Research of the concerns

Cloud services have become a mainstream data storage solution for businesses, governments, and consumers, and like with Mostel & Wilder (M & W), cloud-based file storage has become the expected method for file sharing. However, Cloud environments are not an entirely secure space, and therefore pose many risks to an enterprise (Walden, 2013). Security is the top concern amongst Cloud users (Fixya, n.d.), and with multiple reports on data breaches, compromised credentials, and account hijacking throughout the years of its existence, consumers have every right to be concerned (Rashid, 2016).

The main concern regarding security in Cloud computing is the location of the data centres and servers used by the Cloud service providers to store data, with an issue persistent enough to warrant legislation. However, data protection and security differs between territories, and thus poses territorial challenges in deciding which country's law is applicable when an issue arises. For example, the EU has very strict data protection rules, and are substantially more restrictive than the rules of other territories (Voigt & von dem Bussche, 2017), and European law, covered in the Data Protection Directive 95/46/EC, does not allow exporting of user personally identifiable information (PII) unless the company can demonstrate they will protect the European user's privacy and data (Maunder, 2015). It is understood that an EU member state's law will apply when the establishment of EU-based controller located in its territory processes personal data, and when the controller outside of the EU uses an EU based data centre within the territory (Kennedy & Millard, 2016).

Furthermore, the Data Protection Directive details the purpose and effect of data protection, and guidelines of the transfer of personal data internationally; whilst there are no restrictions on the transfer of personal data to other European Economic Area (EEA) countries, the act requires special precautions to be taken when personal data is transferred to countries outside of the EU/EAA, as no adequate level of protection is guaranteed. In comparison, the US does not have any comprehensive federal law regulating the collection and use of personal data, which led to an agreement between the EU and US, known as the Safe Harbour Privacy Principles. Signed in 2000, the agreement between the US and the EU and Switzerland contained seven privacy principles for which US companies that stored EU customer data would adhere to, to comply with the EU Data Protection Directive. That was until a court ruling declared the Safe Harbour framework invalid in October 2015, when it was discovered that the US National Security Agency perform surveillance on technology companies, and so the US government, which was not held to the Safe Harbour agreement, can access the data of EU citizens. As a result, from February 2016, the EU-US Privacy Shield replaced the US-EU Harbour agreement.

In addition to concerns surrounding the storage of data, there are many security risk concerns which must be addressed to ensure successful business usage of the Cloud. One of the fundamentals of business is the rivalry between competing firms. Across the business sector there are many examples of collusion: where companies come together to either keep profits high or to out-compete another company (Jordan, 2012; Ward, 2012). Collusion will become a very real concern for Mostel & Wilder, should they be storing internal business and customer data with a third-party Cloud vendor. M & W would be unaware if their cloud vendor decided to collaborate with another party (e.g. a rival firm, the state, or possibly with a disgruntled employee) for them to advance their own goals (e.g. putting M & W out of business). This concern is evident in the fact that all literature on Cloud security protocols make certain to address collusion concerns. Despite this, there are no examples of collusion occurring due to Cloud storage (Thilakanathan et al., 2013).

Further evidence that the company's data may be exchanging hands without the owner's knowledge is expressed in Dropbox reports. Dropbox provide reports bi-yearly, detailing the number of search warrants and subpoenas which it has received from the US authorities. Worryingly, almost 80% of the subpoenas – which allow users personal details to be taken – harbour a 'gag' clause: preventing Dropbox from notifying their customers (Dropbox.com, 2017).

Another issue with data being stored with third party vendors is that it is possible for sensitive data to be accidentally leaked. Verison, a large multinational company which in recent years has acquired AOL and Yahoo, was the victim of data leakage due to their cloud provider: NICE. An employee of NICE accidentally allowed the personal details of millions of customers to be accessible via a weblink to an unprotected Amazon S3 server (O'Sullivan, 2017; Spring, 2017).

Another concern is the deletion of data - at the beginning of 2017, Dropbox re-established concerns about whether deleted user data is ever fully removed from the cloud, when customers began reporting folders which had been deleted several years ago re-appeared in their account. This was supposedly due to a bug which prevented these files from being deleted. While trying to fix the issue, Dropbox reportedly restored the data by accident. The fact that it took years for this 'bug' to be discovered is just as concerning (Nichols, 2017; Gallagher, 2017).

In terms of applications for personal cloud users from Mostel & Wilder, one key concern is the availability and freedom of their data. According to Freibrun (2017), if the application of the product which stores clients' information is unavailable, the business of the company could be profoundly impaired. Therefore, the cloud product provider should ensure the application accessible and available for at least 99.5% of the time.

Another significant risk is data privacy and security which refers to the consumers' authentication of information when legal requests are related (Motiwala, 2013). There is no doubt that data of users should be guaranteed non-access to any illegal systems and malicious parties. However, the situation could be complicated when legal enforcement agencies are involved, where they can legally request information from the cloud provider, and may do so without the permission of the user under a court order. However, large, multinational companies, including What's app and Apple, have refused in high profile cases. For example, Apple resisted FBI demand to crack an iPhone linked to the San Bernardino attacks in 2015, under the claim that only the phone's user should be able to access the stored data (Nakashima, 2016), and where the data of a user's phone is accessed by others, even by the FBI with good intention, the authority of information will no longer belong to users themselves. Despite this, the European Commission (EC) has set to propose three options in terms of forming basic motion for cyber security which will be executive by early 2018, for which, employees and clients of M & W who store data on the Cloud, under EU regulation will probably face some form of data exposure due to legal request.

For Mostel and Wilder, Dropbox and Google Drive offer extensive information functionalities which are of benefits as indicated by the employees. However, such extensibility can uncover several vulnerable information dependencies which can render the company a potential target for sensitive information theft / data breach.

According to Bernard Peter (1967), security cannot be obtained in an absolute sense in a multiprogramming system equipped with remote terminals, and any introduction of sensitive data into the system should consider the likelihood of compromise. The remote capabilities of cloud computing and internet system as a whole have exposed both big multinational companies and small alike to a potentially persistent level of cyber threats from any part of the world.
For example, in 2010, hackers successfully breached Google's cyber security and hacked into databases containing sensitive user information. According to the financial times in the same year, security experts warned that businesses could lose faith in the security of cloud computing after Google admitted that its web-based g-mail system was hacked. Events like this has the potential to slow down the willingness of corporations to store their business information in a remotely operated data centre called "The CLOUD".

The extensibility of cloud computing and its subsequent issues clearly depicts the "prophecy" of Thomas P. Rona (1976): that information flow that advance systems required was growing in fragility and it grew in complexity. It cannot be over-emphasised that the vulnerability issues that affect the internet also affect the usage of Cloud computing.

Risks of the concerns to the enterprise

There are clear distinctions between information security (the confidentiality, integrity, and availability of information), and data privacy (where data should be untraceable, and anonymous), and so, in this case, as employees, clients, and contractors will be using personal clouds to upload the data, it poses the question of which laws would be applicable, and as the data controller has ultimate responsibility for complying with the Data Protection Directive, who is the controller? The use of layered services mean that it is possible that several data controllers and data processors working on their behalf, could be acting together to deliver content or services which involve the processing of personal data in the Cloud. The Data Protection Directive recognises that not all organisations involved in the processing of personal data have the same degree of responsibility, and so, makes a fundamental distinction between the data controller and the data processor - data controllers are obligated to follow several principles when they process personal data, and it is the data controller that must exercise control over the processing, and carry data protection responsibility for it (Data Protection Directive, 1995). In addition, the data controller must choose appropriate data processors, and must seek adequate contractual protection from it. As the Cloud customer determines the purpose and manner of the personal data being processed, in most cases, the Cloud customer, in this case, Mostel & Wilder, is the data controller, and thus has overall responsibility of complying with the Data Protection Directive principles. Therefore, the Cloud provider, the data processor (who only processes the data on behalf of the data controller), does not hold responsibility for the data.

As an up-and-coming enterprise that services large multinational businesses, Mostel & Wilder will attract more attention both to competing large accountancy firms and to international governments. It is entirely possible that these 'giants' of the accountancy world may not be in favour of a developing business which will increase competitivity potentially resulting in reduction of their profits and loss of customers. Despite this, there are no examples of collusion occurring due to Cloud storage: this does not mean that it is not occurring, simply that there is no current evidence of it. While collusion is a very important business concern, it appears that this is a lesser security concern when it comes to Cloud computing due to the lack of evidence.

Mostel & Wilder will also likely attract more attention from the authorities' due to the companies which they service. As a result, the US government – along with other governments, may issue the likes of subpoenas to gain information about individuals and the companies which M&W service. This has the potential to reveal personal data about customers and employees, along with the opportunity for authorities and possibly the Cloud vendor being able to see sensitive business data. As a result, this is clearly a justified security risk concern, as unauthorised personal should not be able to view data without permission.

Even more worryingly for the enterprise, would be if this information was accidentally leaked to the public due to vendor error. Much of the data which M&W are harbouring on the Cloud will be sensitive data which relates to either internal business processes, customer's personal details, or their company's data. Should this information come into the public domain then M&W could be facing repercussions, potentially resulting in loss of customers. This generates quite a security risk for M&W as vendor error can be quite common. Only earlier this year Amazon accidentally took down some of their S3 servers due to an incorrect command (Amazon.com).

Not being in direct control of how much of your own data is still being stored by Cloud vendors is also a concern. For example, if M&W were to receive a legal request from a customer to remove all data about them or provide all data on them that they hold, it could result in incorrect data feedback. This is due to if the Cloud vendor still has copies of the information lurking in a server somewhere which M&W does not know about.

For enterprises like M&W, where employees are using Cloud applications, consumers might find their data unavailable when they plan for instant usage which can make the company's business impaired and cause financial loss. Therefore, the full-time accessibility should be ensured for the

Cloud users. Moreover, the enterprise could have privacy issue which may be related to legal request. In such case, legal enforcement agencies are involved, where they can legally request for information from the Cloud provider, and may do so without the permission of the user under a court's order. The company could face the risk of breaking the contract between consumers to unlock their data to legal parties.

With regards to access control and security, the risk to be considered can be numerous. Starting from the user - employees, client or contractors can facilitate a data breach on purpose or by incompetence. Lack of hygiene by the user can expose the company to an application-based attack which can grant access to the Cloud systems. For example, opening unsolicited email containing downloadable files which can expose the company's system to malwares, visiting unapproved websites via company's pc, connecting unapproved/unknown devises to the company's computer systems.

External attack from hackers and vandals who deliberately try to have access into the system/network remotely pose a huge threat. They can be persistent and always try to figure out a loophole to operate from. A single success of these criminals can be very costly to the company. Theft of data during data transfer via a network remote access which can bypass the company's security portal is a concern. There is a risk that the encrypted data being transferred could be intercepted and decrypted by unauthorised persons.

The table below outlines in summary the list of risk being considered from an access control view point:

Risk Considered		
Third party physical access to data	Unauthorised access due to poor provider security measures	Identity of multi-tenants. i.e. sharing tenancy with potential hacker.
Unauthorised network access due to insecure network configuration	Unauthorised access due to inefficient cryptology	Unauthorised access due to poor user data boundary management
Identity and credential theft	Data loss due to Human error (user)	Data theft due to poor hygiene by users

Policy

Mostel & Wilder Cloud Storage Policy *as of October 2017*

i. Scope

This policy applies to all Mostel & Wilder data i.e. information which arises in methods, measurement systems, and procedures for presenting disclosures or financial reporting, research, and administration, and applies to all Mostel & Wilder staff, clients, contractors, and any other party that has access to Mostel & Wilder data. Any exceptions must be documented and approved.

1. Storage of data

Although Cloud data is typically encrypted, it is important to remember that its services are given on terms and conditions which are defined by an external supplier, and that Cloud storage and associated files reside out-with the organisation's domain. Mostel & Wilder therefore, cannot have full control over the encryption of data, or the storage location, which, if resides out-with the EU, is not protected under EU data protection laws. Where data does reside out-with this territory, it may be subject to scrutiny by unknown sources.

2. Third party access

Mostel & Wilder are committed to ensure that client and employee data, under no circumstance is given to any third party without the consent from the individual. The Cloud is, by definition, a third party, but is authorised with duty of care, where a third party of the Cloud service must obtain permission from the user, unless special circumstances prevail. Therefore, all users of any Cloud service used for the storage of Mostel & Wilder information must agree to the Terms and Conditions and associated service level agreements governing the use of the Cloud.

2.1 Confidentiality

Certain employees may have access to collaborative client information, and therefore, security, privacy, and confidentiality commitments must be honoured, where said employees will have a duty of care.

- Clients, employees, contractors, and any other party that has access to Mostel & Wilder data may be given permission to view data that is only relevant for their needs, and may be given access to files or folders that are required for a collaboration to occur. A hierarchy system is in place to limit users on what data they can access, view, and edit.

3. Loss of data

Data stored on the Cloud may be lost, damaged, or corrupted, either by malicious, or non-malicious means. For this reason, it is best advised that highly sensitive data, including that which is of such criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted (*see Information Risk Classification*), is not stored on a consumer-oriented Cloud, and is instead stored only on an external hard drive that remains disconnected from computers that could be exposed to malware.

4. Disposal of Data

As mentioned in section 1, Cloud providers will store uploaded data within their own storage, possibly in different countries. Clients, employees and contractors should all be aware that their Cloud provider may store the data in multiple locations to ensure integrity. It could be possible that upon organisation attempted deletion of documentation from the Cloud that this data may still exist elsewhere in the Cloud providers storage system. As such, users should be cautious when uploading documentation to the Cloud so as not to upload data with high risk as it could result in this documentation being held somewhere even upon supposed deletion (*see Information Risk Classification*).

Implementation and Evaluation of Policy

Implementation

Due to the popularity of Cloud storage usage in Mostel & Wilder to transfer documentation between clients, employees and contractors, the first step in implementing this policy would be to ensure that the aforementioned individuals are made aware of this policy.

The key-decision makers of Mostel & Wilder should begin the process by ensuring that all current management are made aware of the new policy. It should then be up to management to ensure that they properly explain the policy and emphasise the importance of it to current employees. Equally, those in charge of contact with contractors should make their correspondent at the company aware and encourage them to make their staff aware. Current clients of Mostel & Wilder must also be notified of the new policy and advice should also be available should there be any questions. Clients should be informed through the likes of e-mail. This should hopefully allow current operations to continue but with security guidance in place.

In addition, any new employees and contractors must be made aware. Due to Cloud storage communication being important to the business conduct of Mostel & Wilder business and the potential security risk it can harbour, it would be wise to include this policy within an induction to the company. Any new clients which Mostel & Wilder acquire, should be made aware of this guidance policy at the same time as when they are informed of the potential to use Cloud storage to transfer data.

Evaluation

The policy is not as far reaching as would hope due to the context of Cloud storage with the enterprise. Adequate evidence was available on those security concerns which appeared to demonstrate the greatest amount of risk. When it comes to the storage and transfer of sensitive information to and within Mostel & Wilder, it would be ideal to ensure that the enterprise is in complete control of the data at all times. However, to proceed down this pathway would require Mostel & Wilder to invest in their own private cloud for employees, clients and contractors to use. Setting up a private Cloud would require a considerable amount of investment to begin with. As a result, the policy is a guidance upon the usage of the currently available public Cloud storage services to hopefully generate safer usage. Mostel & Wilder cannot enforce adherence to this policy and due to implementation cost cannot provide an alternative, e.g. private Cloud, to circumvent the majority of security concerns raised. Consequently, this means that despite the policy users may continue to use the Cloud storage facilities recklessly.

Appendices

Appendix i.

Mostel & Wilder Information Risk Assessment Criteria

Use this table to determine who is allowed access to Mostel & Wilder information. *When mixed data falls into multiple risk categories, use the highest classification.*

Low Risk	Moderate Risk	High Risk
Data is considered low risk when it is not considered moderate or high risk, and when one of the following conditions are met: 1. The data is intentionally created for public use. 2. The storage of data is of no criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted.	Data is considered moderate risk when it is not considered high risk and when one of the following conditions are met: 1. The data is not generally available to the public. 2. The data in question is defined as 'personal data' by the Data Protection Act. 3. The storage of data is of little criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted.	Data is considered high risk when it when one of the following conditions are met: 1. The data was never created for public use. 2. The storage of data is of such criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted.
Examples include: • Any information in the public domain • Job adverts	**Examples include:** • Client and staff personal contact details	**Examples include:** • Client and staff financial information • Client and staff personally identifiable information, including, but not limited to: physical; physiological; mental; economic; cultural; or social identity factors.

References

Dropbox, n.d. *Transparency Principles & Reports.* [Online] Available at: https://www.dropbox.com/transparency/reports [Accessed 22 October 2017].

Fixya, n.d., *Cloud Storage Report*. [online] Fixya. Available at: <http://www.fixya.com/reports/cloud-storage> [Accessed 21 October 2017].

Freibrun,E. (2017). 11 Key Benefits and Risks of SaaS Contracts. [online] Available at: https://www.springcm.com/blog/key-benefits-and-risks-of-saas-contracts [Accessed 26 Oct. 2017]

Gallagher, S., 2017. *Deleted Dropbox files reappeared because of metadata bug.* [Online] Available at: https://arstechnica.co.uk/information-technology/2017/01/fix-for-metadata-bug-caused-dropbox-files-to-appear-to-rise-from-dead/ [Accessed 20 October 2017].

Gibbs, S. (2017). EU could give police direct access to cloud data in wake of terror attacks. [online] the Guardian. Available at: https://www.theguardian.com/technology/2017/jun/08/european-union-police-direct-access-cloud-data-terror-attacks-threats [Accessed 28 Oct. 2017]

Jordan, J., 2010. *RBS fined £28.6m for price collusion.* [Online] Available at: http://www.independent.co.uk/news/business/news/rbs-fined-163286m-for-price-collusion-1931571.html [Accessed 20th October 2017].

Kennedy, E. & Millard, C. 2016. Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. *Computer Law & Security Review*, vol. 32, no. 1, pp. 91-110.

Motiwala, A. (2017). 4 SaaS Risks Every CSO Needs to Know. [online] Identropy.com. Available at: https://www.identropy.com/blog/IAM-blog/bid/97683/4-SaaS-Risks-Every-CSO-Needs-to-Know [Accessed 27 Oct. 2017].

Nakashima, E. and Nakashima, E. (2017). Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks. [online] Washington Post. Available at: https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.adb926926323 [Accessed 28 Oct. 2017].

Nichols, S., 2017. *Dropbox brings old files back from dead.* [Online] Available at: https://www.theregister.co.uk/2017/01/24/dropbox_brings_old_files_back_from_dead/ [Accessed 20 October 2017].

O'Sullivan, D., 2017. *Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts.* [Online] Available at: https://www.upguard.com/breaches/verizon-cloud-leak [Accessed 22 October 2017].

Peters, B., '*Security Considerations in a Multi-programmed Computer System*', 1967 Spring Joint Computer Conference, AFIPS Proc., vol 30, 1967, pp.283–6 (accessed 26 September 2011).

Rashid, F. Y., 2016, *The dirty dozen: 12 cloud security threats*. [online] Info World. Available at: <https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html> [Accessed 22 October 2017].

Rona, T P., '*Weapon Systems and Information War*' (Seattle: Boeing, 1 July 1976) p.50 5_and_Information_War.pdf

Spring, T., 2017. *Experts Warn Too Often AWS S3 Buckets Are Misconfigures, Leak Data.* [Online] Available at: https://threatpost.com/experts-warn-too-often-aws-s3-buckets-are-misconfigured-leak-data/126826/ [Accessed 20 October 2017].

Thilakanathan, D., Chen, S., Nepal, S. & Calvo, R. A., 2014. Secure Data Sharing in the Cloud. *Security, Privacy and Trust in Cloud Systems,* pp. 45-72.

Voigt P., von dem Bussche A. (2017). *The EU General Data Protection Regulation (GDPR).* Springer, Cham.

Walden I. (2013) Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. In: Pearson S., Yee G. (eds) Privacy and Security for Cloud Computing. Computer Communications and Networks. Springer, London.

Ward, A., 2012. Shell and BP accused of collusion in South Africa. [Online] Available at: https://www.newstatesman.com/business/business/2012/10/shell-and-bp-accused-collusion-south-africa [Accessed 20 October 2017].