Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

MANAGEMENT SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

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

ITSM.10.189
October 2017

Canada

INTRODUCTION

The *Top 10 Information Technology (IT) Security Actions to Protect Internet-Connected Networks and Information* (ITSM.10.189) is based on the Communication Security Establishment's (CSE) analysis of cyber threat activity trends and their impact on Internet-connected networks. Organizations that implement these recommendations will address many vulnerabilities and counter the majority of current cyber threats.

POLICY SUGGESTIONS

The Government of Canada (GC) has several policies that address cyber security practices requirements. These policies identified below, may be used as reference materials when organizations are creating their own policies and building the foundation of their cyber security practices and programs.

- *Policy on Management of Information Technology* [1][1]
- *Policy on Government Security* (PGS) [2]
- *Operational Security Standard: Management of Information Technology Security* (MITS) [3]

APPLICABLE ENVIRONMENTS

The information in ITSM.10.189 provides best practices and guidance for all IT solutions. However, an organization may want to increase security by applying additional measures to protect their most sensitive business information. It is important that organizations understand their organizational environment in order to protect their information assets.

[1] Numbers in square brackets indicate reference material. A list of references is located in the Supporting Content section.

THE TOP 10

Table 1 The Top 10 IT Security Actions To Protect Internet-Connected Networks

Rank	Action	Description of Implementation
1	Consolidate, monitor and defend Internet gateways	Organizations should monitor the traffic at their Internet gateways. To simplify this task, the number of external connections to an organization's network should be reduced. Normal traffic patterns must first be understood in order to detect and react to traffic pattern changes. The organization will benefit from the protection provided by cyber defences that monitor for, and can respond to, unauthorized entry, data exfiltration, or other malicious activity. In response to malicious activity, cyber defences should be able to shut down access points to stop data exfiltration or block unwanted attacks.
2	Patch operating systems (OS) and applications	Organizations should implement a timely patch maintenance policy for OS and third-party applications to reduce the organization's exposure to threats that could exploit publically known vulnerabilities. Organizations should use supported, up-to-date, and tested versions of OS and applications. The deployment of unsupported OS or applications, in which updates are no longer available, will result in a higher risk of exposure to exploitation because there is no mechanism available to mitigate vulnerabilities. Patches must be applied in a timely manner, ideally via an automatic patch management system. It is also important to have a mechanism to identify the patches that have been applied to ensure timely response to threats and to understand the risk of potential exposure. CSE's *ITSB-96 Security Vulnerabilities and Patches Explained* [4] further explains the importance of patching.
3	Enforce the management of administrative privileges	Organizations should minimize the number of users with administrative privileges. The list of administrative users should be validated frequently. The creation of different levels of administrative accounts is a best practice to ensure that, if an administrative account is compromised, the level of exposure is limited. Organizations should either implement a password change process, according to an established schedule, for administrative account passwords or implement an administrative password solution to protect passwords. Where applicable, two-factor authentication (2FA) for accessing sensitive applications or remote networks should be implemented to improve the assurance of user credentials. To prevent exposure from phishing attacks or malware, administrators should perform administrative functions on dedicated workstations that do not have Internet or open e-mail access, or that have Internet and e-mail disabled from administrative accounts. Administrative accounts should be separate from standard organizational accounts; administrators should be aware of which account they are using. A compromised standard account is easier to recover than a compromised administrative account.
4	Harden operating systems (OS) and applications	To prevent compromise of Internet-connected assets and infrastructures, organizations should disable all non-essential ports and services, and remove unnecessary accounts. Both an enterprise-level auditing and an anti-virus solution are key elements of any secure configuration. Further security controls should be applied to when hardening an OS; organizations can consult CSE's *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [5] for more information on selecting and applying security controls. Third-party applications should be assessed for components or functions that are not required, and should be disabled or require human intervention before they are enabled (i.e. macros).

5	Segment and separate information	All organizations should have an inventory of their essential business information. These information stores should be categorized, considering any protection requirements based on the sensitivity or privacy impact of information. Networks should be zoned by segmenting and grouping infrastructure services that have the same information protection requirements or that must adhere to the same communication security policies. This logical design approach is used to control and restrict access and data communication flows. Further, organizations should monitor and enforce controls to maintain zone protection and integrity. For additional guidance, consult CSE's *ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada* [6] and *ITSG-38 Network Security Zoning – Design Considerations for Placement of Services within Zones* [7].
6	Provide tailored awareness and training	Organizations should initiate regular awareness activities to address current user-related vulnerabilities and proper user behaviours. IT security awareness programs and activities should be frequently reviewed, maintained, and made accessible to all users who have access to organizational systems. Although system safeguards are expected to curtail suspected malicious activity on networks, the human element will continue to provide a risk of exposure. Current examples of spear phishing or improper handling of removable media demonstrate the continued need to focus awareness in this area. In addition, regular reports to management on attempted or actual compromises will help to reinforce the behavioural changes required. Management involvement in information protection decisions is essential when choosing appropriate security controls. CSE has a number of publications that can be used to increase employee awareness levels of cyber threats and mitigations. Visit CSE's Web site to read these publications.
7	Protect information at the enterprise level	Organizations may allow users to leverage their own personal devices to conduct business. If it makes business sense, organizations should provide equipment (e.g. servers, desktops, laptops, mobile devices) to employees, leveraging a device management framework and providing control using a configuration change management process. If a bring-your-own-device (BYOD) scheme is being considered, a strict control policy should be implemented. Organizations should investigate technologies and legal requirements to enable BYOD environments in which business information and transactions are segregated and protected from personal use. One such technology is a mobile device management (MDM) system, which protects mobile devices and the network to which they connect.
8	Apply protection at the host-level	Organizations should deploy a host-based intrusion prevention system (HIPS) to protect their systems against both known and unknown malicious attacks such as viruses and malware. HIPS take active measures to protect computer systems against intrusion attempts by using pre-defined sets of rules to recognize suspicious behavior. When this behaviour is identified, the HIPS mechanism blocks the offending program or process from carrying out potentially harmful activity. Monitoring HIPS alerts and logging information will provide early indications of intrusions. There are many commercial vendors that provide HIPS services.
9	Isolate Web-facing applications	Organizations should use virtualization to create an environment where Web-facing applications can run in isolation. Internet browsers and e-mail clients are examples of applications that are susceptible to exploits that execute malware. Security exploits specific to such applications can be confined to this sandbox. Any malware that infects the virtualized environment cannot get out of the sandbox; therefore, the malware cannot infect the host or enterprise.
10	Implement application	Organizations should explicitly identify authorized applications and application components. All other applications and application components should be denied by default to reduce the risk of executing zero-day malware. Application whitelisting technologies can control which

	whitelisting	applications are permitted to be installed or executed on a host. The whitelist can be defined by a selection of several file and folder attributes (e.g. file path, file name, file size, digital signature or publisher, or cryptographic hash). Application whitelisting policies should be defined and deployed across an organization. Whitelisting is described in the following resources: • CSE's *ITSB-95 Application Whitelisting Explained* [8]

SUMMARY

The *CSE Top 10 IT Security Actions to Protect Internet-Connect Networks and Information (ITSM.10.189)* is a list of IT security actions that can be applied within organizations to help reduce the risk of exposure from threat actor activities. Implementing these actions will reduce the risk; however, IT security activities need to be reviewed and improved continuously to address changes in the cyber threat landscape.

CONTACTS AND ASSISTANCE

If you would like more detailed information on how to implement the Top 10 IT Security Actions, please contact:

ITS Client Services
E-mail: itsclientservices@cse-cst.gc.ca

SUPPORTING CONTENT

LIST OF ABBREVIATIONS

Abbreviation	Full Term
2FA	Two-Factor Authentication
BYOD	Bring your own Device
CSE	Communications Security Establishment
HIPS	Host-Based Intrusion Prevention System
IT	Information Technology
ITS	Information Technology Security
OS	Operating System
MDM	Mobile Device Management

REFERENCES

Number	Reference
1	Treasury Board of Canada Secretariat. *Policy on Management of Information Technology,* 1 July 2007.
2	Treasury Board of Canada Secretariat. *Policy on Government Security,* 1 July 2009.
3	Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology (MITS)*, n.d.
4	Communications Security Establishment. *ITSB-96 Security Vulnerabilities and Patches Explained,* March 2015.
5	Communications Security Establishment. *ITSG-33 IT Security Risk Management: A Lifecycle Approach,* December 2014.
6	Communications Security Establishment. ITSG-22 *Baseline Security Requirements for Network Security Zones in the Government of Canada,* June 2007.
7	Communications Security Establishment. ITSG-38 *Network Security Zoning – Design Considerations for Placement of Services within Zones,* May 2009.
8	Communications Security Establishment. *ITSB-95 Application Whitelisting Explained,* March 2015.