CommunityNet security

12

Main points

CommunityNet is Saskatchewan's high-speed, province-wide data network. Private and confidential government information travels over CommunityNet. CommunityNet is a large network, with diverse users, and sensitive information. This means that CommunityNet must have strong security.

We did a study to determine whether the Government has adequate processes to oversee the security of government information carried on CommunityNet. We examined the processes in place at March 1, 2004. Based on our study, we found that the Government does not have adequate processes to oversee the security of government information carried on CommunityNet.

We recommend that the Government:

- clarify which agency is responsible to oversee the security of CommunityNet;
- approve and implement security and data classification policies to protect information carried on CommunityNet; and
- make the agency responsible for overseeing the security of CommunityNet also responsible for monitoring security and ensuring corrective action is taken.

Introduction

CommunityNet is Saskatchewan's high-speed, province-wide data network. CommunityNet connects many users. These include 910 educational facilities, 310 health facilities, 162 public libraries, and 256 government offices in 366 Saskatchewan communities. The Crown Investments Corporation of Saskatchewan and its related agencies do not use CommunityNet. The Information Technology Office (ITO) advises that the annual operating cost of CommunityNet is $12 million.

Private and confidential government information travels over CommunityNet. This includes personal and management information. CommunityNet also has very diverse users, including government employees, health care workers, school children and staff, and library employees and patrons. The large size of the network, the diversity of users, and the sensitivity of information carried means that CommunityNet must have strong security policies, clearly-defined responsibilities, and adequate monitoring.

In our 2002 Fall Report – Volume 2, Chapter 3, we recommended that the Government establish a baseline security policy for agencies using CommunityNet. The policy would help ensure that all agencies sharing information over CommunityNet protect that information to the same high standard.

In this chapter, we consider the security of information carried on CommunityNet and make recommendations to improve the security of that information.

Study objective

The objective of our study was to assess whether the Government has adequate processes to oversee the security of government information carried on CommunityNet. We examined the processes in place at March 1, 2004.

This study did not include a review of security processes at government agencies, other users of CommunityNet, or at SaskTel the service provider. Our study is not an audit.

Study findings

We found that the Government does not have adequate processes to oversee the security of government information carried on CommunityNet. In this section, we set out our expectations (in italics) and our findings.

Responsibility for security

We expect accountability relationships to set out who is responsible to whom, and for what. For a network like CommunityNet, it is critical that the Government define who has responsibility for security. It is also important that this responsibility is not spread over many government agencies. Finally, it is critical that the Government accompany this responsibility with appropriate authority.

The law sets out who is responsible for the security of CommunityNet. However, this does not match how CommunityNet is currently being managed.

CommunityNet, as a shared data network, is the responsibility of the Minister Responsible for Information Technology. The law currently provides that the Minister carries out this responsibility for information technology through the Department of Industry and Resources (Department). However, the Department does not do this. Both the Department and the ITO agree that the ITO fulfills this role and it does so independent of the Department.

However, the Government has not formally established the ITO as a separate government agency with the mandate to carry out the Minister's responsibilities. The Government needs to clarify the legislative responsibility of the ITO and of the Department.

As a result, the responsibilities and authority of the ITO and the Department and their accountability relationships are unclear. It is not clear who is responsible for the security of CommunityNet.

1. We recommend that the Government clarify which agency is responsible to oversee the security of CommunityNet.

The need for security policies

We expect the Government to have government-wide security policies. The policies should include procedures and monitoring processes for security. Policies should also set out the Government's direction and commitment to security. In a complex environment like a government, the policies must set out the services covered and which government agencies follow the policies. For the purpose of this study, the policies need to cover the government agencies using CommunityNet.

Policies require a thorough analysis of the risks involved. The Government should also base the policies on a recognized security model or framework. The framework helps ensure the policies are complete.

Security policies help protect the confidentiality, availability, integrity, and privacy of information. Data classification would help government agencies sharing a service like CommunityNet determine the level of security needed for their information.

The Government has not approved and implemented security policies for CommunityNet. Nor has the Government approved and implemented a data classification system that would assist agencies to identify sensitive information and take appropriate security measures. Currently, the ITO has a draft security policy for CommunityNet and a draft data classification policy based on a national framework.

The Government needs strong security policies to effectively manage privacy. The Government describes its approach to privacy for part of the Government in its Overarching Privacy Framework (Privacy Framework).[1] The Privacy Framework does not include the Crown Investments Corporation of Saskatchewan and its related agencies. Also, the Privacy Framework does not include agencies in the health and learning sectors that use CommunityNet.

The Privacy Framework assigns the ITO to work with other government agencies to develop certain security procedures. Assigning this responsibility to multiple agencies diffuses responsibility for security in the Government. In addition, the Privacy Framework does not recognize the

[1] Government of Saskatchewan, *An Overarching Personal Information Privacy Framework for Executive Government*, September 2, 2003. Available on the internet at http://privacy.gov.sk.ca.

need for a comprehensive security policy based on a recognized security standard. As a result, the security procedures envisioned in the Privacy Framework will not be adequate for CommunityNet.

It is critical that the Government base security for CommunityNet on a thorough assessment of risk and a recognized security standard. Security policies for CommunityNet should ensure security is consistent and adequate at each government agency. Where agencies outside the Government use CommunityNet, the ITO should use contracts to ensure they comply with the security policies.

2. We recommend that the Government approve and implement security and data classification policies to protect information carried on CommunityNet.

Monitoring security

We expect that once the Government clarifies responsibility for security and approves and implements security policies, it will also give an agency formal responsibility to monitor security on CommunityNet.

We expect the Government will ensure government agencies and other users comply with the security policies. To do this, it must first approve the policies so that the users are aware of the rules they need to follow. Secondly, it needs to set up mechanisms to review compliance with the security policies.

Monitoring achieves two purposes. First, it verifies users compliance with security policies. Second, it enables corrective action to be taken against weaknesses and threats. A security weakness at SaskTel the service provider or within a government agency's network could put the information carried on CommunityNet at risk of disclosure, damage, or loss.

Currently no government agency, including the ITO, has clear responsibility and authority to verify user compliance with security policies or to ensure corrective action is taken.

The ITO receives regular information on security threats from the Internet. The ITO has drafted a policy to respond to these external security risks.

In addition, the ITO provides assistance to CommunityNet users for security threats. However, the draft policy does not address risks that may already exist within government agencies and other CommunityNet users.

3. We recommend that the Government make the agency responsible for overseeing the security of CommunityNet also responsible for monitoring security and ensuring corrective action is taken.

Selected references

International Organization for Standardization. (2000). *Information technology: Code of practice for information security management.* Geneva, Switzerland: ISO. (Reference number ISO/IEC 17799 : 2000).

The Canadian Institute of Chartered Accountants. (1998). *Information Technology Control Guidelines*. Toronto: Author.

The Canadian Institute of Chartered Accountants. (2003). *Trust Services Principles and Criteria*. Toronto: Author.

The Information Systems Audit and Control Foundation. (2000). *CoBiT-Governance, Control and Audit for Information and Related Technology*. Rolling Meadows, IL: Author.