Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Ten things to know about data security

First published: May 2024

Introduction

This publication has been developed to assist business owners and information technology managers, particularly those unfamiliar with cybersecurity, with ten things they should know about data security.

Fundamentals of data security

Know what data you have

Know what data your organisation produces, collects or is otherwise accountable for and why. Not doing so makes it very difficult to determine its value, where it resides, who has access to it, how it is protected, and what legislative or regulatory obligations may apply. Consider whether it is absolutely necessary to produce or collect data in the first place and whether it needs to be retained or not, especially when it relates to customer data.

Know the value of your data

Know the value of your data. Identify data for which the confidentiality, integrity or availability is critical to the function of your organisation and the provision of your services. Consider not only the value of individual pieces of data but also the aggregated value of your data.

Know where your data resides

Know where your data is stored, especially data that is critical to your organisation and services. Identify what data is kept on employee devices (both corporate and personal), in the cloud (both onshore and offshore), in corporate data repositories and on removable media. Consider external parties that have or may retain copies of your data and where.

Know who has access to your data

Know who has access to your data. Identify both internal and external parties that have access, such as employees, professional service providers, managed service providers and cloud service providers. Identify the extent of access, including whether it is onsite or remote.

Know your threat environment

Know the threat environment your organisation operates within, as this is integral to understanding what malicious actors may gain from compromising your data. Seek out accurate and timely information on cyberthreats from

reputable sources, such as the Australian Signals Directorate (ASD). Join ASD's Cybersecurity Partnership Program as a deeded partner to access near real-time cyberthreat intelligence through the Cyberthreat Intelligence Sharing platform. Being a deeded partner also provides access to ASD publications, services and tools that aren't available to non-deeded partners. Finally, look within your organisation to your experts, such as your chief information security officer if you have one.

Know how your data is protected

Know who is accountable for the protection of your data and what mitigation strategies are in place. ASD's *Strategies to mitigate cybersecurity incidents* is a prioritised list of mitigation strategies designed to assist in protecting your data from a range of cyberthreats. While no set of mitigation strategies are guaranteed to protect against all cyberthreats, a recommended baseline known as the 'Essential Eight' makes it much harder for malicious actors to compromise your data. To assist with implementing the Essential Eight, ASD's *Essential Eight maturity model* can be used to prioritise and tailor its implementation based upon varying levels of malicious actor sophistication and the extent of their targeting.

ASD's *Information security manual* is a cybersecurity framework that you can holistically apply to protect your data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with the Essential Eight and its *Essential Eight maturity model*, complement this framework.

Finally, ASD provides an extensive range of cybersecurity resources, including advice tailored for small-to-medium businesses (such as Exercise in a Box activities), on its cyber.gov.au website.

Know how to verify your data is protected

Know your organisation's cybersecurity maturity and identify areas that require remediation or further investment. ASD endorses suitably qualified cybersecurity professionals, as part of its Infosec Registered Assessor Program (IRAP), to provide assessment services in order to validate and verify cybersecurity measures, identify cybersecurity risks, and where appropriate, recommend suitable mitigation measures. ASD has also partnered with TAFEcyber to provide education opportunities throughout Australia on how to conduct assessments against the *Essential Eight maturity model*.

Know how to backup and restore your data

Know how to backup and restore your data in case you are a victim of a disruptive or destructive cyberattack. Backups of data, ideally segregated into critical backups, essential backups and non-essential backups, should be performed and retained with a frequency and retention timeframe that aligns with your business criticality and business continuity requirements. In performing backups, make sure they are synchronised to enable restoration to a common point in time and are retained in both a secure and resilient manner, such as with a reputable cloud service provider. Finally, restoration of data from backups to a common point in time should be periodically tested in a coordinated manner to identify any issues and dependencies prior to a disruptive or destructive cyberattack.

Know how to respond to cybersecurity incidents

During a cybersecurity incident, such as a data breach, your organisation may experience both significant internal and external pressures. To prepare yourself beforehand, you should know how to respond and recover. Developing a cybersecurity incident response plan, that aligns with your organisation's emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements, can be highly beneficial. Cybersecurity incident response plans should be regularly reviewed and tested alongside activities that target strategic decision making, operational responses and communication strategies.

One person should also be identified as the cybersecurity incident response coordinator for your organisation, such as the chief information security officer, to ensure clarity of direction and timely operational decisions can be made. In large organisations this person should be supported by a director with relevant cybersecurity or risk management skills who can act as the interface to the board to ensure information can be communicated quickly and critical business decisions can be made.

Importantly, all cybersecurity incidents should be reported to ASD via ReportCyber.

Know your legislative and regulatory obligations

Know what legislative and regulatory obligations apply to your data. Depending on your organisation's sector, you may be subject to the requirements of the *Security of Critical Infrastructure Act 2018*. Furthermore, certain customer data that your organisation produces or collects may be subject to archival, financial, privacy or taxation requirements, for example, protection under the *Privacy Act 1988*, including the *Australian Privacy Principles*. Also, depending on the locality of your business operations and customers, you may be subject to the European Union's *General Data Protection Regulation*.

In the event of a cybersecurity incident, you may also have regulatory obligations under the *Notifiable Data Breaches scheme*, which require you to notify the Office of the Australian Information Commissioner and affected individuals when an eligible data breach has occurred.

Independent legal advice should be sought on any legislative and regulatory obligations that may apply to your data.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate