Capability Development and Profiling at DIIS

Project Description

The Department needed to define, measure and report on their security maturity and establish a baseline across people, information and assets. This included documented evidence of the assessment process. The client needed to demonstrate change in staff capability, confidence knowledge and security behaviours across a specified timeframe.

A new Protective Security Policy Framework (PSPF) was launched which required all Federal agencies to monitor, assess and report to the Attorney-General on the maturity of their security capability and risk culture.

Cyntropy conducted the user research, designed the assessment tool (including survey design and factor analysis), conducted alpha and beta testing, evaluated and interpreted the results.

Approach

Cyntropy assisted the Department in defining, measuring and reporting on user behaviours, motivation and knowledge (enabling the delivery of the Government's Protective Security Requirements).

The project was phased and consisted of these components:

- stakeholder identification and interviews
- user profiling
- assessment criteria and assessment tool design
- alpha and beta testing of the assessment tool
- survey go-live and user response (whole-of-agency)
- results analysis
- recommendations and report.

Phase 1

The first project phase involved analysis of current data sources, defining relevant user groups and personas. Based on the user groups, we iteratively developed the maturity assessment criteria and designing a tool that would capture the motivations, knowledge and behaviours of each user group.

The PSPF places additional requirements on senior leaders to foster a positive security climate. A separate component was developed to assess this cohort, with several iterations (based on alpha and beta testing).

Phase 2

Using the assessment outcomes, we conducted further analysis of user profiles and established baseline profiles – including user motivations, knowledge and behaviours.

We produced a journey map for the client assisting their user groups to come on the compliance journey, through voluntary change to their motivations, knowledge and behaviours.

To ensure continual improvement, Cyntropy aligned the service design with the PSPF and the Federal Cyber Security Framework. We statistically validated the survey and response to ensure validity of the process.

Client

Department of Industry, Innovation and Science (DIIS)

The Department's mission is supporting economic growth and job creation for all Australians.

Timeframe

May to August 2018

Responsibility

Whole delivery: user identification and analysis, assessment tool design, testing, results interpretation and recommendations.

Areas of expertise

- user identification, research, profiling and design
- ideation
- agile delivery
- governance and compliance

Scale

- 2,400 users surveyed
- national workforce
- physical security
- personnel security
- information security

Outcomes

First independent, whole-of-agency security capability baseline, with evidence of security maturity assessment and evaluation.

Compliance with PSPF monitoring, assessment and reporting requirements.

Repeatable method of assessment and evaluation, easily allowing the client to repeat the survey and measure evidence-based cultural improvements.

Actionable insights: identified actions to take and areas requiring further exploration.

User-specific journey maps for behavioural change (non-invasive governance).