Interop® Las Vegas

MAY 2 – 6, 2016 | EXPO: MAY 4 – 5 | MANDALAY BAY

Integrating Cloud Applications into your Infrastructure Strategy

By Sonia Cuff

Presentation Guide

Key Points:

Drivers

Slide 11: Understand the drivers behind why your organisation would look at Software as a Service. For some newer organisations, it's the default standard.

Slide 12: Quote is from a company of ACCOUNTANTS. This is the new workforce. These are your competitors.

Slide 13: Gartner is predicting that Chief Marketing Officers will spend more on I.T. than CIOs will.

Business Drivers:

Slide 15: Data from outside the organization is useful eg customer opinion & behaviours. Social media is a prime example.

Slide 16: SaaS subscriptions can be cheaper than traditional on-prem licensing purchases

Slide 17: AND include the costs of support, maintenance, upgrades etc.. ongoing operating costs left out of on prem software purchase projects.

Slide 18: Minimal end user training.

Slide 19: Minimal wait time for deployment as Cloud apps are just a corporate credit card away.

Slide 20: Vendors adding free Cloud app licenses with traditional purchases or partner programs.

Slide 21: Helping people work from wherever they need to.

I.T. Drivers:

Slide 23: Easily wind up, grow, shrink, wind down as needs change.

Slide 24: SaaS vendor handles the infrastructure resilience.

Slide 28: Don't divert I.T. resources to a new technology that might not even have a long shelf life in your organisation.

Shadow I.T:

Slide 31: 9 million search results for Shadow I.T.

Slide 34: Origin Energy is one of the biggest energy providers in Australia. James Moor is the group manager for **market risk** and he admits that he's not an IT guy. What Moor does know is data and he was keen to find a better way for Origin Energy to deliver gas to customers. Origin had a wealth of data on its customer's energy usage and he knew data analytics had the potential to bring business insights that could help develop new commercial offerings.

The Decision:

Slide 38: Scenario – replace corporate e-mail with Facebook. Silly suggestion, I know but let's apply it.

Slide 39: SaaS is the hardest Cloud capability to add to a legacy environment. There is no Cloud, it's just someone else's computer

Slide 40: BUT with SaaS, it's a computer that you can't control. You are in control of NOTHING.

Slide 41: But you have to integrate things like user accounts or accept the risks of having that isolated. You need to figure out how to add that into your existing house. But there are no instructions. So you need to be..

Slide 42: A MASTER BUILDER. Even if you haven't touched Cloud applications before. The Business are counting on you.

Slide 43: When you set out to do something awesome, it's inevitable you'll meet with resistance. That's not always a bad thing. Sometimes it's there to protect you or the organisation or the organisations information. As soon as corporate data leaves the confines of your infrastructure, you've lost control of it. And I don't want you to think of that data as just customer details or sales records. If you have internal team communication happening in a SaaS product, that's valuable corporate IP you still need to protect.

The Gatekeepers

Slide 46: Think of all of the corporate or IT policies that exist to protect the organisation's data, that YOU have to adhere to internally. Does the SaaS app conform to these? Specifically, policies that exist to PROTECT THE DATA. Where is data **stored?** How is data **transmitted?** Where are the **backups stored?** Is the data **encrypted in transit, at rest & within backups and archives?** How is data **restored/recovered?** How long is **data retained for?** If you can **export the data … who else can?** How do you get **access to the data if you stop** using the service? What's their **media End Of Life process**?

Slide 47: READ the Ts & Cs about what data they have access to. With Facebook, it's a lot!

Slide 48: How does their infrastructure stack up? Is it being kept up to date? Server BIOS, networking gear firmware, Hypervisor software What intrusion detection mechanisms do they have in place? Remember, most of these things you will have no control over and some of these things the SaaS provider won't even disclose to you. But you need to ask the questions. If it doesn't stack up, get someone high enough up to sign off on the exception.

Slide 49: It's one thing to check out compliance of your SaaS application prior to using it, and you're going to cover off Industry specific compliance, Country specific compliance and international compliance (if that's relevant). For example, Facebook is Safe Harbor compliant, but HIPAA compliance comes down to how people use it and what they post. But what happens when the compliance rules change? You are at the mercy of your SaaS provider's compliance team but that doesn't transfer the authority of your organization's compliance to them. Make the business aware of this as a risk.

Slide 50: Is the SaaS provider open to submitting to external audits? How's their eDiscovery? And do they have simple things in place like non-repudiation?

Slide 51: By default, if we have an argument about something I said on Slack, I could go back and edit an older message and completely change it. The only thing you'll see is an EDITED marker, IF you go back and look. Team admin can turn off the ability to edit messages but it's ON BY DEFAULT. So you'll need to do an audit of the apps security settings to see what you can lock down. WHAT DO YOU NEED TO TWEAK IT TO TIGHTEN UP THE DEFAULT SECURITY OF THE APP?

Slide 52: From an infrastructure perspective, you have policies and procedures in place to control correct and timely access to the data. This enables the right people (and only the right people) to have timely, reliable access to the data when they need it. In essence, all of your infrastructure processes and decisions focus on this (access or performance).

Slide 53: This architecture component is one of the most important for maintaining accurate access to your data in the SaaS app. If this isn't done right, you risk having isolated pockets of identity databases to manage, outdated authorised access, access to your internal directory by applications or hackers that shouldn't have access to it and a frustrated IT security department who have to run manual process every time someone starts, leaves, moves department, changes their name or forgets their password. Is your answer …. LDAP Integration? Directory synchronisation? Federation? Can you, should you or do you have to control corporate identities outside of your organisation? Are IDaaS solutions like OneLogin and Azure Active Directory Premium worth investigating? Also check what other integrations you have within your organisation that feed into your identity management? How does that impact your SaaS identities?

Slide 54: With your existing systems, you have provision for: Multi factor authentication, Single Sign On, Password expiry and password reset policies. How does the SaaS app handle these? Does it conform to your policies?

Slide 55: You'll have processes for Identity management including: Security group structures and membership changes, Employee entry / move /exit procedures. How, if at all, will those processes change?

Slide 56: Can you & should you enable self-service password reset, if the directory integration doesn't take care of password sync or a federation equivalent?

Slide 57: Do you have a requirement for integration between the SaaS app and any other apps? For example, remember our ridiculous Facebook proposal … what else would integrate with your email systems? How's their API?

Slide 58: And more importantly, how is their API controlled? If you can hook into it, can the end users authorise access from other apps (especially other SaaS apps) without your knowledge or approval? Can they authorise access to the data for another app that you don't control?

Slide 59: What systems do you already have in place and what dependencies do they have?
Eg does a legacy line of business app require an older browser version and will that have an impact on your Saas? Do you have any browser security restrictions in place, especially those enforced via Group Policy, that will impact the SaaS app?

Slide 60: How do you include a SaaS application into your change management process? Where do you include it in your testing. If you know about it, you can plan for it. But if it's the SaaS application that's changing, how do you stay aware of what's coming up in a new release and when it will be deployed? Chances are you won't have 'pre-release' testing time, so you are at the mercy of the SaaS app devs. This gets more complicated when you bolt on more SaaS apps that integrate with each other, either directly or via another third party service!

Slide 61: Changes to the SaaS app are a ticking time bomb that may hit you with their next release, or never be a problem, so it pays to be aware of it early especially if there are things you can do. Can you get on their beta testing program? Can you follow their product roadmap and be notified of updates & announcements?

Slide 62: Will your current security policies and tools for devices, in house of BYOD, also secure your SaaS app? Can they open a browser and introduce virus ridden documents from home? Can you wipe Saas application data from their personal device if they leave?

Slide 63: What impact is the use of this application going to have on your network performance? You have to consider concurrent usage, data types, upload/download speeds. How will it impact your capacity planning for the future as the business grows, the use of this app grows, the use of other SaaS apps grow.

Slide 64: What impact will your network availability, bandwidth, latency or packet loss have on the user's experience of the SaaS app? Email is fairly resilient when it comes to underlying network performance because network degradation doesn't always lead to an on-screen symptom. But you can bet that you'll hear when Facebook isn't loading fast enough.

Slide 65: How does the use of this app impact your sizing of networks for new locations?

Slide 66: Who is going to get the Helpdesk call when the SaaS app isn't working? The application provider - or your Helpdesk? So plug into their support channels. Raise up a few Helpdesk subject matter experts to handle any support calls. Teach your second level support (and higher) how to log support issues with the provider. Sign up for their service health alerts.

Slide 67: How are you going to monitor the availability and performance of a SaaS app?

Slide 68: What are **their SLAs?** Do they mesh with your own or fall outside your response times for business applications? Is the business aware of this?

Slide 69: And if it all falls down ….? Don't neglect the SaaS app as part of your BCP and DR plans. It might sound silly that you'd have to include it when it's not going to be impacted by a disaster in your infrastructure, but all it takes is one misconfigured firewall and you've missed testing access to an important business tool. If the SaaS app itself goes down, what's their Disaster Recovery plan? Do you care? You might if it doesn't meet your Recovery Time Objective. As business reliance on SaaS apps grow, make sure the business knows that it's DR is outside of your control.

Slide 70: Help the Business create a plan B for unexpected outages. My mother was in the banking industry since before I was born and by the time I entered the workforce, she was the only person in the branch who knew how to be a 'paper bank teller' if the computers went down.

People:

Slide 73: But if the IT Pros in your organisation haven't needed any Cloud skills to-date, they're going to freak out a little. Don't assume they'll be fine with this new direction just because they work in tech.

Slide 74: They need resources to learn new skills, test accounts to play with and direction on if or how their role may change.

Slide 75: **IT management** needs to be on board about what is realistic and what isn't realistic with the introduction of a SaaS app, because if it all goes south, they need to have your back when the business complains. On the flip side, the **Business Management** need to be on board about what is realistic and what isn't with the introduction of a SaaS app. Tell them no we can't change it to the corporate colours. No I can't make Facebook fix it faster.

Slide 76: And finally, your End Users. This might be outside of your realms of responsibility, but really the end users are the key to the success of all of this. You can protect data and keep compliance all you like, but ANY technology decision has to deliver a business benefit to the people using it. It has to make their day a little easier, make it easier for them to work together, or give them data and insights that they didn't have before.

Slide 77: This NOT an adoption plan.

Slide 78: Work with the business to uncover how the tech makes their business process easier or how it helps them to make better business decisions. They might uncover things you hadn't even thought of, because we tend to stereotype what a sales guy needs or what a senior manager needs.

Slide 79: Ultimately, embracing SaaS is about enabling the business. What other roadblocks are in the way? Is your business open to running a Proof of Concept with dummy data?

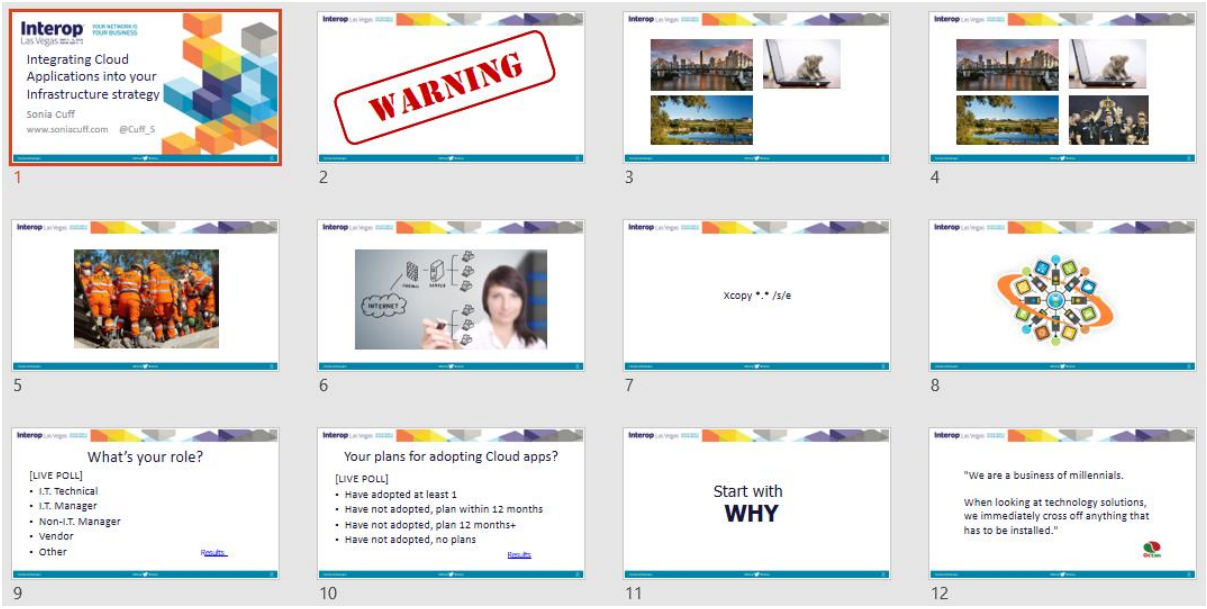
Slide 80: What other departments are stakeholders are in the decision making process and how do we get them to be more agile? Can we keep Risk & Compliance happy?

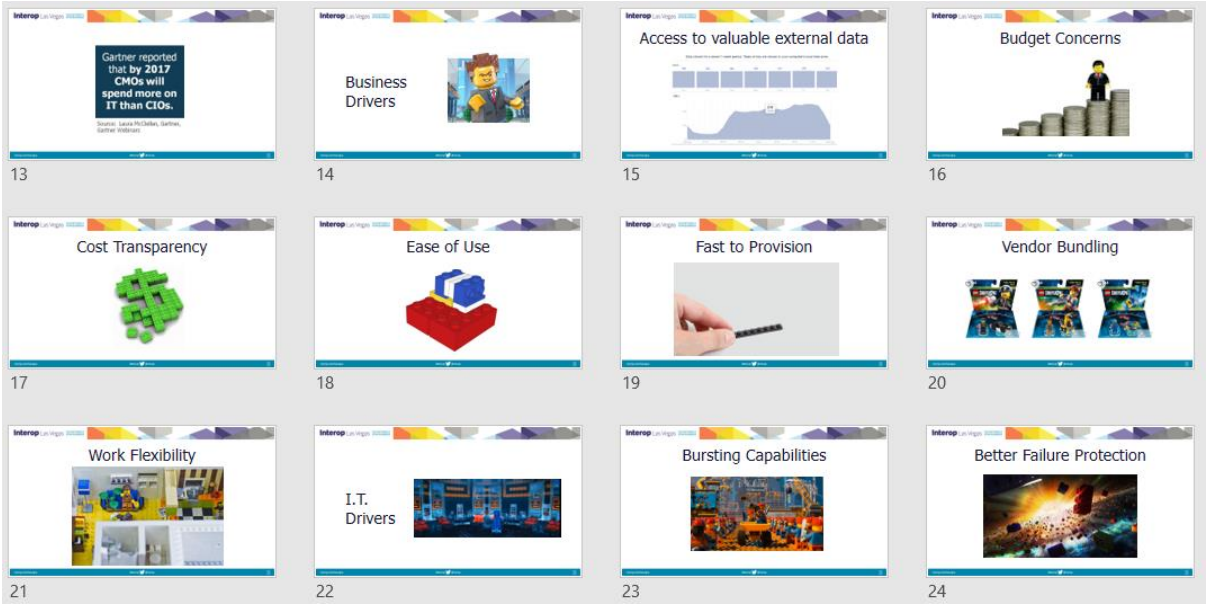
Closing:

Slide 81: So I hope this hasn't put you off adopting SaaS applications. It is possible. And if anyone can do it, you can do it. Because you are The Special.

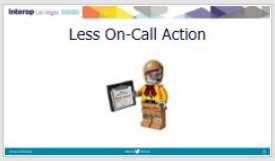
Slide 82: Tweet me when you're back in the office about how you're SaaS project is going!

Slide Deck:

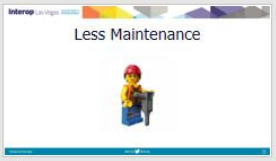




25



26



27

28

29

30


31

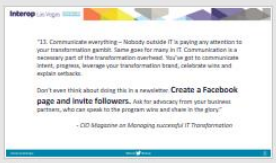
32

33


34


35


36



37

38

39

40


41

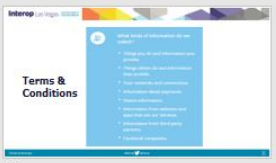

42


43

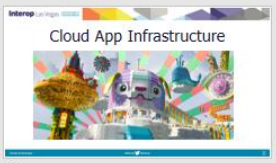

44

45

46



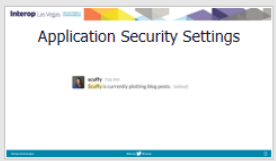
47



48

49

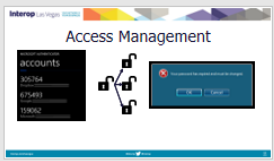
50



51

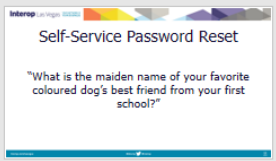
52


53

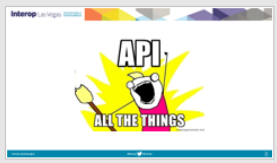


54

55

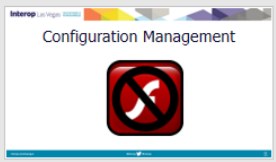


56



57


58



59

60

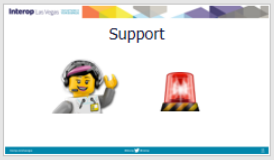
61

62

63

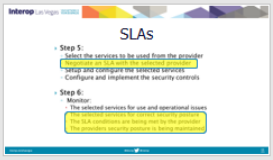
64


65



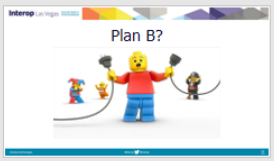
66

67



68

69



70

71

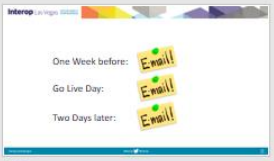
72


73

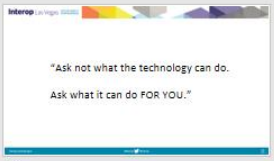

74


75


76



77

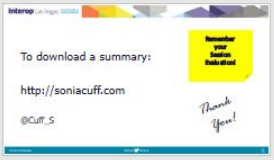


78

79

80


81



82