Chapter 42
Cypress Regional Health Authority—IT Security

1.0 Main Points

This chapter describes our follow-up of management's actions on three recommendations we initially made in our *2008 Report – Volume 3*, Chapter 10 – Part D about Cypress Regional Health Authority's processes to secure its information technology (IT) systems and data.

Since our previous follow-up in 2012, Cypress Regional Health Authority (Cypress RHA) has made progress on each of the outstanding recommendations. However, further work remains so that its information technology systems and data are secure.

2.0 Introduction

In 2010 and 2012, we assessed the progress Cypress RHA made on our 2008 recommendations. Our *2010 Report – Volume 2*, Chapter 11 – Part B and our *2012 Report – Volume 2*, Chapter 43 each concluded that Cypress RHA had implemented two recommendations. At August 31, 2012, Cypress RHA had more work to do to implement the three remaining recommendations.

To conduct this review engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate Cypress RHA's progress towards meeting our recommendations, we used the relevant criteria from the original audit. Cypress RHA's management agreed with the criteria in the original audit.

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation at September 30, 2014, and Cypress RHA's actions up to that date. We found that Cypress RHA has made some progress on the recommendations, but further work remains.

3.1 Configuration and Monitoring Improvements Required

We recommended that Cypress Regional Health Authority configure its computer systems and data to protect them from external threats including theft or loss.
(2008 Report – Volume 3; Public Accounts Committee agreement December 8, 2008)

Status – Partially Implemented

We recommended that Cypress Regional Health Authority monitor the security controls of its information technology systems and data. (2008 Report – Volume 3; Public Accounts Committee agreement December 8, 2008)

Status – Partially Implemented

Most of the IT systems in use at Cypress RHA are systems provided, managed, and hosted by eHealth and 3sHealth. On the computer network that it maintains, Cypress RHA maintains databases for tracking data such as patient and facility resident information and information about staff education and training. In addition, Cypress RHA provides email and network storage for staff. The primary security risks for the information maintained by Cypress RHA relate to confidentiality.

Cypress RHA has taken some steps to improve configuration of its computers and network to protect them from external threats, including theft or loss. For example, Cypress RHA encrypts its laptops. Also, Cypress has implemented a tool so that it receives notification of malware attacks.[1]

However, Cypress RHA has not completed its processes for configuring computers to improve security. It needs to configure computers to log activities and incidents. It needs to address network accounts that have non-expiring passwords. It also needs to implement the policy it has already developed for responding to security incidents.

By not properly configuring its systems and data, not monitoring effectively, and not having policies in place to respond to security incidents, Cypress RHA increases its vulnerability to security incidents.

3.2 Testing Required for Disaster Recovery Plan

We recommended that Cypress Regional Health Authority complete, approve, and test its disaster recovery plan. (2008 Report – Volume 3; Public Accounts Committee agreement December 8, 2008)

Status – This recommendation is replaced by the following recommendation in Chapter 19 of this Report, where we recommended that certain regional health authorities, including Cypress RHA:

- Establish disaster recovery plans and test those plans to ensure their effectiveness. (2009 Report – Volume 3; Public Accounts Committee agreement June 18, 2010)

Cypress RHA has a disaster recovery plan. At September 2014, Cypress RHA had not tested the plan. Management indicated it plans to test the disaster recovery plan in late 2014.

Not having a tested disaster recovery plan increases the risk that systems and data will not be available when needed.

[1] "Malware" is an abbreviation for "malicious software," and refers to software programs designed to damage or do other unwanted actions on a computer system (i.e., viruses, worms, Trojan horses, and spyware). Definition taken from www.techterms.com/definition/malware (14 October 2014).