Real-World Scenarios for Cloud-Based Financial Services

There is something missing in many security conversations for companies within the financial services sector: real-world scenarios. At Nero Blanco, we want to change this by bringing to life specific examples that you can relate to when it comes to deciding on the most compliant and secure way to put your software, services or data in the Cloud.

We've combined information on the latest advances from Microsoft, and knowledge gained from our experiences of implementing Cloud-based solutions for financial services companies, to bring you a list of scenarios and accompanying questions that will provide a starting point for your own Cloud considerations.

1. You want to behave like an agile company, not a small version of a blue chip.

There are benefits to not being one of the 'big guns'; you can respond quickly and thoughtfully to customer needs and make rapid decisions on how your business should be run. Being free of the legacy systems and processes that stifle larger corporate entities also means you can leverage technology so you can focus on delivering the value that sets you apart. **But what's the best tech to use?**

Answer:

We recommend the use of secure Instant Messaging (IM), Skype and secure electronic sharing of data. Low impact and low cost, these applications will keep you directly in touch with your customers in a flexible, personalised way.

2. You want employees to bring their own devices, but don't want accidental data leaks.

If you have employees using their own devices at work, there is the potential that non-work apps could access sensitive information, or an employee could mistakenly select their personal account when sending a business email.
Do you know how to prevent this from happening?

Answer:

To prevent this happening, there is the option to 'containerise', content / apps and even device memory to put a clear line between what's work, and what's not. Talk to us about how this could work for you.

3. An employee has lost a device, and you're worried about the data.

With smartphone launches regularly making headlines it's easy to think the device is king but they are only ever a vessel for data. This becomes clearest when a device is lost or stolen; replacing a handset or laptop is a question of budget, but replacing the contents can cause far greater problems. A laptop or phone left on a train turns into risk, exposure, and the potential for litigation and reputational damage.
What damage limitation measures can you put in place?

Answer:

You can use Intune to remotely wipe company data from devices so should the unthinkable happen, you're in the strongest position to stop your data assets getting into the wrong hands.

4. You don't want a repeat of the 'reply all' mistake.

The most read emails are the ones that are followed by a "Please do not open my last email" message. If you've ever received one of these, you'll know how quickly the information contained is shared and discussed.
Short of checking every email – how do you address this?

Answer:

Prevent these kinds of issues from happening with data encryption and smart alerts. Data encryption makes sure only the right recipient can receive and view the information.Smart alerts enable you to put in place gateways and processes that prompt authors of emails to review their content and/or recipients before hitting 'send'. With the potential to automatically quarantine emails that don't meet corporate policies, embarrassing and costly mistakes can be avoided.

5. You want to introduce flexible working, and comply with legislation.

Public transport strikes, bad weather, a flat tyre, lost keys… These are all reasons why employees may be unable to make it to the office, and they're all outside of your control. What you can control is the decision to implement flexible working. **But can you do it and comply with legislation?**

Answer:

Thanks to Microsoft's compliance with SOC 1, 2 and 3; EU Model Clauses and a wide variety of industry and governmental guidelines, you can now introduce more flexible working options for your staff whilst still adhering to relevant legislation. Gains here include increased productivity, and reduced costs in everything from server storage to the amount of office space required.

6. You want to keep your data in the UK.

Cloud providers are being held to strict account when it comes to compliance with data protection laws. The great news for UK organisations considering the Microsoft Cloud is that there are now three UK datacentres up and running so if legislation requires it, or your customers prefer it, you can keep your data on UK shores.
Do you know how to access these services?

Answer:
Speak to the Nero Blanco team, we can help you make sure your data, and your customer data, stays in the UK.

7. You've never recorded your password, but someone's accessed your device.

Common sense dictates that you never write a password down, but in the context of corporate hacking, criminals are not going to search your wallet or handbag – they're going straight for your hard drive.
Do you know how to stop it being discovered?

Answer:
Windows 10 Enterprise sees the introduction of Credentials Guard – which is designed to keep your password and corporate secrets safe from would-be hackers

8. You've discovered some apps that shouldn't be on your network.

Have you ever undertaken a software audit? If you have, it's likely you'll have found programmes and apps that have no place on your corporate network.
Once your network is clean, you want to keep it that way – but what's the best way?

Answer:
We highly rate the new Windows 10 Enterprise feature Device Guard. Using a 'white list' approach, only pre-approved software and apps can run in your corporate environment meaning that any attempts to install non-approved software (from an innocent download of a free productivity app, to a malicious attack) will be completely blocked.

9. You know there's Malware, but you can't find it.

If a device is not performing properly, one diagnostic approach is to look for programmes that are using disproportionate amounts of memory. Historically this would have helped to identify malware but since then, hackers have found ways to create issues at a process level – something that is much harder to detect and resolve.
What measures can you put in place to detect this kind of threat?

Answer:
Windows Defender Advanced Threat Protection (ATP) uses machine-learning, big-data and endpoint sensors to pinpoint issues as specific as Outlook behaving in a way that is not normal for your organisation. We see this as an incredible development – get in touch to find out why..

10. You want to be hi-tech, without losing your old-school values.

One thing that we have observed is Microsoft combining its commitment to enterprise scale in the Cloud with security that puts so much control in your hands, it feels like you have your own safe.
Do you know what these are, and how you could make them work for your business?

Answer:
One of these is the Customer Lockbox in Office365 where you have the ultimate control over whether a Microsoft engineer can access your data. There are also options to either "Bring Your Own Key (BYOK)" or "Hold Your Own Key (HYOK)" both designed for organisations that need to comply with complex regulation and compliance policies, and those who need to make sure their data is always treated in line with their own strict security policies.

The scenarios are almost limitless, but we hope that this initial glimpse into the kinds of questions that we think financial services companies should consider is useful in helping you to structure your thoughts on your own cloud computing plans. **To learn more, please get in touch.**

At Nero Blanco we specialise in providing black and white advice you can rely on so you can make consistent and informed decisions right from the start. You might also like to know that financial services is in our blood - so far we've helped hundreds of thousands of users in the sector successfully transform their IT.
Click here to find out more.