Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

September 2013

Cyber Security Considerations for Management

Guidance for the Government of Canada

ITSB-67

Introduction

Government of Canada (GC) departments rely on information systems to support their business activities. These interconnected information systems are often subject to serious threats which can have adverse effects on departmental business activities by compromising the confidentiality, integrity or availability of the systems and their information technology (IT) assets. Senior management support is essential in ensuring the continued protection of business applications, information assets, and IT infrastructures. This bulletin identifies key questions to guide leadership discussions between management and their IT security team to enhance national security, protect sensitive GC information and enable the achievement of departmental mission objectives.

Intended Audience

This publication is intended for senior management (non-IT), Chief Information Officers (CIOs), Departmental Security Officers (DSOs), and senior management involved in IT security decision making processes.

The Threat Environment

The most significant cyber threat facing GC networks is the e-mail threat which can result in the wide spread compromise of a network as well as data exfiltration. Cyber threat actors aim to covertly collect sensitive data from information systems or attempt to deny, degrade, disrupt or destroy the data on those information systems.

Malware, or malicious software, is the most commonly used tool to gain access to networks in order to steal information or disrupt business activities. Malicious software can be used to create an entry point into a network; once an entry point has been established, a threat actor has an opportunity to gather information which can be used to perform targeted cyber intrusions and gather information of strategic interest. Your department can also be targeted and compromised as a means to gain access to another department's or partner's network by exploiting trusted connections.

The most commonly used method to spread malware via e-mail is through spear phishing. CSEC recently published Spotting Malicious E-mail Messages (ITSB-100) which describes spear phishing as a tactic that uses social-engineering to tailor e-mails towards individuals or groups based on their line of work, interests, or personal characteristics. Spear phishing e-mails use information that seems relevant to the recipient in order to entice the user to open the e-mail and click on an embedded link.

Cyber Security Considerations for Management

Since cyber threats are becoming increasingly sophisticated and targeted, insufficient IT security can lead to an increase in successful cyber security incidents. These incidents can have a significant and direct impact on organizations in terms of the confidentiality, integrity or availability of the GC systems and IT assets. Properly assessing the security risks specific to your organization can help to minimize your weak points.

1. A serious cyber security incident could be costly to your organization.

With the increase in frequency and sophistication of cyber intrusions compromising departmental IT networks, effective IT security can help avoid the direct costs of cleanup and also indirect costs such as downtime, lost productivity and damage to the reputation of and confidence in your organization.

Are you aware of the cyber security incidents that occur in your organization?

> In its *2013 Global Threat Intelligence Report*, Solutionary, Inc. discovered through case studies that organizations are spending as much as $6,500 US per hour to recover from a distributed denial of service (DDoS) attack and up to 30 days to mitigate and recover from malware intrusions at a cost of $3,000 US per day. These costs do not include revenue that may have been lost due to system downtime.

2. **A threat actor could reap benefits by having access to your information.**

Canada is an attractive target for cyber threat actors due to its wealth, resources, and diplomatic relationships with its partners. Information gathered by cyber threat actors can be used for economic, political, and technological gain. The same information can also be leveraged to enable further cyber intrusions against public and private corporations. It is important to consider the aggregated value of your information, not only the value of individual records. The knowledge gained by a threat actor concerning your network characteristics can be used for future intrusions.

Do you receive damage assessments concerning the cyber incidents that occur in your organization?

Do you have a say in what information is most valuable to your organization and requires enhanced protection?

3. **Controls should be implemented to secure against threats.**

A comprehensive IT security plan that secures your organization against threats benefits all levels of the organization: executive management, each business unit and employees. Management must ensure that clearly defined procedures and policies are implemented, that employees have been trained and that third party assessments have been conducted.

Security is an ongoing process that must continue to adapt to meet the demands of the ever changing threat landscape. Even though cyber threat actors are becoming more sophisticated and targeted, so too are the IT security techniques. There is no silver bullet to ensure your department is completely safe from cyber intrusions; rather, cyber security is an iterative process that manages risks to an acceptable level. To guide your department in managing the risk, CSEC recently published Risk Management – A Lifecycle Approach (ITSG-33). Discuss ITSG-33 with your IT security department and encourage them to take the risk management courses offered through the CSEC IT Learning Centre.

CSEC's recently released CSEC Top 35 Mitigation Measures (ITSB-89A) can be leveraged by your IT security team, along with industry standards and best practices to protect your systems and detect potential problems. Using ITSB-89A along with a risk managed approach to cyber security allows for the comprehensive and cost effective management of cyber threats.

Do you know if your organization is implementing good IT security practices?

4. **The culture of your organization should encourage employees to use strong security techniques.**

Information security is the responsibility of everyone in the organization. Employee responsibility should be clearly defined, communicated and supported with effective education and awareness. It only takes one malicious e-mail attachment to be opened or one malicious website to be accessed to potentially compromise your entire network. Employee diligence and dedication is an important factor for business continuity in the face of today's cyber threats; consequently, awareness should be supported by senior management and be part of the strategic framework.

Do you make information protection everyone's responsibility?

5. **Policies and procedures detailing the proper response to a cyber-security incident should be developed.**

All departments will experience a cyber-incident at some point; therefore it is important to have the correct policies and procedures in place to respond in a timely manner. Knowledge of the current threats and vulnerabilities specific to each organization can help to limit or even prevent damage to IT assets. CSEC offers specialized cyber situational awareness reports to help you understand the threat landscape.

Do you receive GC CTEC reports pertaining to your organization?

Conclusion

An essential part of cyber security is the support of senior management in defining the risk strategy and acceptable levels of risk in such a way that they are aligned with the business needs of the department, such as priority setting and resource allocation. Communication between management and their IT security team is essential, and can provide awareness of the current risks and associated business impact. Risks cannot be assessed by IT practitioners without understanding the business owner's view of the value of the information. In this way, security priorities can be set and resources allocated accordingly. Managers are responsible for the "I" in IT. Make it your business to be involved in IT risk decisions.

Additional Information

For general questions concerning IT Security, contact: itsclientservices@cse-cst.gc.ca.