BUILDING A RESILIENT NETWORK

Recently, Canadians’ attention was piqued when Government of Canada (GC) Web sites were targets of Distributed Denial of Service (DDoS) attacks. Although these cyber security incidents were disruptive, GC systems and sensitive Canadian information remained intact because key security measures were in place to protect them.

GC departments deliver services to Canadians, and are dependent on the resilience of IT systems to provide and maintain a respectable level of service. In the face of increasing security challenges, departments need to understand what security actions are required to protect data and to promptly restore services after a cyber intrusion takes place.

Thousands of attempts are made every day to infiltrate government networks. Do you have a clear picture of your overall security posture? Do you have a realistic plan to address the security gaps?

Since October is Cyber Security Awareness Month, I encourage you to continue these important discussions in your department. In this edition of the Cyber Journal, we’re highlighting why CSE’s Top 10 IT Security Actions are important to you. By understanding the ever-evolving threat landscape and how we can respond as a community, we stand a better chance of protecting our networks and protecting Canada’s information.

Originally signed by,

Toni Moffa
Deputy Chief, IT Security
WHY THE TOP 10 IT SECURITY ACTIONS?

AN INTERVIEW WITH CSE EXECUTIVE SCOTT JONES

Director General, Cyber Defence Branch, CSE
The Cyber Defence Branch is responsible for defending GC systems of importance from cyber intrusions.

Q: Why are the Top 10 so important and why should GC departments implement these security actions?

A: Unlike other IT best practices, The Top 10 are based on CSE’s hands-on knowledge and many years of experience mitigating thousands of cyber incidents impacting GC departments and agencies. This is a practical list of actions departments themselves can take to be more secure, and the actions are specifically tailored to address the real threats impacting the GC.

Q: What will happen if these actions are not implemented by the GC community?

A: Implementation is critical. In 2013, all of the compromises that occurred at GC departments were the direct result of a failure to implement The Top 10 IT Security Actions. These actions, when implemented, significantly decrease the threat surface of departments and make the cost to a cyber adversary much higher.

Q: Are some of these actions more critical than others?

A: The Top 10 is an ordered list. By starting with the first action and implementing each subsequent action, departments will effectively and progressively protect their systems. Implementing Action #1 (Use Shared Services Canada (SSC) Internet Gateways) will give departments a fighting chance, but on its own will not be sufficient.

Q: What advice would you offer to a department new to the Top 10 that is struggling with one or more of the measures?

A: Don’t start from scratch. You are not alone. Other departments might be further along in implementation efforts, so I recommend leveraging the experience of colleagues at other departments. Tap into the various communities via SSC, Treasury Board of Canada Secretariat, Chief Information Officer Branch (TBS-CIOB) and the CIO Council (CIOC). Some departments have already successfully implemented some of the 10 Security Actions.

Q: Do you anticipate these security actions changing significantly in the future?

A: Change is to be expected as the threat landscape continues to evolve. The Top 10 Actions address the vast majority of threats currently seen active on GC systems. These actions will have to be adjusted in response to the evolving threat landscape; however, the basic principles, as illustrated in the Top 10, will still be imperative.

Q: Why was Application Whitelisting moved from #1 to #10?

A: In 2014, CSE released the Top 10 IT Security Actions list. Application Whitelisting was moved from the #1 position to #10 because despite its technical effectiveness, it is one of the most complicated tasks for a CIO to implement. In addition, by being number 1, departments were focusing on application whitelisting and we did not want to see departments struggle with whitelisting and not move forward with the other more critical security actions. Application whitelisting remains a very effective measure and, perhaps, a phased implementation, (such as starting with Application Whitelisting on the servers), will prove easier, more cost-effective and more effective at resisting the threat actors currently impacting the GC.

90% of software attacks can be stopped by an automated patch management solution. (SCMagazine, 2012)

37% of a GC department’s employees clicked on a phishing email in a recent training exercise. (CBC, 2014)

75% of common malware is not detected by traditional antivirus software. (Computer World, 2012)
THE TOP 10 IT SECURITY ACTIONS

1. Use Shared Services Canada Internet Gateways
2. Patch Operating Systems and Applications
3. Enforce the Management of Administrative Privileges
4. Harden Operating Systems
5. Segment and Separate Information
6. Provide Tailored Awareness and Training
7. Manage Devices at the Enterprise Level
8. Apply Protection at the Host Level
9. Isolate Web-Facing Applications
10. Implement Application Whitelisting

Make your internet connection work for you - not threat actors. Consolidate your internet gateways to those provided by SSC and benefit from customized defence solutions.

Don’t leave holes in your network. Keep your systems up to date by establishing a patch management framework.

Safeguard the keys to your network. Minimize the number of users with administrative privileges and enforce regular password changes.

Customize and configure your operating system for stronger protection. Take an enterprise approach by disabling all non-essential ports and services, and by removing unnecessary accounts.

Sort and store your information based on its value. Segment your IT networks and establish distinct information protection requirements, and different security controls and policies.

Foster a culture of security awareness at all levels in your organization.

Protect your information and networks by using equipment you can trust. Implement a device management framework and use GC-furnished equipment.

Deploy a Host-Based Intrusion Prevention System (HIPS) solution to protect multiple weak points simultaneously.

Run web browsers and e-mail clients in an isolated virtual environment as they are susceptible to introducing malware to a system.

Identify applications authorized to run and block all others by default.
Developing Flexible Security Solutions: High, Medium and Basic Assurance for the Government of Canada

Technology innovation is essential to keep pace with evolving demands on Government of Canada (GC) IT communications. The Communications Security Establishment (CSE) in collaboration with Treasury Board and Shared Services Canada is working to redefine security assurance solutions for the GC. This effort will transform the way the government develops and deploys communications solutions ranging from basic, medium to high assurance. The approach lends flexibility to solution development and leverages commercially available technologies. Imagine a day where you could use your government-issued BlackBerry Classic/Passport to have secure voice, instant messaging or e-mail exchanges with a work associate! Join CSE to learn how the new assurance levels are being defined and how they will open new opportunities for the GC.

For more information on the schedule for the speaking sessions, refer to the GTEC Conference Program.

Learn more about cyber security and the Top 10 IT Security Actions you can take to protect your information systems.
For more information visit the GTEC Web site.
Threat actors are known to take advantage of employees’ computer habits to uncover entry points into valued systems. Consequently, departments are strongly encouraged to raise the cyber security awareness of all personnel in order to improve their ability to recognize suspicious activity. By fostering a culture of security awareness at all levels in your organization, you build a stronger first line of defence.

To help, CSE has developed a new interactive cyber security application that covers a wide range of security topics affecting your organization. Visit our ITS Interactive Gallery and play the game.
DENIAL OF SERVICE (DoS) EXPLAINED

We often read about Denial of Service (DoS) attacks as cyber threats, but what exactly are these threats? DoS attacks are the result of an individual or group launching malicious data to degrade or to prevent legitimate users from accessing on-line information or services. The primary aim of DoS attacks is to disrupt, and they are typically conducted for publicity to protest corporate or legislative measures. However, in some cases, DoS attacks may be conducted to gain an information edge by cloaking more serious compromises, such as data exfiltration. Apart from the effect on system functionality, some of the other impacts of a DoS attack may include:

- Costs associated with handling the incident;
- Lost or limited functionality of affected service;
- Decreased productivity; and
- Increased vulnerability when resources are diverted toward mitigation.

Threat actors design DoS attacks to exhaust a network’s resources such as its bandwidth, computing power and/or operating systems. The attack hampers the speed and access to those system functions by paralyzing network performance, by preventing access to a particular Web site, or in some cases, by fully denying web-based Internet services. These disruptions are of concern to industry and government alike.

There are multiple types of DoS attacks - some target specific infrastructure or network applications and internal databases. The most common type uses volume to flood a network with information, which subsequently consumes the bandwidth and overwhelms network server performance.
In this type of attack, multiple computers are remotely controlled by more than one threat actor. This broad-based threat constitutes a Distributed Denial of Service (DDoS), where a group of computers, numbering in the hundreds or thousands of compromised hosts (a.k.a. “botnet”), automatically sends directed malicious software commands to a single target entity, thereby degrading that system. DDoS incursions are deceptive in origin as they implicate the compromised hosts and not the actual threat actor.

GC business depends on many online services that can be targets for DoS attacks. This risk is magnified by the wide availability of DDoS tools on the Internet. In order to limit the risk of DoS activities, it is essential to use network connection-limiting controls, router access controls, an intrusion-detection system and a properly configured firewall. In some cases, GC departments may consider leveraging Internet Service Provider (ISP) networks with sufficient bandwidth to withstand a DDoS.

THE CANADIAN CYBER-INCIDENT RESPONSE CENTRE (CCIRC) SUGGESTS IMPLEMENTING THESE MITIGATION GUIDELINES FOR DOS ATTACKS:

- Regularly patch systems with software upgrades;
- Limit administrator user accounts;
- Maintain the latest versions of anti-virus software;
- Configure firewalls to restrict an appropriate level of traffic; and
- Educate users on the dangers of spear-phishing e-mails.

To protect networks and promote better defences, GC departments should:

- Establish clear and complete procedures and guidelines well before an attack takes place.
- Clearly identify the network perimeter and exposed assets.
- Load network security systems such as modern firewall technologies, and consider using a cloud- or Internet Service Provider (ISP)-based DDoS protection service.
- As soon as possible, review all decisions and steps taken throughout the incident-handling cycle and assess where improvements may be made.
- Clearly identify the network perimeter and exposed assets. Load network security systems such as modern firewall technologies, and consider using a cloud- or Internet Service Provider (ISP)-based DDoS protection service.
- DoS attacks may exploit limits of server resources, so be equipped with a flexible provisioning model for these resources. Connection logs can also provide potentially offending IP addresses (if not spoofed) to the target’s upstream ISP, the national Computer Emergency Response Team (CERT) and law enforcement to help coordinate mitigation and investigation efforts.

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.
Government employees play a vital role in protecting key Government of Canada (GC) assets and information. When using mobile devices (especially during international travel), it is important to remember that your devices can be compromised and can have a negative impact on your department, its information, its operations and its reputation.

**WHY TARGET YOU?**
- Steal and send content
- Collect sensitive data
- Track your locations
- Change your settings
- Slow down processing speeds
- Initiate system-wide crashes

**WHAT ARE THE RISKS?**
- Physical theft
- Interception (voice & data)
- Malware and virus
- Hijacking of device
- Spam and spear phishing
- Denial of service, interference or jamming
- Spoofing or impersonating
- Compromise home or GC network

**TIPS**
- Save important tasks, like online banking, for secure networks.
- Never use your cellphone to conduct sensitive discussions or send sensitive text/SMS.
- Avoid using unknown networks or free Wi-Fi hotspots.
- Using social media can put your information about employment, family and geographic location at risk.

For more information and tips to safeguard your mobile technology when travelling internationally, see CSE’s [Mobile Technologies in International Travel for Business Travellers (ITSB-87)](https://cse-cts.gc.ca) and [Mobile Technologies in International Travel for IT Security Managers (ITSB-88)](https://cse-cts.gc.ca).

**ARE YOU TRAVELLING?**
- Before you travel, contact your IT Security team for departmental policies and additional guidance.
- Use updated GC furnished equipment (GFE) vs. your own device.
- Disable features such as Bluetooth and wireless headsets for the duration of your trip.
- Assume that all communications transmitted over public carrier is at risk of being intercepted.
- Report suspected issues as soon as possible to your IT Directorate.
2015 CYBER SECURITY AWARENESS MONTH

During the month of October, take time to review your online safety practices.
Public Safety Canada has provided the following list of online safety tips for protecting your home computer.

✔ **Protect your identity**
Use different usernames and passwords for different accounts. Choose a combination of numbers, letters and other characters that make them hard to guess.

✔ **Turn on your firewall**
Firewalls are easy to turn on and are the first line of defence: they block connections to unknown or phony sites and prevent viruses and hackers from accessing your computer.

✔ **Use anti-virus software**
Install anti-virus software to prevent viruses from infecting your computer. The anti-virus software should be updated regularly.

✔ **Block spyware attacks**
Install anti-spyware software to prevent spyware from installing itself on your computer.

✔ **Install the latest operating system updates**
Make sure that your operating system and applications are supported and up to date.

✔ **Back up your files**
Protect important files from viruses and physical damage such as flood and fire by regularly backing up your files on an external drive.

✔ **Protect your wireless network**
Wireless (Wi-Fi) networks are vulnerable to intruders if they are not protected once installed. You can either do this yourself or ask an expert to install your wireless router.

✔ **Delete e-mails from unknown senders**
Never open e-mails or attachments from people you do not know, and never follow links to Web sites in these e-mails as they may infect your computer with a virus or spyware. Instead, delete these e-mails immediately.

✔ **Surf the Web safely**
Be careful about sharing your name, address, telephone number and financial information online. Check that the Web site is secure and that the privacy settings are turned on.

✔ **Get expert help**
If you need help installing or maintaining software, call a computer expert or a local supplier.
ZERO-DAY EXPLOITS EXPLAINED

In April 2014, an Open SSL software flaw known as the “Heartbleed bug” affected an estimated two-thirds of web servers worldwide. The “zero-day” exploit allowed for potential disclosure of confidential information (including passwords and personal and corporate information) that was saved in memory, and ultimately resulted in a privacy breach at the Canadian Revenue Agency (CRA).

A zero-day exploit takes advantage of a vulnerability in a computer application or operating system that is unknown to the software developers and for which a patch is not yet available. When security researchers discover software vulnerabilities, they ethically disclose the details to the software developer, confidentially and at no cost. The developer can then prepare and release a patch before anyone takes advantage of the vulnerability.

In some cases, however, those who discover a vulnerability post the information online without informing the software company of the flaw. When this happens, cyber threat actors can devise an exploit before a patch can be released, giving developers zero days to develop a patch. Furthermore, a malicious threat actor can develop an exploit kit for that vulnerability and sell it to other cyber-threat actors. Often, software developers are only made aware of the flaws after the vulnerability has been detected and exploited.

Zero-day exploits continue to be a threat. As part of The Top 10 IT Security Actions, CSE encourages departments to implement application whitelisting by identifying authorized applications and application components and denying all others by default. For more information visit: Top 10 IT Security Actions for Internet Connected Networks and Information.

PHASES OF A ZERO-DAY EXPLOT

- Vulnerability discovered; exploit being developed.
- Exploit available but software company is unaware of vulnerability.
- Vulnerability becomes known; vendor begins developing patch.
- Patch is made available. Patched systems are protected. Unpatched systems remain vulnerable.

387 The number of new malicious software created every minute. (McAfee, 2014)
CSE strongly encourages GC departments and agencies to stop running Windows XP operating system software on their devices.

In accordance with Treasury Board Secretariat (TBS) ITPIN 2015-01, GC departments and agencies are expected to comply with the following directives:

- XP devices must not be connected to GC networks or the Internet after March 31, 2015;
- XP devices required for operational needs are to be isolated and contained within a tightly controlled network environment;
- XP devices operating in isolation zones are to be considered a temporary measure. The rationale and operating strategy are to be submitted to the TBS Chief Information Officer Branch (CIOB) each year as part of the departmental IT plan;
- Departmental Chief Information Officers (CIOs) or equivalents are to establish active measures to ensure compliance with this direction; and
- GC departments are not to arrange Window XP Custom Support Agreements (CSAs) with Microsoft.

Departmental CIOs are reminded that operating unsupported software on GC networks exposes the GC to increased cyber security risks.

### CSE’s Role in GC Cross Domain Solutions

Approved Cross Domain Solutions (CDS) can provide the additional security controls required to mitigate the risks of connecting networks that have different security levels.

With regard to CDS, CSE’s main goal is to raise departmental decision-makers’ and practitioners’ awareness of what CDS are and how to securely deploy them within a robust risk-mitigation framework.

To accomplish this goal, CSE can provide the following services:

- Inform GC clients of CDS-related vulnerabilities and threats; and
- Provide technical advice for a GC departmental CDS project or initiative at defined stages of development.

To help deliver these services, CSE launched a CDS working group in February 2015 as a forum for our partners to share best practices, and for GC departmental IT security practitioners to consult CSE about their current and planned CDS deployments.

For more information about CDS requirements, the working group or other information, contact ITS Client Services.

---

**FOR ADDITIONAL INFORMATION VISIT:**

- [ITPIN 2015-01 Disposition of GC Windows XP Devices](#)
- [CSE ITSB-68, End of Support for Microsoft Windows XP SP3 and Microsoft Office 2003](#)
- [CSE ITSB-89 Version 3, Top 10 Security Actions](#)

You may also address any inquires by e-mail to TBS CIOB IT Division.
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.

TRAINING NEWS

COMSEC CUSTODIAN CERTIFICATION PROGRAM

The CSE Information Technology Security Learning Centre (ITSLC) has introduced the COMSEC Custodian Certification Program (CCCP). The CCCP will provide background knowledge on COMSEC and cryptography principles and concepts, and will offer the necessary skills to perform the duties of a COMSEC Custodian. This certification program combines our existing courses into distinct pathways that will provide the necessary foundation to prepare candidates appointed as COMSEC Custodians. The CCCP will consist of three similar but independent pathways that have been designed to consider COMSEC account composition. For more information on the CCCP, visit the ITSLC Web site.

CSE ITSLC WEB PORTAL ONLINE COURSE REGISTRATION FOR GC EMPLOYEES

The ITSLC now offers a new online course registration tool that enables GC employees to create individualized learning profiles and register for courses online. This tool will facilitate course registration and will allow learners to access all Learning Centre resources. By creating a learning profile, you’ll have access to the ITSLC catalogue, the course schedule, news and highlights. Notably, you’ll be able to directly select courses online; to view and track the status of the courses you’ve registered for; and to view all the courses you’ve taken to date. This new process reduces the time between registration and confirmation of a course. Plus, the system will automatically remind you of your next ITSLC learning experience.

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
📞 General Inquiries: (613) 991-7110

Complete List of ITSLC Programs and Courses is available at: