CYBERSECURITY

Information Sheet
Cybersecurity

365 ARCHITECHS

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

It is inevitable that all organisations today face significant cybersecurity risks that require strong defences to mitigate the consequences of cyberthreats. Cybercriminals operate to disrupt operations, harm reputations and steal information. Organisations must identify attacks, protect information and systems, address vulnerabilities, contain breaches, respond to attacks and recover from security incidents or face significant penalties and reputational damage.

Cybersecurity is not the responsibility of IT teams alone – everyone has a part to play. In fact, many cybersecurity issues require specialist knowledge and skills outside the traditional skills and training of IT teams, so consideration should be given to expert resources where required.

This information sheet provides an introduction to the various terms and issues surrounding cybersecurity and offers an overview of each.

Threat Actors

The governments, organisations and individuals who engage in cybercriminal activities are known as Threat Actors. They include casual criminals, professional hackers, nation states, activists, insiders and child hackers. See Information Sheet: Threat Actors.

Attack Vectors

Attacks are initiated by Threat Actors using Attack Vectors. These are the methods used to penetrate systems to gain access to resources and data to commit cybercriminal activities. They include a range of network threats, host threats, application threats and social engineering. See Information Sheet: Attack Vectors.

Vulnerabilities

All systems, networks, databases and applications have vulnerabilities which can be exploited by threat actors using attack vectors. Vulnerabilities can be managed by reducing the attack surface by deploying cyber defences. See Information Sheet: Vulnerabilities.

Cyber defences

Cyber defences act to mitigate the risks associated with cyber attacks and fall into categories such as:

Identity and access controls	Threat protection	Device management	Information protection

Cyber risks

The combination of attack vectors, likelihood and consequences can be presented as cyber risks. Using a risk-based view of threat actors, attack vectors and vulnerabilities, organisations can develop a measured response to dealing with cybersecurity issues and managing appropriate investment in cyber defences.

Cybersecurity Governance

Governing bodies should ensure appropriate oversight of cybersecurity governance arrangements including:

Cybersecurity			
Frameworks	Policies	Projects	Reporting

See Information Sheet: Cybersecurity Governance.

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