Cybersecurity

The Brief

Recent cyber attacks have highlighted a global trend towards cyber terrorists targeting utility providers. While the client had plans to deal with malicious acts such as viruses and malware attacks, they required additional plans and capabilities to deal with the ever-evolving threat and sophistication of cyber attacks.

Our client, a Government–owned water utility with over 700 permanent staff and approximately $1 billion in annual turnover, approached Business Analysts Pty Ltd (BAPL) to assist them in starting a holistic program of cybersecurity improvement workstreams for the 2018/19 financial year. The programs relate to improving their resilience against cyber attacks that could potentially affect the information and communications technology (ICT) and operational technology (OT) functions of the utility.

The Challenge

The client faced the following challenges:

- An external audit had identified several improvement areas, and a business case was required to enable further funding for the additional remediation activities. develop an understanding of the sequence of functions/events

- Other workstreams were identified as being critical for improving cybersecurity resilience across the organisation. Each of these workstreams would require analysis and project initiation. Areas included:

    - current strategy, architecture, and governance

    - disaster recovery and business continuity plan

    - identity and asset management solution

    - security awareness campaign across the business

    - threat detection for both ICT and OT assets.

Our Approach

With over 10 years of in-depth experience providing consulting services, BAPL are experts at building capability and delivering business analysis services within organisations. Our large team of experienced consultants has an enviable track record in delivering outcomes based on excellent business analysis. Our consultants tailor-make your initiatives to ensure you achieve true business value.

BAPL performed an environmental scan to better understand the context of cybersecurity threats faced by utility providers globally, and to understand best-practice approaches and align these to the audit results. This was followed by stakeholder identification sessions to ensure the client fully understood the depth and breadth of potential issues.

With the scope and alignment to business needs confirmed, BAPL initiated a more in-depth analysis of the issues through regulatory analysis, ideation workshops, and a review of existing processes.

Through iterative writing and delivery approaches, BAPL successfully delivered multiple business cases tailored to both the client's immediate needs and their long-term plans.

The Outcome

Some of the key successes included:

- completion of six business cases, including budgetary requirements, business needs, and justification for investment

- completion of a 'program on a page' template that presented a high-level overview of the workstreams and how they align to the business needs increase in IP retention rates

- successful management of changes to scope as the business cases evolved from a single heavyweight business case to several lightweight business cases.

From the client:

'Thank you so much for the value you brought to our project. It has certainly been very productive and will inform a lot of decisions going forward much better than if I had just gone on what I knew superficially.'

Melbourne　　　　**Sydney**　　　　**Brisbane**　　　　**Canberra**　　　　**Adelaide**