

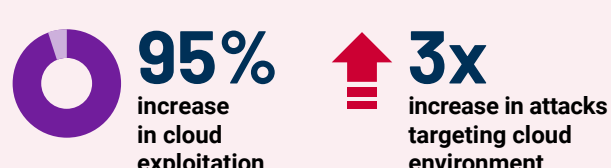
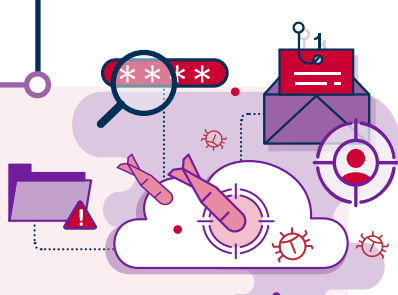
Cloud Security Companion Guide For Cyber Trust

Key shifts and cybersecurity challenges when organisations move to the cloud



	Shared Responsibility Model (SRM)	Large no. of SaaS subscriptions ("SaaS sprawl")	Business-led SaaS (Potential "shadow IT")
Changes	<ul style="list-style-type: none"> Cloud users and providers now take on joint responsibility 	<ul style="list-style-type: none"> Many standalone, potentially silo-ed subscriptions to manage 	<ul style="list-style-type: none"> Different business units directly manage their own SaaS
Cybersecurity challenges	<ul style="list-style-type: none"> Cloud users misunderstand that cloud providers take care of everything 	<ul style="list-style-type: none"> Difficult to scale the management of large number of SaaS subscriptions <p>SaaS - Software-as-a-service</p>	<ul style="list-style-type: none"> Subscriptions may not comply with organisation's cybersecurity processes Business users unaware of cloud security best practices

Evolving tactics of attackers to target cloud environment

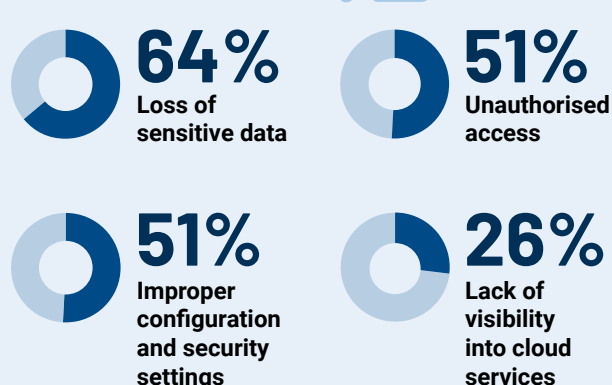


Source: CrowdStrike report

Key attack vectors

- Cloud **credentials** and **identities** targeted
- Lateral movement** across cloud environment
- Cloud **misconfiguration abuse**

Key security concerns of cloud users



Source: Cloud Security Alliance report

Cyber Trust mapping to Cloud Security Alliance Cloud Controls Matrix

This visualisation depicts the mapping of each of the cybersecurity preparedness domains in the Cyber Trust mark to the control specifications in CCMv4.



Cyber Trust Domains	Application & interface security	Audit & assurance	Business continuity management & operational resilience	Change control & configuration management	Cryptography, encryption & key management	Datacenter security	Data security & privacy lifecycle management	Governance, risk & compliance	Human resources	Identity & access management	Infrastructure & virtualisation security	Logging & monitoring	Security incident management, e-discovery & cloud forensics	Supply chain management, transparency & accountability	Threat & vulnerability management	Universal endpoint management
Access control										High						
Anti-virus/anti-malware																
Asset management																
Audit		High														
Backups																
Bring Your Own Device (BYOD)																High
Business continuity/disaster recovery			High													
Compliance		High														
Cyber strategy																
Cyber threat management													High			
Data protection & privacy					High		High									
Governance								High								
Incident response													High			
Network security											High					
Physical/environment security						High										
Policies & procedures								High								
Risk management								High								
Secure Software Development Lifecycle (SDLC)	High			High												
System security	High			High								High				
Third-party risk & oversight														High		
Training & awareness									High							
Vulnerability assessment															High	

Extent of mapping: Low High

Get started with implementing cloud security



Find out more

www.csa.gov.sg/cloudsecurity

[f](https://www.facebook.com/csasingapore) [in](https://www.linkedin.com/company/csasingapore)

@csasingapore