**Objectives**

Do the authors of the report outline clear cyber security goals or objectives? If so, state the cyber security objectives.

|  |
| --- |
| Authors look to ensure that sensitive data does not fall into the hands of third parties which would have consequences for the business. |

**Assessment of Cyber Risk**

How would you rate the overall quality of the assessment of cyber risk within the report?

 very poor



 poor



 fair



 good



 very good



 excellent



 exceptional



Do the authors thoroughly consider the context of risk assessment? If so, state the aspects of context considered. If not, state what the authors should improve.

|  |
| --- |
| Yes. Authors dicuss risk assessment as it relates to the cloud sharing of data in the context of the following areas: Storage of data and documents, freedom of information and other requests, collusion concerns and extensibility and accessibility of applications and other concerns. |

Do the authors appropriately identify cyber risks? If so, state the sources of evidence and process to determine relevancy. If not, state what sources of evidence the authors should consider.

|  |
| --- |
| In the consideration of risk with regard to storage of data, authors cite the US patriots act and dropboxes’ own reports as a reason why data may need to be shared with the US government if it is stored on server stationed in the US as is the case with google and dropbox. Data may also need to be shared due to a freedom of information request as cited in the reference from the Information Commissioners Office.  Collusion is defined and discussed and the case involving the US government vs Apple is cited as an example of a company refusing to collude with the government in order to provide them with their own access to an apple devices storage. This case had implications for data storage in general and is relevant to cyber security. Authors make it clear, however, that risk is still present as the companies mentioned above reserve the right to disclose data for legal reasons without consent.  Authors cite news articles and Microsoft with regards to third parties gaining access through employees personal devices and home networks and user authentication being stolen.  [*This guy has just copied and pasted my work into the review box???*] |

How would rate the analysis of the identified cyber risks?

 too heavy



 about right



 too light



How would rate the evaluation of the identified cyber risks?

 too heavy



 about right



 too light



**Policy**

Does the policy appear to communicate a strategy for dealing with perceived cyber risks?

 Yes



 No



 Don't know



Does the policy demonstrate an understanding of the asset(s) to be protected? If so, state the asset(s) you perceive the policy is attempting to protect. If not, state the asset(s) the authors may want to consider.

|  |
| --- |
| The policy demonstrates an understanding of the assets to be protected and makes it quite clear that personal/financial information as well as copyrighted materials should not end up in the hands of third parties. |

Does the policy reflect consideration of domain best practice, rules and regulation?

 Yes



 No



 Don't know



**Metrics**

Do the authors attempt to understand what the success of the intervention would look like? If so, state how they determine the success of the intervention. If not, suggest how the authors could determine the success of the intervention.

|  |
| --- |
| The authors do not state how they would determine the success of their intervention. Perhaps a regular review of the impact of the policy on members of staff and the data which is being shared by staff to services such as google and dropbox. Something along the lines of regular monitoring and random checks by compliance/IT staff to see check what and why data has been uploaded to the cloud. [*This is in line with what review 1 said, and I agree, need to change our discussion section, but that’s fine. Also, thanks for the idea, guy! lol*] |

Do the authors attempt to understand the implication of any suggested interventions? If so, state how they explain the implication of any intervention. If not, suggest how the author could better understand and explain the implication of intervention.

|  |
| --- |
| The authors understand the implications of their intervention and make it clear that the policies that they have proposed will help protect the company from financial and legal liabilities by helping to safeguard personal and financial information of its customers, employees and private information about the company its self. |

**Communication**

Does the policy communicate directives in a clear and concise manner to all stakeholders? If so, indicate how the policy communicates effectively. If not, indicate how the authors could improve clarity of communication.

|  |
| --- |
| The policy is quite clear and concise with regard to what kind of data should and should not be uploaded to the cloud. The only way that I see that it could be made any clearer would be via the use of examples of what is and is not acceptable to be on the cloud and a more thorough explanation of elements within the policy such as encryption and industry standards and why they are relevant/beneficial. [*Noope, I think that’s a bad idea to put in a policy document.*] |

How would rate the number of references in the report?

 too heavy



 about right



 too light



One-page review

The one-page review should have 1-inch margins all around, A4-size, 12-point font and be in PDF format. The one-page should prioritise areas of improvements for the authors. Teams may want to consider the questions within the interactive rubric when they create their one-page review. In the review, teams should support other teams in improving their drafts, by

* advising the authors what they should **start** demonstrating in the report that is currently missing or incomplete, e.g. proper identification of cyber risks.
* advising the authors what they should **stop** doing within the report itself, e.g. what is not working or is causing confusion. ·
* advising the authors  what they should **continue** doing within the report itself, e.g. referencing strong evidence that cements arguments.

Teams should view the review as opportunity to prioritise to authors what would dramatically improve the draft report. Team members may think there are many areas of improvement, but they should demonstrate that they have prioritised key areas of improvement. Teams are encouraged to discuss and decide the key areas of improvement. Teams should offer advice on how to improve the draft, even if the draft itself is sparse, lacks content or has taken the wrong direction.

**1 page review**

The document as a whole considers and discusses the risks related to cyber security well and covers all the key areas. The authors provide references for most of the relevant information and backs up most statements with suitable references with the exception of a few occasions where comments may come across as baseless, for example:

“…it is highly unlikely that the large companies which control the lion’s share of personal clouds would risk the reputations of their businesses or the trust of the public in their services to participate in such deals. This has in recent times been an issue involving a number of these companies and the United States government…”

“…perception of the key decision makers that BYOD brings benefits…”

As mentioned above, generally well referenced. However the references compiled in the bibliography need to be referenced appropriately.

There is also a lot of repetition within the document. Particularly in the risk assessment portion. Areas with the greatest degree of repetition between the first portion and risk assessment are the Freedom of Information and Extensibility sections.

Be careful of contradictory or inaccurate statements. The collusion concerns area of the risk assessment states that large cloud sharing companies would not risk their reputation through collusion but the very next sentence states that collusion has been a concern involving a number of these companies. [*I think he’s misunderstood what I was trying to say, I can look at that bit and rewrite to be clearer but it wasn’t contradictory it was discussing a point.*]

The authors jump back and forth between discussing consumer based and business based cloud services. This creates confusion as it becomes less clear what type of service is being referred to in certain parts of the document. It would be simpler to cover both areas individually and clarify the differences between the two and then state [*We’re only supposed to cover consumer based, need to go through and check where we talk about business based cause that can’t be in there.*]

The policy is concise and well considered but may wish to present extra examples of which data is appropriate for the cloud, primarily for the benefit of inexperienced or unobservant employees. For the same reason, the authors may wish to explain what certain elements of the policy are and why they may be beneficial/important. E.g. encryption and industry standards.

[*No to examples in policy but maybe put them in implementation/evaluation?*]

The authors also need to consider how they would measure how their policy would impact on the security of data held by the company and what steps could be taken to ensure that policy is being followed.

[*Discussion section re-write, I agree.*]

The authors should continue to reference appropriately and expand upon their suggestions and ideas, why they would they beneficial and how they would measure the effects of their policies. Expanding upon these areas should not be an issue with respect to the size of the document, provided that the authors remove much of the repetition mentioned above.

P.S. “Solutionise” is not a word. [*I mean, it is, its just spelt* ***Solutionize****, reviewer doesn’t need to be a dick.*]