Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

What Executives Should Know About Cyber Security

APRIL 2019

Introduction

Cyber threats to organisations are becoming increasingly sophisticated and targeted. Information that organisation's hold or have access to, if compromised, can provide adversaries with significant political, military or economic gains. Below are five questions on cyber security Executives should be able to answer.

Who would benefit from having access to your organisation's information?

Information is valuable. There are many adversaries who would benefit from having access to your organisation's information. Have you identified critical information of which the confidentiality, integrity and availability is essential to the function of your organisation? Consider not only the value of individual records but also the aggregated value of your information holdings.

What would a serious cyber security incident cost your organisation?

A cyber security incident could affect business continuity. Good cyber security can help avoid direct costs of remediation activities, but also indirect costs such as downtime, lost productivity, and loss of reputation and consumer confidence in your organisation. If information such as customer records, financial data and intellectual property were stolen, could you quickly and accurately determine what was lost? What if you had to take a system offline to conduct a forensic or legal investigation?

Does your organisation foster a strong cyber security culture?

Ongoing staff education and engagement is important. It only takes one malicious email attachment to be opened or one malicious website to be accessed to potentially compromise your entire organisation. Responsibility for protecting your organisation's information should be shared amongst all staff and not left to a single individual or team. Effectively trained and engaged staff who care about protecting the organisation and its information will facilitate a strong cyber security culture.

Does your organisation do the best it can to defend itself?

Cyber security is an ongoing process, not a product. To assist in defending your organisation against cyber threats, have you implemented appropriate cyber security governance, risk management, incident response and business continuity frameworks? There is no silver bullet for cyber security, neither individual security products nor cyber insurance are complete solutions.

Has your organisation applied the Essential Eight?

Help is at hand. The ***Strategies to Mitigate Cyber Security Incidents*** is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of cyber threats. The mitigation strategies can be customised based on your organisation's risk profile and the cyber threats that you are most concerned about.

While no single mitigation strategy is guaranteed to prevent cyber security incidents, all organisations are recommended to implement the eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise your systems.

Further information

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

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).