A review of subscription-based service features set as security controls

Gabriel Edrick Acuña
School of Information Technology
Mapua University
Makati, Philippines
geoacuna@mymail.mapua.edu.ph

Luis Antonio Alvarez
School of Information Technology
Mapua University
Makati, Philippines
lazalvarez@mymail.mapua.edu.ph

John Ramil Funilas
School of Information Technology
Mapua University
Makati, Philippines
jrffunilas@mymail.mapua.edu.ph

Luis Rafael Laurena
School of Information Technology
Mapua University
Makati, Philippines
lrvlaurena@mymail.mapua.edu.ph

Joshua Millard Odicta
School of Information Technology
Mapua University
Makati, Philippines
jmnodicta@mymail.mapua.edu.ph

Ronald Bernardo
School of Information Technology
Mapua University
rbbernardo@mapua.edu.ph

Dr. Eric Blancaflor
Professor of School of Information Technology
Mapua University
Makati, Philippines
ebblancaflor@mapua.edu.ph

Abstract

Information security risks are always changing, and so must the countermeasures against them. A security assessment is essential for ensuring that a company is prepared and secure. In this case study, the researcher conducts a vulnerability assessments and proposed security controls, where recommended security controls are culled from those available subscription-based services online. The study aims to identify and assess five (5) different security issues involving the concerned marketing company, Company ABC, and recommend potential solutions that will mitigate each identified issue. The framework used in the assessment is the ISO 27001. Among the vulnerability findings were lack of security management for storage of company resources, files can be stolen and stored locally and disseminated without detection, there is no change management system and lack of proper documentation for work, interns are not provided corporate emails and instead uses their personal emails for internal and external communication and server access, lack of security management for storage of company resources, lack of centralized management, interns are not provided corporate emails and instead uses their personal emails for internal and external communication and server access. Recommended solutions were detailed in this study and focuses on the usage of the functionalities of these different subscription-based platforms, dropbox, google workspace, gmail, and protonmail.

Keywords

Information security, subscription-based services, dropbox, google workspace, protonmail

1. Introduction

Information security risks are always changing, and so must the countermeasures against them. A flexible reaction based on regular risk assessments is required by many best-practice frameworks, regulations, and laws. A security assessment is essential for ensuring that a company is prepared and secure (ISG, 2021). With this, the researcher was motivated to work on with studies focusing on security assessments and recommending security controls out of the outcome of the assessments conducted.

In this case study, the researcher conducts a vulnerability assessments and proposed security controls, where recommended security controls are culled from those available subscription-based services online. The researcher took the opportunity to promote the benefits of subscription-based services such as enhanced customer service, a safer environment for Your data, increased employee productivity, less IT pressure (Wereb 2019). The case site company in this study takes pride with their expertise in the Marketing and Information Technology scene. A passionate community of consultants who are committed to provide the best solutions for their client's needs, by being updated with the latest trends in marketing and technologies. They aim to reach their target audience by creating relevant content to ensure that technologies created are manageable, efficient, and adaptable to help with the optimization of business operations.

1.1 Objectives

The study aims to identify and assess five (5) different security issues involving the concerned marketing company, Company ABC, and recommend potential solutions that will mitigate each identified issue. An unstructured interview will be conducted to determine the IT processes and components involved within the company's IT operations to determine security issues in the company. Knowing what security issues to be tackled, potential solutions will then be discussed and recommended for each issue accordingly.

1.2 Scope and Limitation

The study is limited to cover and review (5) security issues found within the chosen company, Company ABC. The study will then discuss potential solutions to address the security issues discovered. Solutions discussed and proposed in this paper are based on factors such as company size, projected company yearly income, etc. It is important to note that other security issues existing within the chosen company may not be covered in this study due to the limitations this project requires, and the limited access given by the company. Lastly, it is important to note that the chosen company will be labeled "Company ABC" as per the company's request to anonymize their identity.

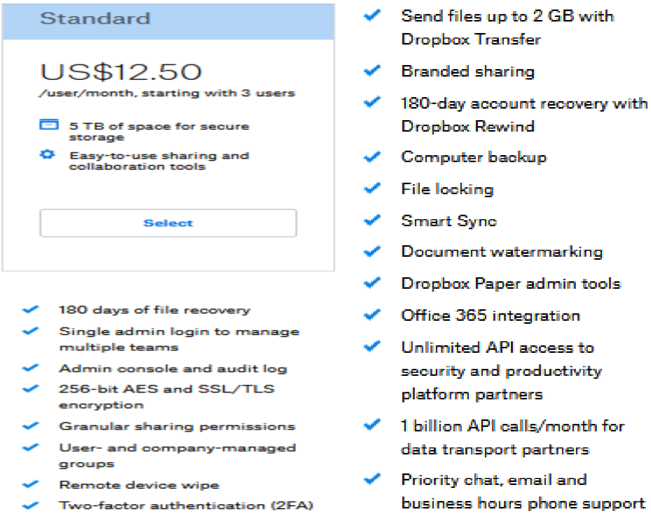
1.3 Significance of the Study

The exposure of security issues and vulnerabilities is a crucial part of maintaining stability and security within an organization as it represents gaps that could be exploited by malicious threat actors and inadvertent disasters caused by its own employees. The documentation of these vulnerabilities or security issues could then highlight what can and cannot be improved depending on the company's situation and investment in security which also serves as the basis of the proposed solutions to mitigate risks associated with the security issues found, by considering and implementing the proposed solutions, an organization reduces the risk and costly impacts the issues might bring if it were to actuate.

2. Literature Review

2.1 Dropbox

Figure 1. shows some of the features included with the Dropbox business standard plan along with the pricing plan per month. To get into more details, file access and data security centralizes all the files within an organization and provides admin control over who can access, for how long and what permissions they have. The admin console also can view stats such as remaining licenses, pending invites, send reminders, view usage data, and most importantly view security alerts. File versioning is also featured in the plan that allows team members to restore previous versions of files and even view file history and activity logs for 180 days after an event occurs. Collaboration is another feature highlighted by the plan by giving access to Dropbox Paper, a collaborative document-editing software like Google Docs. Lastly, if there are any problems or concerns, tech support through live chat, email or phone is provided (Dropbox 2021).



Standard

US$12.50
/user/month, starting with 3 users

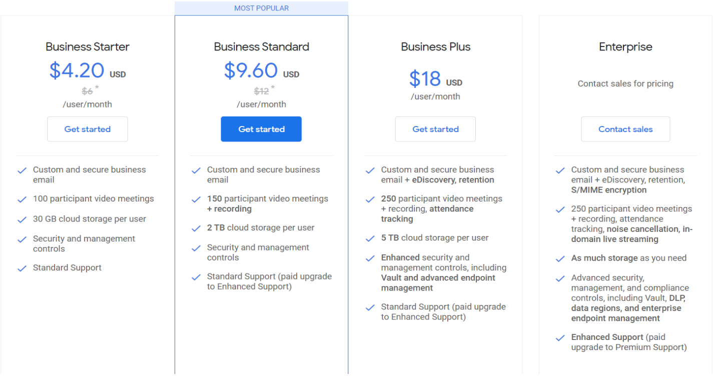
- 5 TB of space for secure storage
- Easy-to-use sharing and collaboration tools

- ✓ 180 days of file recovery
- ✓ Single admin login to manage multiple teams
- ✓ Admin console and audit log
- ✓ 256-bit AES and SSL/TLS encryption
- ✓ Granular sharing permissions
- ✓ User- and company-managed groups
- ✓ Remote device wipe
- ✓ Two-factor authentication (2FA)
- ✓ Send files up to 2 GB with Dropbox Transfer
- ✓ Branded sharing
- ✓ 180-day account recovery with Dropbox Rewind
- ✓ Computer backup
- ✓ File locking
- ✓ Smart Sync
- ✓ Document watermarking
- ✓ Dropbox Paper admin tools
- ✓ Office 365 integration
- ✓ Unlimited API access to security and productivity platform partners
- ✓ 1 billion API calls/month for data transport partners
- ✓ Priority chat, email and business hours phone support

Figure 1. Dropbox Business Standard Features and Pricing Plan

2.2 Google Workspace

Google Workspace also provides an appsheet application that lets users develop applications without coding. Google Workspace also declares itself to be "fast" in which it lets users easily access documents from Google Docs, Calendar, Gmail, and Meet making it easier to plan, share and coordinate with other members [10]. The pricing for Google Workspace, as shown in figure 2, that can be bought for up to 300 users, varies from the services the package offers. There are 4 packages and the standard package, which is priced at $9.60 a month already offers 2TB of cloud storage which is already very important for the storage of work-related files. There are also other options that can fit the company well such as the Business Starter, The Business Plus, and The Enterprise which needs the contact between Google and the company for the pricing (Google Workspace 2020).



	MOST POPULAR		
Business Starter	Business Standard	Business Plus	Enterprise
$4.20 USD ~~$6~~ * /user/month	$9.60 USD ~~$12~~ * /user/month	$18 USD /user/month	Contact sales for pricing
Get started	Get started	Get started	Contact sales
✓ Custom and secure business email	✓ Custom and secure business email	✓ Custom and secure business email + **eDiscovery, retention**	✓ Custom and secure business email + eDiscovery, retention, **S/MIME encryption**
✓ 100 participant video meetings	✓ **150** participant video meetings **+ recording**	✓ **250** participant video meetings + recording, **attendance tracking**	✓ 250 participant video meetings + recording, attendance tracking, **noise cancellation, in-domain live streaming**
✓ 30 GB cloud storage per user	✓ **2 TB** cloud storage per user	✓ **5 TB** cloud storage per user	✓ **As much storage** as you need
✓ Security and management controls	✓ Security and management controls	✓ **Enhanced** security and management controls, including **Vault and advanced endpoint management**	✓ Advanced security, management, and compliance controls, including Vault, **DLP, data regions, and enterprise endpoint management**
✓ Standard Support	✓ Standard Support (paid upgrade to Enhanced Support)	✓ Standard Support (paid upgrade to Enhanced Support)	✓ **Enhanced Support** (paid upgrade to Premium Support)

Figure 2. Package Pricing of Google Workspace

2.3 Tettra

As shown in figure 3, Tettra is a knowledge base combined with an expert system whose goal is to centralize the corporation's knowledge and documents and use it to answer queries. It is stated to route questions to the personnel that are most suited to answer the question. There are also additional features such as role-based access and authentication, team collaboration for documents, integration with Slack, search functionality and user permissions (Tetra n.d.).

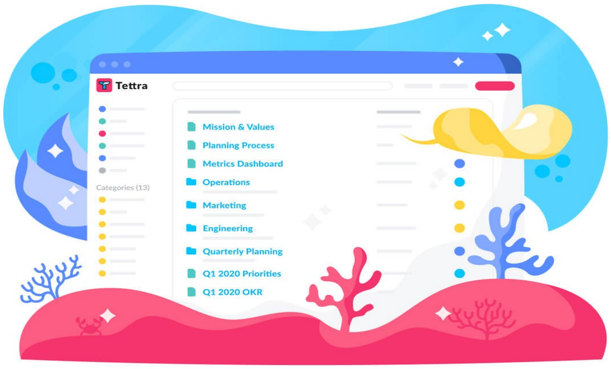


Figure 3. Tettra.

3. Methods

The researchers were guided by the ISO 27001 framework in conducting the security assessment of the Company ABC. The ISO 27001 International Standard takes a process-oriented approach to establishing, implementing, running, monitoring, reviewing, maintaining, and upgrading an organization's information security management system (ISMS). This case study has solely focused on the Plan phase of the ISO 27001 cycle, which includes 4 cycles namely, Plan, Do, Check, and Act. (ISO/IEC 27001 2005). In this study, the researchers conducted an interview to the management and concerned staff of a mid-size marketing company. The aim of the interview is to figure out loopholes and vulnerabilities in their security particularly in their infrastructure, processes, and documentation. Data collected from the interview results are presented below.

4. Data Collection

4.1 Lack of security management for storage of company resources

Company resources and assets like UML diagrams, process flows and schematics for the system are all stored in the cloud which is specifically Google Drive. While the interns are individually given access to the storage based through Google Accounts, Role based access control (RBAC) is not implemented by the company and might result in possible compromise of said resources since anyone with access to the company files will be able to download all the files. Since the company uses the personal or community version of google drive, there are not any administrative controls to manage access nor are there any accounting for files stored in the cloud.

Not having a system for the categorization of users and their respective permissions using their roles will not only make assigning tasks less efficient and optimal but might lead to the accidental deletion of important resources and files by users. The lack of administrative and security controls means that there is no real way of managing permissions, even less providing logs, to ensure file integrity and data exfiltration.

4.2 Files can be stolen and stored locally and disseminated without detection.

Files from the drive can be downloaded and stored locally and disseminated without detection. Since the company does not actually own the assets used by their employees, and lack the sufficient tools to oversee them, there is no real way to detect whether they are exfiltrating sensitive data or not.

The lack of data loss prevention tools could lead to potential data loss which means losing time and money (assets) that is essential to the company or business. This could also disrupt the daily activities (business timeline) of the company depending on the importance of the data loss. It could also damage the image of the company, as a company is obliged to inform the client/customer if sensitive information is lost, reducing the client's trust value. The lack of DLP controls paves the way to disgruntled or malicious employees exfiltrating sensitive data to competitors or otherwise.

4.3 Lack of Centralized Infrastructure

The company lacks enough IT assets to deploy a centralized system where each one of its IT assets are constantly managed and maintained. This lack of IT resources opens the company to a sprawl of unmanaged systems, which may be vulnerable to not only security issues, but also internal threats, where a user lacks the security awareness to make smart security-related decisions.

Having no central management issues can lead to unmanaged systems housing vulnerabilities that can lay undetected for a long period of time. Lack of non-repudiation, because the company lacks administrative control over their systems, there is no real way of proving one's association with an illegal action or otherwise. The lack of centralized management not only opens systems used in business production to external threats, but it also opens it up to internal threats of its own employees, such as disgruntled employees or digitally illiterate users.

4.4 There is no change management system and lack of proper documentation for work.

Websites created by the company do not possess proper documentation policies and rollback policies and mechanisms in the case of a failure in migration or implementation of a patch or update, some backups need to be initiated manually. Proper documentation of code used for the website is not mandatory and may possibly have a large negative impact on the company such as their customer satisfaction and will possibly reduce optimization of employee time due to solving the same problems repeatedly.

Having no change management system in place can increase the chance that one implemented change might render an entire system unusable or at a worse state. If the system is rendered at a worse state, it is unlikely that reverting to a functional state is possible, having a change management system fix this, by keeping track of every change done to a system. The lack of proper documentation will make the lives of employees harder by not providing them instructions for solving problems and fixing bugs which will in turn cost the company more resources and time (Dhillon 2015).

4.5 Interns are not provided corporate emails and instead uses their personal emails for internal and external communication and server access.

Interns are not provided a separate email for internal and external communication. They use their personal emails to communicate with their colleagues and clients. Having a decentralized email infrastructure can lead to difficult management. This can potentially harm not only the victim but also the company if ever the intern's personal email was compromised especially since interns can access the company's server (Myki 2018).

If interns are not associated with the company anymore, compromised intern emails would not only gain access to the intern's personal information but also gain access to confidential information and private data concerning the company (Myki, 2018). A decentralized email infrastructure can prove hard to manage and difficult with coordination, even more hard to administer and implement security controls within the infrastructure. It can also be expensive since more responsibilities will be allocated among members (Sethy K. n.d.).

5. Results and Findings

5.1 Proposed Improvements

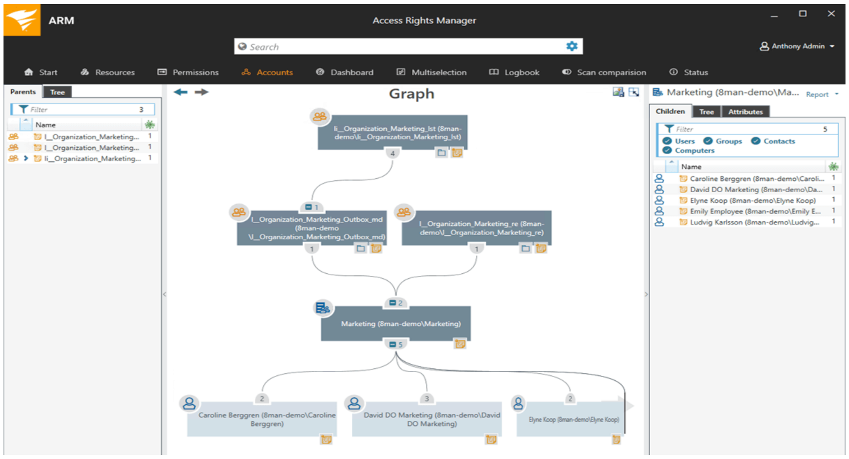
5.1.1 Lack of security management for storage of company resources

Cloud storage has become one of the fastest-growing segments in IT organizations. Much like other critical IT solutions, cloud storage has managed to effectively integrate themselves as a crucial dependency for many organizations. However, according to Gartner.com, 90% of organizations that fail to control public cloud use will inadvertently expose information through 2025 (Panetta 2019). The result of this issue might then spawn a myriad of issues concerning data privacy and compliance penalties. Instead, the company should use a cloud storage solution that can implement file security and appropriate permissions to users. One example is Dropbox Business, Dropbox Business has a pricing plan suited for Company ABC and its needs, specifically the business standard version is catered exactly for small to medium sized businesses that includes 5TB of storage per month, ability to implement file-permissions, password-protected and expiring shared links, administrative controls such as an admin console and tech support, all for roughly 600 pesos a month on a per user basis (Dropbox n.d.) which can then be shared among the department or team of an organization.

5.1.2 Files can be stolen and stored locally and disseminated without detection.

It is recommended to get Data Loss Prevention Tools along with data loss prevention policies to prevent losses of assets that could damage the value and trust of customers to the company. Getting a DLP Tool is the first step to prevent this kind of loss that could damage the brand of the company, and this could also strengthen the company's data security to avoid breaches. For the policies part, they could start with internal training on how to handle sensitive data of the company by setting up rules and parameters on what the employees could do with the data they receive as part of their work and flag instances that break those rules (De Groot, J., 2020). For the Data Loss Prevention Tool, one example would be SolarWinds Data Loss Prevention with ARM, as it has functions that could minimize the impact of insider threat and improve company compliance by detecting changes and identifying who has access to what resources. It has an annual subscription starting with $1,838 and permanent subscription starting with $3,444, this product is a good investment for the company as it could improve the overall security of the company assets and protect the image of the company from security breaches.

Figure 4 shows one of the key features of SolarWinds DLP Tool which could help monitor user activity that can put sensitive data at risk. Another key feature is that it alerts the admin whether there is a suspicious activity such as unauthorized access or escalation of privilege. It also captures user access details and generates custom reports to help track and detect insider risk and improve the company's data leak prevention (Solarwinds 2021).


ARM
Access Rights Manager
Search
Anthony Admin
Start
Resources
Permissions
Accounts
Dashboard
Multiselection
Logbook
Scan comparision
Status
Parents
Tree
Filter
Graph
li_Organization_Marketing_lst (8man-demo\li_Organization_Marketing_lst)
4
1
l_Organization_Marketing_Outbox_md (8man-demo \l_Organization_Marketing_Outbox_md)
l_Organization_Marketing_re (8man-demo\l_Organization_Marketing_re)
1
1
2
Marketing (8man-demo\Marketing)
5
2
3
2
Caroline Berggren (8man-demo\Caroline Berggren)
David DO Marketing (8man-demo\David DO Marketing)
Elyne Koop (8man-demo\Elyne Koop)
Marketing (8man-demo\Ma...
Report
Children
Tree
Attributes
Filter
Users
Groups
Contacts
Computers

Name	3
l_Organization_Marketing...	1
l_Organization_Marketing...	1
li_Organization_Marketing...	1

Name	5
Caroline Berggren (8man-demo\Caroli...	1
David DO Marketing (8man-demo\Da...	1
Elyne Koop (8man-demo\Elyne Koop)	1
Emily Employee (8man-demo\Emily E...	1
Ludvig Karlsson (8man-demo\Ludvig...	1

Figure 4. Automation of user access policy, analysis, and enforcement with data loss prevention tools

5.1.3 Lack of Centralized Infrastructure

Using a "centralized" platform that contains a variety of applications in one platform may be of help for a small company. By getting a license from one of these platforms, they can access many applications that can help in the work process of the company. Having a centralized network "provides more direct control and is generally easier to set up and manage" according to vXchnge while an Admin can manage the whole network (Seal 2020). The efficiency of being able to manage these apps in one platform will very well impact the overall workflow. It also creates a consistent user experience due to the applications in the platform being within one, making them all predictable and stable. Performance and speed are also observed in using centralized networks due to requests and data flow must go through a main server.

5.1.4 There is no change management system and lack of proper documentation for work.

Change management in cybersecurity is defined as a process in controlling and systematizing changes that are applied to a system whether the change itself is hardware or software. Processes covered by Change Management are change identification and post-implementation reviews. Its purpose is to limit the amount of risk that the system is exposed to during major changes like migration to new platforms or minor changes such as an implementation of a new feature to an already established application. However, it is important to note that Change Management itself is not only composed of software and hardware but rather it is a culture that seeks to enforce Cybersecurity's best practices as well by enforcing proper review processes and documentation (Nielerk & Ramluckan 2020).

Documentation is a necessary element in change management especially in software development and engineering. Proper documentation contains standards, instructions and protocols that will serve as the blueprint of the project and a journal for possible bug fixes and errors that are encountered during the development process wherein the steps in solving these problems will be documented and recorded for future use. It is also vital in optimizing communication and teamwork between team members as it is very helpful for helping new members learn or test the system through properly written instructions and documents (Kipyegen, et. al 2013). However, the creation of proper documentation may not be enough if employees have a hard time finding it. Readmes while possible to create and attach to GitHub repositories are not mandatory to Company ABC which makes project continuation by new interns hard due to the lack of proper documentation and instructions. Because of those reasons the implementation of a centralized Knowledge Base is proposed.

Unfortunately, good change management software does not solve all the problems regarding documentation. There is always the human element in the equation. Security policies and instructions for proper documentation must be enforced and employees must be trained to teach them how to document properly and, in the future, cultivate an environment that not only applies best practices but also encourages good documentation (Panorama Consulting Group, 2020).

5.1.5 Interns are not provided corporate emails and instead uses their personal emails for internal and external communication and server access.

It is recommended that the company provide separate emails for their interns to minimize risks especially since they are using Gmail for business communication. Gmail can and allows third party applications and services to access information sent and received (Buxton, 2018). Among various email providers, Gmail is one of the top email providers in this generation along with their many services.

Gmail offers free email services which are provided by Google. Just like other email providers, a user can create, send, and receive emails. Some of its unique features include conversation view, a built-in chat, and call phone (Gmail: Introduction to Gmail. n.d). The following features are perfect for communication especially since Company ABC specializes with marketing where communication is very evident. Despite being encrypted with Transport Layer Security (TLS), providers can still access the information contained with each email (Green, E. 2019).

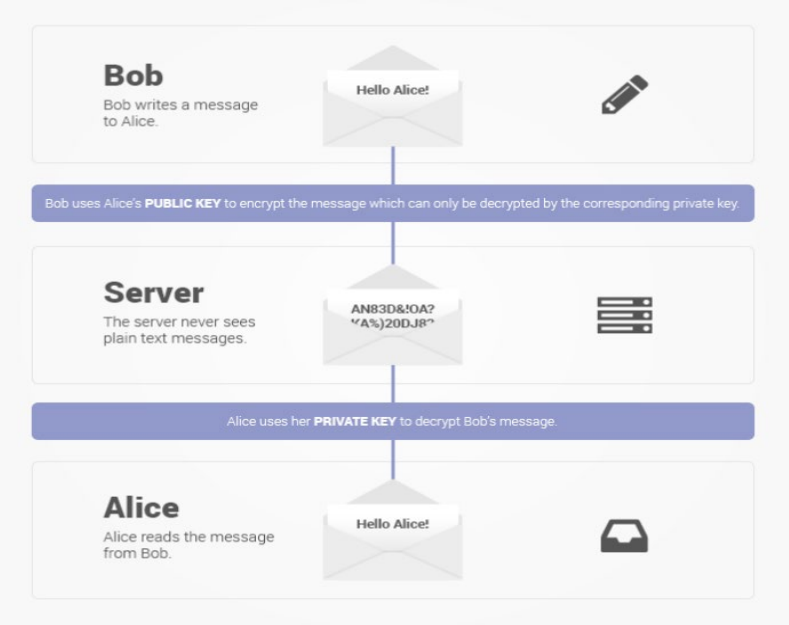
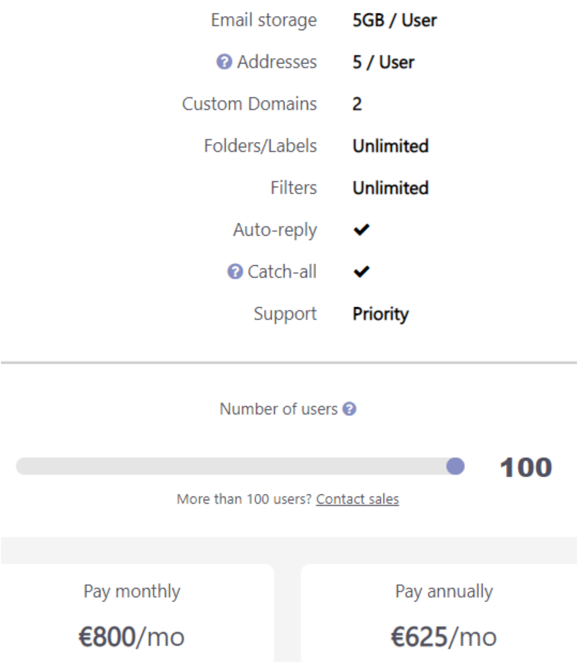

Bob
Bob writes a message to Alice.
Hello Alice!
Bob uses Alice's **PUBLIC KEY** to encrypt the message which can only be decrypted by the corresponding private key.
Server
The server never sees plain text messages.
AN83D&!OA?
A%)20DJ8
Alice uses her **PRIVATE KEY** to decrypt Bob's message.
Alice
Alice reads the message from Bob.
Hello Alice!

Figure 5. Protonmail Business End-to-end encryption

Figure 5 displays the end-to-end encryption of Protonmail. Protonmail is an open-source email provider and a more secure alternative compared to Gmail. Unlike Gmail that has access to every information sent and received, Protonmail's approach provides more security which offers end-to-end encryption wherein no one, even Protonmail itself can read the messages. It also offers zero-access encryption which indicates that no one can decrypt encrypted emails unless a key is used. This adds resiliency especially whenever data breaches do occur (Yen, A. 2017).



Email storage	5GB / User
Addresses	5 / User
Custom Domains	2
Folders/Labels	Unlimited
Filters	Unlimited
Auto-reply	✓
Catch-all	✓
Support	Priority

Number of users

100

More than 100 users? Contact sales

Pay monthly	Pay annually
€800/mo	€625/mo

Figure 6. Protonmail Professional Plan

Figure 6 shows the Protonmail professional plan (ProtonMail for Business n.d.). Company ABC can consider this option to subscribe however due to the potential financial reasons, they may opt out and recommend their interns to create a free Protonmail account due to its approach to data privacy with its end-to-end encryption rather than letting them use their personal mails for internal and external communication in the business environment. Especially since security issues are tackled, more secure alternatives are suggested to reduce the risks.

6. Conclusion

It is vital for an organization to conduct security assessments to strategize remediating vulnerabilities identified during such assessments. Studying information security and existing frameworks such as 27001 are of bog help for a researcher or the individual who will conduct such assessments are well guided and could come out with a viable security assessment result. Reviewing features and functionalities of subscription-based services may aid in providing security solutions discovered in a company or organization. Taking advantage on the benefits of subscription-based services in providing security solution is highly recommended in this study. Given the success of Dollar Shave Club, Harry's, and other subscription-based service firms, they devised a plan that not only targeted their audience, but also expanded on it to maintain and grow their member base providing a pleasant customer service (Blancaflor & Julian 2021).

References

Blancaflor, E. and Julian, J., KingsmanMNL: A Proposed Web Application Designed for Male Grooming Essentials Services. *In 2021 5th International Conference on E-Society, E-Education and E-Technology (ICSET 2021). Association for Computing Machinery, New York, NY, USA, 283–289.* DOI:https://doi.org/10.1145/3485768.3485793, 2021.

Buxton, M., The Gmail Privacy Controversy: How to Review Third Party Access to Your Inbox. Retrieved from: https://www.refinery29.com/en-us/2018/07/203805/gmail-third-party-access, 2018.

De Groot, J., What is Data Loss Prevention (DLP)? A Definition of Data Loss Prevention.
Available: https://digital guardian.com/blog/what- data-loss-prevention-dlp-definition-data-loss-prevention, 2020.

Dhillon, G., What to do Before and After a Cybersecurity Breach? Available:

https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf, 2015.

Dropbox, Find the right Dropbox plan for you. Available: https://www.dropbox.com/business/plans-comparison, 2021

Dropbox, What is the Dropbox Business Standard Plan? Available: https://help.dropbox.com/accounts-billing/plans-, 2021.

Gmail, Introduction to Gmail. Available: https://edu.gcfglobal.org/en/gmail/introduction-to-gmail/1/, 2020.

Google Workspace, Google Workspace. Available: https://workspace.google.com/landing/ partners/referral/trial.html?utm_source=sign- up&utm_medium=affiliatereferral&utm_campaign=apps-referral-program&utm_content=PB7XZB8, 2020.

Green, E., Is Gmail secure enough to protect your emails?. Available: https://nordvpn.com/blog/is-gmail-secure/, 2019.

ISG, Conducting a Successful Security Risk Assessment, Available: https://isg-one.com/third-party-management/articles/conducting-a-successful-security-risk-assessment, 2021.

ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirement. First edition. Published in Swtizerland, 2005.

Kipyegen, N. J., & Korir, W. P. K., Importance of software documentation. International Journal of Computer Science Issues (IJCSI), 10(5), 223-228. Available: https://www.proquest.com/scholarly-journals/importance-software-documentation/docview/1477204708/se-2?accountid=203424, 2013.

Myki, Don't Let Interns Compromise Your Company's Security. Available: https://myki.com/blog/dont-let-interns-compromise-your-companys-security/, 2018.

Nielerk B. & Ramluckan T., A Change Management Perspective to Implementing a Cyber Security Culture. DOI: 10.34190/EWS.20.059, June, 2020.

Panetta, K., Gartner offers recommendations for developing a cloud computing strategy and predictions for the future of cloud security. Available: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/, 2019.

Panorama Consulting Group, Why Cybersecurity Requires a Change Management Plan Available: https://www.panorama-consulting.com/why-cybersecurity-requires-a-change-management-plan/, 2020.

ProtonMail for Business, Available: https://protonmail.com/business/pricing, 2020.

Seal, A., Centralized vs Decentralized Network: Which One Do You Need?. Available: https://www.vxchnge.com/blog/centralized- decentralized-network, 2020.

Sethy, K., Advantages and Disadvantages of Decentralization. Available: https://www.economicsdiscussion.net/management/advantages-and-disadvantages-of-decentralization/31848, n.d..

Solarwinds, Lightweight, Easy-to-Use Data Loss Prevention Software. Available: https://www.solarwinds.com/access-rights-manager/use-cases/data-lossprevention?a_bid=27f1527d&CMP=BIZ-PAP-CMPRTCH-data_loss_prvn-ARM-UC&a_aid=BIZ-PAP-CMPRTCH, 2021.

Tetra, Available: https://tettra.com/, n.d.

Wereb, G., 10 Benefits of Using Subscription-based IT Services for Your Business Enlisting the help of a Managed Service Provider for your IT needs is becoming. Available: https://www.cose.org/en/Mind-Your-Business/Operations/10-Benefts-of-Using-Subscription-Based-IT-Services-for-Your-Business, 2019.

Yen, A., Why Protonmail Is More Secure Than Gmail. Available: https://protonmail.com/blog/protonmail-vs-gmail-security/, 2017.

Biographies

Dr. Eric Blancaflor is an Associate Professor of Mapua University, Philippines. He earned B.S. in Electronics Engineering from Mapua University, Master's in Engineering major in Computer Engineering in the University of the City of Manila and Doctor of Technology in Technological University of the Philippines. He has published conference papers related to IT systems, network design and security.

Gabriel Edrick Acuña is a graduate of Bachelors of Science in Information technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Luis Antonio Alvarez is a graduate of Bachelor of Science in Information technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

John Ramil Funilas is a graduate of Bachelor of Science in Information technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Luis Rafael Laurena is a graduate of Bachelor of Science in Information technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Joshua Millard Odicta is a graduate of Bachelor of Science in Information technology in Mapua University, Philippines. His interests are into programming, web development, internet of things, network and systems administration.

Engr. Ronald Bernardo is an Instructor of Mapua University, Philippines. He earned B.S. in Electronics Engineering from Mapua University and currently working as a security systems analyst.