Module 2.4 Assignment

Submission by Group 2
on 2 Aug 2024

Define your Business

- We are an e-commerce (B2C) business selling men/women clothings, accessories, shoes, etc.
- We located in Singapore with markets in East Asia and Latin Americas.
- We have now 340 mil monthly visitors.

Define the threats if adopt IaaS

- Difficulty in getting the right technical infra resources due to a shortage or high-competition for talents globally
- Big budget and highly-specialized skills are needed to maintain and keep our ecommerce platform applications secure and safe from cyber-threats on an ongoing basis - the application challenge of secure-by-design requirement since the IaaS provider can only ensure the infra security
- Depending on cloud provider's data storage geographic locations, there may be compliance issue with regards to local data sovereignty laws in markets where we operate

https://spot.io/resources/cloud-security/iaas-security/#iaas-security

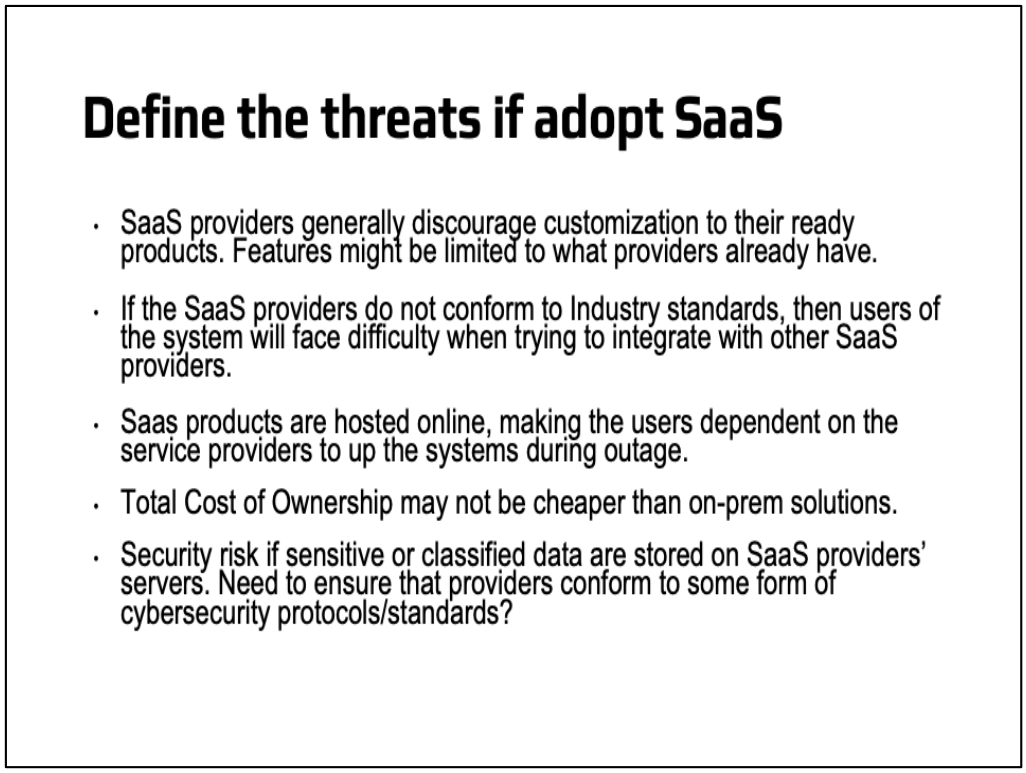
1. Limited Control
2. Security Misconfigurations
3. Escaping Virtual Machines (VMs), Containers, or Sandboxes
4. Compromised Identities
5. Compliance and Regulation Requirements

Define the threats if adopt PaaS

- Though PaaS approach can offer quick-time-to-market for our ecommerce platform, it also presents a high dependency on our cloud provider, AWS, who is also our competitor with Amazon.
- Potential cyber attackers exploiting vulnerabilities on the PaaS platform to gain control or steal sensitive data.
- If applications are not built using secure coding practices, it can result in security vulnerabilities within the application.
- As the complexity of the PaaS infrastructure increases, it can become difficult to achieve visibility, detect security threats, and understand how to mitigate them.

https://spot.io/resources/cloud-security/paas-security-threats-solutions-and-best-practices/#security-threats

1. Platform vulnerabilities
2. Application vulnerabilities
3. Limited visibility



https://spot.io/resources/cloud-security/7-saas-security-risks-and-how-to-prevent-them/#risks-concerns

1. Security misconfiguration
2. Cross-Site Scripting (XSS)
3. Insider threats
4. API security
5. Personal information
6. Account hijacking
7. Compliance requirements