FORESIGHT

Security Engineering Case Study

Utilising multi-faceted professional expertise to deliver holistic security assurance, engineering, and advisory services

Summary

A leading Australian government department ("the Department") required security specialists to conduct a review of their Office 365 and Azure cloud environment. Initially, the engagement commenced as a Governance, Risk, and Compliance (GRC) piece of work for their Microsoft Dynamics 365 system. A consultative approach was adopted throughout the delivery cycle, which uncovered the need to leverage Foresight's technical expertise to conduct security assessments, as well as provide security engineering and advisory services, across the Department's cloud environment. The scope, complexity, and timeframe of this program of work required an agile response from Foresight's Security Engineering team. The initial work undertaken by Foresight was exceptionally well-regarded by the client, which resulted in consecutive engagements later in the year. Foresight was and continues to be seen as a trusted advisor for the Department's cloud environment.

Our client's challenge

As a high-profile government body, the Department operates within a dynamic and demanding cybersecurity threat landscape. The Department sought to implement a hybrid cloud model within its existing PROTECTED Information and Communications Technology (ICT) environment which introduces significant changes to its architectural landscape. The Department itself has limited in-house ICT capability, instead engaging a third-party vendor to provide ongoing ICT services. The Department's security culture was similarly in its infancy, with limited security governance and controls implemented to protect its critical infrastructure.

In response to these challenges, the Department engaged Foresight to bridge the gap and provide a myriad of security assurance and advisory services with respect to the upcoming Azure cloud environment. Since the initial engagement, Foresight has established a strong and trusted relationship with the Department and is strongly relied upon as its industry cybersecurity partner.

Scope of engagement

The scope of the program initially entailed a review of the Department's Dynamics 365 implementation against the Australian Government Information Security Manual (ISM). The review was conducted in alignment with the Australian Signals Directorate's (ASD)

Information Security Registered Assessors Program (IRAP) methodology. The nature of the work requested typically requires a comprehensive review of documentation and system architecture, stakeholder engagement, technical verification of security controls, and risk analysis.

During the discovery and scoping workshops for the system, the Department identified an opportunity to further leverage Foresight's extensive security engineering experience. Additional services provided by Foresight included best practice technical reviews of the Department's Azure and Office 365 hybrid cloud design and deployment, hardening guidance for the cloud environment, and uplift of the Department's Azure Sentinel Security Information and Event Management (SIEM) solution security monitoring capabilities.

Over the course of a year, Foresight completed several pieces of work across the Department's cloud environment, including security and risk assessments, security advisory services, capability uplifts, as well as the development of Security Risk Management Plans (SRMP), System Security Plan (SSP), System Security Plan Annex (SSP Annex), and a technical security assessment report.

How Foresight helped?

Foresight adopted a consultative approach with the Department throughout the journey. Foresight commenced the initial engagement with a discovery and scoping workshop with the Department's subject matter experts to gain an understanding of the system context, architecture, scope, and associated requirements. This approach identified more areas in which Foresight could assist the Department. Foresight's extensive security engineering knowledge and experience enabled them to provide real-time advice and pragmatic recommendations to the client. This approach helped form a trusting and open relationship with the Department and enabled Foresight to deliver services efficiently and effectively.

By comprehensively reviewing system documentation, actively engaging with key client stakeholders, and directly performing assessments on the Department's cloud-based implementations, the Foresight team developed an in-depth understanding of the Department's operational environment. This coupled with Foresight's thorough technical assessment of the Department's cloud environment contributed towards the delivery of outcomes beyond paper-based reviews. By combining their expertise in GRC and security engineering, Foresight was able to provide holistic and practical results which added value for the client.

The outcome

Foresight demonstrated an excellent track record in completing the requested services within expected (and often narrow) timeframes. This was illustrated by the additional engagements won by Foresight to conduct further security assessment and advisory work on other systems within the client's ICT environment.

The Department noted the Foresight team's results-oriented approach and multi-faceted professional experience distinguished Foresight from other vendors. As such, Foresight is not only viewed as a third-party vendor, but a trusted advisor to the client organisation.

foresight.security

FORESIGHT