CYBER SECURITY - DE-RISKING THE USE OF CLOUD SERVICES

Maritz Cloete, CISSP, M.CIIS

16 September 2020

RISK Management
part of Moore Kingston Smith

INTRODUCTIONS

Maritz Cloete

- Information/Cyber Security Consultant
- Background
  - Cyber security risk management
  - Implementing frameworks – e.g. ISO27001, Cyber Essentials
  - Security penetration testing
  - Providing incident response support to customers in distress
  - Security training – general awareness to security specialist training

Sasha Lawrence

- Business Risk Manager, Clearcomm
- From experience in supporting the NHS through the Wannacry outbreak, learned how serious a cyber security attack can get
- Passionate about business resilience, cyber security, information security data protection, continues to research the latest methodologies and techniques to help customers mitigate their business risk

IN TODAY'S SESSION…

- A brief look at the wide-spread migration to the 'Cloud'
- A look at some recent high-profile cloud-related cyber security breaches
  - What went wrong, what was the result?
- Closer to home – fellow charities suffering cloud-related security breaches
  - What happened, effect on the organisation, resolution
- Cloud is here to stay, so how can we manage the risk?
  - Key takeaways from our case studies
- Q&A

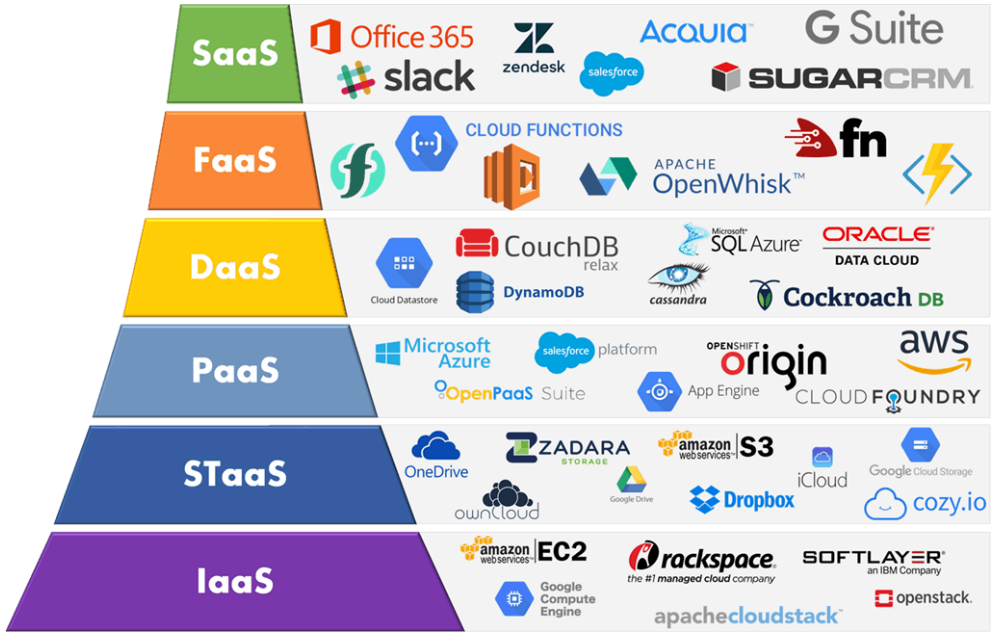
MOVING TO THE CLOUD

Because everyone is doing it…

RISK Management
part of Moore Kingston Smith

WHAT DO WE MEAN BY ‘CLOUD’

- Traditionally on-premise servers ran business applications such as e-mail and business applications
- Expensive and complicated to operate and sustain – needed specialist IT resource, dedicated physical areas, dedicated hardware, upfront investment, etc.
- Outsourcing IT systems to third parties to host, run and operate became the norm for cutting operating cost
- The ‘Cloud’ is a natural extension of this concept, where third parties offer services on a ‘utility’ or pay-as-you-use basis
- These services could be:
  - **Applications** – Office 365, Salesforce, Blackbaud, (Facebook, LinkedIn, Twitter, etc)
  - **Platforms** – environment for developing and deploying own applications, e.g. Microsoft Azure, Amazon Web Services
  - **Infrastructure** – servers in the cloud, e.g. Amazon EC2



RISK Management
part of Moore Kingston Smith

WHY IS EVERYONE MOVING?

- Very attractive cost model – pay-as-you-use
  - E.g. pay per user subscriptions, capacity, performance
  - Typically costs are transparent and predictable
- Limited up-front investment, changes IT spend from CapEx to OpEx
- Easy to scale up and down according to business need (with costs scaling accordingly)
- Someone else is managing the infrastructure – much less technical complexity in this regard and therefore less specialist IT resource required
- Organisations can now focus resources on where the business value lies, rather than “keeping the lights on”
- So Cloud is a “Win-Win” right?

Cloud Adoption Trivia

- **83% of enterprise** ’workloads’ will be in the cloud by 2020.
- **94% of organisations already use** a cloud service.
- **30% of all IT budgets** are allocated to cloud computing.
- Organisations use almost **5 different cloud platforms on average.**

THERE IS ALWAYS A ‘BUT’…

- Your data exists in someone else’s data centre(s), somewhere on Earth.
- You are reliant on the effectiveness of the cloud provider’s security measures to keep your data secure
- You must take further action to make sure your data remains secure, e.g. managing user access
- You remain accountable for security of the data – a breach is still a breach
- If there is a security breach, how will you know?
- The internet provides the basis for connectivity to Cloud services
  - Services are typically visible to anyone on the internet
  - 4.3 billion internet users (Jul 2020)

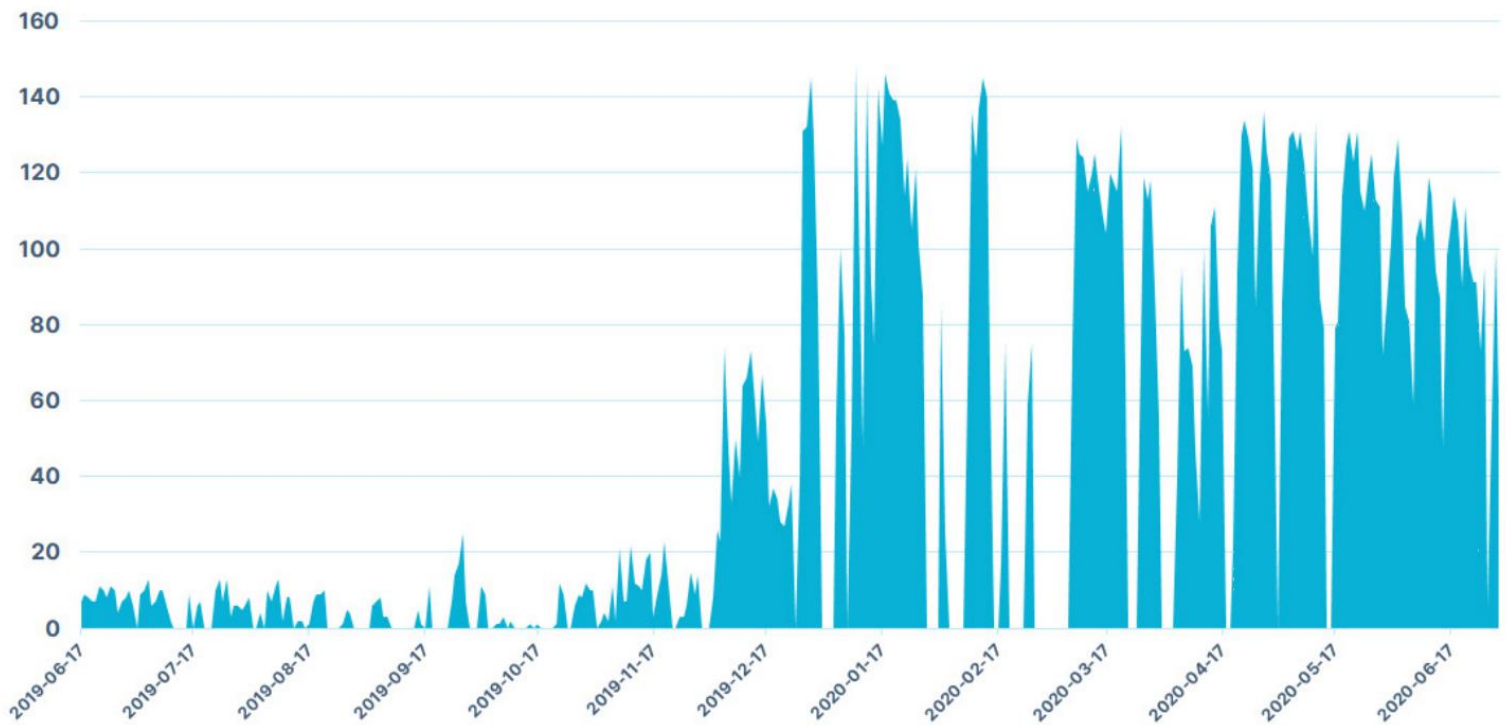
CS RISK Management
part of Moore Kingston Smith

HIGH PROFILE SECURITY BREACHES

Cloud security trip-ups made public

RISK Management
part of Moore Kingston Smith

SIGNIFICANT UPTICK IN CLOUD CYBER ATTACKS



- 2020 saw 250% year on year increase in Cloud cyber attacks
- Apart from data theft or data manipulation, attacks also look to:
  - Steal computing resources for Crypto-mining
  - Re-appropriate resources as part of a bot-net
  - Abuse resources to perpetrate Denial of Service attacks
- Mixture of skilled attackers and ‘script kiddies’

CS RISK Management
part of Moore Kingston Smith

**Source - 2020 Cloud Native Threat Report - Aqua Research Team*

DATA BREACHES DUE TO UNINTENTIONALLY MAKING DATA PUBLIC

54,000 Australian Driver's Licenses Exposed on S3 Bucket (Aug 2020)

- 54,000 scanned driver’s licenses discovered on an unsecured, publicly accessible Amazon S3 ‘bucket’
- Data discovered by security researcher, owner of data not know
- Reported to the Australian Cyber Security Centre and subsequently made private
- Suspected to have been a government roads project
- Free services on the internet to find data in public S3 buckets
- 296,485 – number of S3 buckets publicly accessible
- 3.6 billion – number of files publicly accessible
- https://buckets.grayhatwarfare.com/buckets

CLOUD SECURITY BREACHES DUE TO LAPSE IN BYOD CYBER HYGIENE

Hacker Steals $7.5 Million from Maryland Non-Profit by Compromising Employee's Personal Computer (Sep 2020)

- Jewish Federation of Greater Washington
- Attacker managed to steal $7.5m from endowment funds
- Employee's home computer, used to access company systems, were compromised
- Attacker used the home computer to perpetrate the theft undetected
- Breach was identified by a security contractor who noticed unusual behaviour on the user's Office 365 e-mail account

The Jewish Federation OF GREATER WASHINGTON | CONNECT WITH PURPOSE

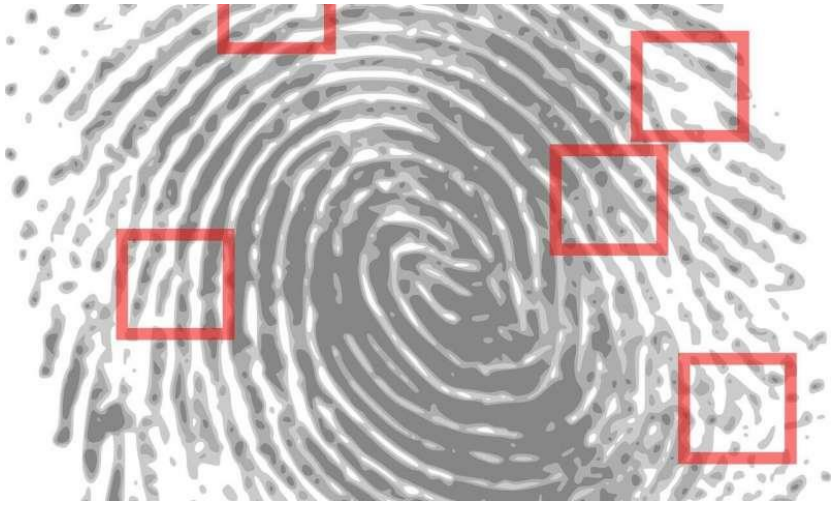
RISK Management
part of Moore Kingston Smith

SECURITY BREACHES DUE TO POOR CONFIGURATION

Antheus Tecnologia Biometric Data Breach (Mar 2020)

- Brazilian biometric solutions company
- left sensitive information, including data on 76,000 fingerprints, exposed on an unsecured cloud database server
- Data could be used to reconstruct fingerprints
- 16GB of data exposed
- Data was not encrypted, and publicly accessible
- Breach was discovered and report by security researchers
- Breach was due to weak configuration of access controls, and lack of encryption

ANTHEUS TECNOLOGIA
soluções biométricas de identificação



CLOSER TO HOME

Fellow UK charities fall foul of cloud security lapses..

RISK Management
part of Moore Kingston Smith

CLOUD APP PROVIDER SECURITY BREACHES

Cloud Company Blackbaud Pays Ransomware Operators to Avoid Data Leak (May 2020)

- Fell foul of ransomware and data theft attack on its CRM/fundraising platform
- Some customer data stolen, but scope of data theft not that clear
- Paid attackers not to release data (fingers crossed!)
- Notified affected customers, including not-for-profits:
  - At least 50 charities lost data Incl. National Trust, Crisis, Sue Rider
  - All had to notify customers and the ICO
  - Mines Advisory Group one of the latest – mid-August 2020
- Expected to have repercussions in the form of sophisticated phishing attacks, identity theft, or other scams

OFFICE 365 – BUSINESS E-MAIL COMPROMISE

UK Charity near miss - £150,000 BEC attempt

- ~70 users on Office 365
- Legitimate e-mail request sent to a third party, authorising the transfer of a £150,000 grant to a new start-up business – with Docu-signed PDF attachment
- Follow-up e-mail received from the same person at the charity, 24 hours later
- E-mail contained altered copy of PDF attachment, reflecting a different business's bank account details, but without the Docu-sign seal.
- The recipient became suspicious, and queried it with another worker at the charity who raised the alarm internally.
- No payment was made, but it was close.

RISK Management
part of Moore Kingston Smith

HOW DID THE BUSINESS E-MAIL COMPROMISE HAPPEN?

- The attackers logged into the person's office 365 account with his credentials (!!) – no failed login attempts!
- The person was based in Madrid, the attackers appeared to be in London on a mobile network, and in the US on a rented server
- The attackers only logged in four times:
  - the evening after the original e-mail was sent, to verify the credentials and possibly locating the original e-mail
  - the morning of the attack, to set up rules to automatically delete the e-mails once it was send
    - Sent items, recycle bin and deleted items
  - Just after noon time, to send the e-mail. The rules automatically destroyed the e-mails.
  - Ten minutes later to check that no responses were received and that the rules worked.
- At this point, the alert was raised and the user's password changed.
- The attackers tried to log in one more time and failed – they knew the game was up. No further attempted logins.

OFFICE 365 - CHARITY MALWARE ATTACK

- 10-person organisation on Office 365
- Received complaints of phishing e-mails from trustees and beneficiaries
- Phishing e-mails were sent in two tranches – on Wednesday and Friday of the same week
- Each e-mail included content from prior e-mail correspondence!
- E-mail linked to a malicious download on a compromised web site
- Suspected that a key shared e-mail account was hacked – ~3GB/1000s of e-mails in the mailbox
- Had to notify the ICO of a potential personal data breach, as mailbox contained benefit application forms

WHAT WE FOUND

- Based on attack characteristics, an Emotet or Qbot malware infection was suspected.
- <u>However:</u>
- *Critical audit logs not turned on or only retained for a short period of time,* so difficult to ascertain when the breach occurred, the extent of the breach or the methods used
  - Office 365 – logs were turned off
  - Windows Server – only 100MB of logs retained = < 1 day
  - Exchange mailboxes – retained for 30 days only, limited activities audited
  - Anti-malware software – no centralised server for alerts/reporting
- Staff were working from home – could not identify which staff member's devices were the source of the breach, could not quarantine devices for inspection
- BYOD in use… secure, patched? How do they even check this?
- Lots of moving parts to investigate – complexity exacerbated by lockdown
- In the end, client lost confidence in IT infrastructure integrity and initiated rebuild from scratch.

CLOUD SERVICES ARE HERE TO STAY

Now how do we manage the risks

CS RISK Management
part of Moore Kingston Smith

CLOUD BRINGS MANY BENEFITS BUT..

Moving to the cloud will change your cyber security risk profile, for example:

- More direct exposure to threats from the internet
- Greater number of potential attackers and types of attacks
- Higher sensitivity to security configuration errors
- Less direct control over where your data resides, how it is stored and potentially who can access it
- More dependency on the effectiveness of the service provider security measures
- More reliant on the Cloud service provider's incident response capabilities
- Cloud services can be procured by anyone, may bypass procurement governance (shadow IT)

HOW CAN WE MANAGE THIS RISK?

Introduce **governance** around the use the cloud services within the organisation:

- Define clear policies and procedures around, for example cloud service procurement, authorised use cases, cloud data security and data restrictions
- Maintain an inventory of authorised cloud services and the type of data held in these services, with specific business owners assigned to each service
- Review the inventory from time to time, assess the appropriateness of the data held in these services.
- Introduce monitoring and reporting around the operation of key controls around cloud services, particularly those that hold sensitive data.
- Include cloud services in your Data Privacy Impact Assessment (DPIA) activities

HOW CAN WE MANAGE THIS RISK?

Rigorous Cloud Service Provider **security due diligence**

- What assurances do they offer around the service's security?
- Do they have third party certifications that underpin these assurances?
  - Valid ISO27001:2013 certificate with a scope that covers the service
  - Cloud Security Alliance (CSA) STAR certification Level 2 or above
  - Service Organisation Control 2 (SOC 2) Type 2
  - For UK providers, do they have Cyber Essentials Plus?
- Monitor existing cloud services – are they maintaining certifications? Results of audits?

HOW CAN WE MANAGE THIS RISK?

Staff have relevant **Cloud configuration skills**:

- Individuals should be able to demonstrate expertise and training in configuring and operating the cloud services in question
- Individuals involved in setting up and maintaining the cloud service on your behalf should have valid certifications, evidence of training or demonstrable prior experience
- Conduct regular training needs analyses for any internal staff, and train accordingly
- Track yours and your IT service provider's competences, particularly as cloud services change continuously

HOW CAN WE MANAGE THIS RISK?

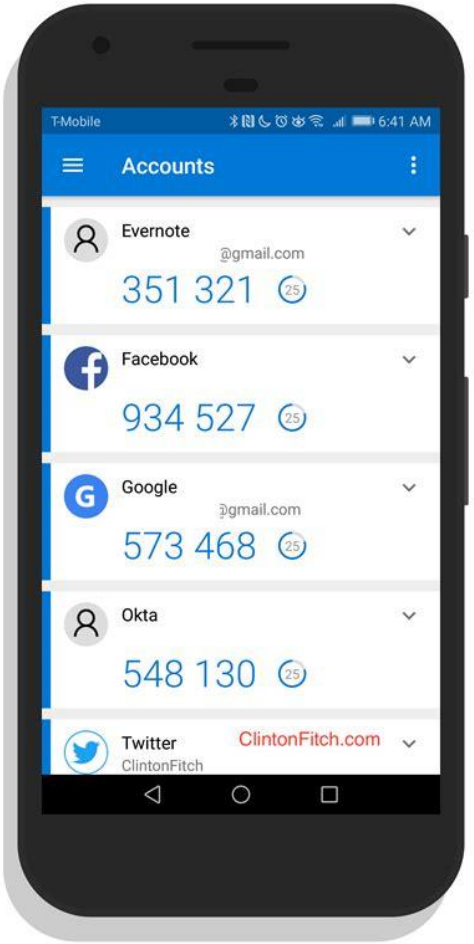
Mandate the application of good practice technical **security baselines**

- Services such as Microsoft 365 and Amazon Web Services are infinitely configurable
- Baseline security guides exist for most of the common services, often provided by the vendors themselves
- Typically covers of technical configuration and security procedures
- For example:
  - Microsoft 365 have a ‘Compliance Score’ with clear actions to take to improve security
  - AWS have security good practice guides for each of its services, including S3 buckets!!!
- Your IT team (in-house or outsourced!) should be aware of these and apply these by default.

HOW CAN WE MANAGE THIS RISK?

Use **strong user authentication** methods

- Most of the services are accessible by anyone on the internet
- Usernames and passwords are not the most effective way to protect these services
  - Passwords can be guessed
  - Username and passwords can be phished
  - Passwords could be reused between services
  - Account details can be leaked (https://haveibeenpwned.com)
- Most cloud services now offer two-step user verification for logging on via the web
  - One-time code via text message
  - One-time code via voice call
  - Phone app – one-time code or access approval



HOW CAN WE MANAGE THIS RISK?

Be firm around the use of staff personal devices (**BYOD**)

- Be clear on whether staff can use their own devices to access cloud services, such as Microsoft 365
- If it is allowed, set out a clear policy around how the personal device should be managed by the individual
  - Minimum System Requirements (e.g. version of Windows or Osx)
  - Security Patching
  - Anti-virus/Anti-malware
  - Computer access controls
  - Shared use devices
- Put technical controls in place to prevent non-compliant devices from being used to access the service
- Often the above is considered onerous and potentially ineffective, so BYOD is not permitted.

RISK Management
part of Moore Kingston Smith

HOW CAN WE MANAGE THIS RISK?

Foster **continuous Cyber Security awareness**, don't become complacent

- Remind staff regularly to look after their login details
- Warn staff about new phishing scams and other methods used to steal login credentials
- Remind them to remain alert, especially when receiving unexpected messages by e-mail, instant messaging apps, text and conference call apps.
- Discourage them from clicking on links in messages or opening attachments without first verifying that they are legitimate and safe.
- Reminding them how to report any concerns or suspicious activity, especially phishing attempts or other unusual requests or e-mails

HOW CAN WE MANAGE THIS RISK?

Prepare for managing a cloud security breach as effectively as possible.

- Formalise and practice your incident response plans
- Prepare “playbooks” for dealing with security breaches likely to occur with the cloud services you use (link back to inventory!)
- Simulate specific breaches to practice working together as an incident response/crisis management team, as well as interaction with the cloud service provider
- Make sure that the cloud services can support an incident investigation (also known as forensic readiness), and that you have the investigative capabilities to hand.

Q&A

CS RISK Management
part of Moore Kingston Smith