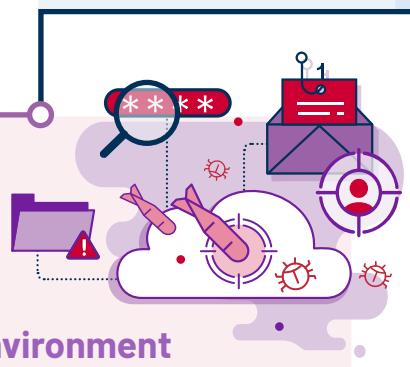
CYBER ESSENTIALS

Cloud Security Companion Guide
For Cyber Essentials

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	• Cloud users and providers now take on joint responsibility	• Many standalone, potentially silo-ed subscriptions to manage	• Different business units directly manage their own SaaS
Cybersecurity challenges	• Cloud users misunderstand that cloud providers take care of everything	• Difficult to scale the management of large number of SaaS subscriptions	• Subscriptions may not comply with organisation's cybersecurity processes • Business users unaware of cloud security best practices

SaaS - Software-as-a-service



Evolving tactics of attackers
to target cloud environment

95% increase in cloud exploitation

3x increase in attacks targeting 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

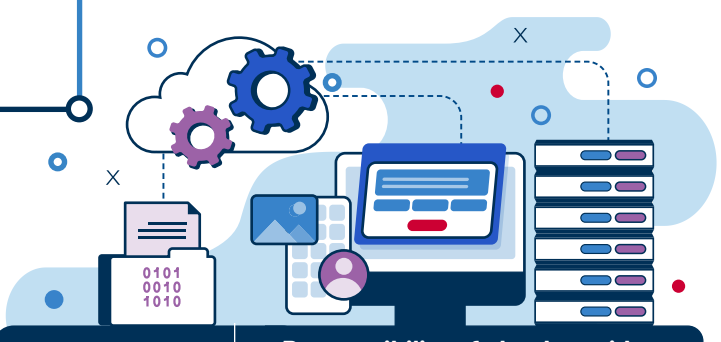
64% Loss of sensitive data

51% Unauthorised access

51% Improper configuration and security settings

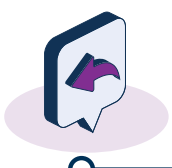
26% Lack of visibility into cloud services

Source: Cloud Security Alliance report



SRM for Cyber Essentials
For SaaS users

- SaaS user responsibility
- Cloud provider responsibility

			Responsibility of SaaS user	Responsibility of cloud provider	
				SaaS provider	Cloud infrastructure provider
Assets		People			
		Hardware and software			
		Data	• Data within SaaS	• Ensure data in the cloud is online	
Secure/Protect		Virus/malware protection		• Protection of SaaS application(s)	• Protection of host infrastructure
		Access control			
		Secure configuration	• User settings in SaaS • Management of logging	• Application-level configuration • Ability to enable logging	• Host infrastructure configuration
Update		Software updates		• Update of SaaS application(s)	• Update of host infrastructure
Backup		Back up essential data	• Backup of organisation's essential data within SaaS	• Backup of SaaS application(s)	• Backup of host infrastructure
Respond		Incident response			

Notes

- Scope of SRM for companion guide focuses on responsibilities of end-user organisations subscribed to SaaS – organisations shall also refer to the SRM published by their respective cloud providers.
- Beyond the SaaS subscriptions, end-user organisations shall continue to be responsible for the cybersecurity of their respective local environment.
- Whilst the SRM has not outlined the respective responsibilities of the cloud providers, they are expected to implement their respective cybersecurity measures and provide assurance of their own cybersecurity posture to their cloud customers — this is also mentioned in the companion guide.

Get started with implementing cloud security

- **Cyber Essentials**
- **Cloud Security Companion Guide for Cyber Essentials** — SRM in the cloud for SaaS users
- **Cloud provider-specific practices**

Find out more
www.csa.gov.sg/cloudsecurity

@csasingapore