Combating Cyber Threats

Case Study

Business Aspect helped assess the security vulnerabilities and plan a program of work focussed on strengthening the cyber security capability of one of Australia's largest financial services organisations.

Situation

In a world where cyber attacks are the new norm, cyber security is an integral component of every organisation's security and risk management approach. As a trusted provider of financial services and solutions our client understood that protecting confidential customer data and continuity of service is critical to their ongoing success.

The executive team wanted a realistic picture of the current state of business readiness to deal with the increasing variety, sophistication and volume of attacks. Through an independent review, they could address any weaknesses and build resilience for the future.

Business Aspect was engaged to help because of its trusted thought leadership in cyber security and extensive knowledge of financial services.

Solution

The project was delivered in two phases:

1. Conducting an assessment of the client's information security framework, and

2. Undertaking a Risk Assessment focussing on cyber security vulnerabilities.

Business Aspect engaged with management stakeholders to assess the impacts of threats and to solicit information on the current control environment, including management, administrative and technical controls.

Key outputs of the project included:

- Information Asset Identification: to initiate an Information Asset Register.

- Risk Identification: Identifying business, strategic, technical, operational and informational risks.

- Risk Analysis inclusive of a Likelihood Assessment, Impact Assessment and Risk Appetite Assessment.

- Risk Assessment Report and associated roadmap containing key findings and recommendations.

A series of risks were identified, analysed and documented and presented in a Risk Register. Risks were contextualised based on confidentiality, integrity and availability of systems. Ratings were defined based upon the client's Operational Risk Management Standard and assessed in the context of the client's business.

Recommendations were targeted at establishing processes and controls to identify, detect, protect, respond, and support recovery from information security incidents.

Processes were designed to leverage the client's information security framework and the recommendations aligned with accepted Industry and Security Frameworks such as NIST, ISO27001:2013 and the Australian Prudential Regulatory Authority (APRA) requirements.

BUSINESS ASPECT

A Fresh Perspective

Combating Cyber Threats

Case Study

Outcome

The client received a comprehensive risk review including identification of high priority risks and recommended mitigation measures as a part of a security program of work. A risk register toolset was also delivered which provides the client with the ability to continue to record risks and manage their associated risk ratings as well as monitoring the progress of risk mitigation activities.

Business Aspect also delivered a Cyber Risk Management Framework, Risk Assessment Practitioners Guide, Risk Register and a range of supporting recommendations consistent with best practice risk management and relevant sector based regulatory frameworks.

The assessment revealed existing vulnerabilities and prepared the client to take steps to attain the highest levels of protection for their customer data into the future.

Business Aspect
A Data#3 Company

1300 06 06 42

www.businessaspect.com.au

BUSINESS ASPECT
A Fresh Perspective