Cypress Regional Health Authority
IT security

10D

Main points

Cypress Regional Health Authority (Cypress) needs to secure its information technology (IT) systems and data.

Cypress did not have adequate processes to secure (i.e., protect the confidentiality, integrity, and availability of) its IT systems and data. Lack of adequate processes to secure IT systems and data could result in loss, inappropriate modification, or unauthorized disclosure of sensitive health information.

Introduction

The Regional Health Services Act makes Cypress Regional Health Authority (Cypress) responsible for the planning, organization, delivery, and evaluation of health services in the Cypress Health Region. To carry out this role, Cypress must manage information.

Cypress uses information technology (IT) systems to provide health services and store health care information. Securing health care information (ensuring its confidentiality, integrity, and availability) is vital to fulfilling Cypress's objectives including delivering health services and protecting the interests of patients. When Cypress uses a contractor to help manage its IT services, it must oversee the security provided by the contractor.

Inadequate security could result in loss, inappropriate modification, and unauthorized disclosure of health information. It could also impede effective planning and decision making at regional, provincial, and inter-provincial levels.

This chapter reports the results of our audit of Cypress's IT security. Chapter 10B reports the results of our other audit work at Cypress for the year ended March 31, 2008.

Audit objective and conclusion

The objective of our audit was to assess whether Cypress had adequate controls to secure (i.e., protect the confidentiality, integrity, and availability of) its information technology systems and data for the period from March 15, 2008 to September 15, 2008.

Throughout our audit, we followed the *Standards for Assurance Engagements* established by The Canadian Institute of Chartered Accountants.

We used the criteria set out in the exhibit below to assess Cypress's processes. The criteria are based on the *Trust Services Criteria and Principles* authored by both The Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants and on international standards, literature, and reports of other legislative auditors. Cypress agreed with the criteria.

Exhibit—Audit criteria

To secure (i.e., protect the confidentiality, integrity, and availability of) its information technology systems and data, Cypress should:

1. **Show management commitment to security**

   Responsibility for security is clearly defined
   IT planning supports security
   Management has approved security policies and procedures
   Management monitors security

2. **Protect systems and data from unauthorized access**

   User access controls protect the systems and data from unauthorized access
   Physical security controls protect against unauthorized access

3. **Keep systems and data available for operation**

   System and data backups occur and are tested
   Disaster recovery plans are in place and are tested

4. **Maintain the integrity of systems and data**

   Change management processes exist and are followed
   Computer operation processes exist and are followed

We concluded that Cypress Regional Health Authority did not have adequate processes to secure its information technology systems and data for the period from March 15, 2008 to September 15, 2008.

Key findings (by criterion) and recommendations

We describe below what we expected (in italics) and our key findings for each criterion together with our recommendations.

Show management commitment to security

Management commitment includes setting up an organizational structure that clearly defines who is responsible for security. We expected Cypress would have a member of senior management who leads an information technology division. Management should effectively monitor service providers who perform work on its behalf. Commitment also includes implementing and monitoring compliance with security policies and procedures.

Cypress's organizational structure defined responsibility for security. Cypress also had an IT strategic plan. However, Cypress did not do a formal threat and risk assessment to support the development of the plan. Therefore, it did not know if the plan addressed all significant threats and risks.

Cypress had IT security policies. Cypress recently reviewed and modified its policies. New employees received training on the security policies as part of their orientation process. Management carried out security reviews to help ensure compliance with *The Health Information Protection Act.* These reviews also monitored compliance with security policies. Cypress did not have a policy setting out how to respond to and report IT security incidents. However, it did take action when such incidents became known, and it documented these actions.

Cypress used the IT unit of the Ministry of Health for specific IT and security services (e.g., firewall management, disaster recovery for some applications). Cypress had signed agreements with the Ministry regarding these services. Under these agreements, most of Cypress's medical information systems and data are located with the Ministry and are subject to Ministry controls.

To know that its computer systems and data are secure, Cypress needs to monitor the adequacy of the security provided by the Ministry. However, Cypress did not seek assurance or other information to make this assessment.

The Ministry did not provide all services Cypress expected during the audit period. For example, the Ministry did not maintain and monitor firewalls. Accordingly, Cypress's systems and data were at risk of inappropriate access and not being available when needed. Because Cypress did not know the firewalls were not maintained, Cypress was not aware of the risks.

1. We recommend the Cypress Regional Health Authority formally assess the threats and risks to its information technology systems and data.

2. We recommend the Cypress Regional Health Authority monitor the security of its information technology systems and data.

Protect systems and data from unauthorized access

We expected Cypress to have adequate physical access and user access processes to protect its systems and data from unauthorized access.

Good physical control means protecting IT infrastructure from harm. Physical access controls protect all computers and network devices from unauthorized access. For example, a locked door could physically prevent unauthorized users from accessing a server room.

User access controls ensure only approved people or processes can use an IT system. A common example of a user access control is a username and a password. The username identifies the user and the password grants access.

Protecting systems from unauthorized access is more critical with the increased use of the Internet, automated processes, and multiple offices. Cypress should protect its data by configuring, updating, and monitoring its systems against security threats.

Cypress had procedures for granting users access to its computer network. However, it had not fully documented those procedures. Documenting the procedures could help ensure that employees responsible for approving access do so consistently.

Cypress had a policy for removing user access when a user's employment ends. However, Cypress did not consistently follow its policy. We found examples of staff who no longer worked for Cypress whose accounts were not terminated. Cypress also did not have a process to verify a user's identity before IT employees reset the password for a user. Inappropriate user access could result in unauthorized disclosure, loss, and modification of information.

Cypress had not appropriately configured all of its systems to protect them from risks of unauthorized access. Certain computers and network devices were not set to help prevent unauthorized access or track unsuccessful attempts at gaining access.

Also, IT employees did not set all password requirements appropriately to maintain security. Cypress's policy requires passwords to be changed every 180 days. However, over 300 network accounts did not have passwords set to expire.

Cypress did not have processes to encrypt computer drives and portable media. When important and confidential data is carried on computers and on portable media, it is necessary to take precautions such as encryption to protect the data in case of theft or loss.

Cypress had devices and processes to guard against email-borne viruses. It kept its computer systems up-to-date to protect against new threats. Cypress also educated users regarding appropriate user security.

As noted above, Cypress used the IT unit of the Ministry of Health to manage some of its security processes, including firewalls. In our 2007 Report—Volume 3, we reported that the Ministry did not adequately protect its clients' systems and data from security threats. The Ministry continued to have full access to Cypress's systems and data. This exposed Cypress to any security risks that may have continued to exist at the Ministry.

While Cypress had some physical access controls, it did not equip its server rooms with standard environmental controls. Access to one of Cypress's two server rooms was not appropriately restricted, and one server room did not have a fire suppression system.

3. We recommend the Cypress Regional Health Authority establish and follow its policies and procedures for granting and removing user access to computer systems and data.

4. We recommend the Cypress Regional Health Authority configure its computer systems and data to protect them from external threats including theft or loss.

5. **We recommend the Cypress Regional Health Authority physically protect its computer systems and data from loss or damage.**

Keep systems and data available for operation

We expected Cypress to have adequate processes to ensure its systems and data are available for operation when needed.

Even with good backup and recovery procedures, Cypress may not be able to continue its operations if a major problem occurred. Therefore, it should have a contingency plan to recover operations in the event of a disaster like a fire or flood. This includes building capacity into systems, when cost effective, so a disaster in one location will not cause applications to quit running at other locations where employees are still able to work.

Cypress needs to improve and document its processes for backing up systems and data. For example, Cypress did not store its backups offsite. As a result, a disaster could destroy the backups along with the servers that hold Cypress's current information. The backup procedures should define data requirements, frequency, security, and offsite needs.

Cypress identified the need for a disaster recovery plan and began developing a plan. Cypress had not completed or tested its disaster recovery plan. Cypress, however, was able to restore specific data when requested. Lack of an approved and tested plan increases the risk that Cypress could not restore systems and data in the event of a disaster.

Cypress made an agreement with the Ministry for backup and disaster recovery of systems and data that the Ministry manages for Cypress. Cypress did not have processes to monitor whether the Ministry was meeting agreed obligations. As a result, Cypress did not know whether systems and data that the Ministry manages would be available when needed.

6. **We recommend the Cypress Regional Health Authority complete, approve, and test its disaster recovery plan.**

Maintain the integrity of systems and data

We expected Cypress to have processes for maintaining the integrity of its systems and data by implementing adequate configuration, update, monitoring, and IT operation processes. Adequate processes require approving and testing system changes before implementation. Cypress must also ensure that it has adequate processes for running and maintaining its computers.

Cypress needs documented processes for making changes to its systems and data. Good change management processes help reduce unintended consequences arising from changes. Cypress should document its approval and testing of changes prior to making them.

The Ministry made some IT changes for Cypress. The Ministry had processes for making these changes. These included informing Cypress of planned changes and receiving Cypress approval before implementing the changes.

Cypress should also have strong processes for maintaining and monitoring systems and data. We describe our findings earlier under the heading "Protect systems and data from unauthorized access."

7. We recommend the Cypress Regional Health Authority implement adequate policies and procedures for managing changes to computer systems and data.

Selected references

Canadian Institute of Chartered Accountants (CICA) & American Institute of Certified Public Accountants (AICPA). (2007). For Security, Availability, Processing Integrity, Confidentiality, and Privacy. In *Trust services principles and criteria*. Toronto: Author. http://www.cica.ca/index.cfm/ci_id/38256/la_id/1. (14 Oct 2008)

Canadian Institute of Chartered Accountants. (CICA). (1998). *Information technology control guidelines*. Toronto: Author.

Information Systems Audit and Control Foundation. (2005). *CoBiT4.0*. Rolling Meadows, IL: Author.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: *The role of IT in the design and implementation of internal control over financial reporting, 2nd Edition*. Rolling Meadows, IL: Author.

Glossary

Account—A unique identity set up on a computer or network that allows access to specific systems and data.

Application—A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Backup (noun)—A copy of systems or data to be used when the originals are not available (e.g., because of loss or damage).

Change management—An organized approach for introducing changes into a program or process, used to minimize unintended consequences.

Configure—To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

Disaster recovery plan—A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Encryption—A method of putting information in code so that only authorized users will be able to see or use the information.

Environmental controls—The controls in place at an organization to manage risks posed by the physical location of computers or network equipment. Examples include fire suppression systems, moisture detectors, and uninterruptable power supplies.

Firewall—A piece of hardware or software intended to restrict or block access to a network or computer. Firewalls can be set up to only allow certain types of data through.

IT infrastructure—An organization’s computer and network assets.

IT strategic plan—A plan indicating how an organization intends to use IT to further its business goals and objectives.

Network—A group of computers that communicate with each other.

Physical access controls—The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

Server—A computer that hosts systems or data for use by other computers on a network.

User access controls—The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.