FORESIGHT

Strategic Advisory Case Study

A risk-based approach to strategic roadmap development

Summary

A major Australian Government department ("the Department") undertook numerous system-based security assessments, generating in an extensive number of findings. To help prioritise the resultant security remediation and uplift initiatives, the Department engaged Foresight to develop a strategic roadmap. Foresight applied both a top-down and a bottom-up approach to provide the Department with a holistic, risk-based and pragmatic strategic roadmap. Foresight collaborated with technology and business stakeholders to co-develop the roadmap. The outcome assisted the client with its investment and operational prioritisations while ensuring strategic congruency. The client has since engaged Foresight to provide similar services to its portfolio agencies.

Our client's challenge

As a major Australian Government department, the client has a commitment to continuous security improvement and ensuring its security posture is commensurate with its organisational risk tolerance level. The Department operates within a complex IT environment with numerous network segments and systems, requiring extensive security assessments. The security assessments undertaken by the Department have identified a number of disparate findings and recommendations. Further opportunities for synergy have arisen from several technology and business-led transformation and uplift initiatives across the organisation. Against this backdrop, the Department identified the need for a synthesised and holistic strategic roadmap to enable effective prioritisation of limited resources while managing competing demands and compliance requirements.

Scope of engagement

In response to the challenges faced, the Department approached Foresight to devise a practical and risk-informed solution to enable the development of a coherent strategic roadmap, while ensuring an appropriate level of stakeholder engagement. To deliver this outcome, the Department required a maturity assessment against the Australian Cyber Security Centre (ACSC) Essential Eight (E8) mitigation strategies, an entity-level compliance assessment against the Australian Government Information Security Manual (ISM), and a security risk assessment coupled with the development of a Security Risk Management Plan (SRMP). With a better understanding of the Department's current security posture, a Strategic Roadmap was to be developed to help guide the organisation to its target security posture.

How Foresight helped?

Foresight commenced the engagement with the E8 maturity assessment and the ISM compliance review, followed by the development of the SRMP, integrating insights from both reviews. These deliverables provided the foundation for the development of the strategic roadmap. To avoid creating consulting shelf-ware which the client could not practically use or implement, Foresight adopted a co-design approach and engaged stakeholders from various areas (business, technology and security) to partake in the roadmap development workshop. This forum provided an open and collaborative environment for stakeholders to identify key strategic priorities in line with the Department's broader objectives and overall risk appetite.

Foresight was able to distil the myriad of risks identified in previous security assessments into several key strategic risks and core mitigation strategies. This allowed the Department to adopt an intuitive "t-shirt sizing" approach to prioritising initiatives based on risk, effort, cost, benefit, dependencies, and related initiatives.

Foresight developed a strategic roadmap based on the outcomes from the workshop. The strategic roadmap provided the Department with a practical way forward and was supported by a detailed plan to implement the various work packages within.

The outcome

The strategic roadmap developed by Foresight helped the Department navigate its competing priorities and devised a clear path forward for improving information security within the organisation. This strategic roadmap also helped deconflict other dependent or complementary initiatives already underway.

The Department has since engaged Foresight to complete further strategic advisory and governance, risk, and compliance work. The Department has also approached Foresight to provide similar services to its portfolio agencies ,replicating the proven methodology from this engagement.

foresight.security

FORESIGHT