Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

How to manage your security when engaging a managed service provider

First published: December 2018
Last updated: October 2021

Introduction

The compromise of several Managed Service Providers (MSPs) was reported in 2017. In response, the Australian Signals Directorate (ASD) provided organisations with the information they needed to protect themselves and others from this threat.

In 2018, malicious actors continued to target and compromise MSPs and, through them, their customers. ASD reiterates the need for organisations to scrutinise the cybersecurity measures implemented in contracted ICT solutions to combat the threat.

Mitigation strategies

This publication shows organisations the actions they can take to manage the security risks posed by engaging and authorising network access to MSPs. Many of the following recommendations apply to any outsourced ICT service provider, not just MSPs.

The number and type of controls used with an MSP will vary depending on the sensitivity of your systems. ASD recommends the following strategies to reduce the risk of compromise via MSPs.

Make sure your own network is secure

Implement cybersecurity guidance, such as the Essential Eight. These eight mitigation strategies are effective in defending against malicious activity such as preventing the execution of malware and reducing the attack surface of an organisation.

Get security in the contract

Security may not be a primary consideration when outsourcing the management of a system; however, the cost of remediation after a compromise far exceeds the cost of upfront implementation.

Clearly state cybersecurity expectations upfront. Ask candidate MSPs to provide evidence of their ability to meet your security requirements while administering your network. During negotiations you may ask a candidate MSP to walk through how they administer a customer's network.

During negotiations, ask the MSP for contact information for other clients. You should be able to have an open conversation about another customer's experience of the MSP's ability to protect customer systems.

Ensure your contract requires your MSP to maintain a good internal security culture, and to implement cybersecurity guidance such as the Essential Eight.

Include cybersecurity incident notification clauses in your contract with your MSP. The MSP must be obligated to notify the customer in the event of any cybersecurity incident that may endanger the customer network. This may include cases in which MSP systems related to the administration, management or storage of information on the customer network have been compromised or accessed by an unauthorised and/or unknown party.

Define the security clearances expected of MSP staff working on your systems and ensure that this is provided to you for validation. There is additional risk from insider threats if the MSP engages staff outside your normal security clearance and background checking procedures.

Control MSP access to your network

To perform their contracted duties, a MSP must administer either a system on your network or your entire network. Without proper controls, this high level of privileged access, combined with the unknown security posture of a network that you do not control, can leave your network vulnerable to intrusion.

Know where the boundaries are between you and your MSP. Ensure that your organisation clearly identifies which systems each MSP can access and how, and keep the record up to date. These accesses should be treated as untrusted for anything outside the scope of the MSP's responsibility. For example, a connection from an MSP into a specific customer system should be treated as an untrusted access with regards to other systems on your network.

Segment your network from the MSP's. This will limit malicious actors' ability to move laterally from a compromised MSP network into the customer network. ASD has observed malicious actors using compromised MSP workstations to move laterally to customer domain controllers located in foreign countries, increasing access to the victim's network. Examples of segmentation include:

- Where an MSP administers an entire network, the customer may stipulate that the MSP network not be used to administer a customer's systems. Instead, MSP staff administer the customer's network from a system within the customer's network.
- Consider segmenting your network into trust zones.

Utilise a secure jump host for MSPs to perform administrative tasks. If a MSP must access your network from theirs, or remotely, specify a dedicated workstation on which MSP administrative staff should perform sensitive administration duties, with restricted access to critical servers. Combine this with multi-factor authentication to limit malicious actors' ability to compromise critical assets.

Mitigate the impact of stolen or abused credentials

Credential management is part of controlling and restricting MSP access to your network. As a key exploitation vector, credentials require special protection. Typically, when malicious actors have full access to your MSP they will have access to all the credentials on their network. This not only includes corporate credentials of the MSP but also credentials for their client's devices and systems managed by the MSP, if they are stored on the MSP system.

Implement least-privilege administration to decrease the impact of malicious actors gaining MSP-level access to customer networks. Provide the MSP with the least privileged account(s) required to do their job.

Strongly control enterprise and domain administrator accounts. Enterprise and domain administrator accounts should have no members by default. Utilise just-in-time principles for privileged accounts like the domain administrator. Use a manual process or privileged access management software to add named accounts to the domain administration role, for a limited duration.

Provide attributable accounts. Accounts should be attributable to the MSP to enable easy identification of MSP activity in privilege allocation and logs. ASD has observed malicious actors using legitimate support accounts provisioned by MSPs to deploy malware to customer networks; rapid attribution of such activity would assist the customer to work with their MSP to remediate compromises of their network.

Enable multi-factor authentication on remotely accessible services used by your MSP to access your network and systems. This will ensure that, even if malicious actors have compromised credentials of MSP accounts, they remain incapable of logging on without a second factor such as a token. Malicious actors have used Remote Desktop Protocol directly from a MSP network to deploy malware to servers anywhere in an administered network; multi-factor authentication can prevent malicious actors from obtaining unauthorised access. Also consider blocking MSP access by default and allowing remote access at an agreed time. Correlate this access with a specific job ticket.

Ensure visibility of MSP actions on your network

Capture relevant logging to improve visibility of potentially malicious activity. Logs should be stored in a centralised location. A security administrator or independent party without access rights/accounts should regularly review logs for suspicious activity in the reviewed systems. Also consider including a contract requirement for your MSP to perform logging of hosts and networks used to remotely connect to the customer environment. Relevant logging includes:

- host-based event logs to provide visibility of malicious activity on workstations and servers
- firewall and proxy logs to provide visibility of network connections associated with malicious actors
- remote access logs to help identify unusual network access from accounts used by MSPs.

MSPs should be responsible for reviewing their logs to ensure their access to the customer network aligns with an actual business requirement and/or job ticket. Further, the MSP should be obligated to provide detailed logs if the customer has security concerns they wish to investigate further.

The recommended event log retention time is at least 18 months; however, some organisations may have a regulatory requirement to retain event logs for a longer period.

Maintaining default sizes of event logs may cause older logs that contained key data to be overwritten prior to commencing an investigation; it is therefore advised that organisations increase the default sizes or forward logs to a central location for storage.

Plan for a cybersecurity incident

Have a practical cybersecurity incident response plan

If you detect a cybersecurity incident, or have been notified by your MSP of a possible cybersecurity incident, ensure you get as much detail as possible. Look for indications of what level of access enabled the cybersecurity incident to occur. A web-facing scan of services is very different to an external system logon, or internal lateral movement. Information to request includes:

- What sort of cybersecurity incident is it?
- What specific data and systems are known to be affected?
- What was the indication that there was a cybersecurity incident?
- Date and time of the cybersecurity incident?

- Is the cybersecurity incident ongoing?
- What actions is the MSP taking to investigate and remediate?
- Has this cybersecurity incident been reported anywhere?

Have a communications strategy

Communicate securely. If the compromise involved your corporate network, you may no longer be able to trust corporate communications. Ensure you have alternate secure communication channels internally and with your MSP. Keep records of any engagement with the MSP for future reference.

Report to the relevant authorities. Firstly, ensure that the appropriate person(s) within your organisation have been notified. If personal information has been lost or compromised, you may be legally required to report the cybersecurity incident to the Office of the Information Commissioner. You should also report the cybersecurity incident to ASD for advice and assistance on how to remediate your network.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Further information for customers on questions they can ask MSPs prior to engaging their services is available in the *Questions to ask managed service providers* publication.

Further information on outsourcing services to cloud service providers is available from the ASD.

The United State's Cybersecurity & Infrastructure Security Agency has also produced guidance on mitigating the risks of engaging with MSPs.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate