Research Proposal Presentation – Robert JAMES

Slide 1

Project Title and introduction

Hello. My name is Robert James, and I am a student at the University of Essex.
This presentation is part of the Research Methods and Professional Practice Module, which itself is a part of the Cyber Security Masters programme.
The presentation is a Research Proposal for the final Capstone Project, which is the final Module for the Master's Degree.

The title of the research proposal is "Adoption of the CLOUD for Data Services: how secure is this data, before, during and after migration to the CLOUD, and the risk to data security versus "on-premise" storage.

As this Research thesis would be part of a Cyber Security Masters, it must fall into a CyBOK knowledge Area category. CLOUD services would fall under the Distributed Systems Security tree (Cybok, 2021), with some of the topics reaching into some of the other relevant branches within the CyBOK framework as well.

Slide 2

Significance of Research to the Problem

What is the significance of this research, and how could it contribute to resolving the problems?

CLOUD computing to many people, is unfamiliar, but it is a pervasive technology nevertheless. In the private sector, people are using the CLOUD to backup data on their iPhones to the iCloud, on their Android handsets to the Google CLOUD, and even their personal Microsoft Office data to Microsoft OneDrive. Many people are not aware of the security aspects of storing their data in this manner, beyond the use perhaps, of a standard account name and password combination.

These risks to security of the confidential data hosted in the CLOUD, are exacerbated in the corporate world. It is estimated that in 2023, more than 94% of enterprise organisations, will use the CLOUD to some degree, many in a design known as "hybrid CLOUD" which is a mix of legacy on-premises and CLOUD-based infrastructure (Cloudzero, 2023). The graphic (Javapoint, ND) details some of the most often quoted benefits for CLOUD adoption.

Slide 3

Gartner (Gartner, 2022) project that this trend will continue to increase in the next years as seen in the graphs upwards trend, with an estimated 65.9% of corporate spending being on applications that can be CLOUD based by 2025, versus 57.7% in 2022, with IT spending in 4 key areas increasing to 51% from 41% over the same time period.

Slide 4

Corporate risks associated with unauthorised data access are huge, so minimizing any security risk or risks is a priority. This is regardless of where any data is stored, but with the current trend to move to CLOUD being so prominent, it is important to determine, if there are risks with the deployment, what the risks are, and why, and if they can be controlled or minimized in some way (SwissCyberInstitute, 2021).

This is relevant to Industry, as many Enterprises are moving completely, or in a hybrid manner to CLOUD computing. The research could be interesting to IT leaders, data governance specialists, and of course, the accountants that control the corporate budgets. With the information gleaned from a relevant report, it will allow these leaders to determine a risk analysis plan, budget for training/consultancy as appropriate, as well as help them to avoid common problems associated with CLOUD throughout the complete deployment lifecycle.

The benefits to companies from migrating some, or all of their data to the CLOUD are varied, but with reduced cost and simplification often cited as the main reasons, they are determining factors for many enterprises (Ibistechnology, 2023).

Slide 5

Research question

What is the question that the research is trying to answer?

At this point, there are 2 potential ways of phrasing the question that we will try to answer as definitively as possible.

Is confidential enterprise data as safe or safer, when it is held in a Service Provider CLOUD, than when it is under direct control from an Enterprise Team “on premise” in a traditional “legacy-type” Datacenter?

Or

Is confidential Enterprise data, inherently more at risk when stored in a Service Provider CLOUD, when compared with the same data stored onsite in a traditional “legacy-type” Datacenter?

Aims and objectives of the research

What are the aims and objectives of the research, what do we hope to show when the research paper is completed and submitted?

The main aims of the Research Study, is to try and determine if the legacy on-premises and self-managed model, is more secure than using the CLOUD environment, if CLOUD deployment is more secure, or if from a neutral standpoint, there is effectively no difference between the two.

If there are differences, the research will try to identify reasons why it could be so – what are the causal factors, and potentially suggest remediation methods to secure the data further in a CLOUD deployment, or suggest further avenues for additional research.

There are different potential factors that appear to be contributors to deploying and managing a secure CLOUD deployment.

Is CLOUD inherently more insecure than on-premises, simply by nature of what it is, the storage of sensitive data off-premises, and therefore, can never be classed as truly secure, or is the security dependent on other factors, that will determine the level of safety of the data?

Analysis of the Secondary and Primary data, should aid us in answering the research question.

Slide 6

CLOUD deployments are always going to have an element of shared responsibility, however, there are different management/deployment models available (Redhat, 2021). These include models called Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS), among others, and they all come with differing levels of control and management, shared between the CLOUD Service Provider and the original Enterprise IT Team. The graphic shows the split of responsibility between the different models (Redhat, 2021).

Does this sharing of roles play a significant part in the perceived risk as well? Is there a preferred model of management, that balances the risk better than the rest?

It is possible that leaving the responsibility for security with the CLOUD Service Provider, actually makes the deployment far more secure than it would be in the hands of the Enterprise IT. Conversely, it could be that the CLOUD Service Provider, has so many customers, it is not reasonable to expect the required level of focus, so the Enterprise IT Team must keep ownership of that responsibility with themselves.

The research may also indicate that the best fit is somewhere in between, with clearly defined roles and responsibilities.

Slide 7

As mentioned previously, a large number of Enterprises, implement different CLOUD models, including the Hybrid model of CLOUD deployment, where they keep some data in their own managed Datacenters, and they move other data to the

CLOUD (Tavbulatova et al, 2020). Many customers also utilise multiple, different CLOUD Service Providers at the same time, but for different purposes or applications, or even to avoid CSP lock-in (cybersecurity-magazine, 2021).
The graphic by the author, is a simplified view of the 3 main models.

Do these types of deployment, add to the complexity sufficiently to make the deployment inherently more insecure, or, would this complexity necessitate the training and understanding of the staff to such a level, that the end result is increased security of the data stored?

Slide 8

This factor of staff education and training for the Enterprise Team is relevant. CLOUD deployment, whilst logically simple, introduces significant complexity that is different to what many IT staff are familiar with.

How much impact does staff knowledge and understanding have on the result of a successful and secure ongoing deployment?

None of these factors can be taken in isolation, and the objective is to try and determine where the weaknesses are as a whole, and more importantly, how they can be overcome.

A Null hypothesis will be posed, to try and determine the relationship between Enterprise and CLOUD data security.

The working null hypothesis for this research study is **"There is no difference in data security levels, for data stored in the CLOUD environment versus onsite at Enterprise IT managed Datacenters".**

Slide 9

Key literature related to the project.

With CLOUD adoption being so widespread, there is an abundance of information available through many different, reliable sources. Where some literature is taken from industry sources, care will be taken to ensure that any bias shown, does not influence the research. Where Industry BLOGs are typically not seen as a reliable source, they often have the best access to statistics and industry knowledge, so should not be discounted.

There are many research documents available in Google Scholar, and through increased citation searching with more appropriate headings, as one becomes familiar with the documents, it becomes easier to find more relevant research studies.

There are very often stories in the IT press, regarding further data breaches of CLOUDs for different reasons, however human error is often said to be to blame. Chen et al, (Chen et al, 2021) highlight a link between the move to CLOUD and security breaches increasing. However, in the same report, they note that human error or accidental loss accounted for 53% of data breaches, and that the legacy

attack methods such as malware, phishing and social engineering, still exist, regardless where the data is stored.

Whilst praising the benefits and flexibility of the CLOUD, Singh et al (Singh et al, 2017) then go on to say that “there are many security and privacy concerns that obstacle to adoption of CLOUD computing. They also agree with Chen, that CLOUD computing, by way of its connectivity, allows for more attack vectors than traditional on-premises data storage.

Alouffi et al (Alouffi et al, 2021) were initially quite scathing in their review of CLOUD security, pointing out, in their opinion, that the main flaws were data tampering and leakage. However, later in the paper, they conceded that with the right security and management policies in place, the advantages of CLOUD computing could be realized. The common problems such as hacking and other unauthorized intrusions, can be prevented or managed, with security policies and encryption. This is the same for on-premises data as well.

Kafhali et al (Kafhali et al, 2022) have put together, a very interesting paper, where they critically appraise the CLOUD security features and vulnerabilities. Other than the fact that CLOUD needs to be available 24/7, the vulnerability and threat vectors listed, are in the majority of cases, also relevant to on-premises data. They also conclude that a CLOUD environment that is built with security and privacy in mind, can be fit for purpose.

These are just some of the many published research documents available for review.

There are many avenues to explore, and whilst initial observations would possibly point to the CLOUD being more of a security risk, there are also many documents that counter it by insisting on appropriate security controls to mitigate the risk.

The proposed topic of research, appears to be valid, as there are multiple viewpoints that should be assessed.

Slide 10

Methodology/strategy of the research and timeline

What is the strategy for the research, how will we perform the research for the study.

What is the timeline that it will be performed over?

The research will be performed in different, clearly defined steps, to enable the processes to fit together neatly.
Research timeline is based on a high-level 4-month timescale from start to finish.
Timelines can be quite fluid dependent on receiving enough questionnaires back to perform detailed analysis earlier.
This may need to be adjusted in due course.

Month 1
Initial thorough secondary research of existing papers and documentation, will be performed, to get an overview of where the current knowledge areas are strong, and where there are currently gaps in the data.
This will be documented, as it will be re-evaluated again later in the study.

Month 2
Once this has been done, we will begin primary research. A questionnaire will be devised, based on the secondary data presented so far, and include focus on the gaps identified. It will contain a mix of quantitative and qualitative questions, and will be aimed at a range of technical IT people. This is necessary to get informed responses in the questionnaire.
The goal will be to try and enforce what we already believe to be true, based on the secondary research, but it will also try and cover any gaps identified as avenues of further research.

Secondary research will continue whilst waiting for return of questionnaires.

Month 3
Perform primary research analysis - receive back questionnaires, analyse in detail and try to establish patterns in the responses that could help to support or counter the secondary research already performed.
Try and ascertain if the secondary research results, are mirrored in the responses from the questionnaire, and if any conclusions can be drawn.

Month 4
Complete analysis of received data, accept or reject the Null hypothesis, present statistical data, and complete research paper, to show all findings from primary research, and contrast it with secondary data already collected.
Present conclusions to this point, and propose additional study as appropriate.
Any avenues for further research will be identified and stated.

All evaluation of data, will be performed without bias.

Slide 11

What artefacts will be created during this research?
This research will consist of the following artefacts –

Questionnaire – a questionnaire will be created, to try and understand current technical understanding from IT people, that would potentially be responsible for current or future CLOUD deployments.

Statistical analysis – results of the questionnaire will be analysed and presented, in order to try and obtain relevant statistics.

The final report itself.

Slide 12

Ethical considerations and risk assessment.
When writing the questionnaire, and asking people to participate, there are a number of factors to consider.

People have a right to confidentiality and anonymity. As such, the questionnaire should be written in such a way that it is not possible to identify the respondents, based only on looking at their completed form (Qualtrics, 2020).

People also need to understand the questionnaire is voluntary and what the data will be used for when they are asked to participate. The survey should begin with a short paragraph (or 2), to describe how it be presented in the finished research paper.

Data protection/confidentiality should be foremost in the mind when performing tasks of this nature, as even innocent lapses of data security, could have wide-ranging consequences. Standards such as the GDPR and others, must be adhered to (GDPR, ND).

The survey should also be written in a respectful way, with no questions that are able to be misinterpreted in a harmful way to some respondents. There should be no questions that could belittle or offend.

References:

Alouffi, Bader. Hasnain, Muhammad. Alharbi, Abdullah. Alosaimi, Wael. Alyami, Hashem. Ayaz, Muhammad. (2021). A Ststematic Literature Review on Cloud Computing Security: threats and Mitigation Strategies. Available from: https://ieeexplore.ieee.org/abstract/document/9404177
[Accessed 15 October 2023].

Chen, Danny. Chowdhury, Minhaz. Latif, Shadman. (2021). Data Breaches in Corporate Setting. Available from: https://ieeexplore.ieee.org/abstract/document/9590974
[Accessed 15 October 2023].

Cloudzero. (2023). 101+ Cloud Computing Statistics That Will Blow Your Mind. Available from: https://www.cloudzero.com/blog/cloud-computing-statistics#:~:text=Cloud%20adoption%20among%20enterprise%20organizations,this%20survey%20of%20800%20organizations.
[Accessed 11 October 2023].

Cybok. (2021). Distributed Systems Security Knowledge Area Version 1.0.1. Available from: https://www.cybok.org/media/downloads/Distributed_Systems_Security_v1.0.1.pdf
[Accessed 11 October 2023].

Cybersecurity-magazine. (2021). What is Vendor Lock-In and how to avoid it? Available from: https://cybersecurity-magazine.com/what-is-vendor-lock-in-and-how-to-avoid-it/
[Accessed 15 October 2023].

Gartner. (2022). Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025. Available from: https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending
[Accessed 11 October 2023].

GDPR. (ND). What is GDPR, the EU's new data protection law? Available from: https://gdpr.eu/what-is-gdpr/
[Accessed 15 October 2023].

Qualtrics. (2020). Ethical issues to consider when conducting survey research. Available from: https://www.qualtrics.com/blog/ethical-issues-for-online-surveys/
[Accessed 15 October 2023].

Redhat. (2021). IaaS vs. Paas. vs. SaaS. Available from: https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas
[Accessed 11 October 2023].

Singh, Ashish. Chatterjee, Kakali. (2017). Cloud security issues and challenges: A survey. Available from: https://www.sciencedirect.com/science/article/pii/S1084804516302983#f0010 [Accessed 15 October 2023].

SwissCyberInstitute. (2021). 21 Cloud Security Statistics You Probably Didn't Know. Available from: https://swisscyberinstitute.com/blog/21-cloud-security-statistics-you-probably-didnt-know/ [Accessed 15 October 2023].

Tavbulatova, Z K. Zhigalov. K. Kuznetsova, S Yu. Patrusova, A M. (2020). Types of Cloud Deployment. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/1582/1/012085/pdf [Accessed 15 October 2023].

Figures:

Gartner. (2022). Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025. Available from: https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending [Accessed 11 October 2023].

Javatpoint. (ND). Advantages and Disadvantages of Cloud Computing. Available from: https://www.javatpoint.com/advantages-and-disadvantages-of-cloud-computing [Accessed 15 October 2023].

JPT, (2013). Ethics and Integrity Matter in the Workplace, Part 1. Available from: https://jpt.spe.org/ethics-and-integrity-matter-workplace-part-i [Accessed 15 October 2023].

SwissCyberInstitute. (2021). 21 Cloud Security Statistics You Probably Didn't Know. Available from: https://swisscyberinstitute.com/blog/21-cloud-security-statistics-you-probably-didnt-know/ [Accessed 15 October 2023].