

The Security and Risk Management of Digital Assets and Connected Data

Simon Chen

Teachers College, Columbia University

HUDK 4050: Managing Education Data

Professor Amy Nurnberger

Reflection Paper

The articles portray a theme of security, safety, and risk management in digital assets and connected data. In the article written by A White (2013), the main issues addressed include the Research Data Programme that was meant to pilot and set up institutional services. It portrays the significance of managing risk and compliance using the research data programs. Another article by Grindley (2015) dictates the importance of the digital curation sustainability model as it is used to sustain digital assets in the future. The issue of security, safety, and risk management is also addressed in the article that states the user's guide to help keep the research data safe (Charles, 2011). The guide is expected to help identify the current and future costs and compare the costs to develop a charging policy for projects. Barend Mons (2020) stated that the expertise, metadata, infrastructure, and technology to re-use data are lacking. Therefore, to ensure that data is safe and available for re-use and sharing, five percent of the overall research cost should be directed to data stewardship, which will help cater to the necessary actions.

Last week, in our workplace, some data went missing due to the collapse of some machines. The machines were old enough, and their decline to work did not come to us as a shock. However, my team has been raising the issue with the company, which was not addressed for a long time. We tried to explain the risks to the data we had if the machines were not replaced, but since the manager was not an IT person, he could never understand our concerns and let them pass. My team knew that we were risking losing a whole load of data, and we could never recover it if lost. Again, we will not be able to share the data as we had to do another research if we lost it.

As an IT person, I felt that the company had failed to invest in the right channels and structures that would help keep the data safe. Once the machines collapsed, everything was gone.

We could no longer access the data or share it, and we were back to researching new data, which delayed work for a few days. In this case, the company should have access to a user guide to help all the employees keep the researched data safely. Again, it should invest in machines that are up to technology to ensure that all data is protected and even in cases of tragedies, risks, and other issues, there will always be a back up to help retrieve the data. In addition, the company should have a budget set aside to cater for technology and infrastructure that will help re-use data on several occasions. This will also call for experts who will help control the data or even train the employees on how to protect data for re-use. This will only be achieved if the company has strategies and setting aside some funds to facilitate the changes and not wait when tragedy arises to take action. The company should be ready to take care of its data at every cost for the digital assets' safety, security, and risk management.

References

- Mons, B. (2020). Invest 5% of research funds in ensuring data are reusable. *Nature*, 578(7796), 491–491. <https://doi.org/10.1038/d41586-020-00505-7>
- Beagrie, C. (2011). pdf (Section 4).
JISC. https://www.beagrie.com/static/resource/KeepingResearchDataSafe_UserGuide_v2.pdf
- Grindley, N. (2015). The Digital Curation Sustainability Model (DCSM) Collaboration to Clarify the Cost of Curation (4Cproject.edu). <https://www.4cproject.eu/documents/DCSM-V1.01-18Mar2015.pdf>
- Whyte, A. (2013). The sweet smell of sustainability—JISC MRD projects make the business case. Digital Curation Centre (DCC). <https://www.dcc.ac.uk/blog/sweet-smell-sustainability-jisc-mrd-projects-make-business-case>