Communications Security Establishment
Centre de la sécurité des télécommunications

CYBER JOURNAL

EDITION 7 – FEBRUARY 2015

IN THIS EDITION

KEEPING PACE WITH EMERGING THREATS

On a daily basis, Government of Canada (GC) networks are being targeted by threat actors from around the globe - threat actors with sophisticated methods who can reap rewards from having access to sensitive government information. These threat actors view Canada as an attractive target due to its wealth, resources, and diplomatic relationships.

To counter today's emerging threats, departments must remain vigilant in defending their networks. All departments must stay up to date and aware of, not only the latest threats, but the best methods to defend against them.

While there is no 'catch-all' solution to secure GC networks, effective security actions exist that, when taken, will reduce threat surfaces in GC networks. This edition of Cyber Journal highlights those security actions.

Toni Moffa
Deputy Chief, IT Security

www.cse-cst.gc.ca

Canada

THE TOP 10 IT SECURITY ACTIONS TO PROTECT GC INTERNET-CONNECTED NETWORKS AND INFORMATION

In light of information and trends derived from several years of collective GC cyber defence operations, CSE has revised the Top 35 into a Top 10 list.

The focus of the Top 10 is to mitigate the effects of common and current exploits against operational GC Internet-connected networks and information.

The Top 10 has been ordered in a way that each action taken builds on the previous one to continually diminish the GC threat surface and in turn increase the difficulty and level of effort required by threat actors to compromise GC networks.

Full text on the Top 10 can be found at:
ITSB-89: The Top 10 Security Actions

THE DANGERS OF FREE DYNAMIC DNS

The Domain Name System (DNS) is a protocol that converts user-friendly website names, called domain names, to IP addresses. Every computer, web server, or device that can connect to the Internet has an IP address assigned to it. Internet Service Providers (ISPs) have DNS servers that communicate with each other, as well as the 13 main Internet root servers, in order to look up IP addresses and direct your computer to the server hosting the website you wish to visit.

Most DNS hosting providers are fee based. There are also a number of public/free DNS hosting providers, mostly providing Dynamic DNS services. Free Dynamic DNS services provide a selection of domain names and allow anonymous account holders to create subdomains for them.

Threat actors may use free Dynamic DNS services because they can bypass the standard domain registration process and operate anonymously as well as proliferate their malware. GC departments are advised to block access to the subdomains served by known free Dynamic DNS providers. To reduce the risks of malware downloads, your organization's firewall or web filter may already have an embedded feature that, once activated, can manage the risk of Dynamic DNS. For more advice and guidance, contact ITS Client Services: itsclientservices@cse-cst.gc.ca.

DIRECTIVE UPDATE

CSE is happy to announce that the IT Security Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) has been published. This publication includes significant changes for COMSEC planners and practitioners. For more information, ITSD-03A can be found on the COMSEC User Portal.

NEW E-LEARNING COURSE!

As part of the CSE and Canada School of Public Service partnership, CSE's IT Security Learning Centre is pleased to announce a new e-learning course.

104E – IT Security Risk Management: A Lifecycle Approach offers a high-level appreciation of the concepts and processes outlined in ITSG-33.

DID YOU KNOW?

Security Implications of Using a BlackBerry as a Hotspot

BlackBerry devices can be used to create a Wi-Fi hotspot and provide access to the carrier wireless network. In this case, Wi-Fi data is routed directly through the carrier wireless network which is unsecured, NOT through the more secure BlackBerry global enterprise infrastructure.

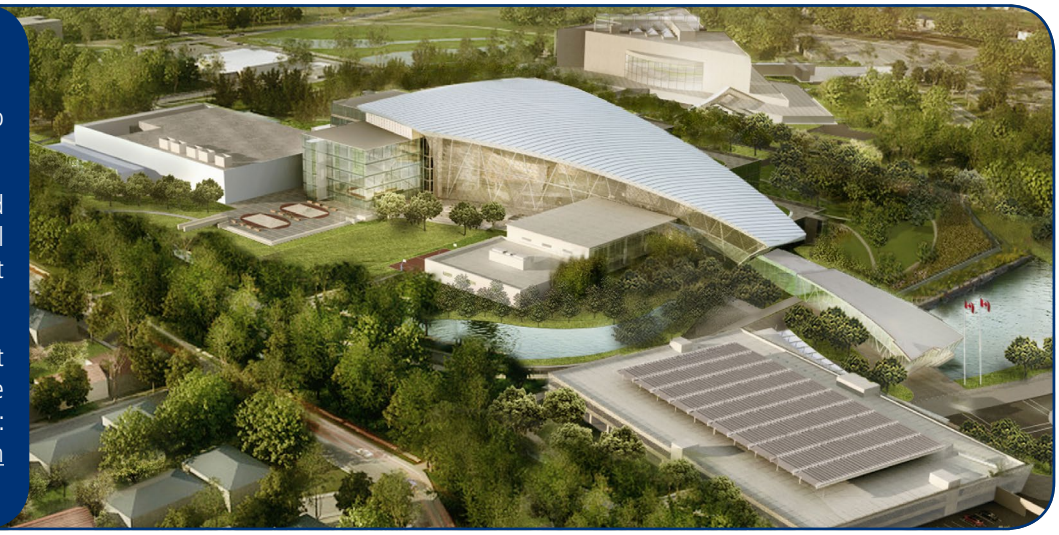
It is recommended that GC departments set the Mobile Hotspot Mode to Disallow to prevent bypassing IT security protection mechanisms. Mobile Hotspot Mode should only be enabled in conjunction with the GC secure remote access or equivalent departmental secure remote access services. Without these conditions, users may inadvertently bypass the GC network monitoring and protection mechanisms.

CSE'S NEW HOME!

We are pleased to announce our move to our new facility at 1929 Ogilvie Road!

This purpose-built, LEED Gold Certified facility consists of both office and special purpose spaces, and is designed to meet the needs of CSE.

CSE's mailing address and contact information remains unchanged. For more information on the new facility, visit: www.cse-cst.gc.ca/accommodation-installation.



In its 2013 Global Threat Intelligence Report, Solutionary, Inc. discovered that private sector organizations are spending as much as $6,500 US per hour to recover from a distributed denial of service (DDoS) attack. It can take up to 30 days to mitigate and recover from malware intrusions at a cost of $3,000 US per day. These costs do not include revenue that may have been lost due to system downtime.

CYBER SECURITY CONSIDERATIONS FOR MANAGEMENT

The information systems that GC departments rely on to support their business activities are often subject to serious threats. These threats can have adverse effects on departmental business activities by compromising the confidentiality, integrity or availability of the information systems and their IT assets that can lead to unauthorized disclosure of sensitive information, costly recovery from an incident and reputation damage.

An essential part of a strong cyber security program is having the support of senior management who must define the risk strategy and acceptable levels of risk that align with the business needs of the department. Regular communication between management and their IT security team is essential to provide the awareness of the current risks and potential business impacts.

DID YOU KNOW?

- A serious cyber security incident could incur significant cost to your organization;
- A threat actor could reap benefits by having access to your sensitive information; and
- Many cyber security incidents rely on employees to unknowingly carry out their execution.

MANAGEMENT CONSIDERATIONS

- ✓ Security controls should be implemented to minimize or limit successful intrusions;
- ✓ The culture of your organization should encourage employees to use strong security techniques;
- ✓ Policies and procedures detailing the proper response to a cyber security incident should be developed before one occurs; and
- ✓ Tracking the implementation of the Top 10 Security Actions will help mitigate common and current exploits against GC networks.

CSE's ITSB-67: Cyber Security Considerations for Management identifies key questions that can help guide leadership discussions between management and their IT security teams to enhance national security, protect sensitive GC information, and enable the achievement of departmental mission objectives.

HARDWARE SECURITY MODULES

The GC depends on the Internet to conduct its business, and while internet-based communications boost productivity and efficiency, using the internet significantly increases the risk of compromise of sensitive information. Hardware Security Modules (HSMs) are a great way to help secure internet communications and protect against exposing cryptographic keys.

HSMs are dedicated processors specifically designed to protect cryptographic keys through secure internal storage, key management, and credential processing. For further protection against vulnerabilities like Heartbleed, organizations could consider storing cryptographic keys on HSMs instead of directly on servers.

HSMs create a physical barrier between the web/application servers and the private cryptographic keys. This barrier helps to keep the keys secure, and ensures the authenticity, confidentially, and integrity of internet-based communications.

HSMs offer the following benefits:

- ★ Secure Key Storage;
- ★ Certification;
- ★ Key Management;
- ★ Access Control; and
- ★ Transport Layer Security Traffic Off-loading.

For advice and guidance on HSMs, contact ITS Client Services.

WINDOWS 7 HARDENING GUIDE

Many GC departments have deployed, or are in the process of deploying, Windows 7 as their primary operating system (OS). However, out-of-the-box configurations of newer OSs present a number of security risks, leaving an organization's IT assets and infrastructure susceptible to compromise.

In response, CSE has recently released ITSB-110: Microsoft Windows 7 Enterprise Edition Hardening Configuration Guidance. ITSB-110 provides mitigation strategies for deploying Microsoft Windows 7 Enterprise Edition OS in a manner that will best prevent compromise of GC IT assets and infrastructures.

Windows® 7

CSE recommends that departments choose one of three baseline configurations, listed in the Windows 7 Hardening Guide, and further tailor that configuration to counter any specific vulnerabilities or threats identified in the TRA of their IT networks.

While there is no 'silver bullet' that will protect against all cyber risks, the Windows 7 Hardening Guide describes additional security features and tools that are either native to Windows 7, or are available as a free download from Microsoft that can be used to further complement CSE's advice that is tailored to your organization.

STAY AHEAD OF THE THREAT: MEASURES TO PROTECT YOUR NETWORK

Given today's cyber threat environment, which includes numerous vulnerabilities and pervasive threat actors with sophisticated methods, it is impossible to prevent compromises 100% of the time. In light of this, IT security practitioners must proactively prepare themselves to mitigate intrusion.

Being prepared for cyber threats will reduce the risk of compromise and significant data loss. The following steps will improve your department's ability to more quickly and more effectively respond to threats and reduce the success of threat actors.

How can you plan to thwart cyber threats?

➔ Understand how and where your systems are vulnerable.

Ensure you are not running outdated Internet browsers, operating systems, and other vulnerable components that are simple to exploit. It is pivotal to understand what components your network uses and where those components are located, as this will enable rapid patching once new vulnerabilities are discovered.

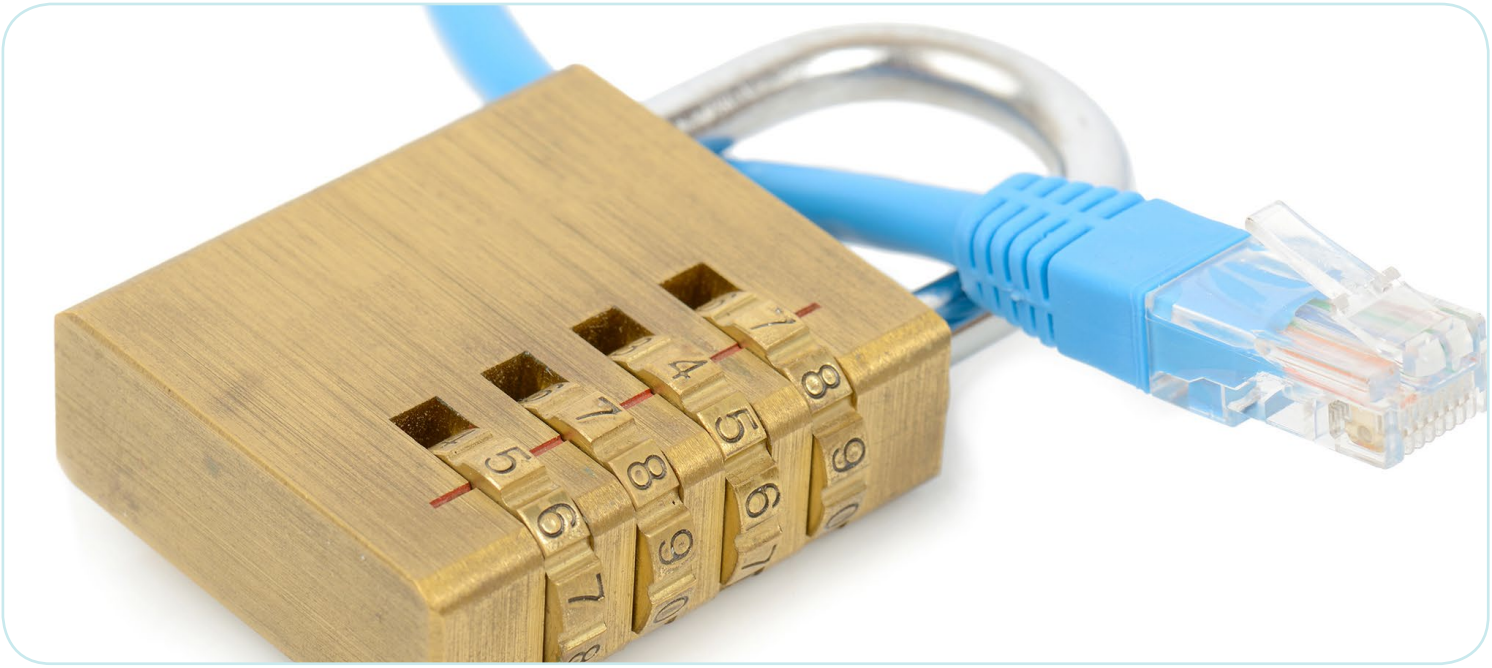
➔ Anticipate the threat actor's objective.

Whether it is obtaining negotiating strategies, sensitive business information, or user credentials, departments are targeted constantly. Identify information of value and its location to allow further strengthening of your department's security posture.

➔ Know how your networks are connected.

Most departments have interconnected networks and links to other departments and organizations, thereby increasing their threat surface. Threat actors quickly and covertly shift from an initial access point to a more lucrative one. Prevent this exposure by ensuring your department's most sensitive information is separated from vulnerable systems which have Internet access.

As compromises are inevitable, strong prevention efforts must become our focus. There are a number of exercises you can conduct to be better prepared in responding swiftly to an incident when it occurs – all of which will go a long way towards collectively protecting electronic information and infrastructure of importance to the GC.



SHARED SERVICES CANADA (SSC) CORNER

SSC'S SUPPLY CHAIN INTEGRITY PROGRAM

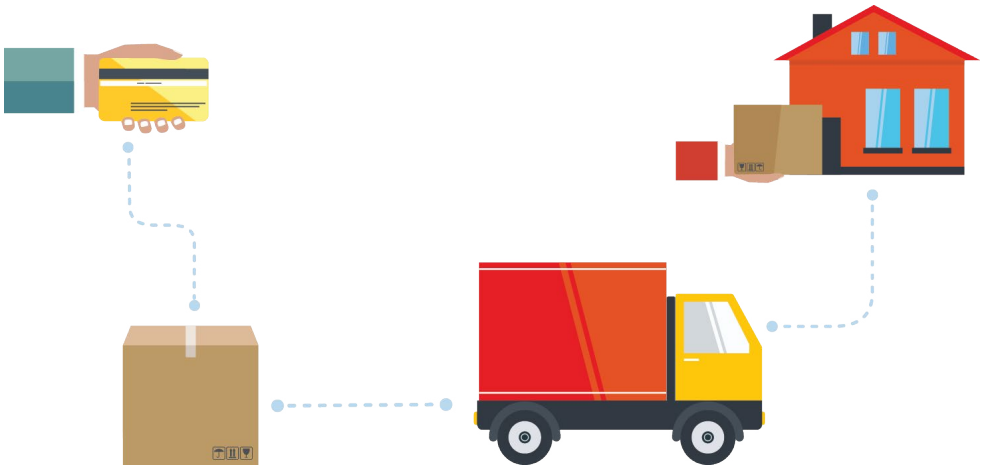
Establishing a GC IT infrastructure that is secure, trusted, and reliable is a key component of SSC's mandate. As the primary custodian of the GC's IT infrastructure, one of the ways SSC counters cyber-security threats is by protecting and securing the integrity of GC's supply chain. Supply chain integrity controls protect data sovereignty by ensuring that untrusted equipment, software and/or services do not become part of the GC IT infrastructure.

In January 2013, SSC launched a two-step procurement process to ensure that untrusted equipment, software, or services are not procured or used by SSC to deliver and/or support GC services. This process requires that bids be pre qualified based on a review by SSC (with advice from CSE) of all IT products, services, and architectures a vendor proposes to use to deliver a managed service. Bidders must successfully pass this review in order to continue the procurement process.

This procurement process is currently applicable to all competitive procurement processes including sole source contracts, standing offers, and outsourced service procurements. The same level of scrutiny is also part of the ongoing audit of existing contracts, and provides SSC with the assurance required to maintain the security of GC systems and networks.

To date, SSC and CSE have:

- ✓ Successfully completed over 2,124 supply chain integrity procurement reviews, 12 Industry Days and assessed 15 Invitations to Qualify (ITQ);
- ✓ Expanded the scope of supply chain integrity to include workplace technology devices, data centres, and all subcontractors that deliver services to the GC;
- ✓ Implemented enhanced security clauses in Request for Proposals; and
- ✓ Implemented processes to identify and mitigate deployed equipment, software, and services that have been identified as having increased risk of compromise.



ENHANCING OUR SECRET NETWORKS

To create and share classified information, GC departments currently use multiple classified environments along with a variety of technology solutions. Of the more than 30 SECRET networks in use across the GC, most are not accessible to the majority of employees who require them. As well, current policies make it difficult, and in some cases cost prohibitive, to expand the footprints of these networks to include those employees who require access to classified information.

These constraints have led to the current ongoing development of the Government of Canada Secret Infrastructure (GCSI). The GCSI has an end goal of replacing the multiple existing SECRET systems with a single enterprise-wide solution that will:

- Strengthen and standardize departmental security postures;
- Realize government-wide business needs of creating and communicating classified information; and
- Obtain efficiencies necessary to sustain operations.

In order to reach this goal, Shared Services Canada (SSC) has engaged all of their partners to validate business requirements. The Treasury Board of Canada Secretariat will also be contacting SSC clients to gather requirements.

CYBER JOURNAL

EDITION 7 – FEBRUARY 2015

THE IT SECURITY LEARNING CENTRE HAS MOVED!

All IT Security Learning Centre (ITSLC) courses are now being conducted at 1929 Ogilvie Road, Ottawa. CSE's new building can be easily accessed from any part of the city by public transportation or by taking Highway 174 - Blair Road North exit.

ITSLC courses will be conducted in state-of-the-art classrooms, located in the Visitor Centre, at the front of our new CSE Headquarters.

All classes will start at 08:30 and finish at 16:00. You can bring your own lunch, or visit one of the several restaurants within walking distance.

Complete List of ITSLC Programs and Courses is available at:

www.cse-cst.gc.ca/en/group-groupe/its-training

To prevent sign-in delays, we strongly advise students to arrive at least 20 minutes prior to the course start time.

Visitor parking is very limited, so we recommend using a taxi or public transportation.

We look forward to seeing you at our new home!

ABOUT THIS NEWSLETTER

Cyber Journal has been prepared for GC IT practitioners and stakeholders and is published on a periodic basis. This publication reflects the CSE IT Security commitment to share information, advice and guidance with the broader GC community to help departments and agencies better protect themselves from cyber threats. The aim is to highlight key security issues and stimulate discussion about security within your Department. In addition, the newsletter profiles key products and services offered by CSE with information on how you can leverage them to help your GC organization. Security awareness throughout an organization is an essential element to improving the GC's security posture. As such, we encourage you to share this information within your organization.

SUBSCRIBE

To be notified of future releases, contact: itsclientservices@cse-cst.gc.ca.

CONTACT US

For general advice and security guidance support, contact:

✉ **itsclientservices@cse-cst.gc.ca**

✆ **General Inquiries: (613) 991-7654**

To contact the Cyber Threat Evaluation Centre:

✉ **ctec@cse-cst.gc.ca**

For planning, support or any issues regarding COMSEC devices, contact COMSEC Client Services:

✉ **comsecclientservices@cse-cst.gc.ca**

✆ **General Inquiries: (613) 991-8495**

COMSEC custodians can contact the Crypto Material Assistance Centre (CMAC):

✉ **cmac-camc@cse-cst.gc.ca**

✆ **General Inquiries: (613) 991-8600**

For education and training services, contact the IT Security Learning Centre:

✉ **its-education@cse-cst.gc.ca**