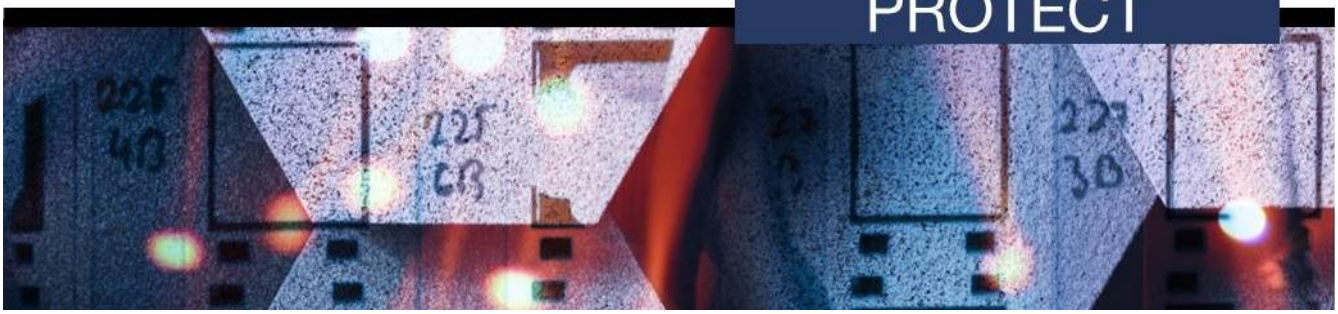

MARCH 2018

Questions to ask Managed Service Providers

Introduction

1. This document has been developed to provide simple yet practical questions to ask managed service providers regarding the cyber resilience of services they provide to your organisation.

Are you implementing best practice cyber security guidance?

2. The Essential Eight from the *Strategies to Mitigation Cyber Security Incidents* is designed to provide prioritised and practical advice to manage cyber threats from:
    a. targeted cyber intrusions and other external adversaries who steal data
    b. ransomware denying access to data for monetary gain
    c. external adversaries who destroy data and prevent computers/networks from functioning
    d. malicious insiders who steal data such as customer details or intellectual property
    e. malicious insiders who destroy data and prevent computers/networks from functioning.

Are you regularly assessing our cyber security posture?

3. In order to protect systems and the information that they process, store or communicate, it is essential that managed service providers are aware of, and appropriately risk manage, security vulnerabilities in the services they provide. This includes regularly conducting vulnerability assessment, vulnerability analysis and vulnerability management activities.

Are you protecting our users from socially engineered emails?

4. Socially engineered emails are one of the most common ways that users are targeted by adversaries. Whether it is to convince users to execute malicious software on their system, visit a malicious website, disclose their credentials or wire money to foreign bank accounts, a number of practical security measures can be implemented to reduce this risk.

5. For more information, see the *Detecting Socially Engineered Messages* publication[1] for users and the *Malicious Email Mitigation Strategies* publication[2] for email infrastructure managers.

[1] https://www.asd.gov.au/publications/protect/socially-engineered-messages.htm

[2] https://www.asd.gov.au/publications/protect/malicious_email_mitigation.htm

Are you backing up our data?

6. Organisations can be significantly impacted, both in terms of productivity and financial loss, due to data loss or destruction from a cyber security incident. Ensuring that your managed service provider has a process for identifying and backing up your data is essential. This process should be regularly tested to ensure backups are correctly performed and successful restoration is possible.

Are you prepared for, and able to respond to, cyber security incidents?

7. Experiencing a cyber security incident is not a question of if but when. The effective preparation for, and management of, a cyber security incident can greatly decrease its impact.

8. For more information, see the *Preparing for and responding to cyber security incidents* publication[3] and the *Cyber security incidents: are you ready?* publication[4].

Are you actively reporting cyber security incidents?

9. Depending on the extent of a cyber security incident, additional assistance by specialists may be required to contain the incident and remediate any security vulnerabilities that were exploited. Actively reporting cyber security incidents can assist in the early and effective management of cyber security incidents by specialists trained in this field.

10. For more information, see the *Cyber Security Incident Reporting* publication[5].

Further information

11. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.asd.gov.au/infosec/ism/.

12. The *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.asd.gov.au/infosec/mitigationstrategies.htm.

Contact details

13. 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).

[3] https://www.asd.gov.au/publications/protect/preparing_for_cyber_incidents.htm

[4] https://www.asd.gov.au/publications/protect/cyber-security-incidents-are-you-ready.htm

[5] https://www.asd.gov.au/publications/protect/cyber-security-incident-reporting.htm