Evaluation of Google Docs

ABSTRACT

Google Docs is “software as service” that is widely used around the world. This report explores the viability of a practicable back up plan towards Google Docs, whether those back up plan could be applied in Google Docs. This report also grasps the issues relating to threat in data storage and processing of which Google Docs is classified in. In order to prevent any threats and harmful behavior to the storage and processing, there are several key points to consider classified in the “ESSENTIAL” section of “Table 6B” along with extra pre-cautions that can be evaluated further in the “RECOMMENDED” section to enhance a secure environment.

INTRODUCTION

Google Docs is a free web-based word processor, which is part of a software office suite offered by Google within its Google drive. Users need to have a Google account in order to use this software as service. Google Docs offers storage file along with processes that can be carried out in the web. This software as service is both a storage medium and a processing software; thus it is evaluated with “Table 6B: Backup Plan Using Remote Storage and Processing”. The evaluation of Google Docs with the backup plan is to comprehend which aspects from the clause that is practicable in terms of Google Docs, to ensure no data loss. This evaluation is critical for the users that utilize this software as service to guarantee data integrity, quality, and secrecy along with its accessibility.

Google Docs is under the Google Corporation that is one of the biggest multinational technology companies in the world that specializes internet-related services and products. The size of the corporation is to an extent quite substantial; thus, they should have enough resources to achieve effectiveness and efficiency in the handling of the data along with associated risk that has to be managed. (Hamburger, 2013) This paper will evaluate what backup arrangement that can be implemented on Google Docs according to the “Table 6B: Backup Plan Using Remote Storage and Processing.”

The investigation evaluates if Google Docs can follow the essential backup plan according to the passages in the backup plan arrangements. Any compromise or threats should be taken into account, which then matches with each points in the backup plan to prevent any from happening.

THE ESSENTIALS

INFRASTRUCTURE

We found it on the website of Google Docs that as Google Docs is a free-web based word processor, the storage for the primary copy of file will be stored in the website. This is beneficial for users so that if they lost their data in their devices, a copy will still be available online. The features also allows users to process data in the website under Microsoft Office based software which correlates with the clause from "infrastructure 1.b" although users have to download Google Docs application to process data in their handheld. Any changes done in the Google Docs is automatically synchronize in the website, so that every time the users access Google Docs in different devices, the data will be there without the need for manual synchronization, beneficial to users.

FILE-PRECAUTIONS

According to the website of Google Docs, all the changes in Google Docs are automatically saved as the users' type. A feature called revision history allows user to see old versions of the same document that is sorted by date and the change made along with who change it. This align with clause number two in ESSENTIAL section where continual savings is required if they were to be failure. Although it doesn't make a new file version while making significant amendment, it is to an extent sufficient because it saves it automatically if they were any changes made and revision history also allows seeing version before the changes (align with clause number 3 from ESSENTIAL section.)

Both process and storage is done online in Google Docs, thus, unless the user decides to download the file into their devices, it depends on the user whether they have software to detect and eradicate malware aligning with clause number 4 under ESSENTIAL. According to a Google support specialist Nick (2015) all files going

into the server or uploaded is run through malware detection automatically. If such threats are found then it will also be deleted or processed. This feature is in accordance with clause no.5 under ESSENTIAL section, and it is beneficial for user because it enhances their files safety.

BACKUPS

According to a Google Drive technician Skylar (2015), a full backup is made to Google Drive only when the user made changes to a file or data. There are also no separate storage mediums. Although the automatic backup ensures that every file is up-to-date, the lack in separate backup storage means that it does not align with clause no.6 under ESSENTIAL section. Google Docs also does not align with clause no.7.a. because it does not perform weekly, fortnightly, or monthly backup as it only saves data that is created or modified. So it depends on the user's frequency in using the service in determining the frequency of the backup.

According to the website of Google Docs, the file that is created, stored, and edited in Google Docs can be downloaded to the user's device(s) that acts as a second-level backup arrangement. This reduces the risk of inaccessibility in the case failure occurred to the first level backup along with the risk of simultaneous corruption of the primary and first-level backup. This downloadable feature of Google Docs aligns with clause no.7.b and no.7.c. in ESSENTIAL section. Clause no.8.a. (in ESSENTIAL) is also practicable as the data can be downloaded from the internet but it depends on the user whether they will do so. Google Docs uses Microsoft Office integrated to their data processing. Microsoft Office is widely use and compatible with most operating system, hence data formatted in Google Docs is readily readable in a large array of platforms (align with clause no.8.b under ESSENTIAL section.

Clause 9.a (in ESSENTIAL) can be implemented depending on the user by simply storing it in different storage-medium. In clause 9.b (in ESSENTIAL) could be implemented quite easily by simply downloading the file and storing it in a separate storage medium, which is not online, such as in a device, desktop, laptop, or file storage.

In clause 10.a (in ESSENTIAL) may be problematic, as Google Docs does not have a separate storage-medium according to Skylar (2015). Thus, this means that clause 10.b (in ESSENTIAL) will not be implemented, as there is no resulting disk image because clause 10.a (in ESSENTIAL) is not implemented by Google Docs. This may pose serious risk of contamination in the software online. But as stated before, being substantial in size, assumptions could be made that Google Docs would likely have enough resources to prevent contamination of software, although this is not certain.

RECOMMENDED

INFRASTURCTURE +

The failure of electricity could be a disaster if the user is writing an important essay on PC. The user would have to start all over again before they could save it. The failure of electricity can be caused by blackout, brownout or power surge. Therefore, power-surge protection and UPS are required to prevent these incidents. However, users of Google Docs do not need these. Because Google Docs enables real time save functions. What is type into the document will be immediately sent to Google server without clicking the save button. All files created and changes made on any documents are automatically saved. This precautionary feature from Google Docs is a major advantage to user, to reduce the hassle of saving their work. In relation with clause no.1 under RECOMMENDED section, it is align with the specifications to reduce the loss of unsaved changes.

When using software as service, users need to upload files to the cloud. If the network the user uses is not secure, it will lead to data corruption and data interception. Virtual private network (VPN) enables a computer to use public network as if it were directly connected to the private network. It improves the security of data flow. Users need to choose a VPN vendor and it is relatively difficult to use. If the virtual network is not stable, it will lead to the crash of data flow in accordance with clause no.2 under RECOMMENDED section.

FILE-PRECAUTIONS +

Trojans in users' personal computers can steal the account information and password of Google Docs. Therefore, it is the priority to check whether there are malware on

PCs. Although it is easy to run weekly malware detection and eradication software on all locally stored files, the result depends on the performance of the software you use. Besides, most of security software can be set to automatically run the detection every week.

There is no paper indicate that can show whether Google Docs runs weekly malware detection and eradication software on all stored files or not. However, according to an interview with a Google technical Nick (2015), all incoming files are run through malware detection software; and eradication if such threat exists. It means that Google Docs is aligning with clause no.4 under a RECOMMENDED section. This is beneficial for users as they can rest assure that there wouldn't be any contamination in their files online.

BACKUPS+

According to our research, Google Docs does not encrypt the data before it head off to Google. But users can install CipherDocs, which is a Firefox add-on. CipherDocs, owned by Impartio, is a secure Cloud Storage Solution and it supports the encryption of data in Google Docs. (Campbell, 2011) It makes sure that each packet of data sent to the Google server is encrypted, which means that even single words will be encrypted. As can be seen in Figure1, CipherDocs generates a symmetric key cipher using AES-256 to encrypt documents. The key is stored locally, which means Google Docs cannot have access to the data (aligned with clause no.5 under RECOMMENDED section).

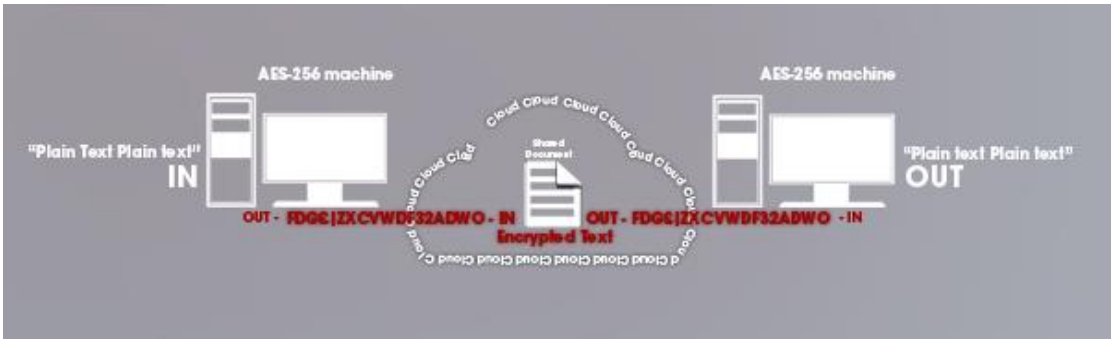

Figure1. How CiperDocs encrypts documents

When the document's owner opens an encrypted stored in Google Docs, the text and the encryption key are fed into the cipher. Then, the document is decoded and shown on the web browser. These happen automatically and the users do not need to do something special. Besides, Google Docs enables users to share documents to other users, and they can edit the document cooperatively. It needs users to share the encryption together. According to Hardiman (2012), the key can be transparently and securely shared via CiperDocs's KeyHub service and it still will not be accessible to Google Docs server, which is accordance with clause no.5 under RECOMMENDED section.

Via an interview with Google Docs, Google technician Nick (2015) stated that Google Docs does not retires a full backup to archive. They do not spool the old archives to new media. It is harmful to users' data. Old archives are more likely to suffer from downtime or event, which could cause data loss. As state before, Google Docs does not have separate backup storage-medium. This means that clause no.6.7.8 can't be applied to this matter. This is to an extent hazardous, but according to Nick (2015), with the advance-classified system that Google Docs implementing, he is assured that there will be no loss of data, no data decay, and concurrency is maintain. As such, a separate backup such as archives and spooling old data to new-media is not needed in this matter.

CONCLUSION

To conclude, the users can implement the practicable backup plan in Table 6B. Most of the clauses in that table is align and in accordance with Google Docs feature, although there is some that can't be implemented. To an extent, Google Docs is a very useful software in terms with the alignment of the clauses from Table 6B, but on the other hand it is also not. Google Docs does not have a separate backup and does not spools old archives to new media, although this is potential hazardous, Google is assured that with the system they are using currently; such demand is not needed. For the average users, this software as service is to an extent sufficient, but for those looking for features such as incremental backup then this service is not for them.

REFERENCES

Campbell, S. (2011). Press Release - Communications Office - Trinity College Dublin. [online] Tcd.ie. Available at: https://www.tcd.ie/Communications/pressreleases/pressRelease.php?headerID=2072&pressReleaseArchive=2012 [Accessed 22 May 2015].

Hamburger, E. (2013). Google Docs began as a hacked together experiment, says creator. [online] The Verge. Available at: http://www.theverge.com/2013/7/3/4484000/sam-schillace-interview-google-docs-creator-box [Accessed 22 May 2015].

Hardiman, N. (2012). Easy-to-use encryption add-on secures your Google Docs. [online] TechRepublic. Available at: http://www.techrepublic.com/blog/the-enterprise-cloud/easy-to-use-encryption-add-on-secures-your-google-docs/ [Accessed 22 May 2015].

Support.google.com, (2015). Overview of Google Docs, Sheets, and Slides - Docs editors Help. [online] Available at: https://support.google.com/docs/answer/49008?hl=en [Accessed 22 May 2015].

(Hamburger, 2013)

(INTERVIEW) Nick 22/5/2015 1:00 pm from https://support.google.com/drive/contact/c2c_drive?hl=en#contact=1

(INTERVIEW) Skylar 20/05/2015 12:24 pm from https://support.google.com/drive/contact/c2c_drive?hl=en#contact=1

APPENDIX

APPENDIX 1 (Interview with Google Technicial Nick)

Points taken from interview with google docs technician Nick

- Google docs does not have separate backup, no archive
- Does not spools old archives to new media
- Google system is quite substantial, so its not needed
- The system is classified
- before data is store in Google server, they conduct malware detection.

APPENDIX 2 (Interview with Google Support Specialist Skylar)