Security and privacy enhancing framework for Social Media Influencers and Content Creators

Kia Finska*
kia.finska@utu.fi
University of Turku
Turku, Finland

Antti Hakkala
antti.hakkala@utu.fi
University of Turku
Turku, Finland

Anne-Maarit Majanoja
anne-maarit.majanoja@utu.fi
University of Turku
Turku, Finland

ABSTRACT

In a relatively short period of time, social media has become a multi-billion dollar industry. One key demographic for social media are Social Medea Influencers (SMIs), who are entrepreneurs that work as independent marketers between companies and consumers. A significant amount of marketing revenue goes through SMIs, making them and their enterprises, often tied to a single social media platform and account, lucrative targets for malicious actors. The cybersecurity posture of a social media entrepreneur is often inadequate, as cybersecurity knowledge and expertise are not core competencies for SMIs. This paper presents a cybersecurity framework for SMIs that can be implemented in their business. The framework has been adapted from an existing framework for organisations into a framework that is directed specifically towards SMIs. The framework takes into account the nature of SMI work, the general technical aptitude of the target demographic and aims to provide an easily adaptable and implementable solution for improving the security posture of SMIs.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; **Social network security and privacy**; • **Applied computing** → Electronic commerce.

KEYWORDS

Social media, Influencer, Cybersecurity, Framework, Entrepreneurship, Risk assessment

ACM Reference Format:
Kia Finska, Antti Hakkala, and Anne-Maarit Majanoja. 2024. Security and privacy enhancing framework for Social Media Influencers and Content Creators. In *International Conference on Computer Systems and Technologies 2024 (CompSysTech '24), June 14–15, 2024, Ruse, Bulgaria.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3674912.3674942

1 INTRODUCTION

Since the rise of social media, a new business field – social media marketing – has been formed. The cost-effectiveness of social media marketing can be attributed to the sale of expertise by content creators, the relationship with their followers, and the platform and marketing space. Social media influencers (SMIs) have capitalised on this development to expand their businesses. Despite its relative youth, this industry has grown rapidly and is now a popular marketing method. [14] The global spending for social media advertising has been estimated by Statista to be $219.8 Billion USD in 2024 [17]. This makes it a lucrative target for malicious actors. Cautionary examples of SMIs losing their platforms and potentially their whole companies and livelihoods have been reported in the news [5]. Cyberbullying and stalking represent a significant threat to users of social media. However, due to the highly visible profile of SMIs, they are particularly susceptible to attacks. On one hand, because SMI's are, more often than not, marketing professionals and not cybersecurity professionals, their understanding of and ability to assess and react to cybersecurity issues and threats is not essential for success in their work. On the other hand, failure to properly plan for and react to cyber threats can lead to catastrophic failure. For a SMI, technology is a facilitator, not the focus of their work [4].

This underscores the necessity for tangible direction for SMI entrepreneurs on how to remain secure online. This paper presents a framework designed for social media content creators and influencers. The framework has been adapted from an existing cybersecurity framework for critical infrastructure. It is noteworthy, however, that other frameworks identified in the research do not provide the requisite perspective for the current case. The practical objective of the framework is to provide SMIs with a tool with which they can educate themselves, maintain focus and comprehend both their own and their companies' cybersecurity requirements. Furthermore, the framework aims to assist in the preparation for potential cybersecurity challenges by taking concrete steps towards the securing of businesses and personal information in the volatile social media industry.

The purpose of this paper is to assist social media content creators and influencers in comprehending the security risks, requirements and priorities that they face. This is necessary in order to develop a more secure methodology for their work on social media platforms. The objective is to create a more accessible and understandable security culture, step by step. The research questions addressed in this paper are as follows:
RQ1: what practical steps are needed to ensure the security of a social media-based company in the cyber world?
RQ2: what are the most significant risks that social media companies face in relation to their cyber security?
RQ3: how to implement this security framework in practice?

This paper is structured as follows. In Section 2 we assess existing literature on social media cybersecurity issues, identify the main threats for SMIs, and provide motivation for our research. In Section

*This paper is based on the prior Master's Thesis done by the author.

CompSysTech '24, June 14–15, 2024, Ruse, Bulgaria

ACM ISBN 979-8-4007-1684-3/24/06
https://doi.org/10.1145/3674912.3674942

3 we present our proposal for a cybersecurity framework for SMIs. In Section 4 we provide discussion and analysis on the proposed framework and identify potential future work in the field. Finally, in Section 5 we conclude the paper with our closing remarks.

2 LITERATURE REVIEW

The growth of Web 2.0 has led to the rise of several social networking sites such as Facebook, Instagram, Twitter, LinkedIn, Pinterest, Tumblr, TikTok, Pinterest, Snapchat, and several others [6, 10]. The number of social network users is expected to grow from 2.86 billion in 2017 to 5.85 billion in 2027 [16]. Current research focuses mainly on social media from the perspective of the ordinary user of the applications [6], leaving out the social media influencer. As the number of social network users increases, the number of security risks that compromise user privacy, authenticity, and confidentiality also increases.

Current research clearly identifies the challenges that different social media applications and technologies pose to users. Attackers use a variety of methods. Previous research has identified the following threats that, in the worst case, can have a significant impact on social media users [6]: *Account related threats*: Profile cloning attack, Sybil attack, Attacks from compromised accounts. *Identity-related threats*: Impersonation, Information leakage, Identity inference attack, Identity theft attack. *Privacy related threats*: Privacy violations by service providers, Violations by Third-party applications, Location leakage attack, De-anonymization attack. *Traditional threats*: Spamming, Phishing, Viruses and Worms, Malware attacks, Cross-site scripting, Bots, Likejacking/clickjacking. *Social threats*: Stalking, Cyberbullying and abuse, Catfishing/dating scams, Online predators. These same security risks have an even more significant (including financial and reputational) impact on social media influencers. What are the (economic) costs of cybercrime to businesses, consumers and social media influencers? It is not a small one. The global "Estimated Cost of Cybercrime" indicator in the cybersecurity market is forecast to grow steadily between 2023 and 2028, reaching $5.7 trillion (+69.9%) [15].

According to Freberg *et al.* [3], social media influencers (SMIs) function as entrepreneurs, operating as an intermediary between a company's marketing strategy and the consumer. Influencers facilitate the creation of an image, dissemination of information, and the shaping of audience attitudes through a social media channel, such as Instagram, TikTok, or a blog. National Geographic Education defines a social media influencer as [2]: "Social media influencers are individuals who utilize social media platforms to build their own personal brand or influence their followers to act (including buying products, supporting a brand, or vacationing in a certain location)". They also describe social media influencers as modern day entrepreneurs [2]. Based on the used platform to share content, previous research has identified five types of influencers: 1) bloggers who post online texts (e.g., X, previously Twitter), 2) YouTubers/vloggers who share through recorded videos, 3) Instagrammers who share images and short videos on Instagram, 4) Streamers who interact with the public through video broadcasts and short live videos, including gamers, 5) and TikTokers whose digital content consists of short live videos on TikTok [18].

As earlier research has stated, technology is often seen as one of the reasons why so many people have access to fame in the digital age, but at the same time, technology is merely seen as a facilitator [4]. Typically, influencers can be considered as marketers who use technology and tools for tracking and measurement of their results, and the focus is on strategy and business planning [4]. As a result, technology itself and the threats it poses are not seen as a necessary skill to succeed as an influencer. To illustrate, an automotive influencer must possess a substantial understanding of automobiles, yet the technology utilized, such as Instagram and TikTok, and the cybersecurity risks associated with it, are not regarded as essential competencies. The security aspects of social media are most often viewed as the responsibility of the social media influencers themselves. Those with non-technical backgrounds may be unaware of discussions held about the security of the platforms themselves, the hacker-proofness of the platform code, and the responsibility of the information that these sites are gathering. [8]

We found that previous studies have failed to focus on cybersecurity risks of social media influencers and content producers. We conducted a literature search on IEEE Xplore, Taylor & Francis, ACM Digital Library, and Elsevier ScienceDirect from the content creator's perspective using various combinations of the words "cybersecurity", "social media", "business", "influencer" or "influencing" and "entrepreneur". IEEE Xplore returned 18 papers from 2019 to 2023, but only 2 papers were relevant to this theme, and none from the SMI perspective. These two papers focused on cyberbullying [11] and general e-marketing, in which they list many risks that digital marketing faces, but not entirely relevant to an individual in social media cyberspace [14]. Taylor & Francis Online database returned 63 papers, and based on paper titles and abstracts, 2 papers were found to be relevant to this study. Martínez-Navarro and Bigné [7] focused on why and how individuals create social media ads, but the paper lacks content creator security. Rochefort [12] focuses on social media policies, which is different from the topic of this paper. From the ACM Digital Library, 82 papers were found, and only one of them is relevant to this research. Allen et al. [1] discuss entrepreneurship in general in the digital age, but it does not discuss the same perspectives as this study. From the Elsevier ScienceDirect database, the search returned 137 results from the years 2019 to 2023. None of the papers were useful for this study based on title and abstract. Consequently, there has been a paucity of research conducted on the security of an SMI business or from the perspective of an individual and their business. The preceding studies lack several key elements of information. These include practical guidelines for an SMI, the actual risks an individual faces when creating a business based on their own identity, the actual practices for securing themselves, and the lived experiences of others in the area of social media influence. Therefore, the relevance and importance of this study is underscored.

3 DESCRIPTION OF THE FRAMEWORK

In this section we address the RQ1 of this paper. It should be noted that several methods were employed in the development of the SMI Security Framework, including the review of literature and frameworks, and the interviewing of social media influencers. However, the results of the latter are not discussed in detail in this paper.

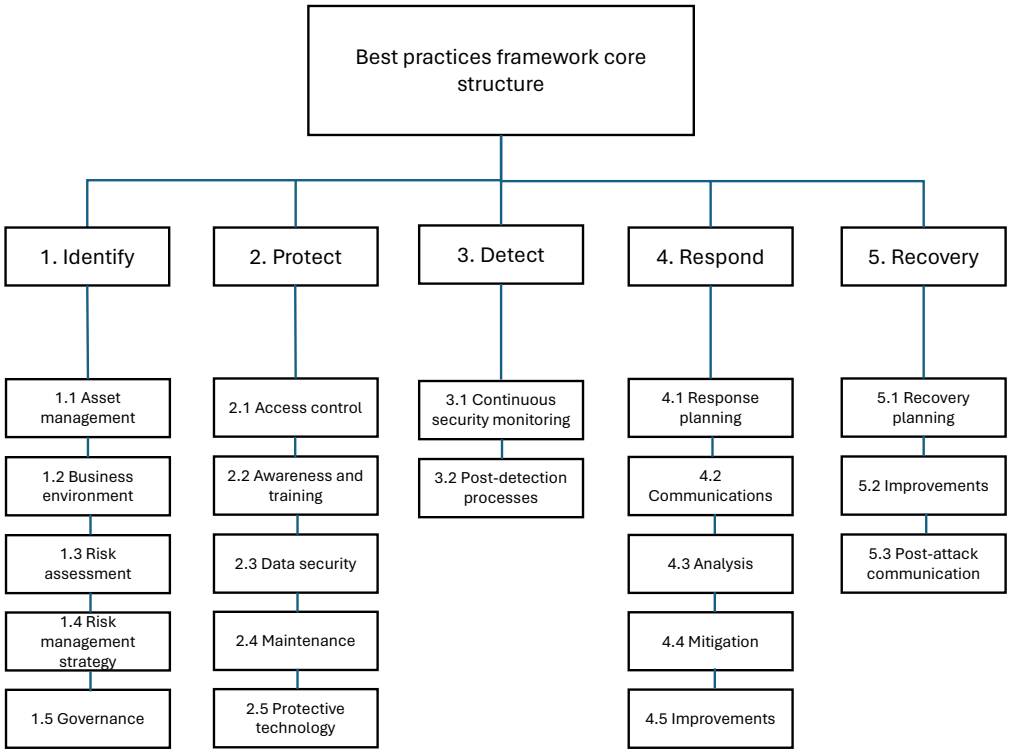

Figure 1: The core structure of the framework

The literature, frameworks, and interviews revealed elements of the SMI framework that require particular attention from SMI. The presented framework is adapted from the NIST Cybersecurity framework for critical infrastructure version 1.1 [9]. It has been designed to be easily approachable for anyone regardless of their background. The goal is for it to be useful for all SMIs, even if they have not attended any technical or business education, which is a common situation with SMIs.

The core structure of the framework is divided into four main groups, also shown in Figure 1. The subcategories and related information are further expanded in Figure 2.

- Functions: The five functions that an entrepreneur can use to uphold and recover from a cybersecurity incident: *identify, protect, detect, respond, and recover.*
- Categories: the activities done in a specific situation to process the functions that need to be done for safety.
- Subcategories: the more specific outcome of each act that needs to be done to fill the needs of the categories.
- Information: additional information regarding each activity.

The subcategories and related information in Figure 2 are the part of the framework that gives the SMI a concrete list of actions and goals for each category in the framework, bringing the more abstract functions closer to real life actions and concepts.

3.1 Risk assessment and evaluation of organizational risk tolerance

As a part of the framework, we have identified a set of concrete risks that are relevant for a SMI entrepreneur in their daily work. In this section we address the RQ2 of this paper. We have identified three main categories: human-related threats, data, and targeted attacks. These are illustrated in Figure 3. While the list is extensive, it is by no means exhaustive. As every business is different from one another, some risks may not apply to certain cases and there may be risks that we have not identified here that can apply to a particular SMI entrepreneur. Our goal is to provide a starting point for the entrepreneur to evaluating their own risk factors, how high or low the risks are, and what are the potential consequences. Our suggested scale is "high"; "medium" or "low" for both probability of risk realization and severity of consequences, and the overall risk for each entry can be evaluated on a case by case basis. Other threats and risks can be added according to the nature of the business adapting this framework to its use.

- Sharing too much personal information
  - Somebody arrives physically to your home or personal surroundings
  - Attack against your family with your information shared online
  - Across platforms attack with prior information
- Problematic followers

Functions	Categories	Subcategories	Information
1. Identify: to be able to secure a business, it is important to identify what needs to be protected and from what.	1.1 Asset management	List of assets – devices, people, locations	It is important to keep track on what assets a company has for their security maintenance and keeping up with their updates, for example.
	1.2 Business environment	List of social media platforms that are in use	Business environment includes all the technical and cyber environments that the business is related to. Identifying these environments is crucial to know what data to protect. It is also important to find out what information there is online about the business and the SMI.
		List of other platforms that are in use	
		Listing of what data different devices and platforms have	
	1.3 Risk assessment	What are the threats that the business faces?	Every company has online threats. It is important to be aware of them and what information, assets or people are at risk in case the threat becomes a reality.
		What could happen if those threats were to happen?	
	1.4 Risk management strategy	Risk management policies in place	How are the risks of the business managed? What applications, policies and guidelines are followed to minimize the risks?
		Applications and software's that are in use for risk management	
	1.5 Governance	Who is governing the company?	Who has responsibility for the company? What are their accesses to different systems? Are those people secure, trustworthy and well trained?
		What accesses do the people governing the company have?	
2. Protect: the ability to protect the business, its data, and resources. Listing on how the protection is done, what are the main goals and identified needs.	2.1 Access control	Who has access to different systems and what levels of access?	Access control includes information about who can access different data, platforms and is in the listing to be notified in the event of certain situations.
		How are the access rights of different systems monitored?	
	2.2 Awareness and training	What are relevant security trainings that should be taken?	Listing of needs what the SMI and people working with/for them need to be trained in, listing of on-going trainings.
	2.3 Data Security	How is the data secured?	What measures have been taken to secure business critical data and how? What is done in practice and at what points? How critical is the mentioned data?
		What is the more sensible data and where is it?	
	2.4 Maintenance	How is the security maintained?	What kinds of updates are done and how often? What kinds of firewall and antivirus applications are in use?
	2.5 Protective Technology	Which software and hardware are in use for protection?	What kind of protection is in use from physical keys to technical encryption practices?
3. Detect: how is the business able to detect possible breaches?	3.1 Continuous security monitoring	Platforms that let the user know is anonymous activity was detected.	Has the user received emails from Instagram or Google if questionable activity is happening on the SMIs accounts? Do platforms have the rights to send these messages to you?
	3.2 Post-detection processes	What is done when a detection is received? What is the process? How does the SMI start the next phase of "respond"?	What action points does the SMI take into use when a warning email is received?
4. Respond: the action points that will be taken into use in case of a security breach.	4.1 Response planning	First point of action	What will be done in practice in case of a breach?
	4.2 Communications	How to communicate to followers?	How will information be shared after the breach? To whom will the information be shared and what will that information be? What channels will be used? What are plan b's if those accounts were not accessible?
		How to communicate to co-operation partners?	
		How to communicate to friends and family?	
	4.3Analysis	How will the breach be analyzed?	Does the company have ready lists that they fill with information of the breach to conduct proper analysis?
	4.4 Mitigation	How can the data be secured so, that even if an attack happens, that the risks of loss are not too big?	How to create an environment where losing specific information is not as harmful as before?
	4.5 Improvements	How will the improving of these systems be conducted?	What will be the first steps in improving systems so that the risks are not as high in the future? Where can the SMI get help from?
5. Recovery: recovering from the attack and getting back to normal business as soon as possible.	5.1 Recovery planning	What are the most important things to do first after an attack?	What is the plan on how the business will get up after an attack to continue normal business?
		Creating a situation-based plan on what to do/editing a plan according to current needs.	
	5.2 Improvements	Where did things go wrong?	How can it be made sure that the attack doesn't happen again? Analysis about what went wrong and how to improve.
		What platforms/resources need improving?	
		Is there a need to put more resources on these aspects in the future?	
	5.3 Post-attack communication	Who needs to be contacted about the current status?	How will the communication about the incident be done? It is important to be careful with information sharing and not share too much information or confidential business aspects.
		What needs to be told about it and to whom?	
		Who will the communication come from?	

Figure 2: Expanded description of key elements of the framework

  - Excessive influx of followers (and due to them, issues with algorithm or DoS)
  - Followers that come too close to the SMIs personal life
- Damage for the brand
  - Ad that hurts the brand of the SMI (for example when not done well or if not suitable for the brand)
  - Someone trying to hurt one's business brand with lies or gossip - sabotage
  - The SMI saying or attending something that causes negative PR around the brand
  - Personal attack towards the SMI due to irritation, personal connections, or other emotional reasoning
- Human error
  - The SMI sends wrong message to the wrong person
  - The SMI posts wrong content
  - The SMI clicks on a malicious link or answers a malicious call
- Loss of data
  - Data leakage due to technical reasons (on a website, cloud or device)
  - Data leakage due to human error
- Integrity of data
  - The modification or destruction of files by malware/technical reason
  - The modification or destruction of files by mistake
- Losing the social media platform
  - Platform is closed down
  - One's page is blocked or closed down
  - Attack on one's page and malicious content spread on it
  - Platform loses relevance
- Attacks via Iot
  - Attack through IoT devices (IoT currently does not typically have a very high security level)
  - Malware spreading from IoT device to connected devices (such as phone or laptop)
- Theft: stolen device
- Shoulder surfing: Someone looking "over one's shoulder" to see what they are doing on their device
- Impersonation
  - Online impersonation of the SMI
  - Phishing sent in the name of the SMI
- Malware
  - Eavesdropping attacks
  - DoS by device battery exhaustion
  - DoS by utilizing built-in blocking functions of a smartphone
  - Virus or other unwanted software
- Phishing
  - Clicking a malicious link and adding payment or other details
  - Clicking a malicious link and accidentally downloading malware
  - Giving too much information about oneself that is then used for other attacks
  - Family member giving out information on the SMI
  - Receiving spam messages

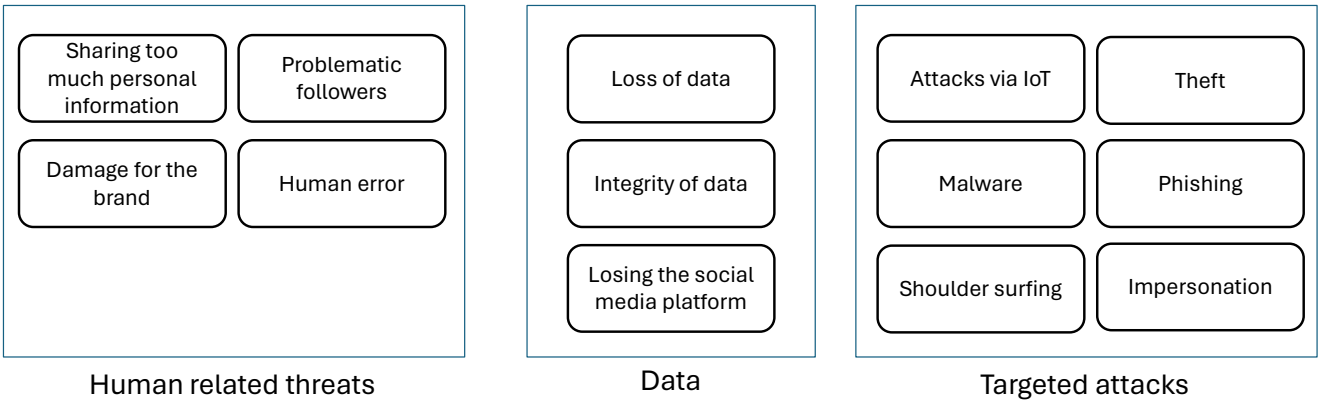

Figure 3: Main categories of identified potential risks for Social Media Influencers

3.2 Implementation and practical application of the framework

The following section outlines the process for implementing this framework in six concrete steps. In this section we address RQ3 of this paper. The initial phase of the process entails an examination of the scope and priorities of the business. The objective is to identify the objectives and strategic priorities. This entails determining the desired future trajectory of the company, understanding the nature of the business, identifying its key priorities, and examining its strategic approach. The second step is the assessment of assets and resources. This necessitates the SMI to identify and name the internal and external parties, systems, assets and requirements involved in the process of running the business. This also includes the identification of social media channels, personnel employed by the business, applications utilised, and relevant platforms. The third step is the risk assessment, which involves the identification, evaluation, and analysis of potential risks to the company. It is important to know what can happen, what could it cause, and what would be the severity level of those situations.

The fourth step is to describe the cybersecurity goals and desired outcomes for the business. The fifth step is to compare the current state of the company to the desired goals and outcomes. The objective is to idenitfy the specific actions and steps required to achieve the desired outcomes and to develop a detailed action plan for the implementation of these actions. The final step is the implementation of the framework into the business's day-to-day operations. This involves implementing the necessary actions and monitoring the ever-changing environment. This final step also involves ongoing reassessment of the original assessments and the implementation of appropriate action in the event of a change in the operating environment for the SMI. In the field of cybersecurity, it is essential to maintain a constant awareness of the evolving landscape and to implement updates to systems and training for personnel on a regular basis. Security is, after all, not a product but a continuous process [13].

4 DISCUSSION

The issue of cybersecurity is of significant importance to any individual who utilises the internet and social media. For SMIs, this is particularly true in comparison to the average user. As SMIs have integrated their online presence into their professional identities, their personal data is particularly vulnerable and in need of protection, given that it is more sensitive than that of a regular user. A SMI may suffer the complete loss of their livelihood as a consequence of a cybersecurity incident. Such incidents may include the compromise of their accounts through the use of malware or social engineering, or the instigation of defamation attacks against the SMI with the intention of damaging their reputation. SMIs are business owners and entrepreneurs with a very public profile. As a result of their public profile, they often divide opinions and aim to awaken critical discussion on current topics. SMIs are not only engaged in social media work but also utilise social media themselves. Consequently, their professional and private lives are often inseparably connected. This gives rise to the necessity of keeping their personal lives as secure as their businesses, but also heightens the risks if data or access were lost. SMIs often revolve around the personal brand of an individual, which must be safeguarded for the benefit of both the business and the individual.

When we consider the environment in which SMIs operate, cybersecurity challenges are evident. In addition to the security of the social media platforms that SMIs utilise, the tools and applications employed for content creation and business management also present an opportunity for malicious actors to launch attacks. While there are numerous applications available for various purposes, the ecosystem of applications for content creation and social media is not homogeneous for all users and influencers. This implies that there are multiple potential avenues for malicious actors to exploit, and security-conscious SMIs must possess a comprehensive understanding of cybersecurity to accurately assess the risks and threats within the environment. Unfortunately, this is not often the case, as technical ability and cybersecurity awareness are not key skills and knowledge areas for social media influencers (SMIs) and content creators. Consequently, a transparent and straightforward framework, such as the one presented in this paper, is particularly

beneficial to SMIs seeking to enhance their security posture within a challenging operational context.

Future work This field in general is not well studied, as is evidenced by the sparse existing literature. There is a lot of room for new research in the field and additional research could focus on use of social media applications and their security features in the context of SMI use. Also the physical and mental well being of SMIs, the practice of social media content creation itself, and the community around SMIs and their support regarding cybersecurity issues would definitely provide a fruitful avenue for future research. Finally, an updated version of the NIST Cybersecurity framework has been published in February 2024, and updating our work to consider the changes in the underlying framework is a natural direction for future work in this area.

5 CONCLUSION

This paper presents a framework that can be implemented by social media influencers (SMIs) in their work, with the goal of providing an improved security posture for social media entrepreneurs. The framework offers SMIs a robust tool set for improving their resilience to cybersecurity attacks. It is based on the NIST Cybersecurity Framework v. 1.1 and has been modified to take into account the specific operating environment in which SMIs operate. The provision of an accessible and implementable framework for SMIs confers benefits upon content creators and influencers, who, by virtue of their public status, attract greater attention from malevolent actors. Furthermore, regular users interact with SMIs, and may themselves become victims of cyberattacks if the SMIs' account is compromised. Consequently, a reduction in the attack surface and an improvement in the security posture of SMIs also benefits regular users, as it enhances the security of social media in general.

REFERENCES

[1] J.P. Allen, T. Paul Thomas, and Jonathan Ford. 2019. Technology Entrepreneurship in the Digital Age. In *Proceedings of the 2019 on Computers and People Research Conference* (Nashville, TN, USA) *(SIGMIS-CPR '19)*. Association for Computing Machinery, New York, NY, USA, 10–11. https://doi.org/10.1145/3322385.3322410

[2] National Geographic Education. [n. d.]. Influencers: The Modern Entrepreneur. https://education.nationalgeographic.org/resource/influencers-modern-entrepreneur/ Accessed 27.03.2024.

[3] Karen Freberg, Kristin Graham, Karen McGaughey, and Laura A. Freberg. 2011. Who are the social media influencers? A study of public perceptions of personality. *Public Relations Review* 37, 1 (2011), 90–92. https://doi.org/10.1016/j.pubrev.2010.11.001

[4] Alexandra Ruiz Gómez. 2019. Digital Fame and Fortune in the age of Social Media: A Classification of social media influencers. *aDResearch: Revista Internacional de Investigación en Comunicación* 19 (2019), 8–29.

[5] Anna Hopi. 2019. Rita Niemi-Mannisen piina päättyi! Paljastaa langenneensa klassiseen WhatsApp-huijaukseen - tällainen viesti meni täydestä. *Iltalehti.* https://www.iltalehti.fi/viihdeuutiset/a/263fc7af-d951-4778-b66d-89b2eeed9ca9 Accessed 27.03.2024.

[6] Gordhan Jethava and Udai Pratap Rao. 2024. Exploring security and trust mechanisms in online social networks: An extensive review. *Computers & Security* 140 (2024), 103790. https://doi.org/10.1016/j.cose.2024.103790

[7] Jesús Martínez-Navarro and Enrique Bigné. 2022. Sponsored consumer-generated advertising in the digital era: what prompts individuals to generate video ads, and what creative strategies do they adopt? *International Journal of Advertising* 41, 4 (2022), 623–654. https://doi.org/10.1080/02650487.2021.1972586

[8] McKringle Xolani Mhlanga, Richard Rabin Maiti, and Bennet Hammer. 2021. Privacy and Security Matters Related To Use Of Mobile Devices and Social Media. In *SoutheastCon 2021*. 1–6. https://doi.org/10.1109/SoutheastCon45413.2021.9401838

[9] National Institute of Standards and Technology. 2018. Cybersecurity framework - CSF 1.1 Archive. https://www.nist.gov/cyberframework/csf-11-archive Accessed 27.03.2024.

[10] Esteban Ortiz-Ospina. 2019. The rise of social media. *Our World in Data* (2019). https://ourworldindata.org/rise-of-social-media Accessed 27.03.2024.

[11] K.Bhavana Raj, Jitendra Kumar Seth, Kamal Gulati, Somya Choubey, Ity Patni, and Bhawna. 2022. Automated Cyberstalking Classification using Social Media. In *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*. 1–6. https://doi.org/10.1109/ICSES55317.2022.9914337

[12] Alex Rochefort. 2020. Regulating Social Media Platforms: A Comparative Policy Analysis. *Communication Law and Policy* 25, 2 (2020), 225–260. https://doi.org/10.1080/10811680.2020.1735194

[13] Bruce Schneier. 2000. The Process of Security. *Schneier on security (blog).* https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html Accessed 27.03.2024.

[14] Pranjal Srivastav and Himanshu Gupta. 2021. Role and Applications of Digital Marketing in Digital Era: A Review. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. 1–5. https://doi.org/10.1109/ICRITO51393.2021.9596087

[15] Statista. 2023. Estimated cost of cybercrime worldwide 2017-2028. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide Accessed 27.03.2024.

[16] Statista. 2024. The number of social network users is expected to grow from 2.86 billion in 2017 to 5.85 billion in 2027. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ Accessed 27.03.2024.

[17] Statista. 2024. Social media advertising spending worldwide from 2019 to 2028, by device. https://www.statista.com/statistics/456785/social-media-advertising-revenue-device-digital-market-outlook-worldwide/ Accessed 27.03.2024.

[18] N. Valenzuela-García, D.J. Maldonado-Guzmán, A. García-Pérez, and et al. 2023. Too Lucky to Be a Victim? An Exploratory Study of Online Harassment and Hate Messages Faced by Social Media Influencers. *European Journal on Criminal Policy and Research* 29 (2023), 297–421. https://doi.org/10.1007/s10610-023-09542-0