CASE STUDY

Comprehensive Cybersecurity Governance Program with Brace168's CISOaaS

The Company

This client is a pure online retail business that is set up to make specific products more accessible to everyone, no matter where they are in the world.

Being 100% online provided the company with the opportunity to disrupt the traditional brick-and-mortar setup within the industry, but it also meant that cybersecurity risks were high and arose across every facet of the business.

The company experienced continuous growth and success as it doubled in size each year. This success was

bolstered by the use of innovative supply chain models that removed the overhead costs from carrying stock.

Because their core business was dependent on these supply chains, any disruption to it due to cybersecurity incidents would have a significant impact on the company's operations and overall brand reputation.

Customer Scenario

The client wanted to reassure its Board that customers could be confident using their brand's online platform and that the company had taken reasonable steps to protect their environment from the impacts of any cybersecurity incident or breach.

However, it was difficult for the company to find internal resources with sufficient expertise to cover all aspects of cyber risk mitigation and develop a suitable governance program to manage these risks on an ongoing basis.

The Solution

By using Brace168's CISO as a Service (CISOaaS), the company was able to assess risks, understand gaps, prioritise mitigation activities and execute a program of work - all tracked through a bespoke and overarching governance framework.
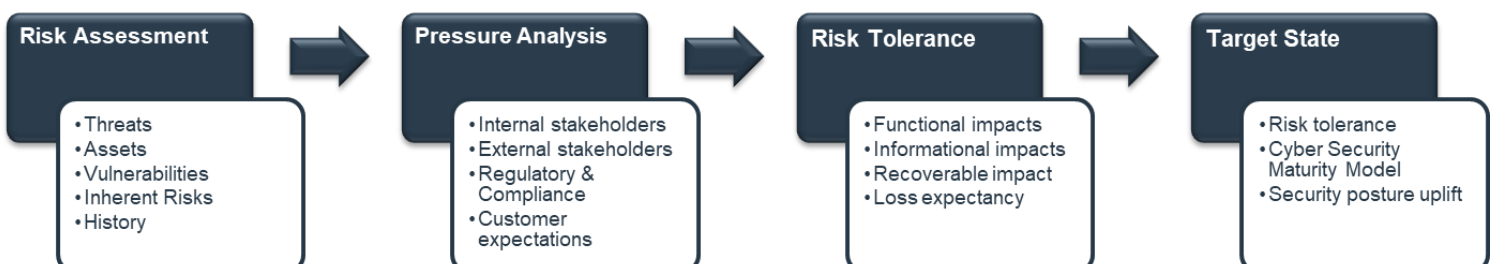
Brace168's extensive range of skills and expertise equipped the company with a more efficient and cost-effective delivery of a governance program that was beyond what their internal resources could have achieved.

The Outcome

Brace168's CISOaaS engagement put the company well on the path to a comprehensive, reliable and mature cybersecurity governance framework.

The identification, assessment and tracking of risks through a risk register has resulted in a 25% reduction of identified risks in just six months, giving the Board the confidence that the management of the company's cybersecurity risks are in capable hands.

Your guided cyber security journey

Risk Assessment
- Threats
- Assets
- Vulnerabilities
- Inherent Risks
- History

Pressure Analysis
- Internal stakeholders
- External stakeholders
- Regulatory & Compliance
- Customer expectations

Risk Tolerance
- Functional impacts
- Informational impacts
- Recoverable impact
- Loss expectancy

Target State
- Risk tolerance
- Cyber Security Maturity Model
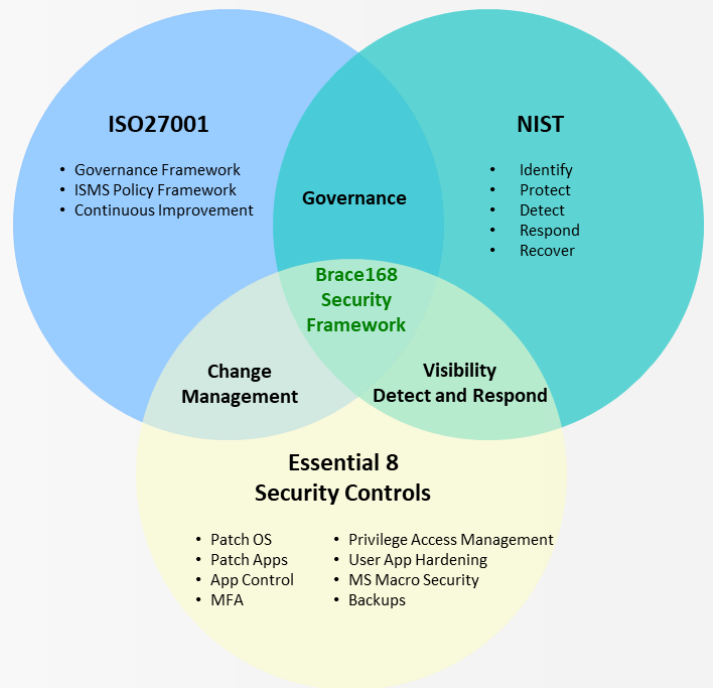- Security posture uplift

How does it work?

The CISOaaS provided by Brace168 has enabled the company to benefit from subject matter experts who deliver specialist tasks and services all within the overall framework. Through CISOaaS, the client has also been able to implement a cybersecurity governance framework and achieve best practice cybersecurity risk management practices with an efficient and transparent approach.

Brace168's CISOaaS helped the client identify both short-term projects which allowed for fast mitigation of risks with low-cost requirements and minimal controls, and a longer-term program that addresses the more challenging areas. All of these have been tracked through a transparent process of reporting to the Board through Senior Management.

The CISOaaS solution utilised well-regarded industry frameworks such as ISO27001, NIST and the ACSC Essential 8 to determine the optimal steps for the company to take. This prevented the client from spending precious time and effort on activities that did not practically improve the overall cybersecurity posture.

Brace168 also ensured that every deliverable and outcome was documented and tracked to provide the company with records that could trace decisions and responsibilities for all aspects of the cybersecurity governance program.

ISO27001
- Governance Framework
- ISMS Policy Framework
- Continuous Improvement

NIST
- Identify
- Protect
- Detect
- Respond
- Recover

Governance

Brace168 Security Framework

Change Management

Visibility Detect and Respond

Essential 8 Security Controls
- Patch OS
- Patch Apps
- App Control
- MFA
- Privilege Access Management
- User App Hardening
- MS Macro Security
- Backups

CISOaaS is both proactive and reactive in safeguarding your business against cyber threats

---

Requirements

Brace168 had to implement an effective cybersecurity governance program that would:

- apply an appropriate, fit-for-purpose, cybersecurity framework to inform the assessment process for applications and their ERP platform

- undertake an "as is" assessment of the organisation's security posture

- determine the desired state in the short, medium and long-term

- complete and maintain a gap analysis of the current state to the target state

- plan and manage a program of work to close identified gaps according to agreed priorities

- inform and obtain guidance from management and the board on the current risk, finalise the risk mitigation plans and track progress in addressing the risks to reach the target state.

The company also wanted to establish necessary contemporary security practices and techniques within its teams.

Opportunities for Enhancement

The CISOaaS solution identifies what needs to be done to reduce cybersecurity risks.

In this case study, the company needed to work on a clear set of actions including Infrastructure Upgrades (FW, WAF, Endpoint), User Awareness Training, Managed Detection and Response, and Penetration Testing.

Brace168 has successfully supported them in accomplishing cybersecurity activities where the company did not have the specific capabilities to achieve on their own.
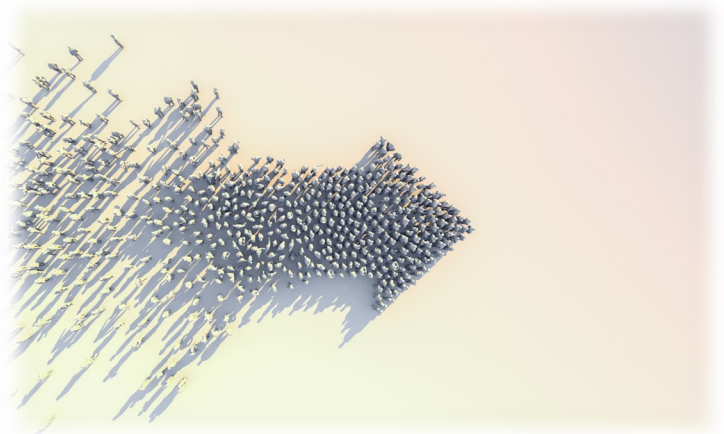
CISOaaS puts cybersecurity at the forefront of any business

Brace168