



What happens when our suppliers migrate to the cloud?

Steve Williamson

Head of Internal Audit (Information Security and Data Privacy) - GSK

Steve Williamson

Worked in IT industry for 30 years

Originally from Scotland, I now live in Northamptonshire, UK

A curious technologist, hands-on learner and a travelling marathon runner.

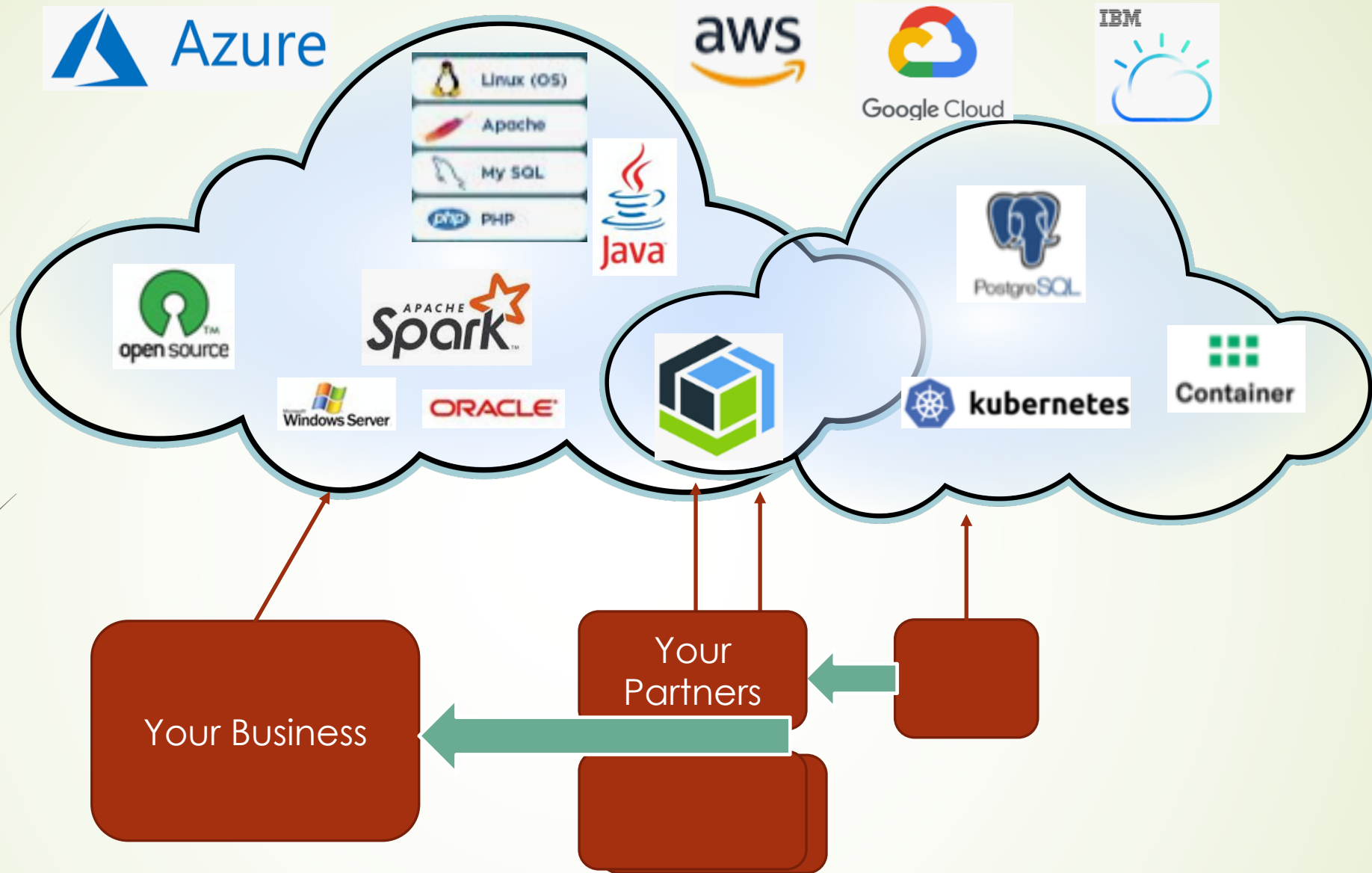


Growth in cloud adoption

	2018	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	41.7	43.7	46.9	50.2	53.8
Cloud Application Infrastructure Services (PaaS)	26.4	32.2	39.7	48.3	58.0
Cloud Application Service (SaaS)	85.7	99.5	116.0	133.0	151.1
Cloud Management and Security Service	10.5	12.0	13.8	15.7	17.6
Cloud System Infrastructure Services (IaaS)	32.4	40.3	50.0	61.3	74.1
Total Market	196.7	227.8	266.4	308.5	354.6

Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

Source: Gartner, 2019



93% of enterprises have a multi-cloud strategy¹

1. Source: Flexera State of Cloud Report, 2020

What can go wrong?

Verizon Data Breach: 6 million customer records when an employee of **Verizon partner** Nice Systems placed log information from customer service calls on a publicly accessible S3 server. ¹

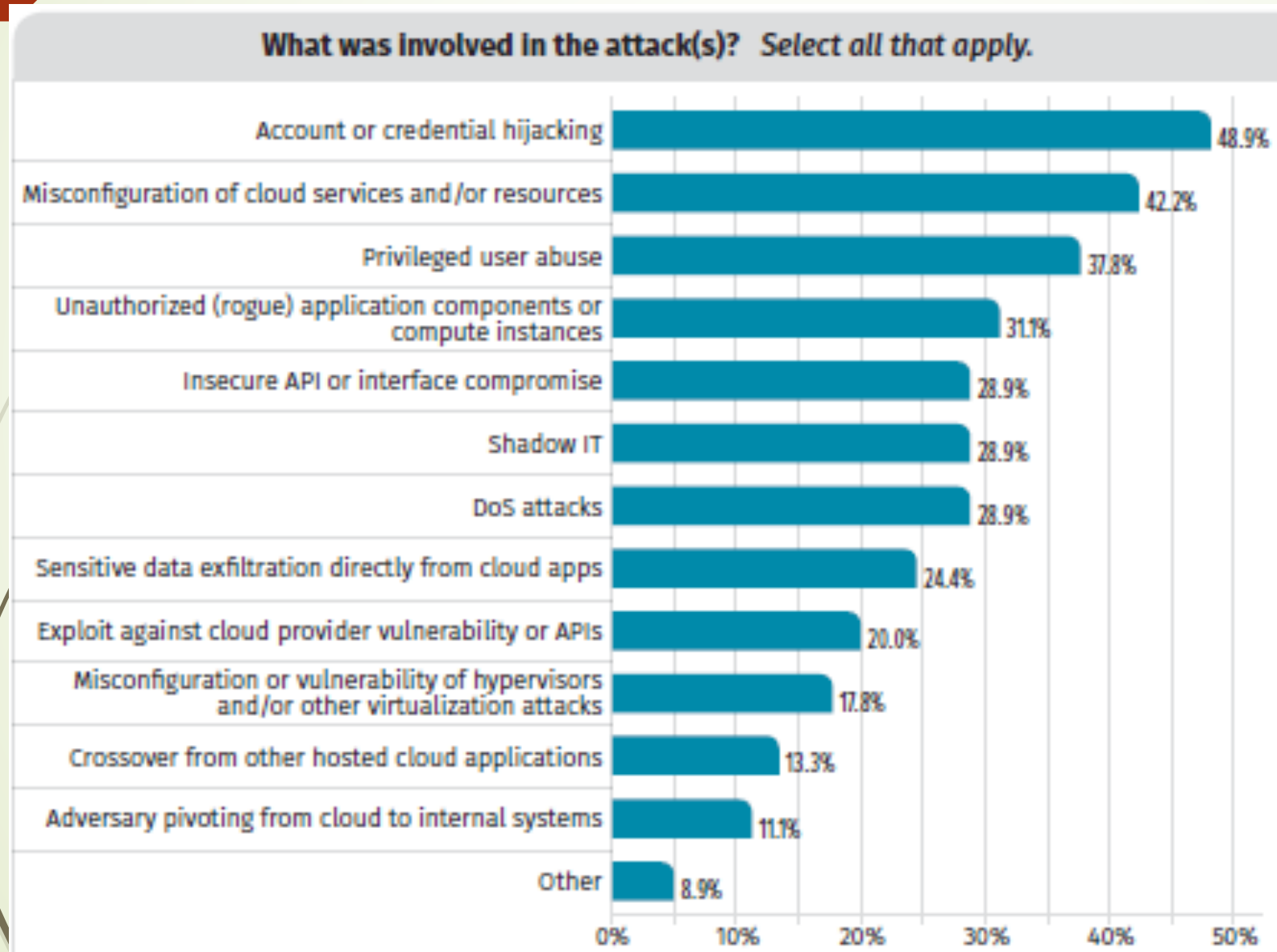
Lacework found 22,672 open admin dashboards; and more than 300 of them were unprotected by any credentials whatsoever. About 95 percent of these are hosted inside of Amazon Web Services (AWS). The firm said that it has alerted the affected companies. ²

Key point: Cloud services are accessed across the internet. A simple mis-configurations can provide an entry point to sensitive data, available to anyone who has the url or who can find it through reconnaissance.

Sources

1. SANS Cloud Security survey, 2019
2. Threatpost.com

Cause of cloud breaches



+ Client responsibility

+ Provider responsibility

Source: SANS Cloud Security Survey, 2019



What should your Partners be doing?

- Up-skilling staff with education programmes (certifications for key roles)
 - Enforcing Multi-Factor authentication for access to the cloud services
 - Continuous Monitoring for insecure configurations
 - Asset Lifecycle Management – fast provisioning, fast deletion
 - Virtual segregation of clients data (unless otherwise authorised)
 - Going cloud native, i.e. using pre-build technology stacks and serverless platforms
 - Appropriate use of advanced data protections (may come at additional costs)
- 

The cloud is secure – use it
like a native

A Woman of our time, by Joao Pinto

