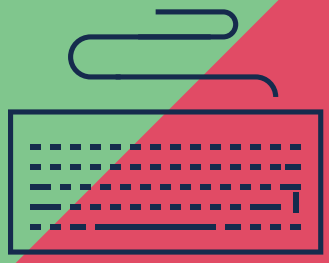
Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Questions to ask your Managed Service Provider



Here are some simple and practical questions that you can ask your managed service provider (MSP), to make sure they're protecting your system and your data.

1 Are you implementing best practice cyber security guidance?

MSPs need to demonstrate best practice cyber security to protect themselves and their customers from risk. The Essential Eight from the *Strategies to Mitigate Cyber Security Incidents* provides prioritised and practical advice to manage cyber threats from targeted cyber intrusions. These threats can stop computers and networks from functioning or enable the theft of data, such as customer details or intellectual property.

2 Are you regularly assessing our cyber security posture?

To protect systems and the information they process, store or communicate, managed service providers must be aware of and appropriately manage security vulnerabilities for their services. This includes regularly conducting vulnerability assessments, analysis and activities.

3 Are you protecting your access to our systems?

Your MSP maintains privileged access to your systems in order to manage them. This level of access exposes your organisation to additional risk of security compromise. Ensure that your MSP is securely managing access to your systems, especially if managed remotely, through secure administration technologies such as multi-factor authentication.

4 Are you protecting users from socially engineered emails?

Socially engineered emails are one of the most common ways that cybercriminals target users. Practical security measures can reduce the risk of receiving emails that may convince users to execute malicious software on their system, visit a malicious website, reveal their credentials or transfer money to foreign bank accounts.

5 Are you backing up our data?

Your or your organisation's productivity and finance can be significantly impacted, due to data loss or system failure during a cyber security incident. Ensuring your managed service provider has a process for identifying and backing up your data is essential. This process should be regularly tested to ensure that successful restoration is possible.

6 Are you prepared for, and actively reporting cyber security incidents?

Experiencing a cyber security incident is not a question of if, but when. The effective preparation for, and management of an incident can greatly decrease its impact. Actively reporting incidents when they occur can assist in early and effective management. A cyber security incident may require additional assistance by specialists to contain the impact and address any security vulnerabilities that have been exploited.

MSP Partner Program

To raise the standard of cyber security of MSPs and provide a level of confidence for customers, the ACSC has developed the MSP Partner Program (MSP[3]). MSPs are encouraged to join the program. Customers should confirm if their MSP will be participating. Please visit **cyber.gov.au** for more details.

Key terms for more information:

- Detecting Socially Engineered Messages
- Malicious Email Mitigation Strategies
- Australian Government Information Security Manual (ISM)
- Strategies to Mitigate Cyber Security Incidents

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing **asd.assist@defence.gov.au** or calling **1300 CYBER1 (1300 292 371).**