Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CYBER JOURNAL

EDITION 4 – FALL 2013

IN THIS EDITION

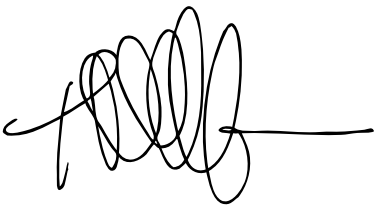
BUILDING A STRONG FOUNDATION FOR THE GC

The Government Technology Exhibition and Conference (GTEC) is around the corner, and the theme is "open and agile government". Agility is an important trait when responding to the ever evolving cyber threat. GTEC offers a unique platform for government departments and agencies to share and collaborate on the latest technology adoptions and implementations.

The GTEC Tradeshow Exhibition runs October 8-9th at the Ottawa Convention Centre. Visit CSEC's exhibit to explore interactive materials on international travel, mobile security and cyber threats, and to learn about essential mitigation measures that will help strengthen your department's security posture. You can also register for the GTEC speaking sessions, where CSEC Chief John Forster and Director General of Cyber Defence Scott Jones will be presenting on cyber security topics. For more details, visit: www.cse-cst.gc.ca/gtec/index-eng.html.

In this edition of the Cyber Journal, we have highlighted topics which align with the theme of GTEC, such as social media and mobile device risks, as well as guidance concerning mitigation measures.

Building strong security foundations and continually improving upon them to meet current security needs provides protection from cyber intrusions and enables GC departments to effectively fulfill their mandates.



Toni Moffa
Deputy Chief, IT Security

www.cse-cst.gc.ca

Canada

GTEC SPEAKING SESSIONS

John Forster, Chief of CSEC
Cyber Security and the GC
9:30am, October 9th

Each day, the GC is subject to cyber intrusion attempts, from any number of vectors. Whether a cyber-breach is intentional or accidental, malicious or misinformed, cyber security affects us all. As government organizations, we need to preserve the trust and confidence in our IT systems. This presentation addresses the current cyber picture facing the GC and how CSEC helps safeguard the GC's vital communications networks and systems. Given the persistent nature of certain threats, departmental and private sector collaboration is imperative in this realm. CSEC will address topics that departments need to consider and highlight measures that organizations should implement to bolster their security posture.

Cyber Security Collaboration Across Municipal Provincial and Federal Government
11:00am, October 9th

As cyber criminals use crowd-sourcing to collaborate in their targeted attacks on governments and enterprises, opportunities exist for greater collaboration on cyber security between all levels of government and with the private sector. Join this interactive discussion between Kent Schramm, Head of Corporate Security for the Ministry of Government Services for the Province of Ontario, Scott Jones, Director General, Cyber Defence, of the Communications Security Establishment Canada, Eric Pulnicki, Manager of IT Systems Operations for the City of Brampton and Trend Micro's VP of Cyber Security, Tom Kellermann. This panel session will illustrate the threats and targeted attacks facing our government and critical infrastructure, and will discuss activities underway for improving our national, provincial and municipal security postures within government departments that are striving to be more open, collaborative and mobile.

Scott Jones, Director General of Cyber Defence, CSEC
Cyber Intrusion Instant Replay
2:00pm, October 9th

This presentation provides an update on new and emerging cyber threats, and challenges facing the GC. Watch as the clock counts down and follow CSEC through an intrusion "in progress" to understand what happens at each phase. Learn what vital actions could have prevented the spread of the intrusion.

For more information on speaking session schedules refer to the GTEC Conference Program.

CSEC "ASK AN EXPERT AT OUR BOOTH!" SESSIONS

TUESDAY, OCTOBER 8TH

Ask a Risk Management Expert: 9:30 am to 12:30 pm

Ask a Cyber Expert: 9:30 am to 4:30 pm

WEDNESDAY, OCTOBER 9TH

Ask a Mobility Expert: 9:30 am to 12:30 pm

Ask a Cyber Expert: 9:30 am to 4:30 pm

HOW YOU USE SOCIAL MEDIA MATTERS!

MEET PETER!

Peter is a government employee who frequently uses social media to stay in touch with family, friends and colleagues. Peter uses Facebook, Twitter, and LinkedIn to keep in touch with his family and friends.

By using popular social media sites, Peter reveals significant personal information online. This makes it possible for cyber threat actors to craft a spear phishing e-mail containing malicious software disguised as an ordinary attachment, which can compromise his account and send malicious messages to his colleagues.

In order to avoid revealing to much information online, government employees must always exercise caution when posting personal or business information. To determine if you are revealing too much information online, ask yourself if you have posted:

1. Your department, job title or resume;
2. Your location or upcoming travel plans;
3. Job specific or internal GC information (conference plans, etc.); or
4. Your business address, personal address or phone numbers.

Visit us at GTEC on October 8th and 9th and have a look at Peter's Facebook page, Twitter feed and LinkedIn profile and see if you can spot personal information that could be used to craft a malicious e-mail and compromise a government network.

To learn more about the steps departments and employees should take when using social media, download: ITSB-66: Security Risks of Using Social Media

THE GC CONTEXT

Social media websites are a way for people to connect and share information with each other, using blogs, wikis, and forums such as Facebook, Twitter, LinkedIn, Google+ and Wikipedia. However, these websites can pose a threat to the Government of Canada (GC), as departments and their networks are frequently targeted by a variety of threat actors looking to gather information on GC employees, projects, and systems.

The primary security risk in using social media for official business is the possibility of employees divulging too much information or information that has not been approved for release to the public. The following risks are also present:

- Spread of viruses;
- Compromise of official accounts;
- Malicious third-party applications; and
- Identity theft.

Before social media is used for official business, each department should conduct a risk assessment to determine which social media sites should be used, and what limitations on access and usage are warranted. The following security measures should also be implemented:

- Develop a social media policy;
- Implement role specific access controls;
- Limit third-party applications;
- Ensure security settings are applied;
- Monitor official accounts for suspicious activity;
- Report any incidents to your IT department immediately; and
- Ensure employees are aware of the general security implications.

Before launching a social media presence, also consult the Treasury Board guidance.

SUCCESS OF YOUR DEPARTMENTAL MISSION: RISK MANAGEMENT

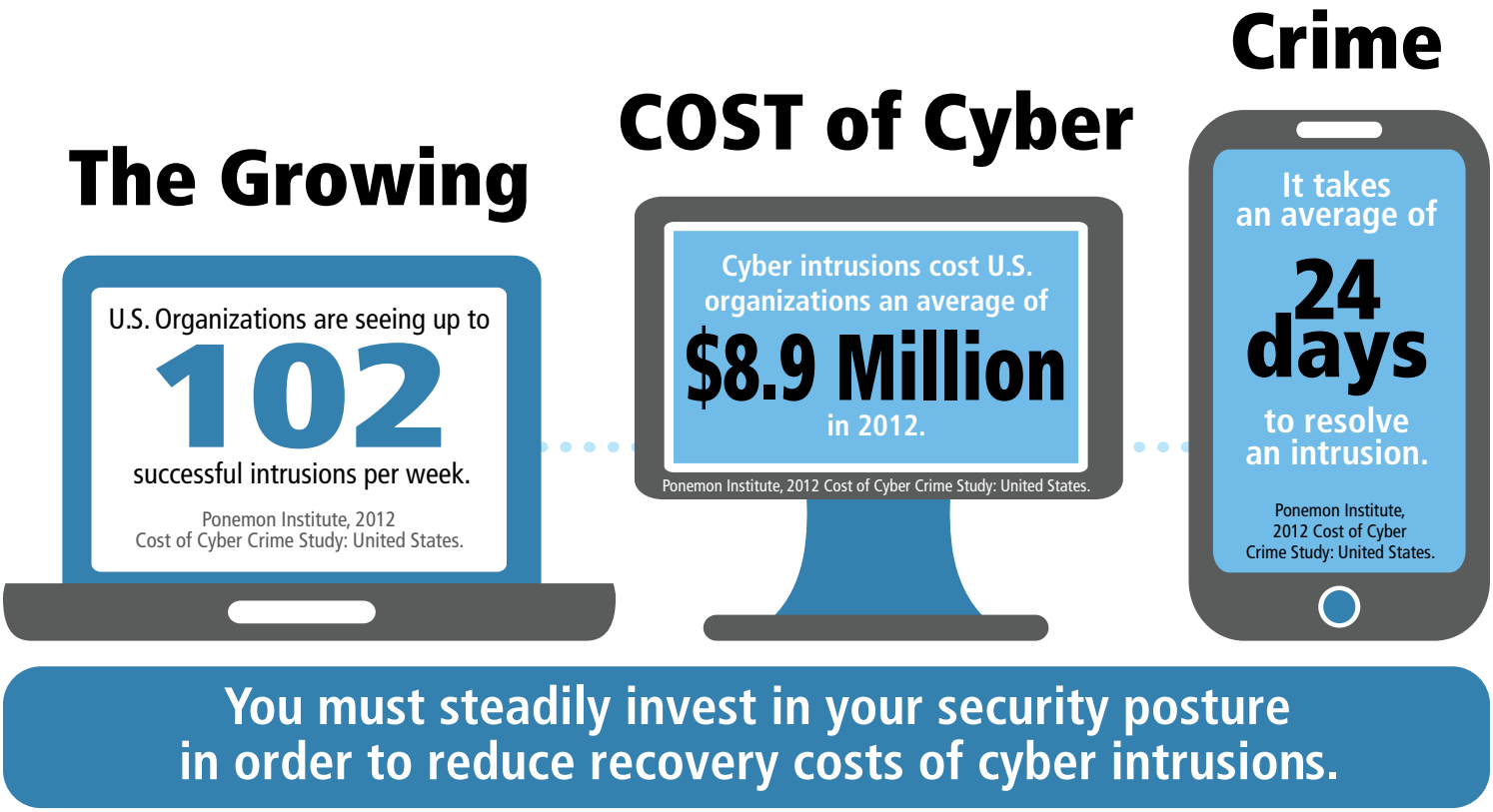
Each department's or agency's mission contributes in some way to improving the health, safety, security, and prosperity of Canadians. Sound management practices form an essential enabler of mission success. Through sound management practices, departments perform their programs and service operations more efficiently and effectively, advance their strategic outcomes, and deliver better results to Canadians.

In August 2010, Treasury Board of Canada Secretariat (TBS) promulgated a **Framework for the Management of Risk for the GC**. This framework recognized that failure to effectively manage risks can result in increased program costs and missed opportunities, which can compromise program outcomes, and ultimately public trust.

The **Management Accountability Framework** (MAF), supported by the **Policy on Government Security** (PGS) and its related directives and standards, outlines Deputy Heads' responsibilities regarding the management of IT security risks. Key responsibilities relate to the elaboration of strategies, goals, objectives, priorities, and timelines for improving departmental security and supporting its implementation; ensuring that managers at all levels integrate security and identity management requirements into plans, programs, activities, and services; and ensuring that periodic reviews are conducted to assess whether the departmental security program is effective.

Sound IT security risk management is an enabler of departmental mission success and can no longer be an afterthought, but rather needs to be a vital component in both departmental and IT project plans. By adequately managing IT security activities, departments and agencies ensure the trustworthy delivery of their programs and services in a way that complies with applicable laws and regulations.

To learn more visit booth 601 at the GTEC Tradeshow on October 8th or 9th.



You must steadily invest in your security posture in order to reduce recovery costs of cyber intrusions.

ANATOMY OF A CYBER INTRUSION

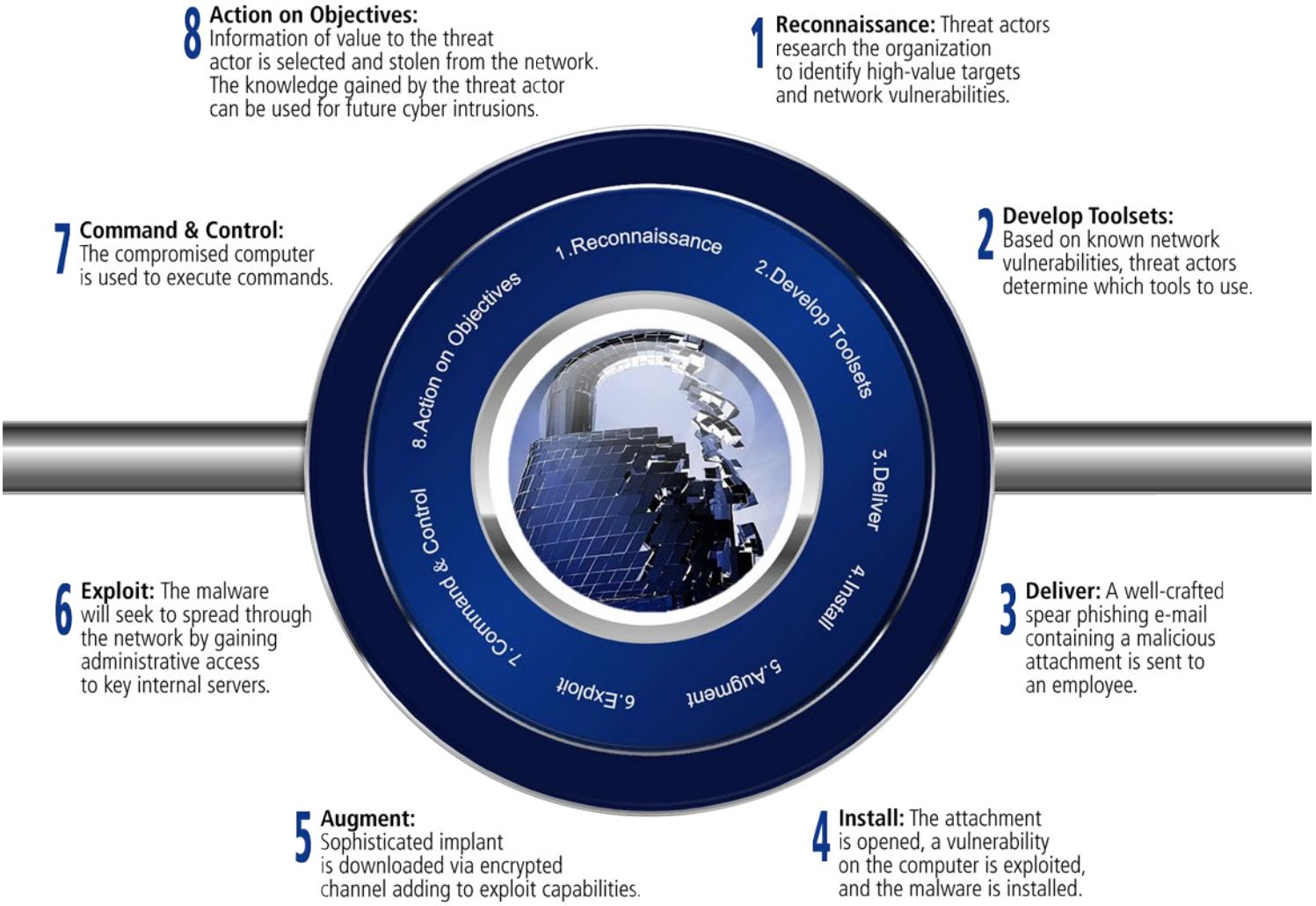
Cyber threat actors are resourceful and seek opportunities to gather information on an organization prior to executing a cyber-intrusion attempt. Threat actors are also sophisticated, motivated, and persistent. They have a wide range of tools at their disposal which can be used to gain access to a network once a target, such as a business or government agency, has been identified.

Cyber threat actors aim to achieve a persistent presence on a network, often with the goal of stealing information. A well-crafted spear phishing e-mail sent to a high-value target is often all that is needed to gain access.

High-value targets might include:

- Senior executives and their assistants;
- Help desk staff, and/or system administrators;
- Users who have access to sensitive information;
- Users with remote access; and
- Users whose role involves interacting with members of the public.

Intrusions can happen quickly, and covertly; therefore, it is important that all GC employees understand the basics of how a cyber-intrusion might occur so that GC networks can be better protected. The diagram below shows the basics steps a threat actor might take in cyber-intrusion attempt.



DID YOU KNOW?

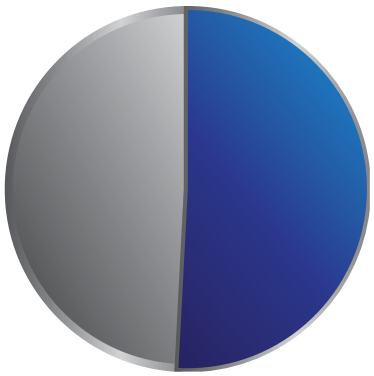
What Mobile Malware Does with your Phone

- Steals and sends content
- Collects sensitive data
- Tracks your location
- Changes settings
- Slows down processing speed
- Initiates system-wide crashes

What Information Can Go Missing From Phones?

- Departmental information
- Calendars
- Personal contacts
- Sensitive business information
- List of passwords
- Electronic documents

34% of employees store work e-mail passwords on their phones



51% of organizations have experienced data loss due to unsecured devices.

Motorola Mobility Survey, November 2011
Confident Technologies, "Mobile (In)Security: A Survey of Security Habits on Smart Phones and Tablets", September 2011.

SECURING BLACKBERRY DEVICES

There are many security risks related to the use of mobile electronic devices for information handling. When agencies are mitigating those risks, special consideration must be given to network architecture choices and security procedures, as well as security controls applied to mobile electronic devices. Mobile Device Management systems such as the BlackBerry® Enterprise Server (BES) play a key role in the hardening of the network security posture.

The BES has been widely deployed across the GC IT infrastructure as an effective component for managing mobile device security. It is capable of controlling many IT policy security settings to improve the security posture of mobile devices and the supporting networks on which they operate.

The BES offers approximately 500 policy rules that can be used to manage BlackBerry® hand-held devices and meet organizational security policy requirements. CSEC will soon be releasing ITSG-57: Configuring Smart Devices Using BlackBerry Mobile Device Management Solutions to provide advice on the most critical of the "IT Policy Rules" and "Application Control Policy Rules" for the Protected B environment. Blackberry also offers a "BES - Planning Guide" as well as a "BES for Microsoft Exchange – Installation and Configuration Guide".

SECURITY RISKS OF USING WI-FI WHILE TRAVELLING

From airports to hotels to coffee shops, free Wi-Fi is being offered by an increasing number of businesses each year. While many of these Wi-Fi "hotspots" have tried to secure their networks by using passwords or SSL encryption (i.e. https), some do not. Connecting to an untrusted network can expose your personal and business data to cyber criminals.

One of the most common ways for a criminal to get your information is to set up a fake, yet legitimate looking Wi-Fi "hotspot" near you. Once you connect to that network, sensitive personal and business information stored on your device can be downloaded. To make matters worse, your device can become infected by viruses, worms or other malware that allow criminals to perpetuate their activities more broadly.

FACT: 77 % of those who use free Wi-Fi have experienced cyber crime, versus 62% of those who do not use free Wi-Fi.

The Norton Cyber Crime Report, 2013.

Here are a few steps that you can use to protect yourself:

1. Only connect to trusted, legitimate 'hotspots' which use some form of encryption or password protection;
2. Remove sensitive data from your device;
3. Save important tasks like online banking for secure networks; and
4. Set your network location to "Public".

Ask your IT Department to help you:

1. Implement a firewall;
2. Patch your operating system; and
3. Implement a VPN (virtual private network).

NEW IT SECURITY PUBLICATIONS!

ITSB-66: Security Risks of Using Social Media

ITSB-67: Cyber Security Considerations for Management

ITSB-68: End of Support for Microsoft Windows XP SP3

ITSB-89A-SC: CSEC Top 35 Mitigation Measures with Security Controls

PROVIDING COMSEC MATERIAL TO THE CANADIAN PRIVATE SECTOR

In order to support GC secure communications requirements, it is often necessary to share Accountable COMSEC Material (ACM) with private sector partners. In these instances, it is vital to the security of your project and in the best interests of project timelines to ensure that appropriate security requirements are identified early in the contracting process. Security officials in your department can ensure this is accomplished by working closely with CSEC and PWGSC.

Detailed information is provided in the new IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector (ITSD-06), which is available by contacting CSEC COMSEC Client Services at comsecclientservices@cse-cst.gc.ca.

TRAINING NEWS

Go Green Initiative

To help reduce CSEC's carbon footprint, the ITSLC is going GREEN. We are asking participants to leave the course materials for the next class and we will send the class material electronically upon completion of the course.

TACLANE Bridging Course

The ITSLC is offering a 1-day TACLANE Bridging course to help current TACLANE users meet the mandatory software upgrade dateline of December 31, 2013.

IT Security Risk Management: A Lifecycle Approach (#104)

Based on client feedback, the ITSLC reviewed the course description for the ITSG-33 (#104) course. An outline which better reflects its content and intended audience is now available online, and will soon appear in the catalogue.

DCA e-Learning Course (#232) – Launching Fall 2013!

The Departmental COMSEC Authority (DCA) course will soon be offered as an online course and will be available through MyAccount at the CSPS. This e-learning course will be free for the first three months after which it will cost $150 as indicated in our Course Calendar. Visit the Learning Centre's website for updates.

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 CSEC 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 CSEC 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 report a cyber-incident 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**