Cyber | **Insight**

Cyber security: Managed service providers

The following paper is the second in our joint cyber security series with NCC Group, raising awareness of the challenges organisations are faced with in the digital business space.

Asia Pacific

Liberty

nccgroup

As business systems and operations increasingly move into digital environments, many organisations are outsourcing IT operations to a third party Managed Service Provider (MSP).

This paper outlines the benefits and pitfalls of using an MSP, and presents strategies that can be used to mitigate the risk associated with these activities

MSPs are able to perform specific tasks such as managing certain pieces of IT infrastructure and cloud environments or, if necessary, managing the entire IT department function altogether – trusting the third party to provide, design and operate business applications and computing infrastructure. For organisations that do not have the in-house capabilities or expertise required to operate a modern IT department, the benefits of using MSPs to perform such functions are clear. However, while it is possible to outsource IT expertise, it is not possible to outsource the associated risk.

The use of a third party can create additional points of entry that an adversary can exploit to gain access to an organisation's data. This paper outlines the benefits and pitfalls of using an MSP, and presents strategies that can be used to mitigate the risk associated with these activities.

Liberty and NCC Group provide recommendations and guidance from cyber agencies for how to best engage with an MSP – as well as real-world examples of where third party access has been compromised.

A brief history of MSPs

Initially emerging as system builders and vendors for data integration, the function of an MSP and the potential benefits which they can provide have changed shape over time. The steady advancement of Cyber technology since the 1990's has transformed the services an MSP is able to offer an organisation, with factors such as the rise of cloud computing significantly impacting the evolution of the client-MSP relationship and the need to utilise a third party to support day-to-day business activities. A constant which has remained through the evolution of MSP service has been the requirement of access to an organisation's 'crown jewels' – critical assets – whether that involves traditional access to a physical data centre, or the granting of privileged access to an organisation's Cloud environment.

The Global Managed Service Providers Industry Research Report, published in September 2022, provides a market value of MSP services at US$244b in 2022 and estimates that this will expand to US$420b by 2027. The report indicates a compound annual growth rate (CAGR) of 11.04% over this forecast period. In the Australian market the value of MSP services is expected to reach US$620m by 2028.

How to mitigate MSP risk

Organisations can take steps to minimise the security risks that arise from providing an external third party privileged and broad network access. Both prospective and existing MSPs are advised to secure their networks using good industry practice, in effect 'bridging' the difference between an organisation's network security with that of the third party. A recommended strategy is through the hardening of security systems in accordance with guidance from a regulatory body, such as the Australian Cyber Security Council (ACSC), UK National Cyber Security Centre (NCSC) and United States Cybersecurity and Infrastructure Security Agency (CISA). If the data is being poorly protected by an MSP system, a well-resourced adversary will likely be able to bypass sophisticated security controls and could obtain Domain Administrator credentials for the client organisation.

As a result, requirements are recommended when partnering with an MSP to ensure a consistent approach to cyber security:

- Contractual requirements that enforce security control implementation and adherence to best industry practices.
- Restrict access by, for example, implementing jump hosts with limited network access.
- Restrict privileges by using privileged access management tooling, and just-in-time principles to prevent the need to share 'the keys to the kingdom'.
- Prepare for a security incident by ensuring an incident response plan is in place, both for an MSP and their client. Additionally, ensure the plans are subject to regular testing to validate suitability and interoperability.

Limiting MSP permissions and methods of access

MSPs require sufficient access to perform contracted duties. However, it is vital that this is not confused with assuming they require unlimited and unfettered access by default. Unless appropriately mitigated, providing such access can result in a security breach.

When considering the scope of access an MSP will have to an organisation's data, the principle of least privilege (PoLP) can be a useful starting point. Grant the minimum permissions required to function – more can be granted if necessary.

What to consider when providing access to MSPs

- Do the contracted duties require full administrative access to every system, or is it possible to restrict access to nominated systems, and/or network zones?
- Does the MSP require the use of its own systems to administer the network, or is it possible to use a supplied device? Although this introduces additional cost, the system could be restricted to only performing the necessary duties and somewhat remove the MSP network from the risk calculus. An example of this would be a privileged access workstation subject to significant security hardening.
- Understand, define, and document the boundaries between MSP systems and internal systems owned by the organisation. Document the acceptable means of access and ensure security tooling is in place to identify and alert in the event of anomalous activity. In addition, ensure that appropriate follow-up is performed to confirm whether a security incident has occurred.
- Require the MSP to access local networks from a 'jump server', commonly referred to as a 'bastion host'.
- This central point of access is subject to significant security hardening, enhanced logging and monitoring, and offers the potential to implement privileged access management (PAM) tooling. Depending on the sophistication of the chosen PAM tooling, capabilities may include a transparent credential vault, therefore not exposing plaintext credentials, automated credential rotation, and even the ability to record the privileged session for later manual playback to verify any suspected misuse. Additionally, introducing the requirement to use multi-factor authentication (MFA) can introduce further challenges for would-be adversaries.

View our paper on MFA implementation within an organisation.

In addition to restricting the scope and scale of MSP access, utilising just-in-time (JIT) administration can introduce additional hurdles for an adversary with access to an MSP network and a goal of breaching client networks. JIT administration, implemented either in an automated manner with tooling or manually through disabling/activating accounts, is a set of temporary permissions designed to limit the time during which an account can be used to access a network or system.

Through these measures, an MSP employee is granted temporary access to perform a specific task within a client network, and the credentials are valid for a short, set period, or revoked once the task has been communicated to the client as complete. Unless the credentials are exposed during the same timeframe as the legitimate system maintenance activity, the window of opportunity for unauthorised access is greatly limited. This control is effective when combined with password rotation mechanisms, such as a temporary password applied to each JIT session, and/or combined with the requirement to use MFA.

Visibility of MSP activity

Logging and monitoring of systems are important security components that support the detection of malicious or anomalous activity.

The topic of logging and monitoring is broad, and it is important to acknowledge a one-size-fits-all perspective is not the appropriate way to approach an MSP relationship. An alternative and recommended approach is to ensure relevant logs are captured to support incident management. This is to include capturing logs that can answer questions like:

- **Which account ran what process?**
- **On how many systems?**
- **At what time did the process run?**

It is essential that shared user accounts are not used, and accounts are instead attributable to named individuals. Attributable accounts enable the identification of activities performed by individuals during their duties and support the detection of anomalous and potentially malicious activity. When shared accounts are used, it is likely that multiple members of the MSP are using the same account concurrently to access different systems, making the detection of anomalous activity much more difficult.

As a starting point, the ACSC recommends the following log types as useful in supporting an incident response investigation:

- Host-based logs to provide visibility of a number of aspects, including workstations and server activity, running processes and logged-on users
- Network logs, including firewall and web proxy logs, to provide visibility of network connections
- Authentication logs to provide visibility of remote network access activity, for example, which user logged on, and from what IP address

It is also recommended that the logs are ingested into a security information and event management (SIEM) tool, where further correlation and analysis can be performed to identify malicious activity. For example:

- Host-based log activity correlated with network logs to identify a suspicious process initiating unique and unexpected network traffic
- The use of SIEM enables logs to be forwarded from endpoints – including both workstations, servers and network appliances – to the SIEM for long-term storage
- The longer logs are retained for, the further an organisation can historically search for any indicators of compromise (IOC). The ACSC recommends logs are retained for at least 18 months to support security investigations

Source: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring

When shared MSP points of access are used, the origin of malicious activity in a target system is much more difficult to detect.

Recent examples of MSP breach

Operation Cloud Hopper

In 2017, the compromise of several global MSPs by a China-based threat actor was identified. The threat actor used the MSPs as conduits in its global espionage campaign. Given the necessarily close relationship between an MSP and its clients, the exploitation of a single MSP provided the threat actor with access to multiple targets. The threat actor used legitimate and highly privileged access points provided to MSPs for initial access, and, once inside, was able to further move laterally through victim networks deploying additional malware by exploiting legitimate system administration functionality.

Prior to the discovery of the breach, unless a victim had deployed mature and sophisticated security controls, the ability to detect the intrusion would have proved challenging.

Source: https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html

Kaseya VSA

In 2021, the ransomware group known collectively as REvil, were successful in obtaining access to a common product used by MSPs globally – Kaseya VSA. The group used the unauthorised access to VSA tooling to deploy ransomware into organisations globally. While based on available evidence, the group did not have direct access to Kaseya, or MSP networks, the popularity of the tooling with MSPs resulted in multiple organisations in the USA, Europe and APAC being forced to shut down business operations until incident response activities and remediation efforts concluded.

Although arguably organisations both with and without MSPs were impacted, the example nonetheless highlights most organisations reliant on MSPs are unaware of the tooling they use, the frequency with which the tooling is subject to security updates, or the speed at which it is patched by the MSP reliant upon it.

Source: https://www.cyber.gov.au/about-us/alerts/kaseya-vsa-supply-chain-ransomware-attack

https://www.cisa.gov/uscert/kaseya-ransomware-attack

https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961

APT29

A suspected Russian threat actor, identified as responsible for the SolarWinds supply chain compromise in 2021, has been identified as targeting organisations that provide a managed cloud service – Cloud Service Providers (CSP). APT29 sought to breach the CSP and used the Admin on Behalf Of (AOBO) feature to gain privileged access to Azure subscriptions of CSP customers. Due to the underlying technology and features that power the cloud systems, it was possible to gain highly privileged access to the customer systems hosted within the cloud environment without the attacker having access to any customer credentials.

Source: https://www.mandiant.com/resources/blog/russian-targeting-gov-business

Implementation of the '**Essential Eight controls**' as set out by the ACSC is an effective strategy in reducing the risk of a breach of data for both an organisation and MSP.

Responding to a security incident

To be prepared for a potential breach, it is essential that both an MSP and client have an incident response plan that is current, reviewed on at least an annual basis, and subject to regular testing. If a security incident does take place, communication needs to be transparent and securely established between both parties to determine the scope and scale of any intrusion, so that containment activities can be coordinated.

In the incident response plan and in practice, it is important to have steps to notify your cyber insurer as soon as reasonably practicable. Involving the insurer safeguards that the incident is dealt with in accordance with the terms of the insurance policy and the cyber insurer can provide guidance in the response and assist in mitigating any potential financial loss. It also provides benefits in ensuring an alignment with the insurer's claims management approach and reduce potential tensions that could arise from the selection of vendors and the rates they charge.

When responding to a significant security incident, such as a ransomware attack, it is strongly recommended that a specialist incident response provider is engaged. Incident response is a dedicated skill set independent from traditional IT system administration and requires precision to ensure incidents are effectively remediated and, where required, evidence is gathered with a provable chain of custody. If there is no existing relationship with an incident response provider you will be able to access a pre-vetted vendor from your cyber insurers.

In the event an incident is responded to haphazardly by an untrained individual, many risks may arise that can continue to compromise an organisation – from not remediating the breach in its entirety and providing further opportunity for an adversary to gain access, to antagonising ransomware operators through bungled negotiations.

Having an incident response or security service retainer in place additionally provides a reduced time-to-respond, which may offer incident containment opportunities that may only exist for a short period of time – for example, the ability to act before an adversary can further compromise a network, therefore increasing the difficulty of eradication, is valuable. The provider can be engaged to perform proactive 'threat hunts' to comb through an organisation's IT environment and identify any sign of intrusion that may have previously been undetected.

Depending on the extent to which the system was compromised, any unauthorised access to personal information might require reporting to the Office of the Australian Information Commissioner (OAIC), alongside reporting requirements for other regulated entities, such as the Australian Prudential Regulation Authority (APRA) CPS 234.

Appropriate legal oversight and advice should be obtained throughout the process to ensure legal and contractual obligations are met as well as ensuring legal professional privilege is maintained across the range of communications.

Process of adversary access through MSP systems

The diagram details a typical process executed by a threat actor to breach a client system by first gaining access to an MSP account. The process depicted is known as a Cyber Kill Chain.

1

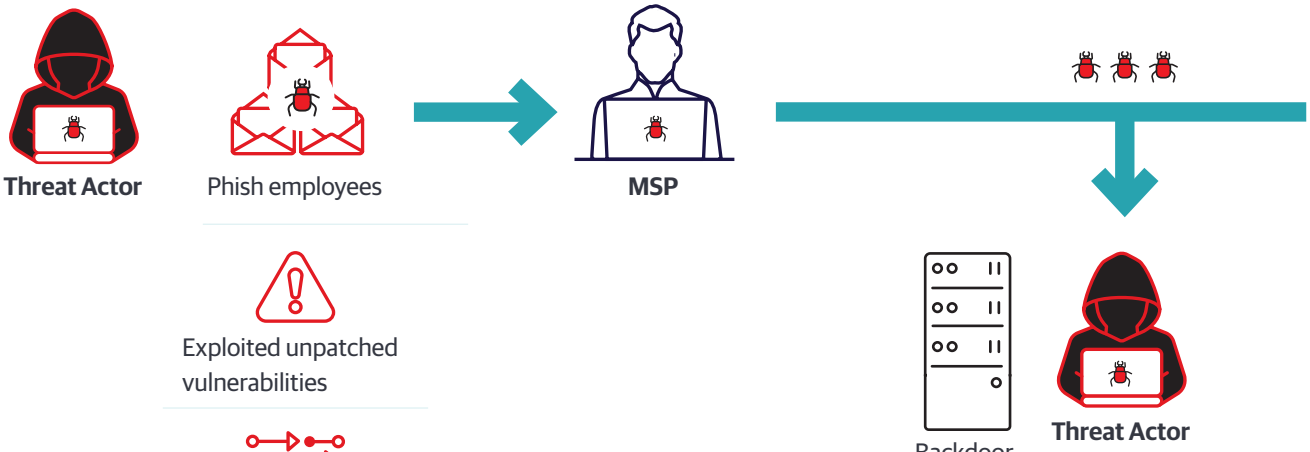
A well-resourced threat actor has the potential to deploy a wide variety of techniques to gain initial access to an MSP system.

2

Once access has been gained, the threat actor will have the ability to move laterally to further compromise systems and access the workstations of MSP employees, as well as the systems they administrate.

3

Using the legitimate access granted to the MSP, the threat actor has the ability to bypass and breach network controls put in place by a client organisation.



4

Once access to the victim system is achieved, they can deploy additional backdoor(s) to gain long-term access. This could include the use of off the shelf and well-known tooling software such as Cobalt strike or Silver. Depending on the sophistication of the adversary, they may additionally deploy custom tooling.

5

Using privileged access – e.g. Domain Administrator – the threat actor has access to key systems and can continue to carry out malicious activities indefinitely if not detected. Actions include but are not limited to deploying ransomware and the stealing of sensitive data.

Third party supplier assurances

The price of security

Traditionally, security has not always been a primary consideration for an organisation when selecting an MSP.

Although the cost of remedying a security incident can likely outweigh any savings gained through the use of a cheaper MSP, common deciding factors have been the price of a particular service when compared to another, and the provider's perceived competence and capability to deliver standard IT services. It can be speculated this is a result of a misaligned perceived value of good security practices versus the 'reasonable' cost at which these services can be obtained from a third party with immature security practices.

When faced with a client's budgetary constraints, MSPs may seek to cut costs, which could include descoping or reducing the scope of services to appear the most attractive when compared to other tenders. Examples of this may come in the form of reducing the number of systems subject to monitoring to save licence costs or reducing the retention period of logs to reduce storage costs.

Although initially, the service may appear attractive from a financial perspective, in the event of a security incident, the length of time required to respond may increase and result in higher costs.

The cost of a security incident may include:

- Impacts to productivity
- Loss of revenue
- Cost of hiring a cyber security incident response provider
- Public relations specialists
- Regulatory fines
- Future losses due to impacted business reputation, which for listed organisations may also directly impact the share price.

MSP Internal Controls

As part of supplier onboarding, MSPs are recommended to be subject to security due diligence that includes confirmation regarding business processes.

- Do they perform background checks on employees?
- How do they manage customer networks?
- How do they segregate access?
- Is it possible to speak with customer(s) who can act as a reference, specifically regarding security practices?

Once the due diligence has concluded, and satisfactory supplementary evidence has been provided, it is essential contractual agreements require the MSP to maintain its approach to security.

This may also include a requirement to, on an annual basis, provide an attestation confirming its security controls have not deviated and, where they have, an explanation as to why. Depending on the size and scope of the MSP agreement, a right to audit clause should be considered, enabling an organisation, or its selected third party cyber security partner, to validate the implementation and effectiveness of the MSP controls and provide an independent assessment.

Contractual liability provisions

Contracts should allow for a reasonable share of responsibility for direct and indirect losses for both the MSP and contracting organisation, with efforts to remedy any damage not being one-sided or unfair from a commercial perspective. The position agreed upon should be balanced in each respective parties potential for liability and take into account the amount paid for the service as part of the MSP agreement.

Notification provisions

Included within the contract should be a requirement for the MSP to notify clients in the event they have been impacted by a security breach incident. For example, any instance in which the systems related to the management and/or storage of client information have been confirmed to, or potentially have been, accessed by an unauthorised third party.

The MSP must also be willing to work directly with an incident response provider, as nominated by the client or client's insurer, to remediate a potential incident. This may include providing relevant 'indicators of compromise' directly to the third party incident investigator to determine the full scope of an unauthorised access event, alongside performing system remediation activities as directed by the client and investigator in a timely manner.

MSP insurances

Clients of an MSP should ensure the MSP holds both Professional Indemnity insurance and Cyber insurance.

Determining adequate policy limits will depend on a number of factors including the size and profile of the MSP. In the event of an outage or data breach there may be numerous clients impacted who seek recovery of financial loss, thus the MSPs policy must be adequate to cover all these potential claims. In Australia, small to medium MSP's typically obtain between AU$5m and AU$10m limits, while larger MSPs obtain AU$20m or greater.

It is important to address with the MSP in the contract or in writing any specific insurance limitations applied by an insurer which will affect the amount of coverage available.

Such limitations commonly include:

- Coverage through Professional Indemnity policies may contain cyber exclusions or sub-limits, while Cyber Liability policies can contain IT or professional services exclusions. This can leave large coverage gaps between the two policies for damages resulting from an error, or omission that was caused or failed to be prevented by the MSP.
- Some insurers apply conditions that restrict widespread coverage for certain events. Such exclusions or limitations include coverage for supply chain attacks, zero-day exploits and severe known vulnerability exploits. An example scenario where the effect of such limitations was seen is the Kaseya VSA attack, in which the method of the breach resulted in a reduced amount of insurance available to MSPs, and therefore to the MSP's client organisations.
- Ransomware exclusions or other ransomware coverage limitations.

A proposed third party agreement should include regular due diligence to ensure a consistent approach to system security.

In summary

Although the benefits of using an MSP for organisations are obvious, it is essential that the risks introduced through engaging an MSP are appropriately mitigated.

- Prior to engaging a prospective MSP, security due diligence is paramount to ensuring the approach the MSP takes regarding information security is compatible with the risk appetite and cyber security of the organisation.
- Security due diligence is to be a reoccurring activity - for example, on at least an annual basis. The MSP is to demonstrate to clients that the security controls implemented during service inception have not degraded.
- Contractual requirements are to be agreed upon between both parties to ensure security control requirements are legally enforceable.
- The systems and network of both parties are to be subject to hardening in accordance with industry best practices, and guidance provided by local cyber security subject matter expertise and governing bodies, such as ACSC, CISA, NCSC.
- Grant MSP system administrators the least privileges (PoLP) required to perform contractual duties.
- Require the use of controlled and limited system access, including employing tight firewall rules, the use of jump host, and privileged access workstations.
- Limit the time frame during which credentials are valid for MSP employees through JIT administration, and rotate passwords where feasible.

Note: Password rotation is recommended where it can be automated, and the MSP employee is not required to select the new password as this may lead to poor selection in the form of easy-to-remember, and easy-to-guess passwords. Password rotation is best performed where password entry is opaque to the MSP administrator due to using PAM tooling. Where password rotation may not be practical, long passwords and passphrases are recommended instead.

- Require MFA as an additional security control for network and system access.
- Log MSP activity at network ingress and egress points, alongside activity performed on systems, including host-based logging. Forward security logs to an SIEM for long-term storage for at least 18 months, as per ACSC guidelines.
- Ensure both parties have an incident response plan in place, that the plan has been reviewed within the last 12 months, is subject to annual testing, and that the respective plans are interoperable with one another.
- Ensure the MSP holds both Professional Indemnity and Cyber insurance and and limitations or exclusions provided by an insurer are addressed to allow potential gaps in coverage to be acknowledged by both parties. This includes coverage limitations for certain services or restrictions depending on the nature and extent of an MSP breach event.

About NCC Group

Liberty engages NCC Group as a cyber security adviser to support clients underwriting Professional and Financial Risk policies.

NCC Group is trusted by more than 15,000 clients to protect their most critical assets from cyber threats. With NCC Group's knowledge, experience and global footprint, they are well placed to help clients identify, assess and treat risks. NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

NCC Group has more than 1,800 colleagues in 12 countries. NCC Group's Technical and Risk Consulting, Incident Response and Managed Services have significant market presence in North America, Europe and Asia Pacific.

For more information please visit:
libertyinternational.com

Office locations

Connect with Liberty

Global reach. Financial strength. Local authority.

Distinct, complex and constantly evolving – every business is as unique as their insurance needs. To confidently progress in the face of risk and uncertainty requires a level of security you can only achieve through working with specialists.

Liberty offers a breadth of world-class insurance and reinsurance services to brokers and insured clients. We bring value and solutions to business and government organisations across Asia Pacific – helping protect what they earn, build and own.