Privacy, Security and Organizational use of Social Media

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

# Introduction

Social media is not only reserved for domestic and informal communication but also plays an important role in the corporate sector and organizations as well. Companies and organizations are using social platforms not only for advertisement purposes but also for internal coordination. Several media platforms that are commonly used nowadays are social networking sites, video sharing, photo sharing and microblogging(*The 6 Most Effective Types of Social Media Advertising in 2020*, n.d.). Like other IT and financial assets of the organization, social media platforms are also prone to cyber-attacks and can be used for exploitation of the target. It is therefore highly recommended that the organization must ensure the presence of an effective plan of action or policy for social media platforms too. In this discussion, some of the effective approaches that can be used for the protection of social media privacy are discussed and solutions are provided as opinions for the upper management especially CISO of the Padgett-Beale.

# Analysis

In PBI-FS, we use social media platforms for publicity, promotion and also for communication within the organization. Out of different social media platforms, PBI-FS uses social networking sites for the purpose which include Facebook, LinkedIn, and Google etc. Privacy concerns associated with the use of these platforms are various. First of all, these sites are a prime source that may help the offender in social engineering. In social engineering, an attacker may use these platforms for gathering information to use it for fraudulent or malicious activities. Social media online platforms are the prime victim of fishing attacks, In fishing attack, a malicious soured hides its identity and insert malicious content in your device which then makes the system vulnerable, denial of service or may add a backdoor in the device to steal the important information(*How to Recognize and Avoid Phishing Scams | FTC Consumer Information*, n.d.). One important threat to consider is a web application attack which is also carried out through social media platforms mostly.

In my opinion, the use of social networking sites should not be allowed to every individual of the origination rather only the department of sales and marketing should be allowed to have access to these platforms for marketing and other organizational uses. The reason is, these sites are the leading victims of cyber-attacks.

The department using these platforms should make sure social media compliance with the relevant standards and policies in order to ensure the privacy of the social media of the company. The CISO of the company must ensure that NIST FIPS Publication 199 is strictly followed in order to categorize all the information which is going to be posted on social media (Via, 2009). This publication determines the fulfilment of the famous CIA triad of security. It should be NA for confidentiality, and no greater than the low impact on Availability and Integrity. Use AUP technology in order to determine the behavior and working or new media technologies from a security point of view (F.I.P.S, 2004). The management must make sure to always update federal level policies in accordance with the available guidance.

# Conclusion

Engaging with social media technologies in the organization is a difficult decision due to their high vulnerability to cyber-attacks. Owing to the potential of social media to attract customers and hence capital, it has become inevitable for the companies to incorporate its use in business. The decisions regarding social media should not be made by the IT department alone rather they must also include the opinions and suggestions from other departments and actors including CISO, risk manager CIO, mission owner and privacy officer as well.

# References

*How to Recognize and Avoid Phishing Scams | FTC Consumer Information*. (n.d.). Retrieved February 17, 2020, from https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

*The 6 Most Effective Types of Social Media Advertising in 2020*. (n.d.). Retrieved February 17, 2020, from https://www.bigcommerce.com/blog/social-media-advertising/#the-6-best-social-networks-for-ecommerce-advertising

Via, E. (2009, August). Guidelines for Secure Use of Social Media by Federal Departments and Agencies. In *Chief Information Officers Council (US)*. Chief Information Officers Council (US).

Pub, F. I. P. S. (2004). Standards for security categorization of federal information and information systems. *NIST FIPS*, *199*.