Cyber Risk Assessment and Security Policy Proposal
Related to the implementation of collaborative messaging tools within a multinational corporation.

Hopper & Grace
Team T
0602452B, 2083549D, 2192245N, 2387688L, 2397282S

Abstract

Hopper & Grace (H&G) have expressed a desire to incorporate the use of collaborative messaging tools, such as Telegram and Slack, into their enterprise. The following report will address the security concerns inherent in using such technology and analyse the potential risk to the enterprise, before outlining a policy which will mitigate these risks and detail how this policy should be implemented, providing the company still wishes to proceed in this endeavour.

Contents

I. Risk Identification

ISO 31000 defines risk as the effect of uncertainty on objectives [1]. As such, it is necessary to identify the objectives of Hopper & Grace (H&G) so as to appropriately establish the risks to the enterprise and how best to protect against them.

Hopper & Grace is a private multinational accountancy firm comprising of many business units. They specialise in financial domains, such as financial auditing and providing advice on tax matters. Nevertheless, given their position as a growing enterprise, they also have supporting departments, such as human resources and marketing. Headquartered in the European Union, H&G's accountancy clients range from large multinationals to small-to-medium businesses. The introduction of collaborative messaging tools to the enterprise would bring with it additional security concerns and create more uncertainty in terms of H&G's ability to achieve their objectives. Bearing this in mind, it is necessary to identify the assets of Hopper & Grace that require additional protection. These assets have been split into the following categories:

A. *Sensitive client data and its accessibility, particularly what happens to it when sent to clients or third parties using external messaging tools*
B. *Storage of data pertaining to clients and/or Hopper & Grace*
C. *Security of hardware, software, office space and employees.*

Having easy to access data is an advantage to large corporations, however, it is often difficult to secure, particularly when this data is sent through external messaging tools. Data breach is a major risk for any corporation. Since H&G, as a multinational accountancy firm, preserves and exchanges a lot of sensitive and confidential data, which is valuable to different kind of third parties, the possibility of a data breach is rather high. Moreover, more and more data breaches have occurred in recent years, which makes the situation more critical.

Businesses regularly use the cloud to store data. The phrase "cloud computing" appeared as early as 1996, with the first known mention in a Compaq internal document. Through investigation, it was found that the storage of data in both Slack and Telegram is within the cloud. Unfortunately, there are many downsides to cloud storage, including, others being able to look at your data, cyberattacks and insider threats. To break it down, each of these factors will be analysed in order to give H&G an insight to the risks involved in their employees using such external messaging tools.

The third point raised can be categorised as access management. Access management and collusion pose a great threat to businesses because it results in larger costs and is harder to detect [2]. Whilst it is important to protect against external actors gaining access to H&G's systems, it is also necessary to protect against the threat within.

Nine risks that could potentially hamper Hopper & Grace's ability to achieve their objectives in these categories are as follows:

1. *Data breach*
2. *Vulnerabilities caused by using external messaging tools*
3. *Failure to comply with GDPR*
4. *Unknown access to the cloud*
5. *Cyberattacks on the cloud*
6. *Insider threat in relation to the cloud*
7. *Former employees maintaining their access to Hopper & Grace*
8. *Compromised accounts*
9. *Physical breach*

Using the identified risks, a risk matrix will also be provided in the appendix of this proposal. This matrix will detail both the likelihood of this risk occurring and the severity of this risk on the

enterprise. This will be done on a five-point scale. On the likelihood(L) axis, a one would mean a risk is unlikely to occur, but a five would mean that the risk is an incredibly likely occurrence. On the severity(S) scale, a five offers the greatest threat to the company, but a one suggests the threat is minimal. Each risk's severity and likelihood ratios, as they appear in the matrix, will also be provided in section 2.

On top of this, it is also important to consider the non-tangible factors which could hamper the continual development of Hopper & Grace, such as the loss of goodwill from clients from failing to secure their data sufficiently.

II. Risk Assessment

A. Data Integrity

1. Data Breach (L4, S5)

As stated in the previous section, data breach is the most critical risk concerning the cyber security of a multinational enterprise of Hopper & Grace's scale. The consequences of a data breach can be catastrophic:

- Loss of business goodwill. A data breach would make the public distrust the company. Therefore, the company may lose a number of current customers and potential customers due to the incident. For example, after Yahoo's 3 billion email accounts' leakage in 2013[2], a large number of users chose to stop using Yahoo's email services.
- Loss of financial interest. Data breaches are often accompanied by a fall in stock price, loss of clients and contracts, which would have a direct impact on the economic interest of the company. For example, Sony's stock price went down more than 10% a week after the data breach of PSN happened. The total loss is estimated at over $171 million [3].
- Facing lawsuits and other legal charges. Once the data breach occurs, there will inevitably be victims, who may be the source of the data or the downstream customers of the enterprise or other partners affected by the data breach.

2. Vulnerabilities Caused by Using External Messaging Tools (L4, S4)

Unfortunately, using external messaging and collaborative tools may cause vulnerability, consequently raising the likelihood of a data breach.

These collaborative tools may have a flawed security design, which could eventually lead to a data breach. For example, Josh Fraser pointed out that Slack has a very insecure default security setting in that anyone who joins a Slack group is allowed to create a malicious API key, which can access everyone in the group's detailed personal information [4]. In Telegram, although it has end-to-end encryption, it wouldn't take effect until users manually activate the "secret chat" option.

Secondly, using an external tool means that all the data transmitted through the platform is stored in a third-party provider's server, which adds uncertainty surrounding data security. It is not alarmist to consider a large data breach of the data centre of Slack or Telegram because such things happened before to both [5, 6]. Although both companies claim that they have high-quality data protection, putting data in the cloud is always risky since there is no system with absolute safety. On top of hacker attacks, the possibility of the collusion between the platform and other companies or governments can't be excluded, which could share a user's information with a third-party without the user's awareness or permission.

3. Failure to Comply with GDPR (L3, S4)

Since the GDPR became enforceable across the European Union on the 25th of May 2018, companies found in breach of the regulations are now liable to pay far greater fines than under the previous system. The consequences to being found in breach of GDPR are severe, as these fines

would have a huge impact on H&G's profitability as well as damaging both clients and shareholders' trust in the company, which would stunt the enterprise's growth. There are two tiers of fines applicable for non-compliance with GDPR:

- Up to €10 million, or 2% of annual global turnover, whichever is higher
- Up to €20 million, or 4% of annual global turnover, whichever is higher [7]

The first-tier deals with infringements listed in Article 83(4) and the second with Article 83(5)[8], meaning that data security breaches would come under the first category and an infringement of an individual's data privacy will be subject to the second tier of fines. It is imperative the company ensures it is compliant with the GDPR to reduce the likelihood of incurring such a fine.

According to the 2017 Verizon Data Breach Investigations report, 24% of data breaches affected financial organisations, making such organisations the most likely victim of a cyberattack [9], reiterating the fact that H&G is a likely target to a cyberattack from a variety of sources. As an accounting firm, H&G also have to keep records of personal data for a number of years, meaning the risk of H&G being liable to pay GDPR-related fines is heightened further. With an appropriate security policy in place, the possibility of H&G suffering a data breach reduces, maintaining the integrity of the enterprise and decreasing the probability of them being subjected to these fines. Whilst both Telegram and Slack have stated their commitment to GDPR [10, 11], it must be noted that incorporating external messaging tools into the corporation will increase the likelihood of data breaches, as third parties have been identified as the number one risk factor for breaches in financial services firms [12].

B. Cloud Security

4. Unknown Access to the Cloud (L3, S4)

Unlike a data centre, the cloud is an offsite storage unit in which users outsource their data. This modern method of storage, although beneficial and a newfound technology, can be very risky, especially for businesses such as H&G. One of the main factors of this, is that by data being stored in cloud storage services the user is basically handing over their data to someone else to store it. In the case of Slack and Telegram, there is no major documentation on how secure their cloud storage is and who has access to it. With regards to Telegram, it is apparent that the data users store on their cloud-based messenger is stored across the globe. Although Telegram claims that the "0 bytes of user data to third parties" [13] have been disclosed, it would seem this is only apparent within secret chats. Therefore meaning if employees of H&G are not using secret chats they are therefore at risk of their data being accessed within the cloud storage, potentially damaging the company, and all due to their lack of awareness on how Telegram encryption works and the storage policies they have.

5. Cyberattacks on the Cloud (L3, S3)

The second risk is cyberattacks and the effect they can have on the employees and the company itself. In 2015, Slack experienced a cyberattack [14], where it is believed hackers managed to gain access to the database giving their users emails, usernames and Skype IDs. From this Slack then went on to introduce two-factor authentication within their application. However, having data stored in the cloud can be problematic and you are almost always at risk of a cyberattack. Although IM companies such as Slack and Telegram are putting up a high-quality defence, cyber-attackers are becoming better versed in methods to gain access and attack through the defence mechanisms in place.

6. Insider Threat in Relation to the Cloud (L2, S4)

Insider threat, although not common, is a malicious and dangerous attack to both the cloud provider and the client. Normally due to their business role in the cloud provider, the insider can use their

authorised user rights to access sensitive data [15]. It could be anyone from an administrator, who could be responsible for data backups and therefore has access to backups, unknown to others, an abuse of power. Cloud services have vastly expanded the scope of insider threats[16]. Another common situation of an insider threat is when someone from within the company leaves. They may be on bad terms with the company and save company data to their own personal cloud, or still have access to the company's cloud storage after they have left. A company such as H&G, is then at risk of their data being used elsewhere in a potentially malicious way.
It is evident that there are risks to using cloud storage, both from outside the company and within. With the risk of employees misusing the cloud and violating company cloud usage policies [16], as well as the potential attacks from cyber-attackers and third-parties, it is important that Hopper & Grace are well-informed on these risks and how best to prepare themselves against them.

C. Access Management

7. Former Employees Maintaining their Access to Hopper & Grace Systems (L2, S3)

One of the benefits to collaborative messaging tools like Slack and Telegram is that the applications are readily available on multiple devices, which aids the rapid exchange of data. Nevertheless, this can cause issues once an employee leaves the company. If their access to Hopper & Grace and their clients' data is not revoked upon them leaving the company, the employee in question could use this data to further their own career by sharing it with their new employers, which would hamper the reputation of Hopper & Grace, and perhaps result in a loss of business.
The likelihood of an ex-employee continuing to have access to Hopper & Grace systems will be greatly reduced if a stringent policy is introduced, otherwise, the enterprise will be at risk of losing business due to the actions of former employees. By ensuring that collaborative messaging tools can only be used on company-owned hardware, the chance of this situation arising is reduced significantly.

8. Compromised Accounts (L2, S3)

According to Verizon's 2016 Data Breach Investigations Report, 63% of known data breaches involved compromising a weak, default, or stolen user password [17]. If the account of someone who holds full access to all the important data is compromised, the consequences would be catastrophic. Another concern is human negligence, such as forgetting to remove a former employee's access. So it is imperative for H&G to build up a strict management inside the use of those messaging tools with good privilege control and quick detection and reaction to anomalous user behaviours.

9. Physical Breach (L2, S2)

In order to ensure the security of Hopper & Grace's systems is at its optimum level, it is important not to neglect the more tangible elements of the enterprise. According to Churchill Security Limited, physical and cyber security are interlinked, and one of the best defences to cyber security is having appropriate physical security protocols in place [18]. Sensitive data stored on the hard disks of Hopper & Grace computers would be easily accessible to anyone who happened to gain access to the computer. It is, therefore, necessary to secure Hopper & Grace's physical assets and ensure all employees are educated in terms of what are the best practices to protect computers from physical security breaches.

III. Policy Statement

1. Enterprise and clients' data must be categorised according to its risk level from low to high.

(a) Hopper & Grace employees are only allowed to use collaborative messaging tools for business communication on devices provided by the company.
(b) Access to highly sensitive data must require adequate authorisation and further be audited and monitored.
(c) Low-risk Public data is allowed to be transferred using external instant messaging tools.
(d) Medium-risk Private data is allowed to be transferred using external messaging tools only if the conversation has been secured by a password.
(e) Any type of data that becomes a subject of an ongoing legal case is instantly re-evaluated and categorised as data of high risk.

2. To protect both enterprise and client data, Hopper & Grace must have cyber insurance.

3. A Data Protection Officer (DPO) must be appointed to maintain compliance of Hopper & Grace with GDPR as well as the employees' compliance with the policy regulations.

4. All data transferred using instant messaging tools must have end-to-end encryption enabled by default.

5. Cryptographically secure long passwords and two-factor authentication must be used by clients and employees for logging into instant messaging applications.

6. The enterprise must ensure that clients, existing and new, are made familiar with Hopper & Grace's policy regarding use of instant messaging tools, and agree to uphold a similar standard on their end when instant messaging tools are being used for the transfer of data.

7. Administrators must remove all access to former employees. In addition, former employees must be removed from any of the existing instant messaging business channels.

8. When using collaborative messaging tools on a particular device/network, safety measures regarding the confidentiality, integrity and availability of data stored on that device/network must be deployed:

(a)Anti-virus and malware removal tools must be deployed on the network to prevent sensitive data from being jeopardised.
(b)Hopper & Grace must ban/restrict a user's activity when visiting websites formerly accused and/or suspected of collusion.
(c)Hopper & Grace must deploy their own VPN when exchanging any communication via instant messaging tools in order to protect the privacy of its clients and employees.
(d)Hopper & Grace's on-premise cloud storage must back-up critical user data and provide an easy mechanism for the restoration of said data in cases of data loss.
(e)HTTPS must be enabled on all devices/networks by default when connected to the internet.
(f)A strong firewall policy must be in place to protect Hopper and Grace's cloud storage.

IV. Implementation and Evaluation Details

Implementation

With regards to policy point 1, Hopper & Grace will adopt a data classification system that is similar to the ones of other large enterprises [20,21,22]. Low risk, moderate risk and high risk data are defined in the appendices (Section VI).

Classification of data should be performed by the appointed Data Protection Officer (DPO). On a periodic basis, the DPO would be required to re-evaluate the classification of Enterprise Data in order to ensure that the assigned classification is relevant and applicable considering any legal and contractual changes as well as changes in the use of the data or its value to the enterprise. The frequency of re-evaluation should be determined by the DPO themselves based on the demands of the enterprise.

In addition to policy point (1.), all data that becomes a subject of an ongoing legal case will be categorised as Restricted Data. As such it is not going to be stored on third party provided online drives and under no circumstances should be transferred or discussed via instant messaging. This would result in the creation of a new job position within the enterprise. Employees who take this new position will be responsible for keeping track of all details regarding legal cases involving clients of the enterprise. Additionally, all clients would be required to agree to alert the enterprise of any legal cases they find themselves involved in. In consideration of this, Hopper & Grace would be responsible for protecting any data that has been transferred and could serve as a potential piece of evidence in a courtroom.

With regards to policy point (2.), Cyber Security Insurance will be applied in order to mitigate any potential consequences that are result from data destruction, DDoS attacks, extortion, theft or human failure. [24]

With regards to policy point (3.) the appointed DPO will be responsible for duties such as the process of Cyber Risk and Cyber Security education within the company and its employees. Staff training on topics such as important compliance requirements. and data processing. Additionally, the DPO will be responsible for conducting audits to ensure compliance and address potential issues proactively as well as the maintenance of comprehensive records of all data processing activities conducted by the company. The DPO will be monitoring staff performance while providing advice on the impact of data protection efforts. Furthermore, the DPO will serve as an important point of contact between the company and GDPR Supervisory Authorities.

Regular briefings must be given to employees to ensure they are adhering to procedures concerning the use of instant messaging applications. Cyber Security workshops should be held on a regular basis. Printed copies of the policy statement as well as cyber security information booklets are going to be made available to all employees, both current and new.

With regards to policy point (4.), research will have to be conducted into the best platform for an enterprise approved Instant Messaging (IM) tool in order to find the one that provides an adequately secure protocol of encryption. If no IM tool is found to provide an adequately secure level of encryption, multiple IM tools will be used for data transfer with the requirement that encryption will be completed by in-house developed encryption protocols.

With regards to policy point (1.d) and policy point (5.), strict password rules and regulations will be implemented. This would be done on the grounds that particular IM applications require authentication and provision of password upon each log-in. Approved Enterprise password management tools will be put into practice in order to ensure the high levels of security when it comes to password protection.

With regards to policy point (6.), contracts and agreements with clients must be devised in accordance with the policy statement. Policy practices would need to be explicitly stated in such documents in order to communicate to clients and any other stake-holders what is expected of them if they are to partake in the sharing of data via Instant Messaging tools. Employees dedicated

to policy expertise might be needed to liaise with clients and other stake-holders and assist them towards the achievement of cyber security goals.
With regards to policy point (7.), dedicated system administrators will be responsible for the maintenance of access for new, current and former employees of the enterprise. Any participant in an instant messaging business communication channel that is no longer an employee of Hopper & Grace should be removed from the channel. The administrator will be responsible for restricting the former employees' access to any data exchanged on those channels or any other private channels.

Evaluation

Policy Strengths

In terms of strengths of the policy, compliance with policy points (1.), (4.) and (8.) will significantly reduce the likelihood of incidents associated with risks 1, 2 and 4. Compliance with policy point (3.) will reduce the levels of risk associated with risk 3. Furthermore, adherence to policy points (5.) and (7.) will decrease the levels of risks associated with risks 7 and 8. In terms of damage control, policy point (2.) will mitigate any potential consequences associated with incidents related to any of these risks and will serve to protect the assets of the enterprise.

Policy Weaknesses

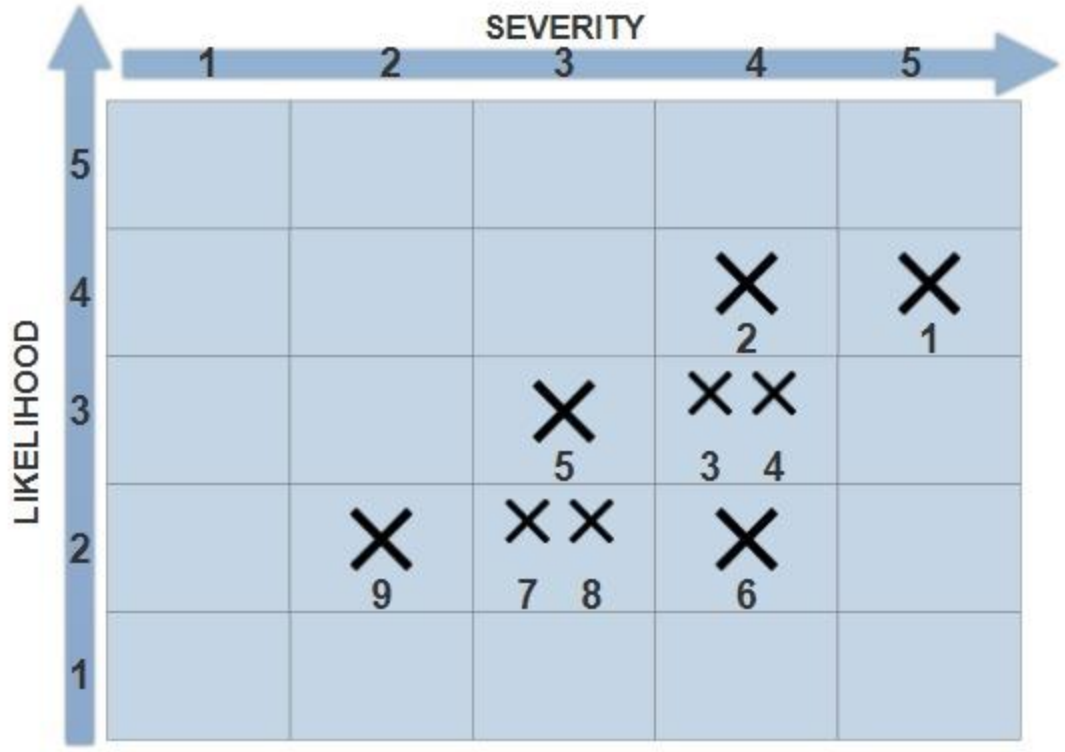
On the other hand, policy point (2.) might be a weak point of the policy. The reason being that it could potentially result in the increase of the likelihood of some of the risks as empirical evidence suggests employees might become too lenient and neglect the regulations proposed in the policy statement. [25]
Furthermore, the policy focuses predominantly on employee conduct which strict regulation is possible to achieve. On the other hand, as Anderson and Moore suggest security of any system is only as strong as its weakest part and in the case of Hopper & Grace clients represent a potential weakness. Further research and evaluation might be needed in order to improve the way by which clients integrate with the policy and the security goals of the enterprise. Considering the weaknesses mentioned above, it would be a good practice for the enterprise to regularly review the policy and implement changes accordingly.

Effects of Implementation

The policy is of rather rigorous character and might impose strict control on employees and possibly clients of the enterprise. This might result in a potential reduction of the productivity boost that is expected to be achieved with the implementation of Instant Messaging tools within the enterprise. A list of some of the metrics to monitor both the positive and negative effects of the policy is suggested below:

- Percentage of clients using Instant Messaging tools for business communication and data exchange.
- Percentage of employees using Instant Messaging tools for business communication and data exchange.
- Rate of gain of new clients post policy implementation
- Rate of loss of existing clients post policy implementation
- Lawsuits filed against Hopper & Grace per month
- Number of disciplinary penalties for employee breach of policy points (1.) and (5.) per month

Appendix I: Risk Matrix



Appendix II: Risk Classification

Public Data (Low Risk) is data which is either intended for public disclosure or that is of no concern if the public or a competitor obtains it. The loss of confidentiality, integrity, or availability of Public Data would have no adverse impact on the enterprise nor its affiliates and clients. Examples of Public Data are press releases, documents containing information about the services which the company provides, job adverts and any information that is available in the public domain.

Private Data (Moderate Risk) is data which is not generally intended for public disclosure and/or contains information which falls under the realm of the data protection act [23]. The loss of confidentiality, integrity, or availability of Private Data could have a mildly adverse impact on the enterprise and its affiliates and clients. This could potentially lead to loss of reputation, financial losses and information leaks to competing enterprises as well as legal compensation claims made by clients. By default, all Enterprise Data that is not explicitly classified as Restricted or Public should be treated as Private. Examples of Private Data are non-public contracts, records containing client/staff personal information (NI/ID numbers, date of birth, etc.) and commercially-sensitive information such as unpublished financial planning and budgeting information.

Restricted Data (High Risk) is data which strict protection is required by state law or federal privacy regulations and data protected by confidentiality agreements. The loss of confidentiality, integrity, or availability of Restricted Data could have a significant adverse impact on the enterprise and its affiliates and clients. Example of Restricted Data is information on individuals' health, racial or ethnic origin, sexual life, political opinion, religious or other beliefs, criminal record or alleged offences, etc. Information regarding client/staff financial records, including credit card/bank numbers is also considered Restricted Data to which the highest level of security controls should be applied.

Appendix III: Bibliography

[1]Iso.org, 2018. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en. [Accessed: 14- Nov- 2018].
[2]B. Rossi, "The threat from within: how to prevent employee collusion - Information Age", Information Age, 2015. [Online]. Available: https://www.information-age.com/threat-within-how-prevent-employee-collusion-123459601/. [Accessed: 19- Nov- 2018].
[3]"Yahoo 2013 data breach hit 'all accounts'", BBC News, 2017. [Online]. Available: https://www.bbc.co.uk/news/business-41493494. [Accessed: 29- Nov- 2018].
[4]J. Schreier, J. Schreier, E. Ellis, B. Barrett, T. Sohn, A. Watercutter, B. Raftery and G. McMillan, "Sony Estimates $171 Million Loss From PSN Hack", WIRED, 2011. [Online]. Available: https://www.wired.com/2011/05/sony-psn-hack-losses/. [Accessed: 29- Nov- 2018].
[5]J. Fraser, "Security Alert: Slack User Info Leaked – Origin Protocol – Medium", Medium, 2018. [Online]. Available: https://medium.com/originprotocol/security-alert-slack-user-info-leaked-2ec5b32d760d. [Accessed: 29- Nov- 2018].
[6]W. Yakowicz, "Hackers Breached Slack's Central Database", Inc.com, 2015. [Online]. Available: https://www.inc.com/will-yakowicz/hackers-breach-slack-central-database.html. [Accessed: 22- Nov- 2018].
[7]M. Gomez, "70 Million Telegram Accounts May Have Been Leaked; What Does That Mean for Telegram’s Blockchain Network? - Cryptovest", Cryptovest, 2018. [Online]. Available: https://cryptovest.com/news/70-million-telegram-accounts-may-have-been-leaked-what-does-that-mean-for-telegrams-blockchain-network/. [Accessed: 29- Nov- 2018].
[8]"GDPR Penalties and Fines | IT Governance UK", Itgovernance.co.uk. [Online]. Available: https://www.itgovernance.co.uk/dpa-and-gdpr-penalties. [Accessed: 29- Nov- 2018].
[9]"Right to erasure", Ico.org.uk. [Online]. Available: http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/. [Accessed: 29- Nov- 2018].
[10]2017 Data Breach Investigations Report. Verizon, 2017.
[11]"Slack's GDPR Commitment", Slack, 2018. [Online]. Available: https://slack.com/gdpr. [Accessed: 29- Nov- 2018].
[12]"Telegram Privacy Policy", Telegram, 2018. [Online]. Available: https://telegram.org/privacy. [Accessed: 29- Nov- 2018].
[13]J. Fisher, "Booz Allen Issues Financial Services Cyber Trends for 2015", Boozallen.com, 2014. [Online]. Available: https://www.boozallen.com/e/media/press-release/booz-allen-issues-financial-services-cyber-trends-for-2015.html. [Accessed: 29- Nov- 2018].
[14]"Telegram F.A.Q.", Telegram. [Online]. Available: https://telegram.org/faq. [Accessed: 29- Nov- 2018].
[15]"Attacks hit BA, GitHub and Slack", BBC News, 2015. [Online]. Available: https://www.bbc.co.uk/news/technology-32115292. [Accessed: 29- Nov- 2018].
[16]M. Kandias, N. Virvilis and D. Gritzalis, The Insider Threat in Cloud Computing. .
[17]K. Narayan, "5 Devious Instances of Insider Threat in the Cloud", Skyhigh. [Online]. Available: https://www.skyhighnetworks.com/cloud-security-blog/5-devious-instances-insider-threat-cloud/. [Accessed: 29- Nov- 2018].
[18]"Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature", Prnewswire.com, 2016. [Online]. Available: http://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html. [Accessed: 29- Nov- 2018].
[19]J. Melling, "The Role of Physical Security in Managing Cyber Security Threats", Churchill Security Ltd, 2017. [Online]. Available: https://www.churchillsecurity.co.uk/2017/01/12/role-physical-security-managing-cyber-security-threats/. [Accessed: 29- Nov- 2018].

[20]C. University, "Guidelines for Data Classification - Information Security Office - Computing Services - Carnegie Mellon University", Cmu.edu, 2016. [Online]. Available: https://www.cmu.edu/iso/governance/guidelines/data-classification.html. [Accessed: 29- Nov- 2018].
[21]C. University, "Data Risk Classification", Chapman.edu. [Online]. Available: https://www.chapman.edu/campus-services/information-systems/security/data-risk-classification.aspx. [Accessed: 29- Nov- 2018].
[22]C. Edwards and D. Montgomery, Information Risk Classifications. Glasgow: University of Glasgow, 2017.
[23]"Data Protection Act 1998", Legislation.gov.uk, 1998. [Online]. Available: https://www.legislation.gov.uk/ukpga/1998/29/contents. [Accessed: 29- Nov- 2018].
[24]T. Ball, "Top 5 cyber insurance providers offering the best cover against attack", Computer Business Review, 2018. [Online]. Available: https://www.cbronline.com/list/top-5-cyber-insurance-providers. [Accessed: 27- Nov- 2018].
[25]R. Anderson and T. Moore, "The Economics of Information Security", Science, vol. 314, no. 5799, pp. 610-613, 2006.
[26]Kaspersky.co.uk.[Online].Available: https://www.kaspersky.co.uk/resource-center/preemptive-safety/malware-remover-vs-antivirus-software. [Accessed: 27- Nov- 2018].
[27]A. Regalado, "Who Coined 'Cloud Computing'?", MIT Technology Review, 2011. [Online]. Available: https://www.technologyreview.com/s/425970/who-coined-cloud-computing/. [Accessed: 29- Nov- 2018].

Appendix IV: Reviews and Plans of Action

Review 1

This review seeks to give suggestions for improvements to the team's report, which was written on a topic related to H&G and its cyber threats in relation to the use of messaging tools by its employees. It will be divided into three separate sections: **Firstly**, it will advise the authors what they should **start** demonstrating in the report that is currently missing or incomplete, e.g. proper identification of cyber risks; **Secondly**, it will advise the authors what they should **stop** doing within the report itself, e.g. what is not working or is causing confusion; **Thirdly**, it will advise the authors what they should **continue** doing within the report itself, e.g. referencing strong evidence that cements arguments.

To begin with, the authors could improve in the way they identify and evaluate cyber risks. One idea for evaluating cyber risks would be for the authors to use a risk matrix, which in a general form has two axes (consequence and likelihood). The process of creating a risk matrix could significantly improve the identification of relevant risks and would give a visual overview for the stakeholders as well about the different risks. In addition to the risk matrix, the authors must focus on the proper way of elaborating their risks with real-life examples. Currently, the report lacks in this regard, not aided by the fact that the authors have not properly referenced their sources regarding the examples. Another area of improvement is the policy and its implementation section. It is evident that it would need a complete overhaul. One area of improvement could be the addition of a coverage matrix in the appendix of the essay. The coverage matrix is designed to communicate to the individual stakeholders, representing the audience, what company security policies are relevant to them with respect to specific domains of data security e.g. secure device usage, data

communication, data storage/management. This final report should include how the directives should be communicated to the stakeholders, for example in the form of a booklet. What is more, the policy should directly cover the risks labelled in the report and must be connected to that section. In addition, the section, which covers the implementation and evaluation of the policy is rather non-existent, hence a focus should be put there in order to have a clear and precise 1-page implementation and evaluation of the policy.
When it comes to suggestion regarding what the authors should stop doing within the report itself, then the current style of writing should be avoided. Instead, the report should contain more precise headings and it should be formatted in a way, which makes reading more straightforward. What is more, as stated in the first section of this review, referencing needs a proper attention, because as of now, the report lacks the proper citation and referencing. It creates confusion, since it is unclear, where do the authors have taken their information on the matters they have discussed in the report as well as it makes the evaluation of sources more difficult, when they are missing from the report.
In regard to the advice on what the authors should keep doing within the report itself, then it is difficult to highlight matters, which should be kept. In general, on the face of it, the draft of the report has covered the sections a policy report should need to cover. However, some sections, such as the section four, which covers the implementation and evaluation of the policy is almost non-existent as well as the section three(policy), which lacks the direct connection with the risks segment of the report. In general, the concerns and risks sections touch the areas they need to, however, as with the other sections, one could also criticise the content of these first two sections. Still, the authors of this review would recommend keeping the content of concerns and risks (to an extent), add a risk matrix to the appendixes and note it in the risk section as well as to edit the last two sections of the report to make it look as a complete policy document with proper referencing.

ENTERPRISE CYBER SECURITY (M)
PLAN FOR ACTION 1

BADGES	**YES/NO**
Independent and Critical Thinker	
Effective Communicator	

STOP
Outline the most important piece of ‘stop’ feedback you received about your draft report from the review (100 words limit).
The reviewers argued that the current style of writing should be avoided. Instead, the report should contain more precise headings and it should be formatted in a way, which makes reading more straightforward. Additionally, they suggested to put references since the draft has very less references.
Outline the actions taken in the final report to address feedback (100 words limit).

a) We added proper headings and sub-headings to the report. b) We have used a clear format which is easy to follow. c) We have provided proper references and citations in the report.
Evidence of actions in final report (provide references)
a) The bibliography section has all the references and the in-text citations can be found in the report. b) Headings and sub-headings are evident from the report structure.

START
Outline the most important piece of 'start' feedback you received about your draft report from the review (100 words limit).
The reviewers insisted that the report must have outlined goals and objectives. Also, the reviewers suggested that the report should consider both internal and external of risk assessment.
Outline the actions taken in the final report to address feedback (100 words limit).
a) We designed the policy section so that it clearly specifies the goals and objectives as well as distinguishes the data subjects into client and enterprise. b) We have considered both internal and external context of risk assessment under the Risk Assessment section. c) We implemented a Risk Matrix to give an overview of the risks. d) We have talked about the metrics and the success of intervention in the implementation part of the report. e) We have a clear and precise 1-page implementation and evaluation section which specifies information about the distribution of cyber security information booklet.
Evidence of actions in final report (provide references)
Section III talks about the policy. Section IV talks about the implementation and evaluation of policy. Risk Matrix is present in the appendix.

CONTINUE
Outline the most important piece of 'continue' feedback you received about your draft report from the review (100 words limit).
a) This report has good policies which just need a bit modification. b) The implementation part should adhere with policy.

Outline the actions taken in the final report to address feedback (100 words limit).
a) We modified the policy section b) We changed our implementation section to adhere with the policy.
Evidence of actions in final report (provide references)
Section III talks about the policy. Section IV talks about the implementation and evaluation of policy.

Review 2

The report on Hopper and Grace's incorporation of messaging tools like Slack and Telegram, and the entailing security risks has outlined the cyber security objectives clearly. It clearly mentions all the risks that are involved with the usage of such applications in an industry. The risks involved in using the independent applications are thoroughly discussed by the authors in the paper. For example, they have found that the third-party integration tool used by Slack is faulty. The user base also attracts the hackers as hacking it would lead them to numerous organization's data. The authors also discussed the mishap of April 2016, when many developers using Slack had posted their credentials online, which is a perfect instance of human errors being a risk in itself. The risks that come with Telegram's using the Secure Hashing Algorithm 2 (SHA-512) are discussed thoroughly as well. The issue of the Telegram leaking the metadata is found to only help the attackers to understand when a user is online or offline. The authors have also stressed on the fact that data breach is the most important point among all other risks. The security of the cloud environments that are used by both the messaging applications is also discussed in detail. The authors have understood and explained all the risks and have also mentioned certain policies that shall help to evade the risks. The most important asset that needs protection is the data. Data belonging to the industry, data of the associates working in the firm and data of the client, needs to be secure along with the industry's cloud storage. However, the authors have failed to understand and explain how exactly an intervention occurs. They could have conducted experiments to check the loopholes that exist which gives access to the attackers easily. It could have also helped to understand how exactly a breach can be efficiently detected and stopped. Also conducting experiments would help them to understand the implications of an intervention. The authors could have also done without stressing on GDPR and its implementation and instead stressed on how the organization in question can comply with the rules of the GDPR, while implementing the messaging applications in the organization. The authors could also have explained the implementation and evaluation of the policies that they have noted down in the paper. In a nutshell, the paper is well constructed and the risks pertaining to the implementation of the messaging applications are discussed well.

ENTERPRISE CYBER SECURITY (M)

PLAN FOR ACTION 2

BADGES	YES/NO
Independent and Critical Thinker	
Effective Communicator	

STOP
Outline the most important piece of 'stop' feedback you received about your draft report from the review (100 words limit).
The reviewers argue that we should stop stressing on GDPR and its implementation and instead stressed on how the organization in question can comply with the rules of the GDPR, while implementing the messaging applications in the organization.
Outline the actions taken in the final report to address feedback (100 words limit).
We disagree with the reviewers' point made on GDPR as we consider it too ambiguous. We have made important points regarding GDPR compliance and we have thoroughly considered the risks of non-compliance with GDPR.
Evidence of actions in final report (provide references)
Section II, category A, risk 3

START
Outline the most important piece of 'start' feedback you received about your draft report from the review (100 words limit).
The reviewers have made important points about our draft report not including the implementation and evaluation of the policy section. Additionally, they suggested that we conduct experiments in order to determine metrics and discuss the success of the intervention.
Outline the actions taken in the final report to address feedback (100 words limit).
We added a detailed implementation section which discusses the methods of policy implementation. We have devised a number of metrics in order to monitor both the positive and negative effects of the implemented policy.
Evidence of actions in final report (provide references)

Section III.

CONTINUE
Outline the most important piece of 'continue' feedback you received about your draft report from the review (100 words limit).
Overall, the review is very positive, as a result, the reviewers suggest that we should continue along the lines.
Outline the actions taken in the final report to address feedback (100 words limit).
Given that the review was in the style of a literature review and it was difficult to identify the stop, start and continue components, we have tried to focus on making general improvements such as the ones outlined in the start section.
Evidence of actions in final report (provide references)
The entire report.

Review 3

The group of this draft has done a great job, looking into quite a few concerns and risks. However, some improvements can still be made. First, when discussing Telegram in the concerns section, the authors mention that only the "secret chat mode" is encrypted. The authors should further consider, that, as they previously mentioned in their draft, no encryption is unbreakable. What if telegram's encryption is not trustworthy? Is it possible to decrypt it and eavesdrop? The authors would benefit from addressing this issue too. Secondly, although various risks in data breach and cloud storage are considered and discussed detailedly, the impact of them was not taken into account which results in the assessment not complete enough, as some risks may have huge impact with little chance of happening can still be a significant matter. The quantitative analysis which combine both likelihood and consequence may contribute to a more comprehensive assessment in finding the most significant risks and hence addressing the resolving policy. Some information in the draft needs to be cited. For instance, the draft in Section 1 mentions that Iran and Russia have banned Telegram. Where do you get this information from? Need to be more careful about the reference. Some spelling and grammar mistakes can be seen in the draft, so going over the draft is quite necessary. The policies are not clear enough. There seems to be confusion for the authors among policies, standards and guidelines. Section 4 seems to be unfinished with an outline.

Too many personal pronouns were used in the draft which make the report slightly subjective. Some of the reference are not professional enough. The goal is too general and vague as just starting to reduce risk. A more specific description could be achieved. For example, they may need to indicate the type of risk and to what degree it will be mitigated by the given policy.

The structure and coherence of the draft is quite good. Concerns and risks are supported by evidence that took place in real life which seems very persuasive. Lots of statistical data is used to support the view such as the 2016 and 2017 Version Data Breach Investigations.

ENTERPRISE CYBER SECURITY (M)

PLAN FOR ACTION

BADGES	YES/NO
Independent and Critical Thinker	
Effective Communicator	

STOP
Outline the most important piece of 'stop' feedback you received about your draft report from the review (100 words limit).
The authors of this review suggested that the draft report was too subjective due to a high number of personal pronouns and that there were occasional grammatical and spelling errors in the report.
Outline the actions taken in the final report to address feedback (100 words limit).
In the final draft, the number of personal pronouns used was limited in order to ensure the report was not too subjective and the report was proofread thoroughly before submission. It was also ensured that there was consistency in terms of spelling, British English being used throughout.
Evidence of actions in final report (provide references)
Throughout the report, personal pronouns were limited. Previously they had appeared a lot in the risk sections, however, in the final report, there were none.

START
Outline the most important piece of 'start' feedback you received about your draft report from the review (100 words limit).
The authors of this review suggested that a "quantitative analysis" would be beneficial in terms of identifying the most significant risks to the company so that the policy could be more specific.
Outline the actions taken in the final report to address feedback (100 words limit).
A likelihood and severity ratio were introduced, and a risk matrix was added to the appendix, in order to better express the impact these risks would have on Hopper & Grace. Each risk that was identified was assigned a number so as to make the report clearer.
Evidence of actions in final report (provide references)

In section 1, each identified risk was assigned a specific number. The appendices include a risk matrix.

CONTINUE
Outline the most important piece of 'continue' feedback you received about your draft report from the review (100 words limit).
This review noted that some good sources had been cited, however, it highlighted that there were other sections of the report which didn't have enough evidence to back up the points that were being made.
Outline the actions taken in the final report to address feedback (100 words limit).
Additional sources were provided so that the points made in the report were cemented in evidence
Evidence of actions in final report (provide references)
Bibliography added to the report's appendix and the indexed citations were clearly marked in the report

Appendix V: Workload Report

All team members have made equal contributions towards the production of the final piece of work. Regular group meetings were held on a weekly basis during which plans for further action were devised. Each member of the team conducted research on different aspects regarding the risks involved with the implementation of collaborative messaging tools within a large enterprise. Risk analysis and policy statement construction were completed by different members being responsible for writing separate parts of each section. The editing and formatting of the final document were carried out as a group effort. Additionally, members of the group were allocated with a feedback review to read and consider. Feedback was taken into consideration and plans of action were discussed and devised in order to follow the requirements for the assessment.