Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CYBERJOURNAL

EDITION 1 – FALL 2012

IN THIS EDITION

IT SECURITY: AN INDIVIDUAL AND COLLECTIVE RESPONSIBILITY

The Government of Canada (GC) is transforming its IT technologies while persistent and pervasive cyber threats also continue to evolve. The IT that we all rely on provides ample opportunity for threat actors to capitalize on the vulnerabilities and inter-connectivity inherent in our networks. In this environment, IT Security has become more critical and more complex than ever before.

On a daily basis, the cost of compromises occurring across the GC range from lost productivity and system down time, to more costly and strenuous recovery efforts. While there is no silver bullet, effective mitigation measures do exist to minimize their occurrence and impact.

Continuous security improvement begins with increased awareness. The objective of this newsletter is to enhance our collective understanding regarding IT security issues and what can be done to strengthen the integrity, resiliency and security of our individual networks which by extension then raises the security baseline within the collective GC enterprise.

I hope you find value in the first issue of this newsletter and in the issues to come.

Toni Moffa
Deputy Chief, IT Security

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

CYBERJOURNAL

EDITION 1 – FALL 2012

RISK MANAGEMENT – STRIKING THE RIGHT BALANCE

With today's dynamic threat environment, IT security can no longer be an afterthought. Departments rely heavily on information systems to support their business activities. These interconnected systems are often subject to serious threats that can have adverse effects on departmental business activities including the compromise of the confidentiality, integrity, or availability of information and IT systems. Security activities need to be a vital component in any IT project plan. With this in mind, **ITSG-33 - IT Security Risk Management: A Lifecycle Approach** has been developed to help Departments integrate security in a cost effective manner from the start.

In applying IT security risk management, Departments should aim at striking a proper balance between the cost of implementing security controls and the levels of acceptable residual risk.

Today, the current risk management process falls short of taking into account the business needs for the security of an organization.

An integrated risk management approach must address all the different types of risks that organizations face: policy risk; operational risk; financial risk; legal risk; and security risks to name a few.

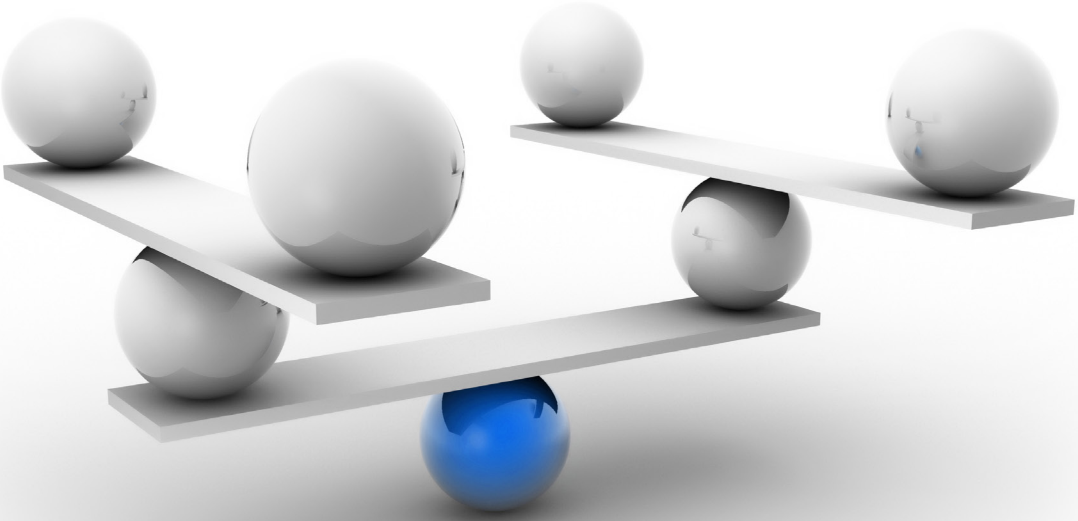
An Integrated Approach

ITSG-33 identifies the roles, responsibilities and activities that will help GC Departments manage IT security risks, drawing from the participation of CIOs, Departmental Security Officers, IT Security Coordinators, Project Owners, Project Managers and IT Security Practitioners. Benefits include:

- Ability to address all aspects of IT security in an efficient manner to satisfy department-wide business needs for security;
- Improved risk management decision making when Departments interconnect their information systems through the use of standardized security control requirements;
- Compliance with the overall risk management strategy and objectives established by the TBS; and
- A process for integrating security assessment and authorization with current departmental processes.

Managing IT security risks is a multifaceted undertaking that requires the involvement of an entire department, from the senior officials establishing organizational objectives to individuals developing and operating information systems.

To learn more, go to www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng to download ITSG-33.



This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

CYBER MITIGATION: TIMELY PATCHING OF OPERATING SYSTEMS AND APPLICATIONS

Threat actors have multiple attack methods in which to penetrate GC systems, one of which is through unpatched vulnerabilities of operating systems and applications. Today, the GC runs many unpatched applications and operating systems, providing even unsophisticated cyber threat actors with an opportunity to compromise systems.

In 2011, the vast majority of known GC cyber incidents could have been avoided with patching.

'Patching' is a method used to minimize the threat of compromise by applying software updates to fix system vulnerabilities and are released frequently. For example, Microsoft releases its application and operating system patches every second Tuesday of the month, which has been coined "Patch Tuesday." As a product supplier, Microsoft must disclose any fixes to its programs, which inadvertently notifies threat actors of the present day vulnerabilities. Given that many people do not install patches as soon as they are released, "Exploit Wednesday" allows a threat actor to analyse the patch and determine how to exploit weak points.

Once a vulnerability has been successfully patched the risk has been mitigated and it no longer poses a threat to the operating environment. With a patch management policy, patches are easy to apply and highly effective. Ask yourself these questions:

Does your department:

- have a configuration management process which includes patch management?
- maintain an inventory of operating systems, applications and equipment?
- have resources to track and monitor patch updates and releases?
- prioritize patches and updates?
- test prior to implementing updates?

Departments need to make patching operating systems and applications a priority. To learn more about other mitigation measures, go to www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb89-eng.html to download **ITSB-89 - CSEC Top 35 Mitigation Measures.**

NEWS FROM THE ITS LEARNING CENTRE

The ITSLC is adapting to better serve the learning needs of GC IT security practitioners. The ITSLC has embarked on a three year program to refresh our training and expand access to our programs and products to better meet IT security practitioners' learning needs including the introduction of e-learning for some of our courses. In addition, we are introducing the following new courses:

- **EMSEC Course** – The ITSLC is developing a Canadian version of the **TEMPEST** training that was delivered by our UK partners. The focus will be on Canadian content with references to GC directives and guidance and aimed at IT specialists and security practitioners. Learning objectives will include applying EMSEC concepts and principles, identifying EMSEC countermeasures, and liaising with national and international authorities in support of GC requirements.
- **Controlling Authority (CA) and Departmental COMSEC Authority (DCA) Courses** – The ITSLC is pleased to announce the offering of the **Controlling Authority** (CA) course beginning this fall. The course is being offered in two parts, an e-learning portion which gives the learner some background in the COMSEC environment and a workshop portion which is primarily focused on the **Key Material Support Plan** (KMSP). The **Departmental COMSEC Authority** (DCA) course, which is being developed in an e-learning format, will be offered in the late fall timeframe.

VISIT US ONLINE

For an updated look at our Programs of Study and other specialized courses or to register for any of our upcoming courses please visit our website at:

🌐 www.cse-cst.gc.ca/its-sti/training-formation/index-eng.html

✉ its-education@cse-cst.gc.ca

THE ART OF STRONG PASSWORDS

Passwords are a necessary tool in a security toolbox, both at work and at home. They authenticate your credentials and safeguard access to sensitive information, whether it is a database at work or online banking at home. Access control is everyone's business and password security is a topic that we should all pay attention to. Consider these points:

- **Strive for complexity.** Weak passwords are easy to crack, while strong passwords are more resilient to cracking techniques. Try using a memorable phrase to create a stronger password using a mix of characters. For example:

  Phrase: "My jersey number when I played sports was 27!"

  Password: Mj#wlpsw27!

- **Be Aware.** Shoulder surfing can happen anywhere, especially in public locations. Be wary of your surroundings and always shield your keyboard or keypad when entering your password.
- **Variety is Good.** Remember that using the same password for multiple accounts increases your risk if your password is revealed. Use different passwords for work and home accounts.
- **Protect Them.** Do not scribe your passwords under a keyboard, on sticky notes next to a computer or save them on the device itself. These are common places to look for passwords.
- **Act Quickly.** If at any time you suspect that your password may have been compromised, act quickly and change it. Changing a compromised password will halt unfettered access to your accounts.

SECURING WIRELESS LOCAL AREA NETWORKS

Wireless Local Area Networks (WLANs) are becoming increasingly common within the GC Departments as the need increases to integrate wireless devices into departmental networks. However, WLANs also present unique security challenges in part due to the fact that the physical boundaries of the network have been extended and the devices themselves are smaller and more mobile, thus making them more prone to loss and theft. In addition, industry trends indicate that organizations are seeing more Bring Your Own Device (BYOD) initiatives whereby employees opt to use their personal devices to connect into corporate networks, introducing an additional dimension of risk because these devices are now being used to process government and public sensitive information.

As a Government of Canada organization, how do I navigate these challenges?

1. **What are the risks?** If not properly deployed, WLAN solutions leave Departments vulnerable to a host of additional threats, including transmission interception, login credential theft, unauthorized access and theft of devices.
2. **Are you protected?** Consider how you plan to use your wireless network and ask yourself:
   - Have you fully planned for wireless (i.e.: have you conducted a TRA, is it all unclassified information, have you established an acceptable use policy, etc.)?
   - Have you implemented wireless securely (i.e.: have you used robust authentication and access controls, are you using WPA2 enterprise encryption, have you minimized administrative privileges, are you patching to maintain the integrity of your systems and applications, etc.)?
   - Do you have a wireless intrusion detection system (WIDS) in place (i.e.: are you logging and monitoring for unauthorized activities, do you have adequate personnel assigned to support intrusion detection efforts, are you able to detect and respond to the deployment of non-authorized access points within your facility, etc.)?
   - Have you invested in the cultivation of security awareness and wireless expertise within your department for both IT practitioners and employees?
3. **Are you considering risks beyond WiFi?** We encourage you to think past the WLAN scope and consider associated security challenges attributed to wireless devices such as Bluetooth, Cellular, Wireless keyboards and other desk space appliances.

WLAN deployments are complex and deploying them securely is challenging. CSEC has provided advice and guidance for certain wireless deployments within the GC. For general questions contact IT Security Client Services itsclientservices@cse-cst.gc.ca.

The IT Security Learning Centre
offers wireless training courses and demonstrations.
✉ its-education@cse-cst.gc.ca

IN CANADA, ALL COMSEC ROADS LEAD TO CSEC!

Canada's commitment to safeguard and control COMSEC Material for classified information is no secret! As the national authority for COMSEC material for Canada, CSEC is continually refining its rules and tools to support Government of Canada's users and Canada's international partners in this common endeavour.

Departmental Security Officers (DSO), Departmental COMSEC Authorities (DCA) and COMSEC Custodians can access essential information pertaining to the protection of their COMSEC Material through the following channels:

COMSEC Client Services

COMSEC Client Services is the service point for COMSEC support enquiries. Whether it is for the approval for use of cryptographic equipment or for advice and guidance on a specific product or on a special client requirement, COMSEC Client Services can be reached via email comsecclientservices@cse-cst.gc.ca or by phone (613) 991-8495 and is available to answer any question a user may have.

Crypto Material Assistance Centre (CMAC)

For existing Crypto Material users, CMAC is the front door for all Crypto Material management inquiries and problems. All questions regarding COMSEC Accounts and key orders can be directed via email to cmac-camc@cse-cst.gc.ca or via phone (613) 991-8600.

COMSEC User Portal (CUP)

The CUP (comsecportal.cse-cst.gc.ca) provides COMSEC-related UNCLASSIFIED and PROTECTED A information and Field Software Upgrades (FSUs) associated with high assurance products, systems and services. Updated regularly, this portal offers timely information to its registered users. COMSEC Custodians and DCAs can get registered by contacting COMSEC Client Services.

CSEC's Website

UNCLASSIFIED COMSEC directives, information and services are available at www.cse-cst.gc.ca/its-sti/publications/index-eng.html.

NEW!

ITSD-03: Directive for the Control of COMSEC Material in the Government of Canada
This must-have comprehensive reference material supersedes the COMSEC Material Control Manual (ITSG-10).

ITSD-04: Directive for the use of CSEC-Approved COMSEC Equipment and Key on a Telecommunications Network
All the information you need to ensure proper life-cycle management of the COMSEC Material supporting your secure network.

ITSD-05: Directive for Reporting and Evaluating COMSEC Incidents Involving Accountable COMSEC Material
The newest IT Security Directive, this document explains roles and responsibilities associated with handling a COMSEC incident.

BEFORE PACKING, THINK SECURITY!

Traveling to an international location and planning to bring your lifeline of mobile devices with you? You may be at increased risk of cyber security threats!

For more information, consult:

- ITSB-87: Mobile Technologies in International Travel – Guidance for Government of Canada Business Travelers
- ITSB-88: Mobile Technologies in International Travel – Guidance for Government of Canada IT Security Managers

PROCURING ASSURED PRODUCTS FOR PROTECTED B NETWORKS

You've captured your business and security requirements, designed your network with all the right security controls, and now you're ready to procure the components - but how do you know if a product will do what it says? Do you trust the vendor's claims that the product performs the security functionality as advertised?

When procuring products that need to ensure IT security functionality, make sure you ask for CC and CMVP assured products.

The Common Criteria (CC) and Cryptographic Module Validation Program (CMVP) offer you this assurance. These programs ensure the trustworthiness of products that provide IT security, by validating that they have been built to CSEC recognized standards. As a result of these programs, there is a comprehensive pool of products available for procurement, satisfying all types of IT security functionality for technology classes such as operating systems, server applications, network appliances, authentication tokens, and mobile communication devices.

The CC is a wide-ranging international program based on evaluations of IT products which are performed against Protection Profiles to fulfill the complete set of security requirements for technology classes. The specific cryptographic modules within the IT products are evaluated through the CMVP. More information on the Canadian CC program is available online: www.cse-cst.gc.ca/its-sti/services/cc/index-eng.html, and you can view a complete list of all CC certified products at: www.commoncriteriaportal.org/products/.

The CMVP is a joint effort between the National Institute of Standards and Technology (NIST) in the U.S. and your GC lead IT Security agency - CSEC. The CMVP ensures that cryptographic modules within IT products have been designed and built to the FIPS140-2 standard. You can view the list of over 1700 Validated Modules here: csrc.nist.gov/groups/STM/cmvp/validation.html and you can find out more about the CMVP here: www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-eng.html.

ABOUT THIS NEWSLETTER

Cyber Journal has been prepared for GC IT stakeholders and is published on a periodic basis. This publication reflects the CSEC IT Security business line's 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 of this initiative 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

- **Commercial Assurance Services** provides architecture and engineering support for the GC enterprise, including COTS product assurance and security guidance.

  ✉ **itsclientservices@cse-cst.gc.ca** ☎ **General Inquiries: (613) 991-7654**

- **Cyber Threat Evaluation Centre** provides front line cyber threat response services for the GC, deploys operational capabilities and produces situational awareness reports.

  ✉ **ctec@cse-cst.gc.ca**

- **COMSEC Client Services** provides general information on COMSEC policy and equipment, as well as client support for planning, procurement, integration and lifecycle maintenance of COMSEC equipment.

  ✉ **comsecclientservices@cse-cst.gc.ca** ☎ **General Inquiries: (613) 991-8495**

- **Crypto Material Assistance Centre (CMAC)** is the front door for COMSEC custodians for inquiries related to key orders and key or equipment problems.

  ✉ **cmac-camc@cse-cst.gc.ca** ☎ **General Inquiries: (613) 991-8600**

- **IT Security Learning Centre** provides education and training services for the Government of Canada. ✉ **its-education@cse-cst.gc.ca**

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.