BLOG POST

Using MSPs to administer your cloud services

Andrew A explains what you must check before giving Managed Service Providers (MSPs) the keys to your kingdom.

Andrew A

Any conversation about securing cloud services will swiftly turn towards the cloud shared responsibility model, which boils down to '*both you and your cloud provider have to take security seriously*'. Attackers will seize **any** opportunity they can, so if you or your service provider has any weak spots, they could access your data and services.

Building, operating, and securing technology is hard. It takes a lot of time, effort, and skills. And like many of the challenges in modern enterprises, it's subject to ever-tightening budgets. It's for these reasons that we advocate giving as much security responsibility to your cloud provider as possible, as they operate at a scale that makes it more practical for them to carry out key security activities.

However, the shared responsibility model still requires you to:

- choose a cloud provider that can meet your needs
- configure (and use) the service well

That includes making effective use of the cloud service's security features, and continuing to operate and secure the things you've put in the cloud.

Outsourcing your responsibilities in the cloud

Many organisations choose to outsource the operation of their cloud services in the same way that they previously outsourced their on-premises IT. This is often to a third-party Managed Service Provider (MSP).

Some organisations contract an MSP or reseller to do specific things like providing software licenses, operating a security operations centre, or provisioning new cloud instances when a project requests one.

Others go 'all in', and outsource the provision, design and operation of their business applications (whether as a shared SaaS, an individual deployment that happens to be hosted on cloud fabric in some way or the entirety of an organisation's cloud service provision). There are obvious benefits to doing this, especially if you haven't got the right set of people to do those things yourself. In doing so, you benefit from the expertise, efficiencies and experience of those other companies.

A third party is a third attack surface

Using an MSP is a security trade-off. You will gain the security benefits that come with using the MSP's expertise, which will often include more cloud security expertise than you'll have been able to hire yourself. However, you usually also almost always end up having to give the MSP administrative access to your data. This increases the attack surface, as there are now more systems that, if attacked, would compromise your data.

As such, the MSPs own IT system can be a juicy target for attackers, given that they (and hence any successful attackers) can use that common system to log in to and manage their various customers' cloud deployments. As we stated last year in a joint cyber security advisory published by CISA, it's not just a theoretical risk. Publications from Microsoft and N-able highlight that this real threat uses techniques that are relatively unchanged from those documented by PWC in 2017, and is part of a trend that we expect to continue.

We would hope that such infrastructure is well-defended, and MSPs use different devices and accounts for administrative functions than are used for email and browsing the web. In other words, they implement all the good things we describe in the NCSC's secure system administration guidance and cloud security principle 12. However, we've previously heard of companies not implementing this crucial control, so you should confirm this rather than assuming it.

Check the following sooner rather than later...

For those of you that are already using an outsourced provider such as an MSP (or are considering using one) there are a few things we'd recommend that you check sooner rather than later:

Are MSP's cloud privileges proportionate to what they've been tasked and contracted to do?

If you're using an MSP to manage billing and initial account provision (and nothing else), they shouldn't be able to read your sensitive data, or be able to write configuration to the service. You should apply the principle of least privilege to the access granted to your MSP and their people, avoiding giving them the high privileges that you also try to avoid granting your own staff. For example, you shouldn't give MSPs a permanent root or global administrator account to your cloud accounts as these should be used as a break-glass mechanism. If you must, make sure it's a **conscious decision** to hand over the keys to the kingdom, and limit this to the **specific** ones that they need, **when** they need them.

If you have your own SOC, does it have full visibility of the actions taken on your cloud services by the MSP and their people?

You should expect the same levels of detail that you have when your own developers and administrators interact with your cloud services. Ensure that the SOC can tie specific actions taken in your environment to specific people's accounts (ie that MSPs are **not** using generic shared management accounts).

Does the MSP publish evidence that they follow secure administration practices when interacting with your cloud?

Having established what an attractive target they are, your MSP's security standards should exceed your own levels. As a minimum, their staff should be required to use multi-factor authentication when they authenticate to your cloud's admin interfaces, and this should only be performed from a privileged access workstation.

Does the named MSP have access to your cloud services, or does it show the name of another organisation?

It's possible that your MSP has outsourced the administration of your services to another organisation (that you don't have a *direct* contract with). If this is the case, check that security-related clauses in your contract also cover any suppliers that your MSP is using.

Does your contract with the MSP require them to inform you of any possible breach that affects your service or data?

Also check if they're obliged to work with your incidents team if either you, they, or your cloud provider detect something suspicious. This will need to include any breaches that happened in the MSP's own supply chain.

Finally, the Joint Cyber Security Advisory (Alert AA22-131A) includes a more detailed set of recommendations that help both MSPs and their customers. **We suggest using these recommendations to audit your existing suppliers**, and to determine whether appropriate contractual arrangements are in place for new and existing partnerships.

Gaining confidence in your MSP

As CISA reported in 2021, *"outsourcing IT services provides both increased benefits and risk to an organization"*.

If you're using an MSP to manage your cloud services, the **minimum** bar you should aim for is 'avoid adding unnecessary risk'. You should hold your MSP to the same high standards that you'd expect of cloud providers themselves. Doing so will minimise the security risk.

One way of gaining confidence in an MSP's cloud offering is to treat them as a cloud provider themselves, and measure how well they operate measured against the NCSC's 14 cloud security principles. This approach:

- will consider practical mitigations you should look for (that can complement an assessment of your supply chain security)
- fits quite naturally if they're providing a service that your organisation consumes (as you're effectively treating it as SaaS)

A number of the NCSC's cloud security principles are also relevant for all MSPs that have privileged accesses to your cloud services (including protective monitoring, secure service administration, and providing audit information for your customers). But it's useful to acknowledge that we outsource all sorts of things to MSPs, not just cloud provision. You may already be assessing your MSP's wider services using a framework that covers 'cloud security'; the important thing is that

your chosen framework/standard/process gives you reason to have confidence in your supplier's ability to defend your data and services against attack.

Outsourcing to an MSP can be a great way of making sure that security responsibilities in the cloud are met. Just be sure that you're consciously holding MSP's to the same high security standards that you hold yourselves (and your cloud provider) to.

Andrew A
Cloud Security Research Lead, NCSC

WRITTEN BY

Andrew A
Cloud Security Research Lead, NCSC

PUBLISHED

10 January 2023

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

PART OF BLOG

NCSC publications