Analysis of Cyber Security Concerns of Employees

The aim of this report is to identify, investigate security concerns, expressed by the client company's key decision makers, regarding the use of personal cloud storage by employees; particularly the issues surrounding use of these clouds for storage of business information and content, which is potentially sensitive, proprietary material. After detailing these concerns, the risk posed by each in turn is assessed, and policy is suggested to combat or contain these risks. The client is understood to be a large multinational accountancy firm headquartered in the European Union; as such the policy suggested and legal concerns addressed maintain a focus on this context. The key concerns raised are regarding the storage of data and documents in personal clouds, the freedom of information, collusion concerns between the provider and competing firms or other third parties, and the extensibility and accessibility of applications, both authorised and otherwise.

Storage of Data and Documents

Each department and business function within the accountancy firm will most likely be using processed customer data. The Data Protection Act principles clearly state that: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."[1]

There are two types of cloud services: consumer-based and business-based cloud platforms. The latter give more assurances to businesses over the locality of their data, and also provide deeper contracts to provide assurances over data recovery and issues surrounding access to the data in the cloud. With the former, there are no such assurances. The rise in consumer-based cloud systems, based on a Trend Micro survey, 19% of employees relies on consumer-oriented cloud to store their documents at work [2]. This is worrying given the lack of terms that seek to protect the user's data. Even with such assurances given by formal contracts, there can be no guarantees that data will be safe, as can be seen in the recent loss of customer data by Cisco, one of the world's leading cloud providers and IT giants [3].

Freedom of Information and other requests

Freedom of information requests play a vital role in providing information to the public held by public authorities and companies. Obligations on public authorities and companies are dictated in the EU Directive 95/46/EC and national legislation is enacted nationally via acts such as the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2000. The firm may receive a request to information held about an individual at any time. Organisations must respond within the prescribed 20-day timeframe, or the Information Commissioner may serve an enforcement notice [4]. There is no legal remedy, but organisations can be compelled to comply, often publicly, eroding the goodwill and reputation of the company [5].

Under the Data Protection Directive and the national implementations such as the Data Protection Act 1998, individuals have a right to make a 'subject request' to get information held about them. A request under the Act can be made to any organisation (A Data Controller) using personal information to supply copies of the data being held, shared, or related data.

Unlike the Freedom of Information requests, breaches of the Act have more serious repercussions, both financial and to the reputational goodwill of the company. An individual may complain to the Information Commissioner Officer (ICO) to perform a compliance assessment. If the company fails to bring themselves within compliance, the ICO may serve an enforcement notice, or if the company has committed a serious breach, then the ICO has a statutory power to impose a financial penalty [6].

Failure to adequately respond to requests for financial auditing purposes represents the most profound consequences. PricewaterhouseCoopers was fined a record £5.1 million for "The admitted acts of misconduct include failures to obtain sufficient appropriate audit evidence and failures to exercise sufficient professional scepticism. [7]"

Collusion Concerns

In a strictly legal sense, collusion is defined as two parties entering "a deceitful agreement, usually secret, to defraud and/or gain an unfair advantage over a third party, competitors, consumers or those with whom they are negotiating. [8]" The assumption is made that all of the client's employees who use personal clouds will be using services provided by the set of most popular cloud providers. CloudRail reports that the top 4 cloud storage service providers are Dropbox, Google Drive, Microsoft OneDrive and Box. CloudRail does not support all cloud services, and so this report also investigates Apple iCloud and Mega [9].

Powers and privileges given to cloud providers upon acceptance of the terms of service by a user (an employee of the firm) expose a risk to the firm. Terms are hidden in plain sight, the majority[4] of users do not read these terms, leaving them unaware of the access they allow to their stored information and content. The critical issue observed in the terms of service of all six major providers is that they each individually reserve the right to maintain user uploaded content and provide it to any government or otherwise involved organisation, such as is necessary for the legal case in question. For example, Mega reserves the right to "deny you access to your data but keep it for evidential purposes". This evidently is cause for concern as the handover of control of information and the disclosure of corporate content stored by employees, while strictly defined as being under legal direction only, is no longer the sole responsibility of the client, but also of the cloud service provider.

Extensibility and accessibility of applications and other concerns

The perception of the key decision makers that Bring Your Own Devices (BYOD) brings benefits to the business is a worrying aspect. Issues with devices being lost frequently reach the press, whether that is a laptop or a smartphone, as was the case when two laptops were stolen from Glasgow City Council offices with more than 20,000 people [10].

Increased use of non-commercial cloud platforms and BYOD increases the risk of indirect attacks such as man in the middle (MITM) attacks. Communication with a personal cloud over an insufficiently protected home network may give an attacker the advantage they need to sample data from the communication [11]. Of course, this is notwithstanding the added complexity of managing numerous employee created credentials.

Risk Assessment

Storage of Data and Documents

Given that both Google Drive and Dropbox have their data centres in the US, the dangers of using any of these personal, consumer-based cloud platforms. Immediately, the uploaded data will be placed in a Third Country, breaching the Data Protection Act and exposing the firm to legal enforcement and fines.

In addition, the data cannot be completely controlled by the firm and it will have to rely on the cloud vendors. And the vendors may help USA government to monitor the data which stored in the clouds because of the USA Patriot Act [12]. From the Government Request Principles of Dropbox, it has the responsibility to provide its users' data to the government for legal issue. In the last quarter of 2016, there were 25.6% of the non-disclosure orders from court Dropbox has received without notifying the users [13].

Additionally, cloud storage allows users to use a multitude of devices. Employee will for convenience purpose using their mobile phone to upload, download or transfer the firm's information. It will improve the risk of data breach if the employee lost their mobile phones. It may bring significant monetary loss for both company and clients. However, in this case, personal cloud means consumer-orientated cloud service. The provider has no guarantee on data protection and backup.

Freedom of Information and other requests

Risks from failure to comply with obligations imposed on the company by legal requests are great. Damage to the company's reputation is a real risk; however, it is the potential to breach the Data Protection Directive or financial auditing obligations that could potentially cripple the company both financially and their goodwill and reputation.

In the case of Freedom of Information, if the company cannot access the data that they are obligated to provide, then there is the risk of enforcement from the Information Commissioner. There is a chance of escalation to a court order [14], however, the consequences are not as severe as breaches of the DTA or financial / taxation requirements. Furthermore, the DTA will be replaced by the General Data Protection Regulation (GDPR) in 2018 [15]. The GDPR responds to the increase in information sharing using cloud platforms and broadens the scope of the DTA to encapsulate more types of data. Penalties for non-compliance can be up to 4% of worldwide turnover or up to 20 million euros [16].

Collusion Concerns

In the strict sense of collusion as a deceitful, secret and potentially unlawful practice, 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. Dropbox makes a statement to this end in their transparency declaration describing their resistance to overly broad government data requests and their rejection of the idea of government backdoor-access [17]. Famously over the issue of the San Bernardino shooting, the FBI demanded that Apple create software to allow the agency to bypass the locking and encryption methods in place on the phone, an

effective government backdoor to data encrypted on iPhones [18]. While this specific case is in regards to local data stored on a device, its high profile nature and the very public resistance displayed by Apple to resist creation of encryption bypassing mechanisms for the government has clear and resounding implications for the integrity of cloud stored data in similar circumstances. Thus it can be surmised that risk to the provider of public trust being undermined is so great that risk of provider collusion with third parties, states or otherwise is determinately low.

However, the risk of legal cooperation without consent of the client is substantial. The major cloud providers all clearly detail in their respective terms of service that they retain the right to disclose private user information and content in suitable legal or emergency circumstances. This is a risk to the client as a corporation if employees store sensitive company data on personal clouds, as the client would be concerned over losing their sole privilege and responsibility in regards to disclosure of information.

Extensibility and accessibility of applications and other concerns

Whilst it may be an attractive prospect for employer's to encourage usage of employee owned devices, for the purpose of saving money, or increasing efficiency – the risks are far too great.

Employees that are using their own, or mobile devices issued to them by the firm, introduce a number of risks that are difficult to mitigate. The first is that employees may lose the device, which means that the firm will not be able to account for the locality of the data. For instance, the data held on that device may be the only data source of information that may be required for financial audit, freedom of information request or legal evidence, as discussed above. Secondly, the employee may install insecure applications or inadvertently install malware, all of which will further expose the data to attackers. Thirdly, management of user credentials becomes unmanageable for IT Teams; employees may change credentials without informing the IT Team, or even worse, have no security on the device at all.

Mobile devices that are not protected sufficiently can be subject to *man in the middle* (MITM) attacks. MITM attacks can be executed on a device by first gaining access to the device and then cloning the authentication token [19]. Once this has been done, the attacker can gain access to the documents in the cloud. MITM attacks are difficult to defend against as existing malware cannot detect the mechanism that enables attackers to clone the authentication token.

Furthermore, usage of employee owned devices over unsecured networks, perhaps a home network, an unsecured client location, or even a coffee shop may subject the data to an attack. Industry standard requirements dictate at least 128 bit for data encryption [20] and Transport Network Layer (TLS) protocol usage for data in transit [21].

Policy

Below is a proposed policy to mitigate the most significant risks posed to Mostel & Wilder; subject to peer review and amendments:

1. Appoint a ***Data Protection Officer*** and ***Freedom of Information*** contact
2. Regular data protection good-practice sessions should be held with each department
3. Access to personal / financial data must be limited based on a need to know basis.
4. If data requires to be transferred via a cloud platform, then it should be done using a cloud service with excellent SLA / Terms guaranteeing:
    i. Locality of data with the EU
    ii. Ownership of data
    iii. Backup and disaster recovery plans
5. Personal / Financial data must not be uploaded to personal cloud platforms
6. Copyrighted material must not be uploaded to personal clouds.
7. Data in transit (both internally and externally) must be encrypted and meet required industry standards.
8. Data at rest on an approved cloud platform [as per policy 4.] must be encrypted and meet required industry standards.
9. Only devices issued by the firm's IT Team will be used to transmit sensitive data or assets subject to copyright. [This explicitly excludes usage of employee owned devices (BYOD)]
10. All devices that are used for transmission of personal data must have secure logins
11. Credential management must be managed by the IT Team
12. Credentials must be stored in a secure repository.

Discussion

According to Wood, "Policies are a relatively inexpensive and straightforward way for management to define appropriate behaviour, demonstrate its concern, and specify which behaviours are acceptable / unacceptable."[22] In other words, policies do not describe the 'how to'; that is up to the management and the specialists employed by the firm to ensure that the techniques used fall within the Cyber Security Policy. Based on this, we have not attempted to solutionise any of the issues in the brief.

Some assumptions have been made around the core business functions. For instance, we have assumed that some business functions will make more use of customer data than others. Finance, Auditing, and HR we have assumed will make use of sensitive customer information, while marketing may make use of personal data and copyrighted data such as branded materials, or copyrighted assets that are not in their ownership.

The policy is stringent around the use of personal clouds for sharing personal / customer information due to the seriousness of consequences of breaching data protection and financial auditing legislation. As a team, we have garnered that there can be no assurances as to how data will be managed when it is up in a personal cloud, such as DropBox or Google Drive. If employees were to store personal and copyrighted data in personal clouds, then it is incontrovertible that the firm will be at risk.

As per Garcia and Horowitz, evaluation of the more significant risks to the firm means evaluating the value that the firm places on consequences, and as a consequence they further that "security measures must be a function of organizational value." [23] From the previous analysis, a firm of this nature, i.e. financial, the greatest risks are financial losses due to breaches and the subsequent damage to reputational goodwill. Of course, there are organisational objectives that must be balanced when writing such policies. However, we have drafted the policy to reduce ambiguity for employees and minimise leeway for would-be-attackers. Had the organisational objectives been different, for instance, had the firm been a graphic design company where copyrighted material is perceived as having a higher value than customer information, then the policy might have taken a different form.

There are mechanisms that allow data to be transmitted with sufficient adequacy to Third regions, such as the Model Contract Clauses, Privacy Shield, Standard Contractual Clauses (SCCs) [24], and the Safe Harbor Scheme, which facilitate adequacy for personal data transmissions between the EU and the USA. However, the implementation of these mechanisms is convoluted and complex and there is much uncertainty surrounding their validity. The European Court of Justice recently ruled that the Safe Harbor Scheme was 'invalid.' [25]

In conclusion, our findings support the implementation of a strict policy of not using consumer-orientated clouds for personal or copyrighted data within the firm. In balancing the objectives of the business, policy has also been strict around the usage of mobile devices; some compromise has been given. However, usage of such devices must be subject to policies dictated and within the controls of the relevant specialists.

Bibliography

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/. Retrieved 16/10/17

[2] http://blog.trendmicro.com/icebergs-the-nordics-and-other-byod-considerations/. Retrieved 16/10/17

[3] https://www.theregister.co.uk/2017/08/06/cisco_meraki_data_loss/. Retrieved 18/10/17

[4] https://ico.org.uk/about-the-ico/what-we-do/taking-action-freedom-of-information-and-environmental-information/. Retrieved 20/10/17

[5] http://www.bbc.co.uk/news/uk-politics-11451004. Retrieved 21/10/17

[6] https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf. Retrieved 16/10/17

[7] http://www.telegraph.co.uk/business/2017/08/16/pwc-hit-largest-ever-fine-financial-watchdog-rsm-tenon-audit/. Retrieved 22/10/17

[8] http://dictionary.law.com/Default.aspx?selected=232. Retrieved 18/10/17

[9] http://www.techradar.com/news/top-10-best-cloud-storage-services-of-2017. Retrieved 18/10/17. Retrieved 18/10/17

[10] http://www.bbc.co.uk/news/uk-scotland-glasgow-west-22807593 . Retrieved 18/10/17

[11] https://www.theinquirer.net/inquirer/news/2453541/tls-security-neglect-exposes-web-users-to-man-in-the-middle-attacks. Retrieved 20/10/17

[12] Kshetri, N, Murugean, S., Cloud Computing and EU Data Privacy Regulations, See http://ieeexplore.ieee.org.ezproxy.lib.gla.ac.uk/document/6489955/. Retrieved 18/10/17

[13] https://www.dropbox.com/transparency/reports. Retrieved 21/10/17

[14] https://ico.org.uk/media/about-the-ico/policies-and-procedures/1859/freedom_of_information_regulatory_action_policy.pdf . Retrieved 18/10/17

[15] https://www.wolterskluwer.co.uk/blog/gdpr-intro . Retrieved 19/10/17

[16] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties. Retrieved 22/10/17

[17] https://www.dropbox.com/transparency. Retrieved 23/10/17

[18] https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple. Retrieved 17/10/17

[19] https://www.theregister.co.uk/2015/08/07/imperva_cloud_maninthemiddle_attack/. Retrieved 24/10/17

[20] https://www.microsoft.com/en-us/trustcenter/security/encryption. Retrieved 22/10/17

[21] https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest. Retrieved 21/10/17

[22] Wood, C.C, *Writing InfoSec Polices, Computers & Security,* Computers and Security, Vol 14. 1995, at pp 669. Retrieved 18/10/17

[23] Pfleeger, S.L & Cunningham, Robert K., *Why Measuring Security Is Hard*, Security Metrics, at pp 51.

[24] https://ico.org.uk/media/for-organisations/documents/2014413/data-transfers-to-the-us-and-privacy-shield.pdf. Retrieved 24/10/17

[25] https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection. Retrieved 22/10/17