CYBERSECURITY

365 ARCHITECHS

Information Sheet

Cybersecurity Governance

Tags: Cybersecurity, Governance

Who is responsible for cybersecurity in any organisation? What mechanisms are in place to oversee cybersecurity operations? To what extent should organisations engage third party providers, or should cybersecurity be kept in-house? What policy frameworks, what projects and what level of reporting is appropriate? Which standards, frameworks or guidelines should be followed? All the above questions are within the domain of cybersecurity governance.

The answers to the questions raised above generally depend on the nature, size and risk appetite of individual organisations. However, the governance of cybersecurity is essential for all.

Responsibility

Ultimately, the governing board of Board of Directors of an organisation is responsible for ensuring effective governance of cybersecurity risks. This typically involves delegating operational activities to management, who may in turn engage specialist third party providers for some or all cybersecurity functions.

It is important to note that cybersecurity is a different skillset to IT operations. Cybersecurity may also encompass data privacy. In some organisations, responsibility for these domains rest with accounting, legal, technology or operational teams. It should not be taken for granted that cybersecurity is an "IT" issue.

Frameworks and Standards

A range of different cybersecurity frameworks and standards are available that organisations can choose to align to. They represent agreed methodologies for developing defences to protect against cyber risks.

Common frameworks and standards include:

- Microsoft Secure Score
- NIST Cybersecurity Framework
- Australian Cyber Security Centre (ACSC) Essential Eight
- ISO27001: Information Security Management

See Information Sheet: Cybersecurity Frameworks and Standards.

Policies

It is good practice for a series of cybersecurity policies to be established, documented and shared to ensure that there is agreement and alignment between projects and activities designed to manage cyber risks.

Projects

Cybersecurity projects should be undertaken within a strong discipline of project management, inclusive of stakeholder management, issue management, quality management and risk management.

Reporting

Organisations should consider the appropriate frequency, level of detail and information to be included in reporting against cybersecurity events, projects, plans and activities.

Regular reporting should be made available to management as well as governing bodies, to ensure that cyber risks are being managed within risk appetites.

About us
365 Architechs is a technology company based in Brisbane, Australia. We deliver solutions to support organisations on their digital transformation including cloud, modern applications, cybersecurity and artificial intelligence to drive profitability, growth and achievement of strategic objectives.
(07) 3393 1186 | www.365a.com.au | sales@365a.com.au

Disclaimer
These Information Sheets are designed to provide general information only. They should not be relied upon without consulting professional advice on your specific circumstances. 365 Architechs will not be held liable for any acts or reliance upon the information provided contained within.