CYBERSECURITY

365 ARCHITECHS

Information Sheet

Five Pillars of Security Controls

Tags: Threat Actors, Attack Vectors, Vulnerabilities, Cyber Defences, Cyber Risks, Cybersecurity Governance

To protect against today's modern threats, organisations need a layered approach to cybersecurity, inclusive of identity management, threat protection, device protection, information protection and security management. These five pillars of cybersecurity can be used to assist those charged with responsibility for cyber governance to ask questions and assess the maturity of cybersecurity controls in each of these areas and the overall cyber posture of the organisation to stay ahead of attackers.

Identity Management

It is critically important to ensure accounts are authenticated prior to granting access to organisational data - ensuring that only the right users are able to access the right systems and data at the right time.

Identity and Access controls include password policies, limiting administrator access, multi-factor authentication, single sign-on and risk-based conditional access.

Threat Protection

The range of potential cyber threats being faced by every organisation is continually on the rise.

Threat protection controls include automatic patching of operating systems and applications, anti-virus and anti-malware software, spam protection and advanced threat protection.

Device Protection

Desktop computers, laptops, notebooks, tablets and smartphones are vulnerable to attack.

Ensuring these devices are centrally managed is the first step to protecting them and also provides an opportunity for automated configuration and management.

Device protection includes mobile device management, device encryption and automated updates and patching.

Information Protection

In addition to protecting systems and devices, it is critical to place protection around individual documents and data stored within the technology systems. This ensures that data remains protected even when outside the corporate firewall.

Information protection includes Email Online Protection, Data Loss Prevention, backups and Information Rights Management.

Security Management

Security software and applications can only go so far in protecting the valuable digital assets of an organisation.

Regular review of security audit logs can identify when actions are to be taken to adjust security settings.

Security management includes audit log reviews, tuning of security parameters and regular reporting of security incidents, activities and performance against targets.

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 3999 7000 | www.365a.com.au | sales@365a.com.au