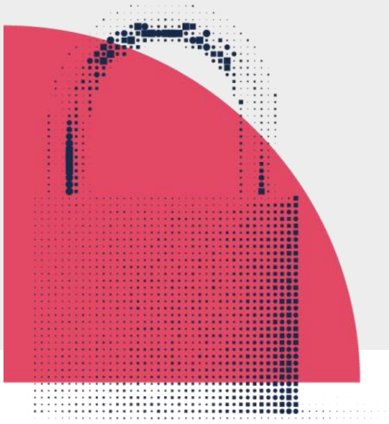
Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

ACSC PROTECT:

# Managed Service Providers: How to manage risk to customer networks



December 2018

## Introduction

The compromise of several Managed Service Providers' (MSPs) global networks was reported in 2017. In response, the ACSC provided stakeholders with the information they needed to protect themselves and others from this threat. Impacted MSPs were made aware, and some are actively managing their own internal response to the threat.

In 2018, sophisticated cyber adversaries continued to target and compromise MSPs and, through them, their customers. The ACSC reiterates the need for organisations to scrutinise the cyber security measures implemented in contracted ICT solutions to combat the threat.

## Managed Service Providers and the ACSC

To provide a level of confidence and improve the standard of cyber security of MSPs, the ACSC has developed an MSP Partnership Program. MSPs are encouraged to participate in the program and provide feedback. Likewise, prospective MSP customers are encouraged to consider their potential providers' participation in this program as a factor in their procurement process. Please see https://cyber.gov.au for more details[1].

## Mitigation strategies

Many of the compromises involving customers of MSPs occurred because MSPs themselves were the initial point of compromise. That is, the customer was not the initial victim; the MSP was the vector to compromise their customers. An MSP must manage the cyber security risks they pose to their customers' systems by protecting their own network from basic intrusion attempts, and by protecting the trust relationship with a customer.

This document provides strategies MSPs can implement to protect their own networks and manage the security risks posed to customer networks. Note that many of these recommendations apply to any outsourced ICT service provider, not just MSPs. The number and type of controls an MSP will utilise with their customers will vary depending on the sensitivity of the customer's systems and data.

[1] https://cyber.gov.au/government/publications/msp-better-practice-principles/

## 1. Ensure your own network is secure

(a) Determine if you have been affected by the recent campaign targeting MSPs. Resources are available from the US's National Cybersecurity & Communications Integration Centre[2] and the UK's National Cyber Security Centre[3]. MSPs should fully investigate any indications of an intrusion and report any malicious activity to the ACSC.

(b) Be aware that an absence of specific indicators of compromise (IOC) is not evidence of absence of intrusion. Cyber adversaries can utilise different tools and infrastructure in different victims, particularly when IOCs are publically or broadly exposed.

(c) Implement a cyber security standard within your own organisation, and promote it in the systems you manage for your customers. For example, the ACSC Essential Eight developed by the Australian Signals Directorate is a prioritised list of strategies to mitigate cyber security incidents[4]. These strategies are effective in defending against malicious activity such as preventing the execution of malware and reducing the vulnerability surface of an organisation.

## 2. Have an upfront and transparent cyber security conversation with your customers

(a) MSPs have a responsibility to protect their customers' data, which includes notifying them of breaches and compromises. MSPs should be transparent when a compromise occurs, including what steps they should take to remediate and mitigate the risk of a compromise reoccurring.

(b) Ensure mutually agreed **cyber security expectations**. MSPs should ensure a discussion about what security a customer can expect is part of the negotiation and ongoing relationship. This should be a differentiator for a good MSP.

(c) Include **breach notification clauses** in your contract with your customer. The MSP must notify the customer in the event of any breach 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. MSPs must consider reporting obligations required by mandatory breach disclosure legislation in Australia.

(d) Understand the **clearance level expected of MSP staff working on customer systems**. There is additional risk to customers from insider threat if staff are engaged outside a customer's clearance and background check procedures.

## 3. Securely administer access to customer systems

To perform their contracted duties, an MSP may administer either a system on a customer network, or their entire network. Without proper controls, this high-level privileged access, combined with potential dependency of a customer on the security of the MSP network, can leave customer networks and data vulnerable to intrusion.

Know where the boundaries are between you and your customers. Ensure that you clearly identify which customer systems you administer and how, and keep the record up to date.

[2] NCCIC - https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers

[3] NCSC - https://www.ncsc.gov.uk/information/global-targeting-enterprises-managed-service-providers

[4] https://acsc.gov.au/publications/protect/essential-eight-explained.htm

(a) Segment the customer network from the MSP's. This will limit an adversary's ability to move laterally from a compromised MSP network into any customer network and vice-versa. The ACSC has observed cyber adversaries using compromised MSP workstations to move laterally to customer networks, including critical systems such as Windows Domain Controllers. Examples of segmentation include:

(i) Where an MSP administers an entire network, the MSP network should not be used to administer a customer's systems. Instead, MSP staff should administer the customer's network from a system within the customer's network.

(ii) Consider segmenting your network into trust zones.[5]

(b) Segment customers from each other, or into risk domains. Ensure that a customer with a high security requirement is not co-hosted or co-managed with low security or higher risk customers. At a minimum, ensure that a customer is aware that they are hosted in a low security assurance area. An example of this behaviour is shared web hosting. In 2018, the ACSC investigated multiple web-hosting providers that were compromised through a vulnerable web service on one client that then compromised the underlying infrastructure due to its poor security configuration, which led to the compromise of all sites hosted on that service.

(c) Utilise a secure jump host to perform administrative tasks. If you must access a customer network from your own network, or remotely, specify a dedicated workstation on which your administrative staff should perform sensitive administration duties, with restricted access to critical servers. Combine this with multi-factor authentication to limit an adversary's ability to compromise critical assets. Detailed guidance on implementing a secure administration environment can be found at: https://www.acsc.gov.au/publications/protect/Secure_Administration.pdf

## 4. Mitigate the impact of stolen or abused credentials

(a) The theft and abuse of credentials is presently a common and effective intrusion vector. Credential theft does not necessarily require the internal network to be compromised, for example, phishing pages and NTLM credential leaks are alternative methods. Typically, when an intruder has full access to an MSP they will have access to all the credentials on their network. This not only includes corporate credentials of the MSP, but likely also credentials for their client's devices and systems managed by the MSP, if they are stored or accessed on the MSP systems.

(b) Credential management is part of controlling and restricting MSP access to customer networks, and limiting the consequence of stolen credentials.

(c) Implement least-privilege administration on customer systems to decrease the impact of cyber adversaries gaining MSP-level access to customer networks. Use the least privileged account(s) required to administer customer networks.[6]

(d) Strongly control enterprise and domain administrator accounts. Enterprise and domain administrator accounts should have no members by default. Utilise just-in-time principles for broad privilege 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.

(e) Provide attributable accounts. Accounts should be attributable to the MSP to enable easy identification of MSP activity in privilege allocation and logs. The ACSC has observed cyber adversaries 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 their network.

[5] https://acsc.gov.au/publications/protect/network_segmentation_segregation.htm

[6] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models.

(f) Enable multi-factor authentication (MFA) on remotely accessible services used to access customer networks and systems. This will ensure that, even if a malicious actor has compromised credentials of MSP accounts, they remain incapable of logging on without a second factor such as a hardware token. Cyber adversaries have used Remote Desktop Protocol directly from the MSP network to deploy malware to servers anywhere in the administered network. [7]

## 5. Record and review MSP actions on customer networks

### Why collect log data

(a) Good logging is essential for conducting an effective cyber security investigation, reducing the overall cost of responding to incidents.

### Data collection considerations

(b) Log data should be collected from diverse sources in order to enable correlation and validation of events. Some data sources and events within those sources are more valuable than others, so consideration should be made to prioritise data collected if storage space is a concern.

(c) Log data should be centralised into one system for correlation, have the ability to be queried with standard alerting and customised queries, and be reviewed.

(d) The following types of data are useful to a cyber security investigation:

(i) **Host-based event logs** to provide visibility of malicious activity on workstations and servers[8].

(ii) **Firewall and proxy logs** to provide visibility of network connections associated with malicious actors.

(iii) **Remote access logs** to identify abuse of legitimate external access.

(e) Maintaining default sizes of event logs, when stored on a local system, may cause older logs that contained key information 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.

(f) Based on ACSC experience in cyber security investigations, a minimum of 18 months logging assists incident investigations.

### MSP and their customers' data

(g) In addition to monitoring an MSP's own network, an MSP must monitor their access to their customer networks.

(h) Consider scheduling remote access to customer networks at an agreed time and correlating logs with a specific job ticket.

(i) Be prepared to provide detailed logs related to customer systems if a customer has security concerns they wish to investigate further.

[7] https://acsc.gov.au/publications/protect/multi_factor_authentication.htm

[8] https://acsc.gov.au/publications/protect/windows-event-logging-technical-guidance.htm

## 6. Plan for a cyber security incident

### Have a practical incident response plan

(a) If you detect a cyber security breach, or have been notified of a possible breach, ensure you **get as much detail as possible**. Look for indications of what vulnerability enabled the incident to occur. For example, a web-facing scan of services is very different to an unauthorised external system logon, or internal lateral movement. Relevant information will ensure accurate prioritisation and messaging. This information may include:

(i) What sort of incident is it?

(ii) What specific data and systems are known to be affected?

(iii) What was the indication that there was an incident?

(iv) What was the date and time of the incident?

(v) Is the incident ongoing?

(vi) What actions are being taken to investigate and remediate?

(vii) Has this incident been reported anywhere?

### Have an incident communications strategy – internally, with customers, and the public

(b) If an incident occurs, and it likely affects customer data, it is better to **be open and transparent with customers** and steer the response, than to wait. If customer data has been stolen, there is a high probability that a third party will discover the breach because the actor is often less interested in your security  and the security of your customers' data.

(i) **Communicate securely.** If the compromise involved your corporate network, you may no longer be able to trust corporate communications. Particularly early in an investigation, ensure you have alternate, secure communication channels internally and with your customer. Keep records of any engagement with the customer for future reference.

(ii) **Report to the relevant authorities.** 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 breach to the Office of the Information Commissioner (https://www.oaic.gov.au/). You should also report the incident to the ACSC for advice and assistance on how to remediate your network, as well as to both contribute to and benefit from the ACSC's broad situational awareness.

(iii) If the incident is reported publically, or is made public during or after investigation, have **public talking points pre-prepared**. If other stakeholders are mentioned in the public communication, ensure they are consulted or notified as soon as possible.

# Further Information

The ACSC has published a PROTECT product for customers of MSPs [9]. This provides mitigation strategies for organisations to manage the security risks posed by engaging and authorising network access to MSPs.

[9] https://cyber.gov.au/government/publications/msp-risk-for-clients/

ACSC has developed a set of questions that customers can ask MSPs prior to engaging their services. The full document can be found at: https://acsc.gov.au/publications/protect/questions-for-service-providers.htm

For services outsourced to a cloud service provider, see ACSC cloud computing advice at: https://acsc.gov.au/infosec/cloudsecurity.htm

The United States Computer Emergency Response Team (U.S CERT) has also produced guidance on mitigating the risks of engaging with MSPs. The full document can be found at https://www.us-cert.gov/ncas/alerts/TA18-276B.

# Contact details

If you have questions regarding this advice, contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).