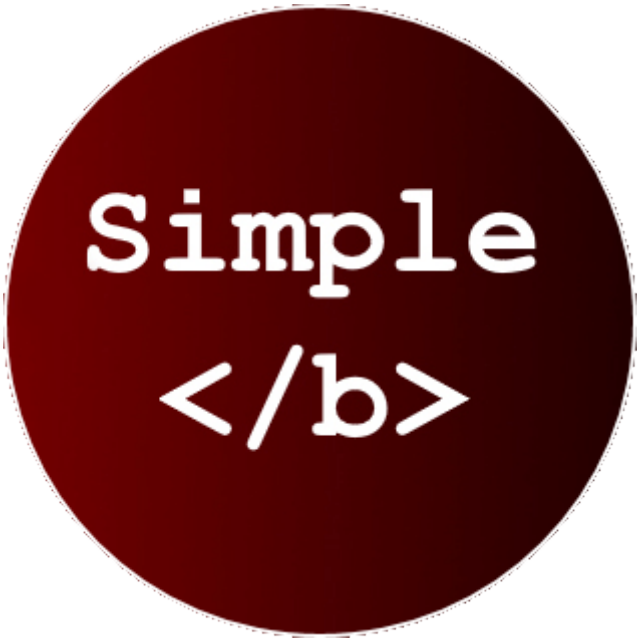

Simple
IT Department
Data Protection Plan

Jess Bayly s3766658
Chris Lai S3866221
Ian McElwaine S3863018
Charles Patterson s3865499
and Jayden Stewart S3863559

Background

- Simple provides an online learning management system (LMS) service called Mentor.
- Simple keeps data in the form of:
  - Records of interactions with clients—Institutions only. No sales to individuals.
  - Billing information.
  - Intellectual property such as source code development
  - Project records and files
  - Marketing plans
  - Commercial-in-Confidence information like contracts and terms of service.
  - Employee records

General Data Protection Principles

As a company that operates within Australia, Simple is required to comply with Australian laws and regulations relating to data security. It is best practise to design our data protection principles based on:

- Compliance with the current regulatory environment,
- A complete risk assessment of the possible causes of data loss.

Inline with Australian Government cyber-security recommendations (Business.gov.au 2020)[1], we recommend the following actions:

- The Simple IT Department should develop clear policies and procedures for the business and employees. In these we will outline security measures to protect our systems and information.
- Produce a cyber security incident response management plan to support these policies and procedures.
- Train new and existing staff on our cyber security policies and procedures. We should include information on what to do if a cyber threat or incident occurs.
- Plan to keep all computers, website and customer portals up-to-date with all software updates or patches.
- Back-up important data and information regularly to reduce the damage if something happens.

We further recommend that a complete risk assessment be completed in accordance with current best practise. (Allodi, Luca, and Massacci, Fabio 2017)[2]

Data Storage Options

We have are three options available to our business for data storage.

Option 1 – Store data on-site on our own Network Attached Storage (NAS).

The benefits are:
a) We have high speed access to our data over our local network
b) We have full control over the data and are not locked to a specific vendor (Shacklett 2018)[7]

The risks are:
a) We need to self-manage the physical infrastructure including replacing hard drives on a scheduled basis to avoid data loss. (Martinez 2018)[6]
b) In the event of a fire or other emergency, there is a risk that the physical infrastructure may be damaged. This could result in data loss and affect business critical functions. (Nuncic 2017)[5]
c) We need to manage cyber-security risks in-house.

Option 2 – Store data with a cloud-service provider

The benefits are:
a) Data management and backup processes are simplified.
b) We have a choice of different Cloud-service providers, with Amazon Web Services, Microsoft Azure, and Google Cloud being the leaders in this space. (Vize, 2020)[3]
c) Cybersecurity risks can be managed with policies across our suite of virtual machine instances and network attached storage (Google, 2020)[4]

The risks are:
a) In the case of internet outage, the company will lose access to its data
b) There is a possibility of vendor lock-in (Shacklett 2018)[7]
c) The cost of a cloud provider may be higher than self-hosting, but this is beyond the scope of this repor.
d) The company is not in full control of our data.

Option 3 – A Hybrid Approach

A hybrid approach would be for Simple to host our data on our own NAS to enjoy the benefits of having local storage, then back up our data to the cloud as an off-site backup. This is scenario that is recommended by the Simple IT Department.

References

1. Business.gov.au 2020, *"Cyber security and your business"*. Commonwealth of Australia, viewed online 25 July 2020, <https://www.business.gov.au/risk-management/cyber-security/cyber-security-and-your-business>

2. Allodi, Luca, and Massacci, Fabio. *"Security Events and Vulnerability Data for Cybersecurity Risk Estimation."* Risk Analysis, vol. 37, no. 8, 2017, pp. 1606–1627.

3. Vize, S, 2020, "Enterprise Cloud Computing Providers: Which Should You Invest In?", Mondo, viewed online 25 July 2020, <https://www.mondo.com/enterprise-cloud-computing-providers/>

4. Google 2020, "*Cloud Storage"*, Google Cloud, viewed online 25 July 2020, <https://cloud.google.com/storage>

5. Nuncic , M, 2017, *"Protect Your NAS Device From Data Loss: NAS Data Recovery".* Ontrack, viewed online 25 July 2020, <https://www.ontrack.com/en-us/blog/nas-devices-data-loss>

6. Martinez, J, 2018, *"12 Things Business Owners Should Know Before Buying NAS Devices",* PC Magazine, viewed online 25 July 2020, <https://au.pcmag.com/business/46483/12-things-business-owners-should-know-before-buying-nas-devices>

7. Shacklett, M, 2018, "5 ways to avoid vendor lock-in", TechRepublic, viewed online 25 July 2020, <https://www.techrepublic.com/article/5-ways-to-avoid-vendor-lock-in/>

Data Storage