Chapter 43
Cypress Regional Health Authority—IT Security Follow Up

1.0 Main Points

In this chapter, we report that Cypress Regional Health Authority (Cypress) has implemented four of the seven recommendations that we made in 2008. In our 2008 Report – Volume 3, we reported that Cypress needed to strengthen its controls to secure its information technology systems and data. Cypress has more work to do on the remaining three recommendations. It still does not have a complete, approved and tested disaster recovery plan and it needs to configure its systems to protect them from external threats.

2.0 Introduction

In 2008, we audited Cypress's controls to secure (i.e., protect the confidentiality, integrity, and availability) its information technology systems and data. We reported the results of our audit in Chapter 10D of our 2008 Report – Volume 3 and made seven recommendations for Cypress to improve its processes.

We did our first follow-up in 2010. In Chapter 11B of our 2010 Report – Volume 2, we reported the results of our work and concluded that management had implemented two of our seven recommendations. This is our second follow-up.

3.0 Status of Recommendations

This section sets out the five outstanding recommendations and management's progress up to August 31, 2012. We concluded management has implemented two of these recommendations, but needs to do more for the remaining three.

3.1 Monitor Security

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 – We continue to make this recommendation.

Cypress has configured some of its computers and devices to log security events. It has also drafted a policy to respond to identified security incidents.

Cypress has not yet established a process to monitor its logs for security threats. Therefore, Cypress may not be aware of potential security incidents. Also, Cypress does not monitor the effectiveness of its service provider.

To effectively monitor the security of its IT systems and data, Cypress needs to implement policies and procedures for monitoring and responding to security incidents. Cypress also needs to monitor its service provider to ensure that its systems and data are secure and will be available when needed.

3.2 User Access Controlled

We recommended that Cypress Regional Health Authority establish and follow its policies and procedures for granting and removing user access to computer systems and data. (2008 Report – Volume 3; Public Accounts Committee agreement December 8, 2008)

Status – Implemented.

Cypress has improved its controls over user access. Cypress has documented its processes for granting user access. Cypress now verifies user identity before resetting a user's password or account and also promptly removes access when employees leave.

3.3 Configure Computer Systems and Data

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 – We continue to make this recommendation.

Cypress has taken some steps to improve configuration of its computers to protect them from external threats. For example, Cypress uses reports from antivirus devices to identify and respond to possible security incidents.

However, to effectively secure systems and data, Cypress needs to address all other configuration issues. For example, it needs to periodically change system passwords, improve security of its laptop computers, and implement effective logging processes.

3.4 Complete, Approve, and Test 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 – We continue to make this recommendation.

Cypress has created contingency plans for two of its applications and has created a strategy for disaster recovery. Cypress copies some of its data to a secondary location. Management is investigating ways to copy all of its data to a secondary location to be able to recover data effectively and securely.

Cypress still does not have a complete, approved and tested disaster recovery plan. Not having an up-to-date and tested disaster recovery plan increases the risk that systems and data may not be available when needed.

3.5 Managing IT Changes

We recommended that Cypress Regional Health Authority implement adequate policies and procedures for managing changes to computer systems and data. (2008 Report – Volume 3; Public Accounts Committee agreement December 8, 2008)

Status – Implemented.

Cypress now has procedures for managing changes to computer systems and has established a process to track changes, including approvals and testing. Cypress uses an application that tracks and records significant details about the changes including approvals and testing.