IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Technology and Innovation

Secure the Cloud by Bringing Your 'A' Game

Nathan Britton

Nathan Britton
Application and Cloud Security Practice Lead (UK)
NTT Ltd

Biography

Nathan Britton is Application and Cloud Security Practice Lead (UK), at the Security division of NTT Ltd (https://hello.global.ntt/). With over 15 years of experience, Nathan is responsible for the design and implementation of technical solutions that support clients in achieving their security goals.

He has a strong focus on application security and provides technical governance and leadership on consultancy projects, and has extensive experience in a range of industry sectors including local government, banking and finance.

Nathan blogs at https://technical.nttsecurity.com/u/102eu6y/nathan-britton

Keywords Cloud, Security, Digital transformation, Secure by design
Paper type Research

Abstract

Keeping data safe in the cloud is an ongoing, evolving endeavour. In a survey carried out at Cloud Expo last year, NTT (https://hello.global.ntt/) asked attendees what they thought was the biggest challenge to cloud security. Moving data without the appropriate access controls, encryption and back-up strategies was felt to be the most pressing issue, closely followed by a lack of cloud experience and a lack of risk assessments.

Introduction

Securing the cloud can feel a bit like eating an elephant – and how do you eat an elephant? One bite at a time. The same is true for cloud security – the challenges become a lot more manageable if you break the process down into four practical steps: Assess, Analyze, Act and Assure.

Cloud adoption is on the rise, driven by digital transformation and the promise of greater agility, flexibility, scalability and cost efficiency. In 2018, 73% of organizations already had at least one app, or a part of their computing infrastructure, in the cloud according to research[1] from IDG. Meanwhile, VMware says that 50% of workloads will run in public clouds by 2030[2].

Cloud related breaches are rising in parallel. The Department for Digital, Culture, Media and Sport reported in its Cyber Security Breaches Survey 2018[3] that


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

businesses using cloud computing were more likely to have faced breaches than those who do not (52% v 43%).

The Uber breach uncovered last year came as a result of the company storing AWS credentials in a Github repository, which were subsequently retrieved by hackers and used to access Uber's AWS account. Another high-profile breach occurred at Verizon, where a misconfigured S3 bucket owned and operated by supplier NICE Systems exposed the names, addresses, account details and PINS of as many as 14 million US customers.

With great opportunity comes great responsibility

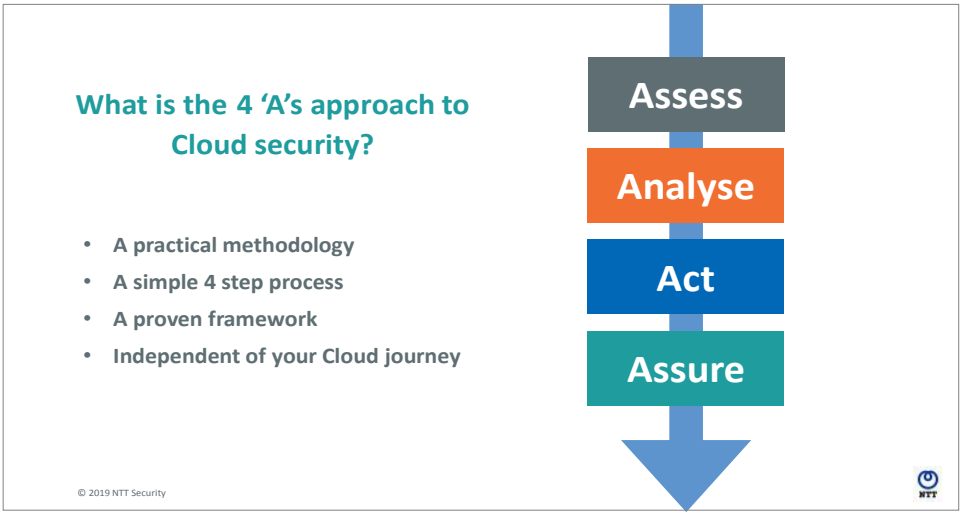
The cloud isn't inherently more insecure than on-premise infrastructure, in fact it gives organizations an opportunity to be more secure. So why, then, is data more likely to be exposed in the cloud? On closer analysis most breaches can be attributed to errors in misconfiguration, or even a misunderstanding of who actually owns cloud security.

Many security teams find it difficult to keep up with the fast pace of cloud deployments. The 'lift and shift' of security controls can also leave gaps. Cloud applications don't always mirror their on-premise version, so controls have to be revisited to support apps which have been rehosted, replatformed or refactored.

Another potential issue is a lack of cloud-specific security policies or guidelines to drive 'secure by design' cloud adoption. Shared security models can also leave data vulnerable, if it is unclear whether the responsibility for protecting data lies with the business, cloud provider, consumer, or combination of the three. The cloud model – whether it's IaaS, PaaS or SaaS – may affect the lines of responsibility.

The 4 As approach

This four stage process will help organizations to understand how to secure cloud deployments, gain visibility of their cloud footprint, understand pain points and risks and – most importantly – use that knowledge to drive a roadmap for improving cloud security.



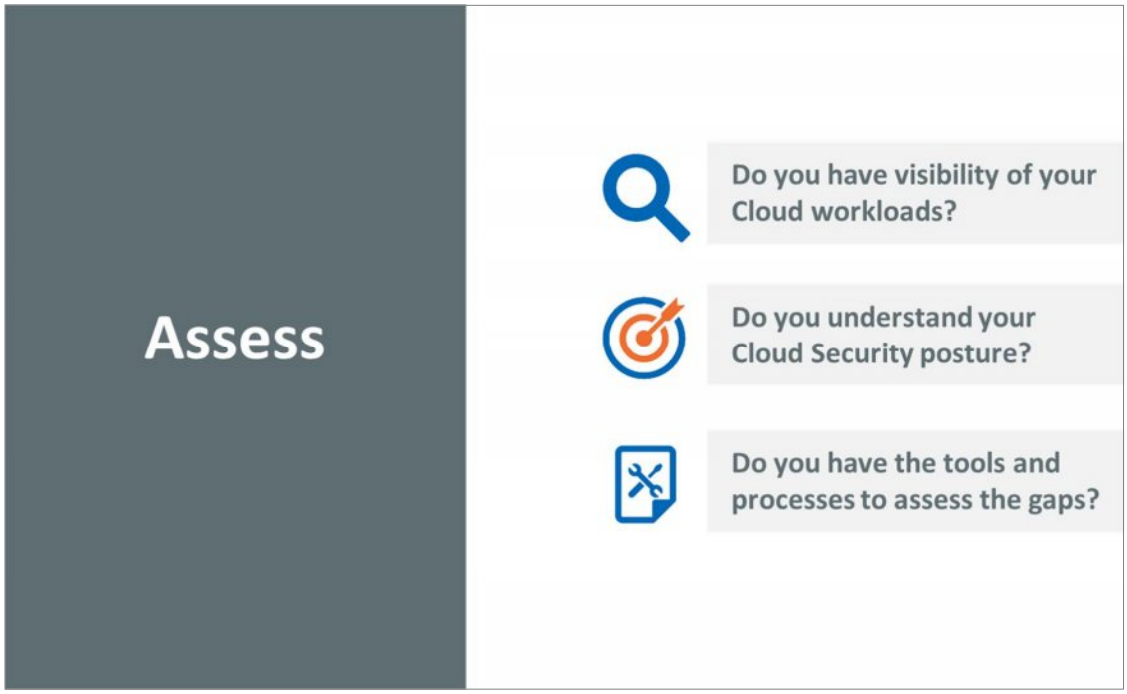
IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

1. **Assess –** You can't secure what you don't see. Assessing and auditing your cloud solutions will provide visibility over the assets and workloads deployed there. It will also highlight potential threats, gaps in security, and your overall security posture.

   This is the right time to look at where security is 'built in' by the Cloud Solution Provider (CSP) itself, and where it needs to be added or augmented. It's a good idea to seek out tools and processes that will help you to assess where there may be gaps.

   The findings of the assessment can then be used as a benchmark to capture where you are today, and build a cloud security roadmap for the future.



2. **Analyze –** This phase begins with identifying how a cloud deployment measures up against good security practices or frameworks – including requirements for regulatory compliance.

   Next, examine the security gaps this analysis highlights, and quantify the potential risks and threats that result from them. From there, you can map threats to the right security controls to remediate the gaps, and prioritize the order in which you implement them.

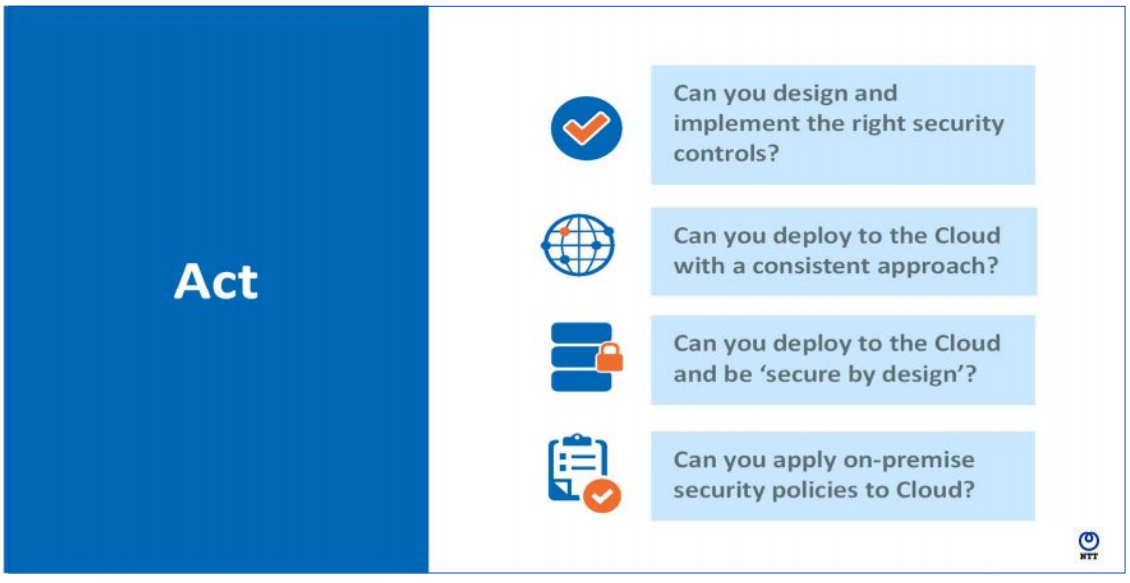
   The knowledge you gain in the Analyze stage will help you make informed decisions on your cloud security design and controls implementation in a way that ensures consistency across the deployment.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

3. **Act** – Once you have a clearer picture of the security posture of a cloud deployment and visibility of the assets, you will be in a position to address security issues by designing and implementing the required security controls. This will ensure a consistent approach to deployment to the cloud, and that security is 'by design'.

   It's a good idea to start with the CSP's native security controls and configurations, using these as a foundation to create a minimum viable security template that can be applied to build future cloud resources securely and consistently. These can then be complemented with embedded cloud native security controls.

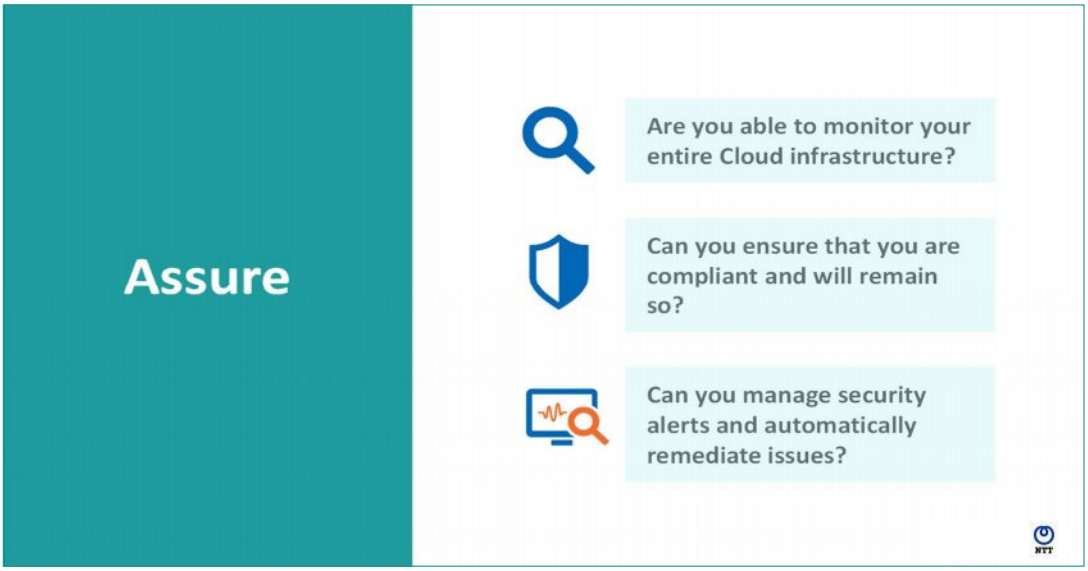


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

4. **Assure –** When it comes to securing cloud deployments, your work is never done. Your cloud security will need to grow as deployments increase and more workloads are migrated to the cloud, or built in the cloud. To maintain regulatory compliance and address evolving threats cloud deployments need to be continually monitored, with any deviation from agreed security standards alerted upon. Automation is vital here to guarantee fast remediation of issues.

   To get the most from this stage of the process, you will require the support of security monitoring and compliance tools and platforms which are aligned with your security operational requirements.



In conclusion

By breaking down cloud security using this proactive four As approach, organizations can benefit from increased visibility of cloud workloads and assets, and the risks and threats that need to be addressed. This will provide the insights they need to build a prioritized roadmap of remediation and improvement, and ensure that security is consistent across and 'baked in' to all current and future deployments.

Reference

1 https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/
2 https://www.computerweekly.com/news/450401262/VMworld-2016-VMware-progresses-its-hybrid-strategy
3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf