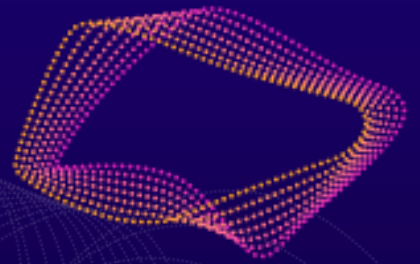
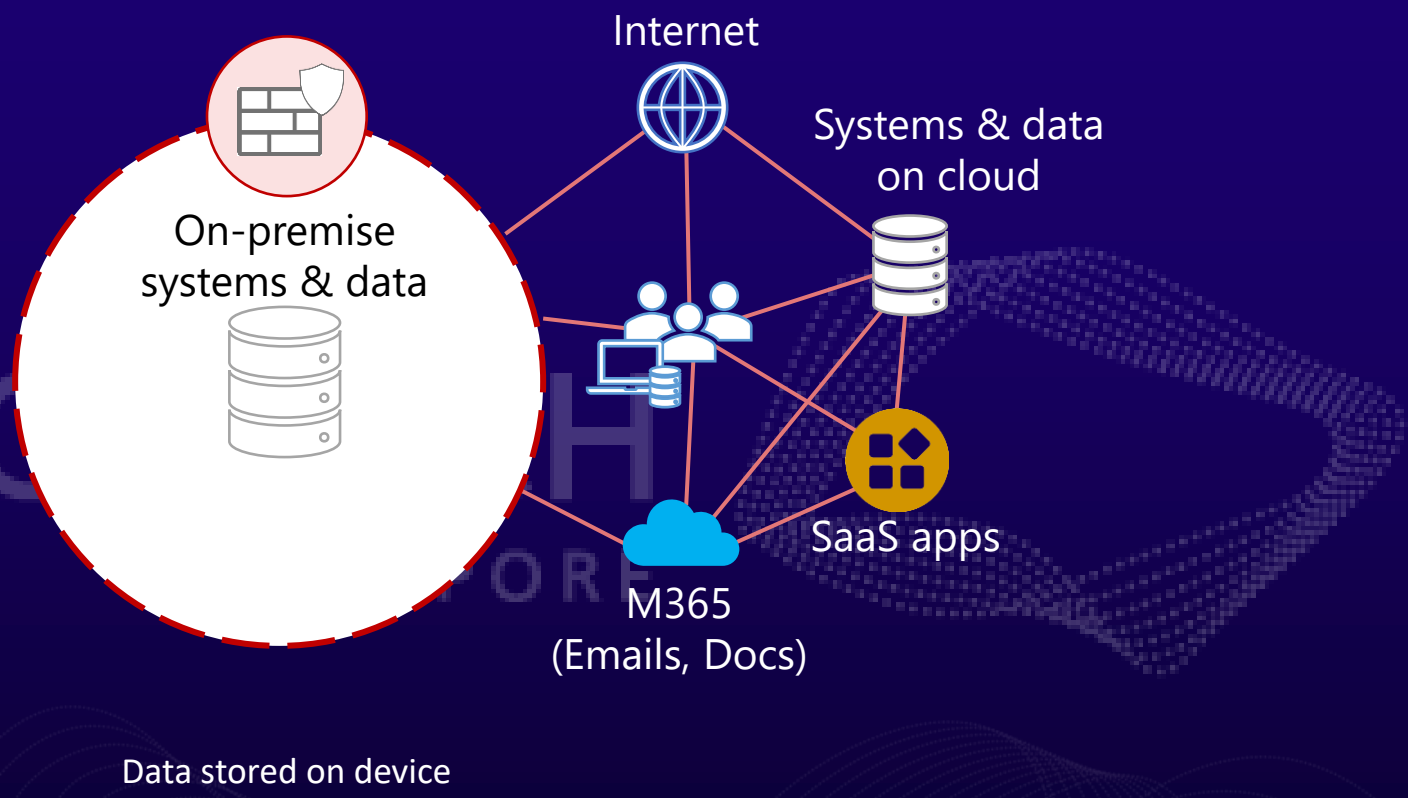
The Government's Risk-Based Approach to Mitigate the Risks of Using the Cloud



Chai Chin Loon
Senior Director (Cyber Security Group)
Government Chief Information Security Officer (GovTech)

Yes or no?

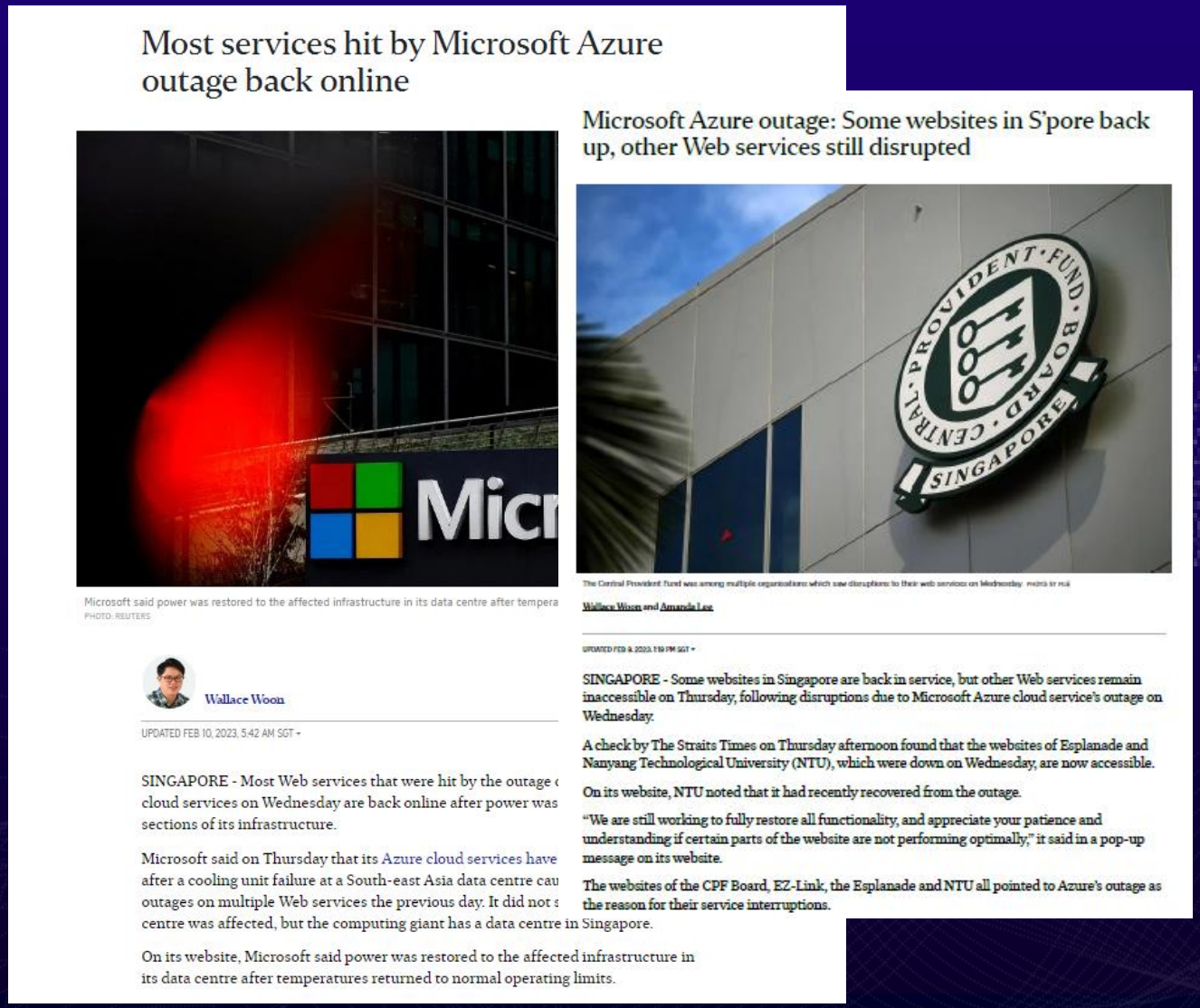


Does your organization have a cloud-first strategy?

Of the organizations using cloud services, more than 75% indicate they have a cloud-first strategy.

- Gartner

Are You Aware of the Risks that Come Along with Using the Cloud?



Most services hit by Microsoft Azure outage back online

Microsoft said power was restored to the affected infrastructure in its data centre after tempera

PHOTO: REUTERS

Wallace Woon

UPDATED FEB 10, 2023, 5:42 AM SGT

SINGAPORE - Most Web services that were hit by the outage
cloud services on Wednesday are back online after power was
sections of its infrastructure.

Microsoft said on Thursday that its Azure cloud services have
after a cooling unit failure at a South-east Asia data centre cau
outages on multiple Web services the previous day. It did not s
centre was affected, but the computing giant has a data centre in Singapore.

On its website, Microsoft said power was restored to the affected infrastructure in its data centre after temperatures returned to normal operating limits.

Microsoft Azure outage: Some websites in S'pore back up, other Web services still disrupted

The Central Provident Fund was among multiple organisations which saw disruptions to their web services on Wednesday.

Wallace Woon and Amanda Lee

UPDATED FEB 8, 2023, 1:19 PM SGT

SINGAPORE - Some websites in Singapore are back in service, but other Web services remain inaccessible on Thursday, following disruptions due to Microsoft Azure cloud service's outage on Wednesday.

A check by The Straits Times on Thursday afternoon found that the websites of Esplanade and Nanyang Technological University (NTU), which were down on Wednesday, are now accessible.

On its website, NTU noted that it had recently recovered from the outage.

"We are still working to fully restore all functionality, and appreciate your patience and understanding if certain parts of the website are not performing optimally," it said in a pop-up message on its website.

The websites of the CPF Board, EZ-Link, the Esplanade and NTU all pointed to Azure's outage as the reason for their service interruptions.

Key Learning Points

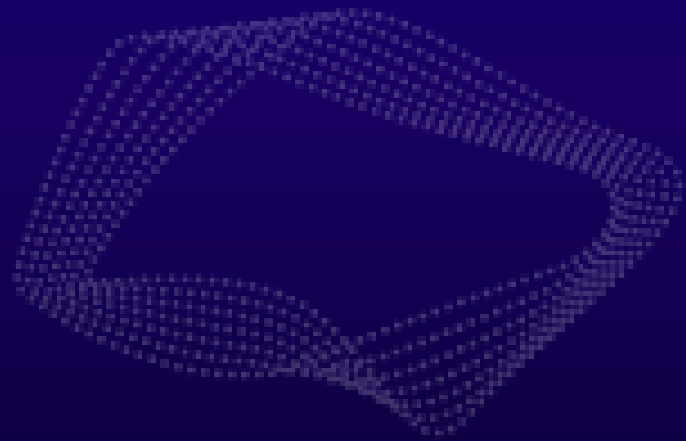
(1) Some assumptions we had about the reliability and resiliency of the Cloud were not validated

(2) Importance of Service Level Agreements and Business Continuity Plans (BCP)

(3) Validate readiness through regular Incident Response, BCP and Disaster Recovery exercises

We Classify Cloud Risk into Four Main Categories

1. **Supply chain risks**
2. **Cloud sovereignty risks**
3. **Concentration risks**
4. **Resiliency risks**



**Note: The four risk categories highlighted above are the key areas prioritized by the Government. However, they are only a portion of all other types of Cloud risks.*

Potential Residual Risks for the Use of Cloud Services

Supply Chain Risks

The Government **relies** on the CSPs to defend their services from third-party threats, including their ability to **react in a timely manner** and **alert the affected system owners** when such attacks occur.

Cloud Sovereignty Risks

The Cloud could be "**weaponized**" if CSPs unilaterally deny or withdraw services, either on behalf of their home nation or out of their own will.

Potential Residual Risks for the Use of Cloud Services

Concentration Risks

Significant dependency on the CSPs, whereby the Government is **vulnerable** to the CSPs' **ability to maintain resiliency** of their cloud services.

Resiliency Risks

Concerns the **lack of backups** to **maintain availability** in the event of **CSP failure**.

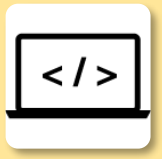
How the Government Addresses These Risks

People

1) Hone up competencies and expertise in cost tracking to facilitate **budget management**.
2) Build and leverage the community of practice in **cloud engineering** and **security** domain.

Process

1) Employ **soft levers** through **contract agreements**.
2) Be prepared for risk scenarios specific to Government services by covering them in our **Business Continuity Plan**.
3) Perform BCP/DRP exercises to **validate data and system backup processes**, and **recovery measures**.



Technology

1) Leverage on **multi-AZ** and **multi-cloud strategies** to maintain high availability.
2) Build **interoperability** & **portability** for multi-cloud readiness.

1) Assess **total risks** when considering which CSPs to use, and **adjust policies and contracts** to manage risks to the Government. Importance of implementing **cloud security policy** into **contractual requirements and cloud practice**.
2) Tap on dashboards/reports to do **continuous risk analysis and planning** to ensure the **operational readiness** of the cloud environment.

What More Can We Do to Leverage on Cloud Services Securely?

The Government's Move to Adopt the Zero Trust Framework that Covers End-to-End Digital Communication

GovZTA
Government Zero Trust Architecture

Identity

Strong Authentication and **Granular Authorization**

Device

Gain **greater identification, visibility** and **overall control** of all endpoints

Infrastructure

Break down into **Smallest Possible Trust Zones and Micro-Perimeters**

Application

Secure application sign-on managed through **on-demand sessions**

Data

Control data access throughout its lifecycle

Visibility & Automation

Gain insight of **all activities** across **all layers** to make **real-time decisions and** execute **policy-based response** at **speed**

**Note: GovZTA cannot mitigate all types of Cloud risks.*

How GovZTA Secures our Cloud Workload

Identity

Secure access with a single identity

a) Authorizing and authenticating through a **single identity**

b) Use **multi-factor authentication (MFA)** to verify identities

c) Use of **conditional access** and **risk scoring** to control access

techpass

Device

Enforce Posture Compliance

a) Use of Endpoint Detection & Response (EDR) tools to ensure **device health** before connecting to the **internal network**

b) Device management solutions to **secure mobile devices and applications**

SEED

Security Suite for Engineering Endpoint Devices

How GovZTA Secures our Cloud Workload

Infrastructure

Harden defenses, and detect and respond to threats in real time

a) Enhance **visibility** and provide **automated response** to specified alerts

b) **Micro-segmentation** through the use of **software defined policies**

c) Identify **how attackers move** within a network

Microsoft Azure

aws

Google Cloud

Secure Service Edge (SSE)

Application

Discover, control and protect applications from risks and threats across the cloud

a) Application **telemetry**

b) Use of **thin client application** to facilitate **single sign-on** with **session-based** access policies

c) **Micro-segmentation** for applications

shiphats

Data

Enforce the right protection actions based on data attributes

a) **Data tagging** and **loss protection**

b) **Ransomware proof** storage

Data Loss Protection Suite

How GovZTA Secures our Cloud Workload

Visibility & Automation (across all pillars)

Achieve near real-time and risk-based response to events

a) Enhance **detection and response capabilities** through continuous monitoring, automation and analysis from **sensors across the five pillars.**

b) Real-time dashboards help users to make **accurate, quick and sound decisions**.

Government Cyber Security Operations Centre (GCSOC)

Encourage Use of SG Tech Stack and Central Platforms to Leverage Built-in Security

shiphats

SEED DEEP

CloudSCAPE

Scan here to find out more!

Key Takeaways

1) The Government is well aware of the risks of using the Cloud and is constantly finding ways to enhance our security and resiliency posture

2) The Government has started adopting Zero Trust

3) The Government needs to partner with the industry

Join GovTech at our upcoming event: STACK Meetup 2023

Our Speakers:

CHAI CHIN LOON
Government Chief Information Security Officer, GovTech

BERNARD TAN
Director, GovTech

JAMES CHUA
Assistant Director, GovTech

DESMOND CHER
Senior Cybersecurity Engineer, GovTech

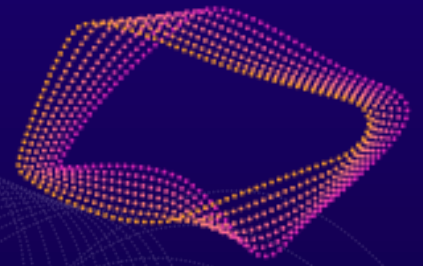
7:00PM – 8:30PM, 11 May 2023 (Thursday)

GovTech HQ

Scan here to find out more!

go.gov.sg/stackmeetuppage11may23

Thank You



GOVTECH
SINGAPORE