Information Technology Security

3

Executive summary

This chapter is a continuation of our review of Information Technology (IT) security from our previous reports. This chapter compares the results of a recent survey with the results of the survey completed in 1999 and reported in our 1999 Fall Report – Volume 2. We also surveyed government agencies (agencies) and reported results in our 1996 Spring Report and our 1997 Spring Report.

The information and the technology that supports government programs is one of the Government's most important assets. As a result, agencies need to protect their information from unauthorized disclosure, accidental or deliberate changes, and accidental or deliberate destruction. Agencies must also ensure their procedures are adequate to recover from system interruptions.

There are a number of trends occurring that indicate IT security will become even more critical to the Government. These include increased dependence on IT; use of the Internet and Intranets to provide government services; the use of e-commerce to do business; the increased sharing of information electronically with other organizations; and the increased use of networks.

Overall, the results showed little improvement from the previous survey and more improvement is required. For example:

- Agencies need to improve their employees' awareness of their responsibility and accountability for ensuring the confidentiality, privacy, integrity, and availability of their critical IT systems and data.

- To ensure an appropriate level of security, senior management needs to become aware of the risks agencies are assuming if they are not fully protecting the confidentiality, privacy, integrity, and availability of its critical IT systems and data.

- IT security officials in most agencies are not independent of IT operations. They are placed in a conflict of interest position because IT operations objectives are often in conflict with IT security objectives.

Introduction

This chapter reports the results of our survey of information technology (IT) security practices in government agencies (i.e. departments, Crown corporations, boards, commissions, and post-secondary institutions). We also report the results of our follow-up work on our previous recommendations on IT security.

To assess the progress the Government has made in improving IT security, we compared the results of the current survey to the results of past surveys. The survey results show little improvement in security practices in the Government. We concluded that the Government must do more to improve its IT security in its agencies.

The need for IT security

IT security means the measures agencies use to protect the confidentiality, privacy, integrity, and availability of their IT systems and data.

Good security is critical to the successful use of IT. If security is poor, government agencies (agencies) risk not having accurate and reliable information to achieve their goals.

Today, agencies use IT to deliver their programs and services, provide the information they need to make decisions, manage their resources, and account for what they do. As a result, agencies must adequately protect their information from unauthorized disclosure, accidental or deliberate changes, and accidental or deliberate destruction. Agencies must also ensure their procedures are adequate to recover from system interruptions.

There are a number of trends occurring that indicate IT security will become even more important to the Government.

1. The agencies' use of and reliance on IT to conduct their business and to interact with other agencies, other levels of government, private corporations, and the public continues to increase. More computers are being connected together to form networks. As more computers are connected, the risk of security breaches

increases. Security is only as strong as its weakest link. In addition, networks are becoming more complicated as technologies improve and the demand for more speed and access increases. The Government is implementing CommunityNet, a province-wide network that connects over 1500 public facilities in over 300 locations to deliver its programs and services electronically.

2. Agencies are increasing their use of the Internet and of Intranets (i.e., private secure Internet sites). As agencies transmit information across the Internet and Intranets, the risk of unauthorized access to that information increases.

3. Agencies are increasing their use of electronic-commerce (e-commerce). E-commerce is the use of telecommunications and computer processing to conduct business electronically.[1] Almost 70% of agencies we surveyed indicate that they are currently using some form of e-commerce to conduct business. We expect that this number will continue to rise. Poor security over e-commerce introduces the risk of direct financial losses.

4. More employees are gaining access to agencies' computer networks from outside the agencies' offices. The survey showed agencies have staff or customers accessing the agencies' systems from outside their offices. This increases the risk of unauthorized access to their networks because agencies cannot restrict access by just using the physical security of their offices. Therefore, good physical security is not as effective as it once was in helping to prevent unauthorized access. In addition to good physical security, agencies need to have stronger access controls.

5. Agencies are starting to recognize the importance of reporting non-financial indicators in measuring their successes and reporting on their performance. The trend is that agencies are realizing that more of their non-financial systems are critical[2]. Agencies are becoming aware that some of these systems are

[1] Adapted from the *Information Technology Control Guidelines* published by The Canadian Institute of Chartered Accountants.

[2] To assess what is critical, agencies were asked to consider the significance, impact and magnitude of the system.

more important than financial systems. This shows the agencies' increasing reliance on IT to deliver their products and services.

6. The agencies we surveyed reported that they spent almost $290 million last year on information technology. They also estimate they will spend over $310 million on information technology in this year.

7. Fifty per cent of the agencies surveyed indicated that they had outsourced the management of at least one of their critical systems.

8. The Government is increasingly concerned about privacy. Currently the Government is doing a study and report on the privacy practices in its agencies. At the time of this report, the Government's report on privacy was not public.

The Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) also recognize this increasing importance and reliance on IT. They jointly drafted a new assurance standard called the *Trust Services Principles and Criteria* to give assurance on the reliability (availability, security, integrity, confidentiality, and privacy) of Internet sites and computer systems. This standard gives organizations the ability to provide assurance to others that the organizations' systems meet a set of security principles and criteria.

For example, an organization that uses its Internet site to conduct business can hire an independent auditor to evaluate and test the site and its systems to see if it meets the principles and criteria. If it does, the auditor will allow the agency to display on its Internet site the *WebTrust* seal to tell users there is a high level of assurance the information on its Internet site is reliable and Internet business transactions will be secure.

Because of the increasing importance of IT security to the Government, we plan to review security practices every three years. The results of our survey showed that agencies made little progress from 1999 and that they need to improve their IT security. Also, given the increasing importance of and risk to IT, the security standards must improve to keep pace with changes in IT.

Our work

Our study involved an analysis of the results of 32 of the 34 key government agencies surveyed. We based the survey questions on standards recommended by the Technical Security Branch of the Royal Canadian Mounted Police (http://www.rcmp-grc.gc.ca/tsb/index.htm). We asked the agencies to evaluate themselves as of August 31, 2002. Exhibit 1 contains a listing of the agencies surveyed.

We assessed the reasonability of the responses against our knowledge of the agencies' security practices. In carrying out the assessment, we concluded that the responses were reasonable.

In this chapter, we also compare the results of the current survey (denoted as *current* on the bar graphs) with the results of the survey completed in 1999 (denoted as *prior* on the bar graphs). We published the prior survey results in our 1999 Fall Report – Volume 2. In our previous chapters on IT security, we made several recommendations. The Standing Committee on Public Accounts reviewed those chapters in May of 1996 and December of 2000 and concurred with our recommendations. There are no new recommendations in this chapter.

We assess the Government's security management practices using the following six criteria:

1. responsibility for security
2. security policies and procedures
3. security awareness
4. protection of IT resources
5. confidentiality and integrity of IT resources and
6. availability of IT resources

The following section details our findings.

Detailed results

Responsibility for security

We expected agencies would clearly define the roles and responsibilities for IT security. Agencies would have policies and procedures that:

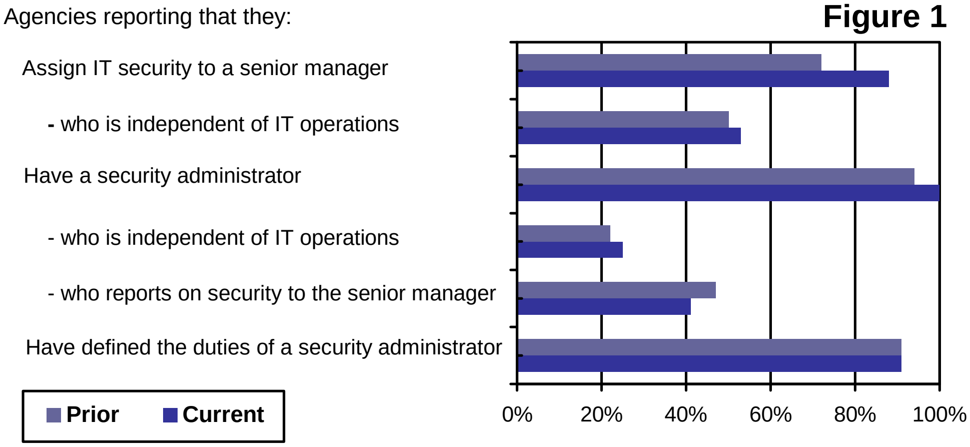
- ♦ *assign responsibility for IT security to a senior manager who is not responsible for IT operations and programming;*
- ♦ *appoint a security administrator who is independent of IT operations and programming and is accountable to the senior manager responsible for IT security; and*
- ♦ *set out the roles and responsibilities of a security administrator.*

Given the significant reliance on information technology in today's world, organizations should assign the responsibility for IT security to a senior manager. This would give IT security the priority it needs. In addition, senior management can strengthen security by making a written commitment (e.g., Government of Saskatchewan Security Charter) to have good security.

Agencies need to have adequate segregation of incompatible duties by separating the responsibilities for IT security from computer operations and programming. If they do not, employees may not carry out approved policies and procedures or may reduce security to increase the speed at which computer systems process and retrieve data. Good security practices can reduce the performance of systems. For example, to protect against computer viruses, agencies have installed programs to check and eliminate computer viruses. These programs can cause the IT system to run slower.

In smaller agencies, the separation of IT security from computer operations may be impractical. Each Agency should assess this during its analysis of threats and risks. Senior management should document its approval if it plans to take this risk.

Figure 1



Our survey results on Figure 1 indicate that 53% of agencies assign IT security to a senior manager who is independent of IT operations. There is still a need for improvement. Only 25% of agencies have security administrators that are independent of IT operations. There has been no significant change in this number from the previous survey. Agencies need to improve the reporting process between the security administrator and the senior manager who has the overall responsibility for security. Forty-one per cent of the agencies surveyed indicate that the security administrator reports directly to the senior manager responsible for IT security and security matters. This is a small drop from the last survey.

We continue to recommend:

- agencies assign the responsibility of IT security to a senior manager who is independent of IT operations; and

- the security administrator(s) report directly to the senior manager responsible for IT security.

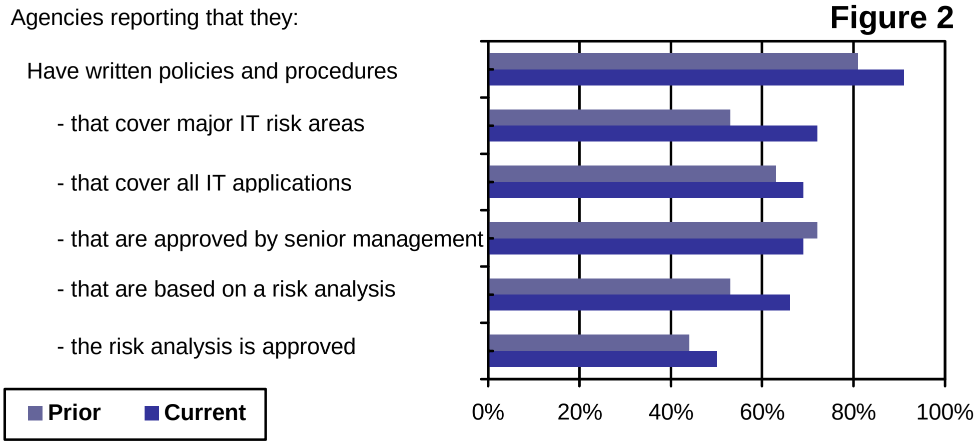
Security policies and procedures

We expected agencies would have written and approved security policies and procedures that are based on a sound threat and risk analysis.

Without written and approved security policies and procedures, agencies may not have adequate safeguards to ensure the confidentiality, privacy, integrity, and availability of information systems and data. Also, employees may not know the rules they need to ensure good security.

A threat and risk analysis is key to developing adequate security policies and procedures. This analysis is essential for good IT security management. Senior management must ensure the threats and risks to IT security are addressed with appropriate security policies and procedures. The analysis should compare the costs of the security measures to the benefits of reducing the threats and risks. Senior management should review and approve the analysis to ensure they are aware of the threats and risks facing the agency and the cost-benefit trade-offs.

Figure 2



Since our last survey, the Information Technology Office[3] has conducted workshops to help agencies write good security policies and do a good threat and risk analysis. Many agencies have not yet completed their new security policies.

The above graph indicates there has been little improvement since the prior survey. There are still a significant number of agencies without adequate written policies and procedures. The survey results indicate that 91% of agencies have written policies and procedures, but only 38% of the agencies have up-to-date security policies and procedures that:

- cover all major risk areas;

[3] Operating under the leadership of the Chief Information and Services Officer for Saskatchewan, the Information Technology Office (ITO) establishes and co-ordinates policies and programs that use information technology to enhance public access, strengthen the government's ability to undertake electronic service delivery, and enable electronic commerce throughout the province.

- cover all applications; and
- are approved by senior management.

Given the reliance on IT, it is essential that all agencies have written and approved security policies and procedures.

The current results show that only 50% of agencies do a risk analysis and have it approved by senior management. Policies and procedures need regular monitoring to ensure they continue to meet the needs of the agency. This monitoring includes ensuring policies and procedures meet a minimum standard and agencies operate within the standard.

While the surveys showed 91% of agencies have written policies and procedures, our review of those policies and procedures showed that the level of detail varies from agency to agency. For example, one agency refers to the acceptable use policy published by a central government agency as their only documented security policy. It is acceptable to refer to other published policies, but agencies need to ensure their documented policies cover all significant areas of IT security, not just acceptable use of personal computers.

In our 1999 Spring Report, we recommend that the Government establish a government-wide general security policy for its IT systems. The general security policy would set out the security performance standard that the agencies must meet. The ITO has provided most agencies with a template to prepare their security policies. The Government must establish a baseline security policy for agencies using CommunityNet.

We continue to recommend:

- the Government establish a government-wide general security policy for its IT systems;
- that all agencies establish security policies and procedures for their significant IT systems;
- that agencies set and approve security policies and procedures that meet the government-wide general security policy and the

security needs of the agency based on an appropriate threat and risk analysis; and

- that agencies continue to monitor their security policies and procedures to ensure that they meet the needs of the agency and meet or exceed minimum standards.

Security awareness

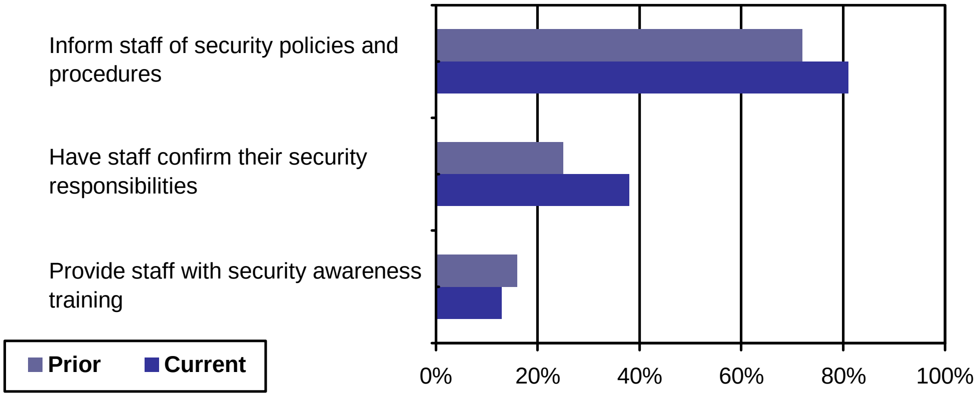
We expected agencies would make employees aware of security by informing and training them in their IT security responsibilities.

Agencies need to ensure employees are aware of the security policies and procedures. Generally, this is a simple and efficient way to improve security. A majority of the security breaches or incidents originate from within the organization. Employees not aware of the policies or the consequences of their actions account for a large portion of the security breaches. Management can prevent most security breaches by informing employees of their security responsibilities and training them properly.

Employees need to confirm periodically that they are aware of the policies. This promotes accountability for and awareness of the agency's policies.

Figure 3

Agencies reporting that they:



The survey results indicate there is very little improvement in this area. Only 38% of the agencies surveyed say they have employees confirm their security responsibilities (e.g. confidentiality, privacy, integrity, and availability).

The surveys indicate that the agencies have not taken seriously the need for security awareness training. Only 13% of agencies provide their employees with regular security awareness training. Management must make employees aware of the responsibilities and skills needed to ensure the security of their agencies' information.

Agencies need to improve their procedures for revoking employees' access to information when they quit or change responsibilities. Forty per cent of the agencies surveyed do not have written rules and procedures for revoking employees' access. Written rules and procedures ensure employees are aware of the procedures they need to follow.

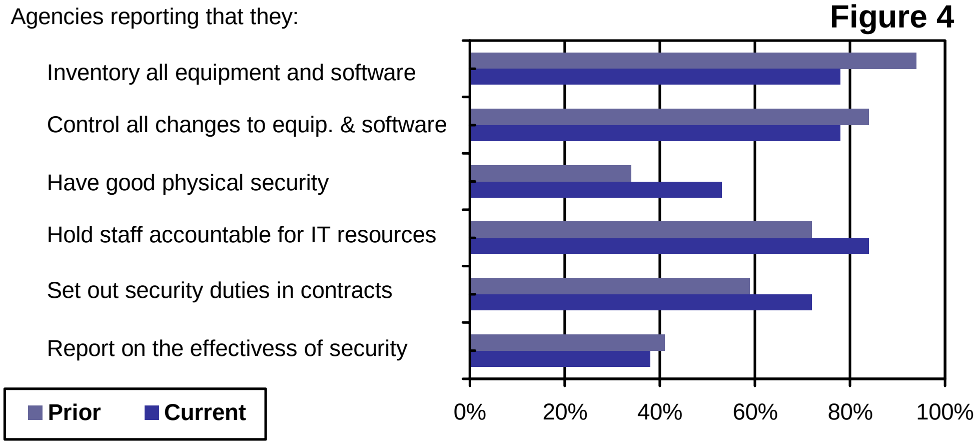
We continue to recommend that agencies:

- provide security awareness training;
- have employees agree periodically in writing with their security responsibilities; and
- ensure they have written policies and procedures for revoking employees' access to information when their employment ends.

Protection of IT resources

We expected agencies would have strong physical security, control all changes to computer equipment and software, specify security requirements in service contracts, and monitor and report on the effectiveness of their security measures.

Figure 4



The survey results indicate that there is little improvement in physical security. Only 53% of agencies surveyed indicate that they have good physical security. Physical security is an essential part of good IT security. If agencies have their IT systems and data physically secure, then password security becomes more effective. Twenty-five per cent of agencies thought they should improve physical security.

We found that only 38% of the agencies report on the effectiveness of their security policies. Senior management needs to know whether employees comply with their agencies' policies. Also, senior management needs to know if their security policies and procedures are effective in ensuring the confidentiality, privacy, integrity, and availability of information resources.

Seventy-two per cent of agencies report that they set out security requirements in service contracts. If agencies do not specify security requirements in contracts, they are at risk of the contractor disclosing information.

We continue to recommend that agencies:

- ♦ determine their physical security needs and assess the adequacy of their security measures;
- ♦ periodically report on the effectiveness of their security policies and procedures. Senior management should review these reports and take corrective action if necessary; and
- ♦ ensure their service contracts include requirements for security and confidentiality.

Confidentiality and integrity of IT resources

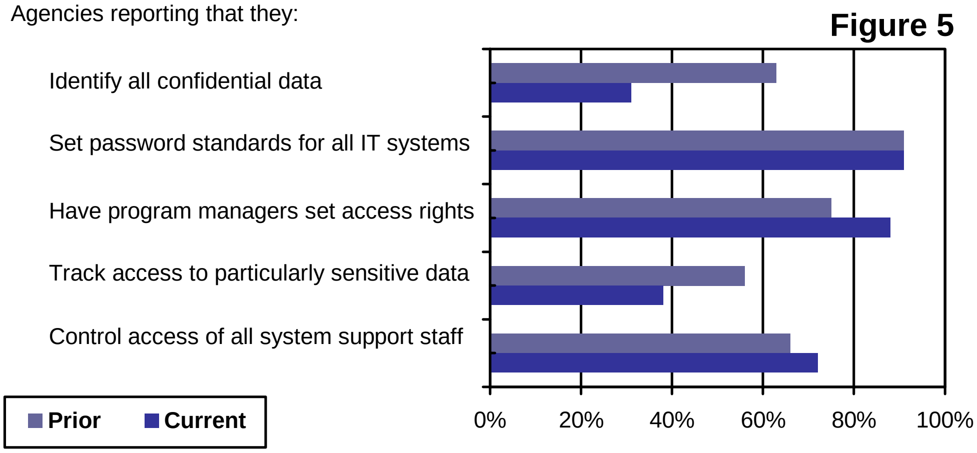
We expected agencies would protect the confidentiality and integrity of IT systems. To do this, agencies need to:

- ♦ *identify all confidential data kept on IT systems;*
- ♦ *set standards for the composition and changing of passwords that permit access to confidential data;*

- *have owners of data (program managers) define and authorize who can access or change their data; and*

- *track who accesses very sensitive data.*

Figure 5



Ninety-one per cent of the agencies report that they have password standards for their IT systems. However, the standards vary for each agency including the required minimum length of a password and the maximum number of days that a password can be used. It would be beneficial to have password standards included as part of a government-wide policy. More agencies are sharing information through the interconnection of their computer systems and the agencies must keep the information confidential. Standards, such as password policies, will help ensure agencies that share confidential information maintain the confidentiality, privacy, integrity, and availability of the data.

Agencies still need to improve the way they classify confidential data and track access to sensitive data. This includes defining who can access data. Classifying and tracking confidential and sensitive data will help to control access to the data. Figure 5 shows that only 31% of agencies identify confidential data, only 38% of agencies track access to sensitive data. The government has introduced a draft framework for classifying data and agencies have not yet put it into practice.

We continue to recommend that agencies:

- use government-wide security criteria to set password standards for all their IT systems;

- identify their confidential data. This should be based on government-wide security criteria;

- require program managers to define who can access their data; and

- control and monitor the access that IT support employees have to IT systems.

Availability of IT resources

We expected agencies would have adequate back-up and recovery procedures, and tested and documented contingency plans.

Agencies need current, written, and tested contingency plans for critical functions and for the 'business' as a whole. To ensure contingency plans are adequate, agencies need to perform a threat and risk analysis. A threat and risk analysis ensures management is aware of significant risks so that the agency can adequately address those risks. Even if agencies are relatively certain their systems will not fail, they still need to do a threat and risk analysis and prepare contingency plans.

Agencies need to be clear on which of their systems are critical. Designating a system as critical affects the level of contingency planning that is necessary. Senior management needs to:

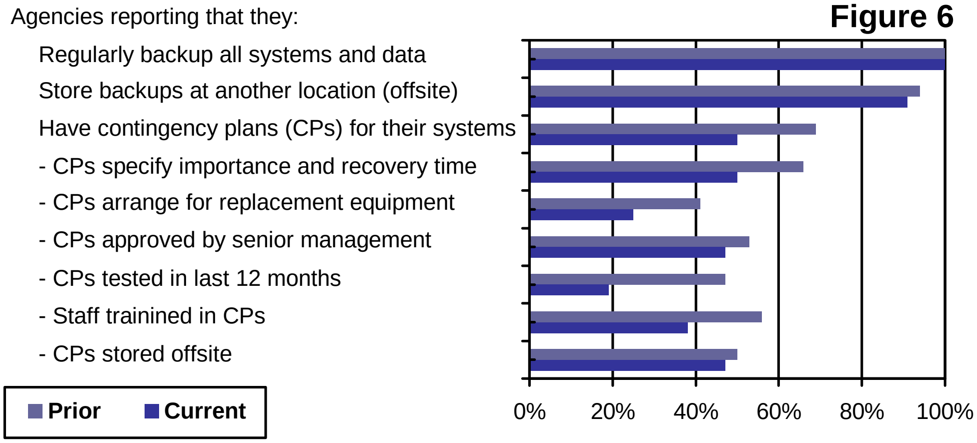
- *know what systems are critical and how long its agencies can operate without the system;*

- *ensure adequate policies and procedures are in place relating to contingency plans;*

- *approve and accept risks not covered by the contingency plan; and*

- *ensure the availability of any outsourced critical systems.*

Figure 6



The survey results indicate that many agencies that had contingency plans in 1999 have not kept them current. Most of the agencies reported that they periodically back-up their systems and data, and store their back-ups offsite.

Fifty per cent of agencies reported that they have a contingency plan for their significant IT systems. This is down considerably from 1999.

Only 16% of agencies that have contingency plans meet all of the criteria listed in Figure 6.

The 32 agencies that completed the survey listed over 400 critical systems. Agencies ranked over 250 of these systems as being very critical.

We continue to recommend that agencies:

- specify which systems are critical to the mission of the agency;
- base their contingency plans on a risk analysis which ensures management is aware of its significant risks and how to address those risks;
- that agencies specify in their contingency plans the acceptable recovery time for each IT system; and
- that agencies test and approve their contingency plans and store them off-site in a safe location.

Conclusions

Some agencies indicate that security issues have not been made as high a priority as they would like. A majority of agencies stated that there is a lack of money to improve security. Some of the government departments surveyed have undergone significant organizational changes. They have noted that they are working on making the necessary changes to improve security.

Overall, the results showed little improvement in IT security from the previous survey. Some agencies are strengthening their security policies and procedures to ensure the confidentiality, privacy, integrity and availability of their information systems and data while others have not progressed. It is clear more improvement is required. For example:

- Agencies need to improve their employees' awareness of their responsibility and accountability for ensuring the confidentiality, privacy, integrity, and availability of their critical IT systems and data.

- To ensure an appropriate level of security, senior management needs to become aware of the risks agencies are assuming if they are not fully protecting the confidentiality, privacy, integrity, and availability of its critical IT systems and data.

- IT security officials in most agencies are not independent of IT operations. They are placed in a conflict of interest position because IT operations objectives are often in conflict with IT security objectives.

- Only 53% of agencies say they have good physical security over their IT systems.

Government agencies are also working on improving security policies. The Information Technology Office and the System Management Council have developed a document to assist in the process of setting security standards. We encourage all government agencies to adopt the security standards. This would be a major step toward better security for all government agencies.

Meeting the recommendations listed earlier requires a significant commitment by management. This includes ensuring management is involved in the security decision-making process and committing resources to improve IT security.

Exhibit 1 – Agencies surveyed by our Office

Crown Investments Corporation of Saskatchewan
Department of Agriculture, Food and Rural Revitalization
Department of Environment
Department of Finance
Department of Government Relations and Aboriginal Affairs
Department of Health
Department of Highways and Transportation
Department of Industry and Resources
Department of Justice (Includes Department of Corrections and Public Safety for the purposes of the survey)
Department of Labour
Department of Learning
Department of Social Services
Executive Council
Information Services Corporation of Saskatchewan
Public Employees Benefits Agency
Public Service Commission, The
Regina Qu'Appelle Regional Health Authority
Saskatchewan Crop Insurance Corporation
Saskatchewan Gaming Corporation
Saskatchewan Government Insurance
Saskatchewan Health Information Network
Saskatchewan Indian Gaming Authority
Saskatchewan Institute of Applied Science and Technology
Saskatchewan Liquor and Gaming Authority
Saskatchewan Power Corporation
Saskatchewan Property Management Corporation
Saskatchewan Telecommunications
Saskatchewan Transportation Company
Saskatoon Regional Health Authority
SaskEnergy Incorporated
Teachers' Superannuation Commission*
University of Regina, The
University of Saskatchewan, The*
Workers' Compensation Board

* Responses were not received from these agencies.

Glossary

Electronic Commerce – The buying and selling of products and services over an electronic medium such as the Internet. A key component of electronic commerce is the payment for the goods and services through electronic means such as the transfer of credit card information electronically or the transfer of funds directly through a bank.

Internet – A world wide web of interconnected networks providing access to a multitude of servers and to information resident on such servers[4].

Intranet – A private network or Local-Area Network connected to a web server that acts as a storage area for information for use within an organization. Users can access the information from their workstations by using Internet browser software[4].

Network – A set of connected devices (computers, modems, printers, etc.) that can be physically located across a diverse set of locations or in a single office.

[4] Adapted from the *Information Technology Control Guidelines* published by The Canadian Institute of Chartered Accountants.