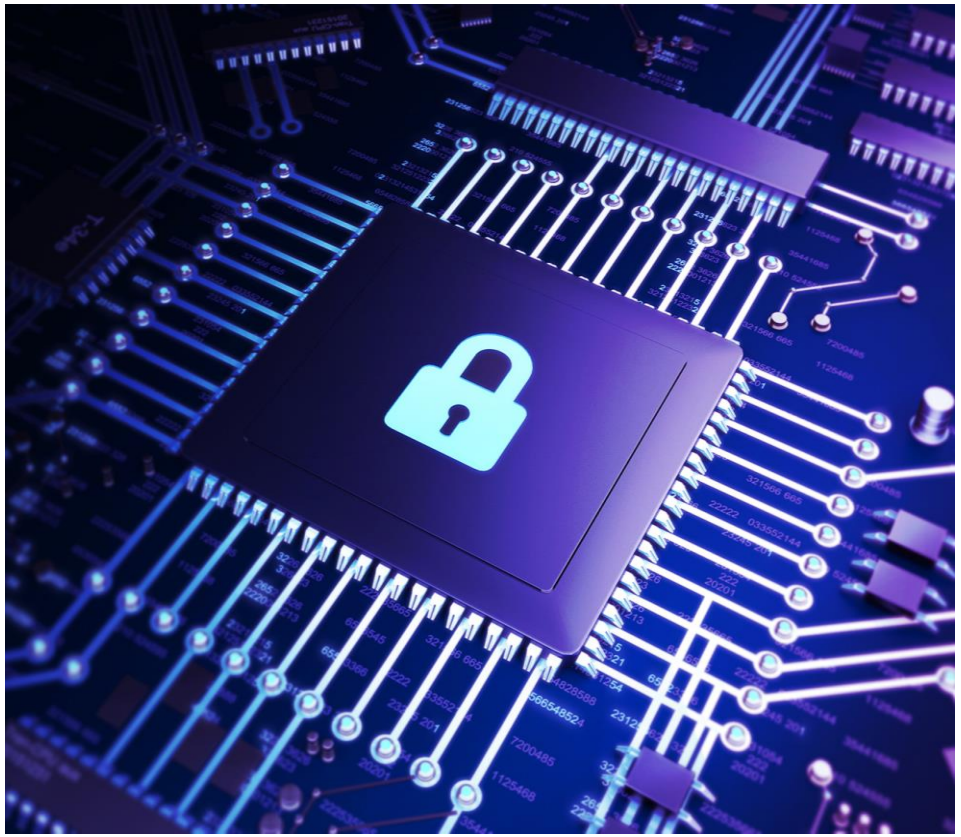


Human error and impulses greatly impact network security (e.g. phishing attacks).

Obtain training resources and participate in the development of a Security Awareness and Training plan.

Communicate with employees about their role in preventing cyber attacks.

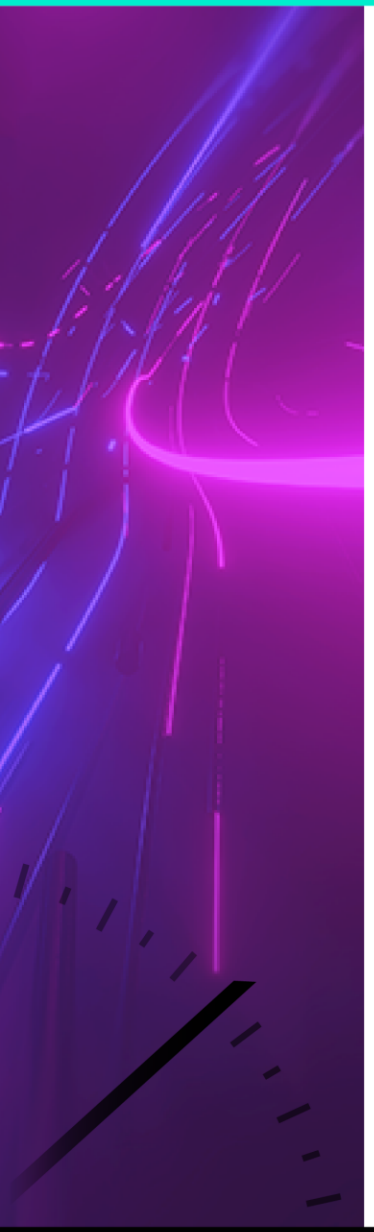
Takeaways



SSC works to provide efficient procurement of solutions and availability of hosting solutions and platforms.

My goal is for SSC's enterprise approach in cyber security to turn into a roadmap for enterprise cyber security services.

An enterprise approach is not just SSC, it is all of us.



Questions?