Communications Security Establishment
Centre de la sécurité des télécommunications

CYBER JOURNAL

EDITION 11 | JUNE 2017

IN THIS EDITION

BE PROACTIVE: PREVENT MALICIOUS ATTACKS ON YOUR NETWORK

Cyber incidents continue to grow in scale, complexity and damage every day. As we saw recently with the global ransomware attack, WannaCry, cyber threat actors have the motive and the ability to compromise critical government, business and personal systems whenever they see vulnerabilities. CSE works diligently to do our part to ensure Government of Canada (GC) systems are protected against the most sophisticated cyber threats, but it takes a collaborative effort from government, private sector and academia to ensure Canada's most important information is secure.

It is clear that in today's dynamic threat environment, IT security cannot be an afterthought. By following the steps in our Top 10 IT Security Actions, organizations can learn cyber best practices to defend and protect their own systems from malicious cyber attacks. In this edition of Cyber Journal, you will find featured IT security tips that could help prevent malicious ransomware, such as WannaCry, from encrypting your files in the future.

In the case of a compromise, departments must integrate IT security into their emergency plans to ensure minimal damage to their critical systems. Learn how the Treasury Board of Canada Secretariat (TBS) addressed the importance of testing IT-focused emergency plans with its Engarde exercise. This exercise is an important reminder to create and test a cyber security plan to ensure you're prepared in the event of a serious intrusion.

GC departments are working together to better protect sensitive Canadian information. CSE believes in taking a proactive approach to cyber security, which means encouraging organizations and individuals to implement adequate security systems before a major attack takes place.

Originally signed by
Scott Jones
Deputy Chief, IT Security

cse-cst.gc.ca/en/its

Canada

DON'T FALL VICTIM TO RANSOMWARE: 5 ACTIONS TO PROTECT YOUR NETWORK

Beginning on May 12th, a global ransomware attack named WannaCry affected over 200,000 victims in 150 countries. Collaborating with industry partners, CSE was able to obtain defensive threat information which was immediately deployed to protect GC systems and networks against this threat. In today's digital world, it is no longer an option to ignore security protocols and hope an attack doesn't happen. GC departments that updated their Windows systems with the March 2017 Microsoft MS17-010 patch were not susceptible to the WannaCry ransomware.

This widespread global ransomware attack proves that malicious threat actors can target our systems at any time, in any place, to achieve any goal.

Ransomware is a type of malicious software designed to infect users' networks, blocking access to systems and data until a sum of money is paid. Even if you do pay the ransom to get your data back, some threat actors still don't release your information and demand even more money. This can continue and you may never retrieve your data. It is not effective to pay the ransom. Paying ransom encourages threat actors and only further validates the effectiveness of this cybercrime.

The risks associated with weak cyber security practices can only be mitigated with continual and dedicated investments to IT infrastructure. While it may be resource intensive to implement strong cyber security practices such as patching and whitelisting, the cost of ignoring IT security is much greater. It's important to remember that security practices can be prioritized to match the importance of the data being protected. The real question is: can you afford not to implement cyber security into your organization?

CSE recommends implementing the Top 10 IT Security Actions to protect your systems against malicious cyber attacks. On the next page you will find 5 actions best suited to protect against ransomware.

DON'T FALL VICTIM TO RANSOMWARE: 5 ACTIONS TO PROTECT YOUR NETWORK

2 PATCH OPERATING SYSTEMS AND APPLICATIONS

Don't let known vulnerabilities be exploited. Keep everything up to date (including: operating systems, applications, and browser plugins). Deploying patches as soon as they are released is the most effective way to prevent systems from being compromised.

3 ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES

Minimize the number of users with administrative privileges and ensure users do not have privileges to install software on their devices without the authorisation of an administrator. Perform administrative functions on a dedicated workstation that does not have Internet or open e-mail access.

5 SEGMENT AND SEPARATE INFORMATION

Back up your data on a separate dedicated machine; you can't be held ransom for data you have stored elsewhere. Have a plan for restoring your data should a compromise occur and be sure to test recovery regularly.

6 PROVIDE TAILORED AWARENESS AND TRAINING

Although system safeguards are expected to curtail suspected malicious activity, the human element will continue to provide an element of exposure. Initiate regular awareness activities on current user-related vulnerabilities and educate on proper user behaviours.

10 IMPLEMENT APPLICATION WHITELISTING

Application whitelisting is an essential and extremely effective security discipline. Whitelisting reduces risk by blocking unauthorized software, including malware, from being installed and executed.

BEST PRACTICE:

If you receive a suspicious e-mail (at work or at home) do not open the e-mail, do not click on any links or open attachments, promptly delete the email and contact your department's IT support team.

GOVERNMENT OF CANADA CYBER SECURITY EVENT MANAGEMENT PLAN

WHAT IS THE GC CSEMP?

The Government of Canada Cyber Security Event Management Plan (GC CSEMP), issued by the Treasury Board of Canada Secretariat (TBS), took effect on August 4, 2015, replacing the May 10, 2012, GC Information Technology Incident Management Plan (GC IT IMP). The GC CSEMP outlines the stakeholders and actions required to ensure that cyber security is addressed in a consistent, coordinated and timely fashion GC-wide.

WHY IS THE GC CSEMP IMPORTANT?

The GC CSEMP is important because it provides GC departments with the following support for their information systems classified up to the SECRET level:

- An operational framework for managing cyber security events that impact, or threaten to impact, the GC's ability to deliver programs and services to Canadians.
- Context for the plans and procedures departments and agencies develop to manage cyber security events related to the programs and services for which they are responsible.
- Direction for handling incidents such as system failure and loss of service, denial of service, errors for incomplete or inaccurate business data, breaches of confidentiality and unauthorized changes.

GOVERNMENT OF CANADA CYBER SECURITY EVENT MANAGEMENT PLAN

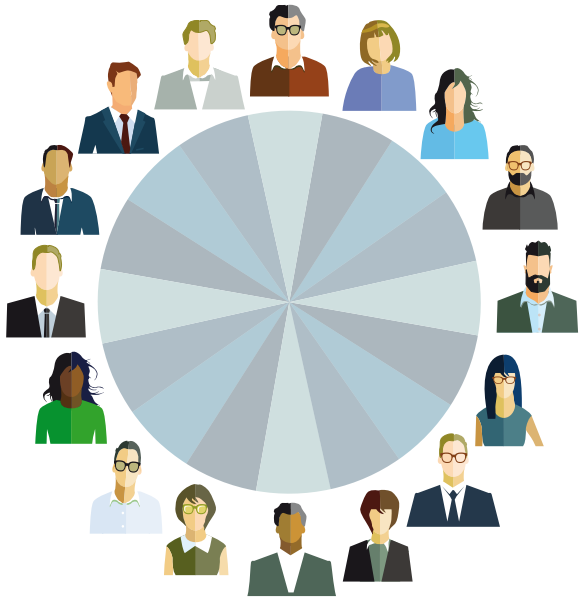
WHY SHOULD DEPARTMENTS CARE ABOUT THE GC CSEMP?

1. The GC is increasingly dependent upon IT to deliver services to Canadians and to maintain operations. Any compromise to their IT systems can hinder the delivery of these services.
2. Departments need to be prepared to react quickly and effectively to any event that may adversely affect services to Canadians, government operations or confidence in government.
3. Cyber security events related to GC information systems can have a significant impact on the delivery of government programs and services.

WHO ARE THE GC CSEMP STAKEHOLDERS?

There are a number of stakeholders implicated in the GC CSEMP. These stakeholders are categorized as follows:

- **Primary Lead Security Agency (LSA) Stakeholders** - TBS, Shared Services Canada (SSC), CSE and Public Safety (PS);
- **Specialized LSA Stakeholders** - Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS), and the Department of National Defence (DND);
- **Other stakeholders** - GC Chief Information Officer (CIO), Government Operations Centre (GOC), Privy Council Office (PCO), Canadian Committee on National Security Systems (CCNSS) and the DG Event Response Committee (GC ERC).



Each of the stakeholder's involvement is dependent upon the type of security event. The GC CSEMP provides a description of the triggers for escalation that invoke the appropriate stakeholders at the appropriate time. Escalation from one response level to the next is determined jointly by the stakeholders involved, using injury to the GC as a trigger.

Read the complete version of the GC CSEMP on the TBS Web site.

TBS "ENGARDE" CYBER EXERCISE

Contributed by Treasury Board of Canada Secretariat

In 2016, the TBS Chief Information Officer Branch (CIOB) conducted an Associate Deputy Ministers' cyber security exercise titled Engarde 2016 Cyber Leadership. The exercise was designed to support the new Government of Canada Cyber Security Event Management Plan (GC CSEMP), familiarizing senior-level stakeholders with aspects of the plan such as new processes, governance and upda ted roles and responsibilities. The exercise also introduced participants to TBS' Cyber Security Communications Framework and the associated communication protocols to be activated during a cyber incident.

SCENARIO

The simulation scenario consisted of six phases designed around the premise of a ransomware threat targeting the GC.

TECHNICAL BACKGROUND
Level 3 incident with multiple departments affected by ransomware

BUSINESS IMPACT
CBSA's business operations impacted by ransomware

COMMUNICATIONS
TBS/SCMA delivered communications overview

ATTRIBUTION
RCMP, CSIS, CSE, DND, CRTC, CCIRC, GOC off-ramps, source of malware revealed

PAYOUT
Discussions around the implication of a department paying out ransomware in the absence of policy

CLOSEOUT
Technical and communications closure of the incident

PARTICIPANTS

Incumbent executives from federal departments and agencies with GC incident management, response and support responsibilities and/or capabilities for cyber incidents, participated in the Engarde exercise. Participants arrived at the exercise with varying levels of information.

PRIMARY CSEMP PARTNERS	
TBS	Chief Information Officer Branch
SSC	Security Operations Centre (GC-CIRT, FIPC, ITSIRT)
CSE	Cyber Threat Evaluation Centre
PUBLIC SAFETY	Canadian Cyber Incident Response Centre

ADDITIONAL CSEMP STAKEHOLDERS

COMMUNICATIONS STAKEHOLDERS	SPECIALIZED PARTNERS	STRATEGIC PARTNERS	DEPARTMENTAL PERSPECTIVE
TBS	DND	PCO/ S&I	CRA
SSC	RCMP	GOC	Elections Canada
CSE	CSIS		CBSA
Public Safety	CRTC (Enforcement)		CRTC
PCO			

TBS "ENGARDE" CYBER EXERCISE

Contributed by Treasury Board of Canada Secretariat

LOGISTICS

Engarde was successful in moving away from the traditional paper exercise. This was a hands-on simulation of a real-life scenario. A live video feed enabled support personnel to follow the action in the main room and allowed them to constantly provide detailed information to participants. Scenario injects were delivered through text, audio and video, which further increased the level of urgency.

OUTCOME

The exercise focused on the following key areas:

- GC CSEMP processes
- Mitigation roles and strategies
- Internal/external communications
- Decision-making balancing continuity of business vs security
- Operational interpretation of policy

During the exercise, there were three common observations among participants.

1. Many noted that they rarely face cyber security incidents in their current roles and that they would benefit from additional simulation exercises.
2. At several points during the exercise, roles of decision-making and authority were unclear to participants since they were not explicitly defined in the plan.
3. Lastly, it was observed that information which would trigger parallel processes (investigations, national security responses, etc.) was not consistently shared to the appropriate stakeholders in a timely fashion.

CONCLUSION

The Engarde scenarios generated discussions and decisions, snippets of information and side discussions which achieve the desired outcome of familiarizing senior-level stakeholders with the new plan, processes, governance and updated roles and responsibilities.

A post-exercise report was produced which included recommendations for improving GC response processes. Some of these recommendations included developing and communicating an operational governance structure, more frequent education and training, clearly defined authoritative roles, and external communications being formalized and communicated to appropriate stakeholders.

The complete report is available upon request by contacting tbs.csemp-pgec.sct@tbs-sct.gc.ca.

HOW ARE YOUR CYBER HYGIENE HABITS?

CSE has developed a Cyber Hygiene fact sheet that gives tips and tricks to help keep you cyber secure. Over the next few editions, we will be taking a closer look at each topic. Take a look and see how your cyber hygiene habits measure up!

MOBILE SECURITY

Mobile devices are attractive targets that provide unique opportunities for threat actors intent on gathering information. A compromised device has the potential to allow unauthorized access to your network, placing not only your own information at risk, but also that of your organization.

It is important to remember that Canada is an attractive target for cyber-threat actors.

- Use a PIN or password to access the device and change these passwords regularly
- Disable features not in use such as GPS, Bluetooth, or Wi-Fi
- Avoid opening files, clicking links, or calling numbers contained in unsolicited text messages or e-mails
- Maintain up-to-date software, including operating systems and applications
- Do not use "Remember Me" features on websites and mobile applications — always type in your ID and password
- Encrypt personal or sensitive data and messages
- Understand the risks, keep track of your devices, and maintain situational awareness
- Review and understand the privacy and access requirements of all apps before installing them on mobile devices
- Delete all information stored on a device prior to discarding it
- Do important tasks, like online banking on a private or known, trusted secure network

QUICK REFERENCE GUIDE (IN CANADA)

Understand the security measures that exist on your devices.

- **VOICE COMMUNICATION:**
  Acceptable for non-sensitive information only
- **TEXTS AND MESSAGING APPS:**
  NOT acceptable for any sensitive communications
- **E-MAIL:**
  Consult your IT support team before using your email for sensitive communications

BE CLEAN, PRACTICE GOOD MOBILE HYGIENE!

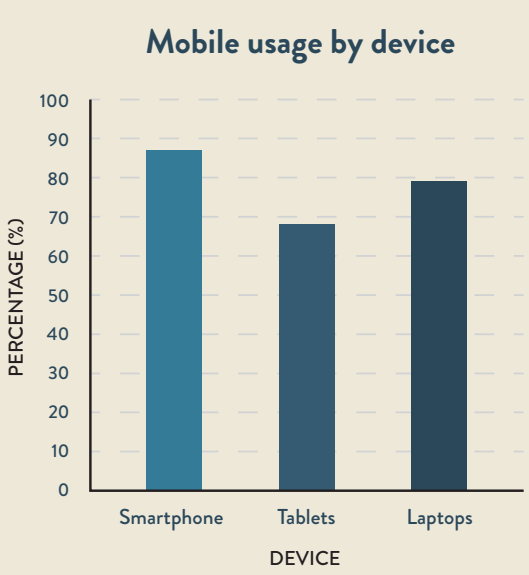
Mobile devices host important business and personal information that is sought after by cyber threat actors. You don't need to completely unplug your mobile device in order to be mobile secure. A few simple actions can help reduce your mobile threat surface and keep you protected against cyber threats.

MOBILE SECURITY

Mobile devices are attractive targets that provide unique opportunities for threat actors intent on gathering information. A compromised device has the potential to allow unauthorized access to your network, placing not only your own information at risk, but also that of your organization.

It is important to remember that Canada is an attractive target for cyber-threat actors.

- Use a PIN or password to access the device and change these passwords regularly
- Disable features not in use such as GPS, Bluetooth, or Wi-Fi
- Avoid opening files, clicking links, or calling numbers contained in unsolicited text messages or e-mails
- Maintain up-to-date software, including operating systems and applications
- Do not use "Remember Me" features on websites and mobile applications — always type in your ID and password
- Encrypt personal or sensitive data and messages
- Understand the risks, keep track of your devices, and maintain situational awareness
- Review and understand the privacy and access requirements of all apps before installing them on mobile devices
- Delete all information stored on a device prior to discarding it
- Do important tasks, like online banking on a private or known, trusted secure network



GC OFFICIAL COMMUNICATIONS

Do you know what type of information you can communicate? Are you sure of where and how you can send it? Here are some reminders:

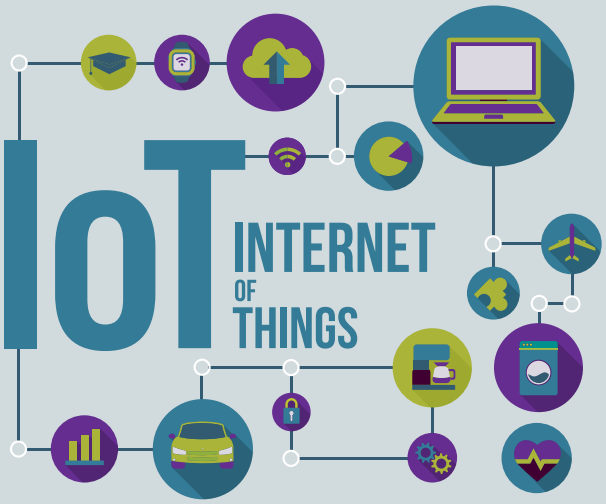
QUICK REFERENCE GUIDE (IN CANADA)

Understand the security measures that exist on your devices.

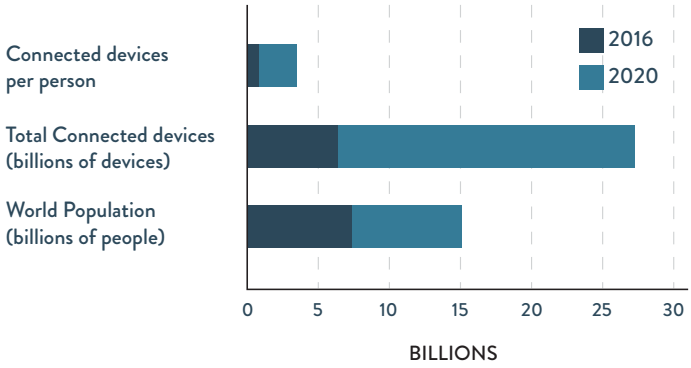
- **VOICE COMMUNICATION:**
  Acceptable for non-sensitive information only
- **TEXTS AND MESSAGING APPS:**
  NOT acceptable for any sensitive communications
- **E-MAIL:**
  Consult your IT support team before using your email for sensitive communications

CSE provides best-practices and guidance for all Government of Canada departments and agencies on various aspects of wireless and mobility network security. Take a look at our updated publications for more information on how to secure your wireless networks and mobile devices.

INTERNET OF THINGS – THE FUTURE IS NOW



The Internet of Things (IoT) is a popular term used to describe everyday electronic products that are able to communicate with other connected devices and networks, such as the Internet. IoT devices include anything from fitness trackers, TVs, lightbulbs, or even your coffee maker. While IoT devices can be economical and convenient, using them can have a significant impact on security and privacy.



HOW WILL IoT IMPACT YOUR NETWORK'S SECURITY?

There is currently no standard for communication between IoT devices, which increases the complexity of managing network security. Most IoT devices use proprietary software with weak encryption schemes and limited endpoint security to protect your information.

HOW DO THREAT ACTORS TARGET IoT VULNERABILITIES?

In many cases, IoT devices lack the technical ability to apply security patches when vulnerabilities are discovered. As a result, vulnerable IoT devices can be used to carry out malicious activities such as launching Distributed Denial of Service (DDOS) attacks, manipulating smart building controls or even turning off automobile safety features.

HOW CAN YOU MINIMIZE IoT SECURITY AND PRIVACY CONCERNS?

As an emerging technology, mitigations are not always available. Organizations must learn how to manage these new end-points within their networks by introducing appropriate governance, policies and security controls into their departmental security plans. Data generated by IoT devices can reveal private information about your daily activities. Conventional methods of protecting private information continue to evolve as federal authorities work to anticipate the possible privacy impacts of IoT.

While IoT may provide many benefits, departments will have to effectively manage the additional IT security and privacy risks by following the principles in CSE's ITSG-33 and Top 10 IT Security Actions.

CSE IS HIRING. APPLY NOW.

Cyber threats — including foreign states, hacktivists, criminals, enthusiasts, and terrorists — continually probe government systems, looking for vulnerabilities in order to gain access to a computer. CSE works to detect those attempts, block them and repair any damage. We make sure the government's networks are among the most secure in the world.

It is CSE's responsibility to safeguard Canada through information superiority. We have a purpose built facility in Ottawa and some of the most powerful computing technology in the country to do so. But the threat environment is constantly evolving.

To continue protecting Canada and Canadians, we need your help. The strength of our organization is built on a diverse mix of staff with talent, adaptability, imagination, and above all, a sense of duty to our country. It's why we actively seek the brightest minds in Canada.

WE STRONGLY ENCOURAGE APPLICANTS FROM ACROSS THE COUNTRY TO APPLY NOW.

Current opportunities:

C/C++ Software Developers

Enterprise Systems Administrator

Cryptanalyst / Cryptoscientist

Cybersecurity Analyst

Data Miner

Full-Stack Developer (Java/Python/JavaScript)

High Performance Computing (HPC) Researcher

Network Analyst

System Administrator

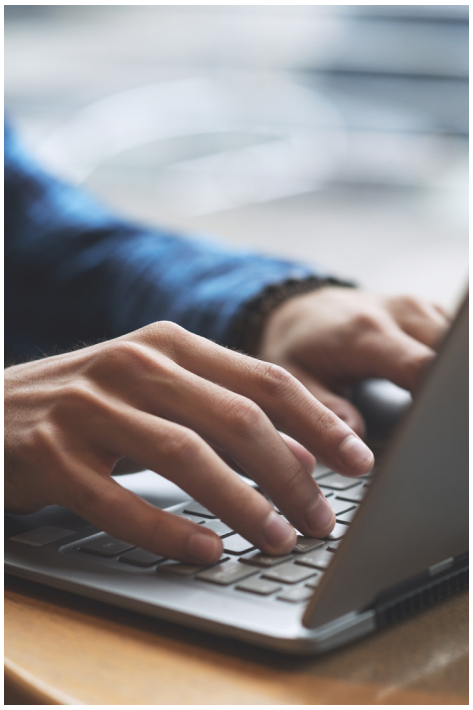
Telecom Technologist & Network Analyst

Vulnerability Research Engineers / Telecom Engineers

ITSLC NEWS

In January 2017, the IT Security Tripartite Steering Commitee endorsed the formation of a Cyber Security Training and Education Working Group. Lead security agencies with assigned cyber security responsibilities within the GC will provide the core membership. This includes TBS, CSE, SSC, Public Safety, RCMP, DND and other participants as required. The primary focus of the working group will be to identify a set of common standards and source out effective technical learning solutions for job-based required knowledge and skills in areas such as incident handling, malware analysis, digital forensics, vulnerability assessment and penetration testing.

NEW ITSLC COURSES



The ITS Learning Centre is constantly developing relevant content to ensure the skills of GC IT security practitioners are up-to-date.

200	T3MD Audit Trail Workshop: The Insider Threat
215	Emission Security (EMSEC)
229	COMSEC Account Management Course for Private Sector Companies
233	Cryptographic Key Management & Ordering Course
385	Cross Domain Solutions: A Primer
910	ITS Bootcamp
108	How to use HTRA Methodology within the ITSG-33 ISSIP

For additional information or to register for a course, log into your ITSLC Learning Account or visit the ITSLC web site.

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

General Inquiries: (613) 991-7110