2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) | 979-8-3503-8674-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/TPS-ISA62245.2024.00059

Towards Inclusive Cybersecurity: Protecting the Vulnerable with Social Cyber Vulnerability Metrics

Shutonu Mitra*, Qi Zhang*, Chen-Wei Chang*, Hossein Salemi†, Hemant Purohit†, Fengxiu Zhang‡,
Michin Hong§, Chang-Tien Lu*, Jin-Hee Cho*,
* Department of Computer Science, Virginia Tech, USA
†Department of Information Sciences and Technology, George Mason University, USA
‡School of Policy and Government, George Mason University, USA
§School of Social Work, Indiana University, USA

***Abstract*—This paper addresses the need for developing an inclusive social cyber vulnerability (`iSCV`) metric to assess the unique risks faced by underrepresented groups in cyberspace. Current metrics often fail to capture the vulnerabilities specific to marginalized populations, particularly in terms of digital literacy, access to resources, and behavioral traits. By integrating demographic representation, psychosocial stressors, and exposure to targeted attacks, the proposed `iSCV` aims to serve as a practical tool for improving security measures. The study emphasizes the importance of tailored interventions to enhance the resilience of vulnerable groups against social cyberattacks. Future research will focus on refining the metric through real-world applications and expanding its scope to address intersectional vulnerabilities.**

***Index Terms*—Social cyber vulnerability, Inclusive metrics, Marginalized populations, Cybersecurity, Tailored interventions**

I. Introduction

The safety and trustworthiness of cyberspace are vital to modern society, yet cyberattacks increasingly threaten underrepresented groups. Existing social cyber vulnerability metrics overlook the specific risks faced by these populations, leaving gaps in protection strategies. This research tackles the challenge of developing an inclusive metric that captures the vulnerabilities of marginalized communities in the digital world. Despite progress in cybersecurity, state-of-the-art approaches often generalize vulnerabilities without considering the diverse experiences of underrepresented groups, compromising defense mechanisms and equitable resource distribution. The absence of inclusion-focused metrics limits comprehensive risk assessments and targeted interventions, undermining the security of the most vulnerable in cyberspace.

Scholars have highlighted the inadequacy of current cybersecurity measures for underrepresented groups. Holt and Bossler [1] emphasizes that phishing and social engineering disproportionately affect certain demographics, underscoring the need for inclusive metrics that consider social and cultural factors. Lyon [2] found that older individuals and women are less knowledgeable about security practices, making them vulnerable targets. Jones et al. [3] notes that people with cognitive disabilities often overshare online, making them more susceptible to scams and phishing, highlighting the need for tailored digital safety measures.

This paper seeks to create an inclusive social cyber vulnerability metric as a decision-making tool. By integrating inclusion metrics, we can better protect at-risk groups and improve overall cyberspace trustworthiness. Given the rise of social cyberattacks and the increasing diversity of online communities, addressing this issue is both timely and essential.

This work explores the development of an inclusive metric that captures the unique vulnerabilities of underrepresented groups. It will assess how existing metrics incorporate inclusion, identify key factors for designing an inclusive metric, and demonstrate its application as a decision-making tool for protecting vulnerable populations in cyberspace.

To this end, we will aim to answer the following research questions in this work:

1) To what extent do current social cyber vulnerability metrics include the vulnerabilities of underrepresented groups?
2) What key factors are critical for developing an inclusive metric to capture the unique vulnerabilities of underrepresented groups to social cyberattacks?
3) How can an inclusive vulnerability metric aid in decision-making to enhance the security of underrepresented groups in cyberspace?

II. Related Work

A. Concept of Inclusion and Its Measurement

"Inclusion" refers to creating environments where individuals feel valued and can fully participate. 'Social inclusion' enhances participation for disadvantaged groups by improving access to resources and respect for rights [4]. 'Organizational inclusion' ensures that all individuals are welcomed and can engage in decision-making processes [5]. Inclusion is measured using tools like the *Gartner Inclusion Index* to evaluate fair treatment and psychological safety [6], and qualitative methods to assess inclusivity through feedback systems and conflict resolution plans [7]. Diversity and inclusion metrics help track progress towards inclusive practices [8].

Though inclusion metrics are crucial in organizational and social settings, "inclusion" has not been sufficiently addressed in evaluating the susceptibility of vulnerable populations to social cyberattacks like scams. This oversight leaves underrepresented groups, who often lack resources and support, more exposed to exploitation in the evolving cyber landscape.

979-8-3503-8674-5/24/$31.00 ©2024 IEEE
DOI 10.1109/TPS-ISA62245.2024.00059

B. Vulnerability Metrics to Cyberattacks

Existing cyber vulnerability metrics often overlook the social vulnerabilities of underrepresented groups. For example, Black et al. [9] evaluated the Common Vulnerability Scoring System (CVSS), which primarily addresses technical risks but fails to consider threats stemming from social media. Similarly, while Flanagan et al. [10] discussed the Social Vulnerability Index (SVI) in relation to socio-economic factors, it does not account for cyber threats. Bolpagni [11] proposed a Cyber Risk Index that links a higher Human Development Index (HDI), a measure of life expectancy, education, and standard of living, with lower cyber risk, yet this model overlooks the unique challenges posed by social platforms and vulnerable populations. Additionally, Bhol et al. [12] developed a comprehensive cybersecurity taxonomy covering vulnerabilities, threats, and users, but cultural and contextual factors remain unaddressed.

These gaps underscore the urgent need for inclusive social cyber vulnerability (iSCV) metrics that address the specific risks faced by marginalized groups. Specialized tools will safeguard these populations from evolving social cyberattacks.

III. Key Factors of an Inclusive Social Cyber Vulnerability Metric

A. Key Attributes for Measuring an iSCV Metric

Key inclusive attributes for measuring SCV should account for both social and technical factors, particularly for marginalized and underrepresented groups:

- **Demographic Representation** [13]: Ensuring diverse groups (e.g., race, gender, age, socioeconomic status) are represented in vulnerability assessments to capture threats specific to these populations.
- **Digital Literacy and Access** [14]: Evaluating the digital literacy and technology access of different groups, as lower literacy or limited access increases cyber risks.
- **Social and Cultural Context** [15]: Considering cultural practices, values, and norms that could make certain groups more vulnerable to social engineering or cyber scams.
- **Network and Social Media Engagement** [16]: Measuring social media reliance, as vulnerable groups may face increased exposure to cyberattacks due to insecure practices or high platform usage.
- **Psychosocial Stressors** [17]: Assessing stressors like economic hardship, discrimination, or isolation that elevate susceptibility to social scams and phishing.
- **Access to Cybersecurity Resources** [18]: Evaluating the availability of cybersecurity training and resources, as vulnerable groups may lack adequate protection.
- **Exposure to Targeted Cyberattacks** [19]: Identifying whether certain populations are disproportionately targeted by attacks like phishing or identity theft based on their demographics.
- **Social Capital and Support Networks** [20]: Assessing the strength of social support systems, as weaker networks can leave individuals more vulnerable.

These attributes highlight the need for *inclusive* metrics that consider both technological factors and *social dynamics* influencing group vulnerability.

B. Inclusive Social Cyber Vulnerability Metric

In this section, we propose an inclusive social cyber vulnerability (iSCV) metric aimed at measuring an individual online user's vulnerability to social cyberattacks. While iSCV is designed as a generic metric for assessing any user's vulnerability to a given attack, we specifically evaluate whether it is *inclusive* enough to capture the susceptibility of vulnerable populations to social cyberattacks.

We construct the iSCV based on an individual's vulnerability to social cyberattacks across four key dimensions:

- **Accessibility (A)** represents the user's access to cybersecurity resources, education, and protection, which enhance awareness of social cyberattacks. Demographic factors such as race, gender, age, socioeconomic status, educational background, and cultural context influence this dimension.
- **Behavioral Traits (B)** reflects the user's digital literacy, access to technology, risk behaviors, and social behaviors, including online engagement with social media and networks.
- **Psychological Traits (P)** captures psychological stressors, influenced by social, economic, and emotional factors, including the level of social support available to the individual or risk perception.
- **Experiences (E)** relates to the user's previous experiences with social cyberattacks (e.g., exposure to scams) and access to cybersecurity training or education which can make responses to a given cyberattack different.

The iSCV metric for a given attack type k is expressed as a function of these four dimensions, each with multiple attributes. Let $w_{k,X}$ denote the weight assigned to each dimension, and $\mathcal{IV}_X$ represent the set of individual vulnerability factors related to dimension X. The iSCV metric is:

$$iSCV_k = w_{k,A} \cdot \frac{\sum_{i \in \mathcal{IV}_A} A_i}{|\mathcal{IV}_A|} + w_{k,B} \cdot \frac{\sum_{i \in \mathcal{IV}_B} B_i}{|\mathcal{IV}_B|} + w_{k,P} \cdot \frac{\sum_{i \in \mathcal{IV}_P} P_i}{|\mathcal{IV}_P|} + w_{k,E} \cdot \frac{\sum_{i \in \mathcal{IV}_E} E_i}{|\mathcal{IV}_E|}. \quad (1)$$

C. Case Study: Measurement of an iSCV Metric

To measure the iSCV metric as a case study, we utilize the IPoll dataset [21], entitled "The Impostors: Stealing Money, Damaging Lives" which is a 2020 dataset from an American Association of Retired Persons (AARP) national survey of adults aged 18+. This survey examined the prevalence and impact of financial fraud and scams, focusing on how impostor scams affect different demographic groups across the United States. Specifically, we estimate the iSCV and its key dimensions, each consisting of multiple factors, as illustrated in Tables I, II, and III. For simplicity, we used the same weight for $w_{k,X}$'s (i.e., 0.25).

TABLE I
iSCV Measurements for Each Age Group

Age Group	Overall Vulnerability	A		B	P	E	
		Lack of Familiarity	Lack of Knowledge	Risk-Enhancing Behavior	Risk Perception	Past Encounters	Responses to Encounters
18-24	2.358992	1.461095	2.901381	2.524905	3.305621	2.186184	1.213753
25-29	2.354902	1.315352	3.241784	2.559304	3.305258	2.160640	0.871444
30-44	2.408148	1.386785	3.452487	2.505008	3.495521	2.271413	0.700398
45-49	2.357246	1.359215	3.623867	2.205237	3.535650	2.277743	0.527407
50-54	2.308543	1.366465	3.797835	2.110679	3.548338	2.364279	0.415114
55-64	2.254403	1.334414	3.805652	1.818555	3.730999	2.344211	0.290008
65+	2.168280	1.389844	3.988628	1.460839	3.894039	2.398260	0.233100

TABLE II
iSCV Measurements for Each Ethnic Group

Ethinic Group	Overall Vulnerability	A		B	P	E	
		Lack of Familiarity	Lack of Knowledge	Risk-Enhancing Behavior	Risk Perception	Past Encounters	Responses to Encounters
White, Non-Hispanic	2.315119	1.364094	3.744012	2.027939	3.628603	2.308811	0.412704
Black, Non-Hispanic	2.224912	1.366038	3.076520	2.275425	3.643396	2.314316	1.068825
Asian, Non-Hispanic	2.352403	1.488816	3.297461	2.371612	3.601987	2.228999	0.689683
Other, Non-Hispanic	2.284588	1.465464	3.571306	2.032989	3.481944	2.437802	0.826531
Mix of 2+ Non-Hispanic	2.286515	1.394030	3.485075	2.230787	3.456767	2.211322	0.485119
Hispanic	2.284522	1.384204	3.204078	2.305051	3.469675	2.296946	0.919712

TABLE III
iSCV Metrics for Each Gender Group

Gender Group	Overall Vulnerability	A		B	P	E	
		Lack of Familiarity	Lack of Knowledge	Risk-Enhancing Behavior	Risk Perception	Past Encounters	Responses to Encounters
Women	2.304338	1.362286	3.579430	2.070077	3.661298	2.283440	0.459636
Men	2.306075	1.387414	3.664484	2.116810	3.536452	2.331911	0.609544

In our analysis, we identified distinct patterns in the observed iSCV and their attributes across age, gender, and ethnic groups. The data from the iSCV measurements reveal several key trends across the dimensions of Accessibility (**A**), Behavioral Traits (**B**), Psychological Traits (**P**), and Experiences (**E**).

Age Group Analysis: Younger individuals (18-24) show higher overall vulnerability due to impulsivity and lower risk perception. They engage more frequently in risk-enhancing behaviors (**B**), but have better protection knowledge (**A**) compared to older groups. As age increases, risky behaviors decline sharply, while trust in potential threats (**P**) rises, particularly among those aged 55+. These older individuals also exhibit significant gaps in protection knowledge (**A**), highlighting the need for targeted cybersecurity education. Additionally, responses to past encounters (**E**) decrease with age, suggesting a reduced adaptability following cyber incidents.

Ethnic Group Analysis: Ethnic group variations show distinct trends. Asian, Non-Hispanic individuals demonstrate higher familiarity with protection measures (**A**) and fewer knowledge gaps. Black, Non-Hispanic and Hispanic individuals show higher responsiveness to past encounters (**E**), likely due to previous experiences. White, Non-Hispanic individuals exhibit the highest trust levels (**P**), potentially increasing their susceptibility to social cyberattacks, while the "Other, Non-Hispanic" group experiences more past encounters (**E**), indicating the need for better prevention.

Gender Group Analysis: Overall vulnerability is similar between men and women. However, men tend to show higher scores in lack of knowledge (**A**) and trust levels (**P**), indicating they may be more trusting and less informed about protective measures. Women, on the other hand, exhibit lower reactivity to past encounters (**E**), suggesting a more cautious approach in handling cyber threats.

Overall Trends: Age plays a significant role in vulnerability, with younger individuals at higher risk due to impulsivity and risky behavior, while older individuals face knowledge gaps in protection measures. Ethnic differences indicate varied levels of familiarity with protective measures and responsiveness to past cyber incidents, necessitating tailored interventions for different demographic groups. Gender differences, though minimal in overall vulnerability, reveal distinct patterns in behavior and perception between men and women.

IV. Conclusion and Future Work

This study highlights the need for a more inclusive social cyber vulnerability (iSCV) metric that accounts for the specific vulnerabilities of underrepresented groups in cyberspace.

Current metrics often overlook key factors like digital literacy and access to cybersecurity resources, which are crucial for understanding how marginalized populations experience cyber risks. Including attributes like demographic representation and behavioral traits provides a more holistic view than traditional approaches [9, 10, 13]. An inclusive metric will improve decision-making by enabling tailored interventions to protect at-risk groups, such as women, the elderly, and individuals with disabilities [1, 2].

Future work should focus on refining this metric through real-world applications and expanding it to cover intersectional vulnerabilities across various social dimensions. Additionally, collaboration with diverse stakeholders will be key to ensuring the practical relevance of the `iSCV` metric.

Acknowledgment

This research is partly supported by the grant # HN-4Q24-057 from Commonwealth Cyber Initiative (CCI), which focuses on inclusion and accessibility in cybersecurity.

References

[1] T. Holt and A. Bossler, *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge, 2015.

[2] G. Lyon, "Informational inequality: the role of resources and attributes in information security awareness," *Information & Computer Security*, vol. 32, no. 2, pp. 197–217, 2024.

[3] D. Jones, S. Ghasemi, D. Gračanin, and M. Azab, "Privacy, safety, and security in extended reality: user experience challenges for neurodiverse users," in *International Conference on Human-Computer Interaction*. Springer, 2023, pp. 511–528.

[4] A. Saran, X. Hunt, H. White, and H. Kuper, "Effectiveness of interventions for improving social inclusion outcomes for people with disabilities in low-and middle-income countries: A systematic review," *Campbell Systematic Reviews*, vol. 19, no. 1, p. e1316, 2023.

[5] A. E. Mullin, I. R. Coe, E. A. Gooden, M. Tunde-Byass, and R. E. Wiley, "Inclusion, diversity, equity, and accessibility: From organizational responsibility to leadership competency," in *Healthcare Management Forum*, vol. 34, no. 6. SAGE Publications Sage CA: Los Angeles, CA, 2021, pp. 311–315.

[6] L. Romansky, M. Garrod, K. Brown, and K. Deo, "How to measure inclusion in the workplace," *Harvard Business Review*, vol. 27, 2021.

[7] H.-J. D. Lubiano, "A qualitative approach in measuring inclusion," 2019.

[8] M. Mitchell, D. Baker, N. Moorosi, E. Denton, B. Hutchinson, A. Hanna, T. Gebru, and J. Morgenstern, "Diversity and inclusion metrics in subset selection," in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, pp. 117–123.

[9] P. E. Black, K. Scarfone, M. Souppaya *et al.*, "Cyber security metrics and measures," *Wiley Handbook of Science and Technology for Homeland Security*, pp. 1–15, 2008.

[10] B. E. Flanagan, E. W. Gregory, E. J. Hallisey, J. L. Heitgerd, and B. Lewis, "A social vulnerability index for disaster management," *Journal of Homeland Security and Emergency Management*, vol. 8, no. 1, p. 0000102202154773551792, 2011.

[11] M. Bolpagni, "Cyber risk index: a socio-technical composite index for assessing risk of cyber attacks with negative outcome," *Quality & Quantity*, vol. 56, no. 3, pp. 1643–1659, 2022.

[12] S. G. Bhol, J. Mohanty, and P. K. Pattnaik, "Taxonomy of cyber security metrics to measure strength of cyber security," *Materials Today: Proceedings*, vol. 80, pp. 2274–2279, 2023.

[13] H. Jung and E. W. Welch, "The impact of demographic composition of social networks on perceived inclusion in the workplace," *Public Administration Review*, vol. 82, no. 3, pp. 522–536, 2022.

[14] K. Renaud and L. Coles-Kemp, "Accessible and inclusive cyber security: a nuanced and complex challenge," *SN Computer Science*, vol. 3, no. 5, p. 346, 2022.

[15] S. Creese, W. H. Dutton, and P. Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," *Personal and Ubiquitous Computing*, vol. 25, no. 5, pp. 941–955, 2021.

[16] N. F. Khan, N. Ikram, H. Murtaza, and M. A. Asadi, "Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach," *Kybernetes*, vol. 52, no. 1, pp. 401–421, 2023.

[17] R. Montañez, E. Golob, and S. Xu, "Human cognition through the lens of social engineering cyberattacks," *Frontiers in psychology*, vol. 11, p. 1755, 2020.

[18] S. Wongkrachang, "Cybersecurity awareness and training programs for racial and sexual minority populations: An examination of effectiveness and best practices," *Contemporary Issues in Behavioral and Social Sciences*, vol. 7, no. 1, pp. 35–53, 2023.

[19] T. Lin, D. E. Capecci, D. M. Ellis, H. A. Rocha, S. Dommaraju, D. S. Oliveira, and N. C. Ebner, "Susceptibility to spear-phishing emails: Effects of internet user demographics and email content," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 26, no. 5, pp. 1–28, 2019.

[20] Z. Guo, J.-H. Cho, R. Chen, S. Sengupta, M. Hong, and T. Mitra, "SAFER: Social capital-based friend recommendation to defend against phishing attacks," in *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 16, 2022, pp. 241–252.

[21] American Association of Retired Persons (AARP), "The impostors: Stealing money, damaging lives." 2020, an AARP National Survey of Adults 18+. [Online]. Available: https://ropercenter.cornell.edu/ipoll/study/31119515