

Healthcare Provider's Compliance Journey Gains Momentum

industry:

Healthcare and Pharmaceuticals

country:

Americas

business challenge:

Eliminate business risk by ensuring compliance with healthcare and financial services-specific regulations

solution:

Undertake a thorough review and evaluation of the organisation's security profile

services:

Consulting Services: A Governance, Risk and Compliance Assessment, which included a sharp focus on technical vulnerabilities

Executive Summary

While a leading US healthcare provider had a **mature information security programme in place**, it nevertheless **faced a number of compliance challenges**. Specifically, these related to HIPAA and PCI. A thorough Governance, Risk and Compliance Assessment, which included **a sharp focus on technical vulnerabilities, put the organisation on the fast track to meeting its regulatory imperatives**.

Client Overview

Our client is a major US health care provider. It is anchored by the 580-bed university hospital, and serves Augusta-Richmond County and the surrounding region. Founded in 1818, its campus has expanded to include a heart and vascular institute and office buildings that house more than 600 private practice physicians and various treatment centres. The organisation has a long history as a leader in delivering cardiovascular, cancer and women's services.

Business Challenge

Despite having a mature and robust information security programme in place, the healthcare provider was plagued by a number of persistent regulatory and compliance challenges. Due to the nature of its operations it's required to comply with both PCI and HIPAA legislation.

HIPAA is aimed at ensuring the confidentiality of patient information and includes guidelines relating to how this information must be stored, by whom it may be accessed, as well as the network

segmentation and encryption processes that need to be put in place. They also prescribe mandatory penetration testing and numerous internal and healthcare industry-specific audits several times a year.

PCI legislation applies to organisations that store or process credit card data and is focused on ensuring the protection of that data and the application of adequate levels of encryption.

The Way Forward

A successful track record with respect to a series of networking projects gave the healthcare provider the confidence that Dimension Data would be able to help it move ahead on its journey towards compliance, in a structured and risk-free fashion.

Solution Delivered

Recognising the healthcare provider's unique challenges and drawing on its experience in assisting similar organisations achieve regulatory compliance, Dimension Data recommended that a series of assessments be undertaken to identify where the organisation's weaknesses lay from a governance, risk and compliance perspective.

Services Provided

Dimension Data adopted a two-phased approach to the task at hand. First, we undertook a Governance, Risk and Compliance Assessment to benchmark the client's security controls against industry best practice, specifically ISO27001/2. The decision to select this particular framework as the benchmark was influenced by the fact that ISO27001/2 is robust and all encompassing, and thus is a good baseline towards the fulfilment of HIPAA and PCI requirements. It therefore mapped closely to the healthcare provider's needs.

“A **successful track record** with respect to a series of networking projects gave the healthcare provider the **confidence that Dimension Data would be able to help it move ahead on its journey towards compliance, in a structured and risk-free fashion.**”

Upon completion of the assessment, Dimension Data conducted a facilitated self-assessment workshop at the client's site to review every aspect of the client's operations covered by the ISO27001/2 standard. This amounted to 12-15 discrete areas of focus, and extended beyond technology to include supporting policies and procedures.

Next, we undertook a technical validation of the results uncovered in the workshop. This involved randomly selecting approximately 100 infrastructure items within the client's IT estate, including servers, applications and laptops, and undertaking a thorough inspection of each, to ascertain any areas of weakness. The final step involved mapping these findings back to the information gathered during the workshop.

Armed with these insights, Dimension Data was able to produce a consolidated report of its findings and provide recommendations with respect to remedial next steps.

Value Derived

The value that Dimension Data provided to this client was immense – the team was able to pinpoint previously undetected areas of weakness in endpoint third-party software security and systems hardening.

Through this process, Dimension Data helped the client to evaluate various vulnerability scanning technologies and trained its users on each technology.

The healthcare provider subsequently invited Dimension Data to participate in a security strategy and architecture discussion. It regularly turns to Dimension Data for input into initiatives such as security intelligence monitoring, network admission control and also, more informally, for opinions on various products.