Properties for Cybersecurity Awareness Posters' Design and Quality Assessment

Sunil Chaudhary*
Norwegian University of Science and Technology
Gjøvik, Norway
sunil.chaudhary@ntnu.no

Marko Kompara
University of Maribor
Maribor, Slovenia
marko.kompara@um.si

Sebastian Pape
Goethe University
Frankfurt am Main, Germany
sebastian.pape@m-chair.de

Vasileios Gkioulos
Norwegian University of Science and Technology
Gjøvik, Norway
vasileios.gkioulos@ntnu.no

ABSTRACT

Posters are widely in practice to communicate cybersecurity awareness (CSA) messages. This popularity could be because it is one of the simplest mechanisms, and most people are accustomed to poster usage. Despite this, very little effort has been made to make the CSA poster design and assessment more systematic. Due to this, there exists a wide variation in CSA poster design. Alarmingly, many of them do not align with the needs and objectives of CSA. This study, therefore, intends to collect and analyze the properties that can guide the production of more uniform and effective posters for CSA purposes. At the same time, the study contributes to making the poster design and quality assessment approach more systematic. In order to do so, this study used a literature review for the elicitation of properties and an online assessment to analyze the relevancy of the elicited properties. As a final result, the study provides six main properties (i.e., topic, information quality, message framing, suggestions quality, content presentation, localization, and style and formatting) and their respective twenty-one sub-properties that can facilitate CSA poster design and its quality assessment.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; *Cybersecurity awareness.*

KEYWORDS

cybersecurity awareness, poster design, poster quality assessment

ACM Reference Format:
Sunil Chaudhary, Marko Kompara, Sebastian Pape, and Vasileios Gkioulos. 2018. Properties for Cybersecurity Awareness Posters' Design and Quality Assessment. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX).* ACM, New York, NY, USA, 8 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Cybersecurity awareness (CSA) refers to being mindful of cybersecurity issues that affect one's personal and professional life. It primarily entails *cognition* (acquiring knowledge and comprehension of cybersecurity challenges), which leads to cybersecurity *behavioral* adjustments brought about by positive changes in cybersecurity *attitudes* [10] [40] . The ultimate purpose of CSA is to persuade or motivate people to adopt secure behavior while discouraging them from engaging in risky activities. This is best accomplished by delivering the right security information in the right amount and format to the right audience at the right time, via the right dissemination channels. The information provided is often enough to draw individuals' attention to security risks, comprehend their potential consequences, and respond appropriately. CSA activities are usually aimed at a large audience, who are primarily passive recipients of the information [37].

CSA initiatives use various communication channels, for example, posters, illustrations, videos, emails, infographics, comics, brochures, websites, leaflets, newspapers, events, games, and so on, to reach and deliver the awareness message/information to the target audience [11]. These communication channels have their own advantages and disadvantages of using them [21]. Similar to in other fields, such as advertisement, healthcare awareness, and social issues awareness, posters are popular and common in CSA. Many organizations including ENISA, EUROPOL, InfoSec Institute, SANS Institute, and Cyber Safe Work, produce and distribute posters to raise the CSA of people. The popularity of a poster could be because it is one of the simplest and cost-effective awareness mechanisms and also people are largely accustomed to its usage. Posters initially used to be a conventional method of CSA (i.e., generally uses textual and image content), but this has changed with digital transformation. Utilizing digital technology, posters' *information richness* [53] is easily improved, for example, posters include a clickable link or QR code that directs interested people to a website with detailed information on the subject or with a feedback form. Moreover, using mass media like email, social media, and websites, such posters are effortlessly disseminated, and their message is communicated to a mass audience.

Currently, CSA posters with one-line text and whole page text, with and without images on them, with fancy and plain typography, or with and without weblink are in use. With such diversifications in the poster, it is worthwhile to ask which design approach can

Conference acronym 'XX, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

be the most effective for CSA purposes. On the one hand, many organizations depend on posters for CSA, whereas on the other hand, very little effort has been made to make the poster more uniform and effective for the purpose. For instance, it is still not well-defined what message to include for an effective CSA poster. Furthermore, the poster design and assessment are also largely based on unsystematic approaches. Therefore, this study intends to elicit and analyze the properties that can guide or be useful for CSA poster design and its quality assessment. By properties, we mean aspects like the content of a poster, the poster's appearance, and so on. To the best of our knowledge, there does not exist any proper and comprehensive study to analyze and systematize poster design and its quality assessment exclusively for CSA purposes. Indeed, there exist many templates and guidelines for poster design, however, they are fundamentally for scientific (i.e., research presentation) [51], marketing (i.e., advertisement) [50], and other purposes posters. Moreover, these available templates and guidelines do not align with or fulfill the specific needs and objectives of CSA.

The nature of cybersecurity, its sensitiveness, and the expectation from its awareness is vastly different from, for example, advertisement, scientific research presentation, and even awareness of healthcare and various social issues. Cyberspace and its security are often considered to be complex in nature; unlike the physical world the concepts of, for example, distance, border, proximity, laws, thieves (bad people), and valuables are obscure. In cyberspace, an individual from one country, regardless of its distance, border, or legal system can attack and steal valuable data stored on servers stationed in another country. Similarly, who is responsible for the surveillance and protection of what is unclear. For example, in an organization, it is well-defined that security guards are responsible for surveilling and protecting its physical premises and property, whereas the responsibility of surveilling and protecting its IT systems and assets from potential cyberattacks is on every employee. Obscurities like these make cybersecurity a difficult concept to understand and comprehend for many people. And raising awareness of this concept with the purpose to result in actions and a long-term behavior change by using static information on posters is obviously a challenging endeavor.

2 RELATED WORKS

While there exists quite some work on how to measure security awareness programs [3] [2] [57] [45], all of these address awareness campaigns in general and none of them is specifically targeting posters. While posters were included in some of the awareness campaigns [48] [8], they were not specifically evaluated. Even though Boujettif and Wang [6] asked participants to create and evaluate posters, the hidden task was that the participants should deal with the content on the posters. Neither were there specific design criteria explained, besides the task to make the poster *as creative and as funny as possible*, nor were there the results or criteria of the evaluation discussed. Closest to our work is the work from Kajzer et al. [36] who investigated in an experiment which message types on a CSA poster were better memorized by the participants. However, they did not assess the effects of the poster on the success of the CSA campaign. Besides this work, to the best of our knowledge, our work is the first specifically focusing on CSA posters.

3 ELICITATION OF CSA POSTERS' PROPERTIES

In order to elicit the properties, we utilized a *nonsystematic (purposive) literature review (LR)* [14]. In contrast to a systematic LR, a nonsystematic LR is not obligated to be explicit about the methods, particularly, the search strategy and selection criteria used for the identification and inclusion of relevant literature [32]. Eliciting properties for poster design and quality assessment required exploration of concepts from diverse disciplines and leveraging them for the study's purposes. This includes concepts both from within and outside the cybersecurity discipline, notably but not limited to message framing, usability and user experience, and user psychology. And to cover such a wide range of fields and thereby yield insights could not be achievable by using a systematic LR. In addition, a nonsystematic LR provides the flexibility to pursue ideas and findings that emerge unexpectedly during the process of the review [14].

However, to ensure the quality of selected literature, we used mostly peer-reviewed journal and conference papers, and reports from organizations with a reputation for security research. The elicited properties and their respective sub-properties are listed in Figure 1. Apart from *Style and Formatting*, the remaining properties are applicable to CSA when using other communication channels than posters. The properties and their sub-properties, their meaning, rationale, as well as viable mechanisms to apply them are explained next.

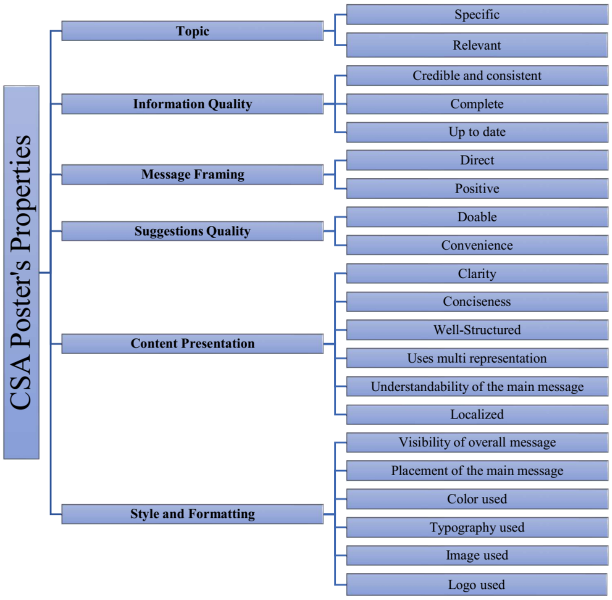

Figure 1: Properties for CSA Poster's Design and Quality Assessment

3.1 Topic

3.1.1 Specific. The topic should focus on a single security issue at a time [27]. Focusing on a variety of issues at the same time can be complex, confusing, and more importantly, *cognitively overloading* for the audience. Naturally, some topics may require discussion on multiple related issues, for example, phishing includes email phishing, website forgery, smishing, vishing, spear phishing, whaling, clone phishing, and social engineering. Such a topic should be appropriately broken down into smaller, more manageable, and cognitively friendly sub-topics where each sub-topic is discussed or organized separately.

3.1.2 Relevant. The topic should be relevant to and align with the roles and responsibilities of the target audience (or the goals and objectives of their organization) [21] [56]. More importantly, it should be inclusive to cover everyone in the audience group [9]. This is important particularly to attract and catch the audience's attention towards the awareness initiative as well as posters. Many organizations, notably ENISA [22], publish threat landscape reports on a regular basis, and consulting these reports will help to identify prime threats as well as major trends in threats, threat actors, and attack techniques. However, a needs assessment [56] can be used to determine the topics that are specifically relevant to the target audience group.

3.2 Information Quality

3.2.1 Credible and consistent. Accuracy and consistency in information help to build trust [42], and trust fosters compliance [7]. As a matter of fact, correctness represents one of the components of 7Cs for effective communication [4]. So, the information should be correct (preferably as advised by cybersecurity experts or authorized bodies [20]) and consistent in language, design, and more importantly factual. Moreover, it should put a realistic perspective (and not an exaggeration of the cybersecurity issue) [26], and no information should conflict with or contradict each other.

3.2.2 Complete. The basic information that the audience needs to know and, if applicable, to act should be included [4]. For instance, Entman's [24] message-framing process, if adapted for a CSA purpose, recommends including i) stating the problem or threat, ii) explaining why it is relevant to the audience i.e., its effects and impacts, iii) mechanisms to assess and identify it, and iv) its potential preventions or mitigations. Interestingly, Arain et al.[1] found and suggested including a similar list of information for CSA purposes. Sometimes, when it is difficult to accommodate all the information in a poster, a reference (as a web link) from where to get more information should be included. Suggesting this reference could motivate the interested audience to further explore it.

3.2.3 Up to date. Cybersecurity is dynamic in nature. So, the information should continually manage to include current changes in cyber risk profiles [3]. They include the changes in security threats, technologies, and protections and also in policies and procedures [21] relevant to, for instance, the audience's job functions. While failing to do so will obviously minimize the impact of posters. More alarmingly, equipping the audience with outdated cyber security information (instead of the current one) could potentially do more harm than good. As has been quoted by Daniel J. Boorstin, "*the greatest enemy of knowledge is not ignorance, it is the illusion of knowledge*", such supposedly aware people with a false sense of security may misidentify or underestimate the cyber threats and become more vulnerable to them.

3.3 Message Framing

3.3.1 Direct. The message should be explicitly directed at the audience [26]. A message is more likely to be accepted and acted upon if the individual feels that it is explicitly directed at him or her rather than generically to everyone. This means the message should be more personalized to the audience and connect to the issues relevant and stimulating to them. The message can be made more direct and tangible by using evidence-based framing strategies [18], for example,

- Putting the need of cybersecurity in a practical context.
- Making it apparent who the enemies are in the fight against cyberattacks.
- Putting a face to cybersecurity by highlighting its heroes (i.e., the audience group).
- Demonstrating the importance of cybersecurity to society.
- Connecting cybersecurity to people's daily lives.

3.3.2 Positive. The message should focus on good security habits (i.e., *informing what to do*) rather than explaining bad security habits (i.e., *informing what not to do*) and their consequences. Since security is rarely the primary concern [19], so telling what to do and how to do it correctly can be presumably more actionable. Moreover, a study has shown that positively framed messages are more persuasive where there is little emphasis on details [43], which is suitable in the case of CSA, which deals with providing enough information to make an individual stay vigilant about cyber risks and know what to look out for [37]. Not to mention, fear and anxiety undermine the cognitive capacity hampering the learning process [17], and do not produce a positive impact on security behavior whereas providing a coping message (i.e., information on how to minimize exposure to risk) does [5] Then, there is always a risk of experiencing *psychological reactance* [52] by some people, who perceive that many of their online behaviors have been restricted by the information on what not to do.

3.4 Suggestions Quality

3.4.1 Doable. In awareness, making clear calls for achievable actions is vital to motivate people to act [13]. As a result, the suggestions made should be meaningful to the audience (i.e., avoid impractical proposals) that they can correctly apply or implement. With impractical suggestions, it is highly possible that the audience would ignore or bypass them, and if applied, they could be incorrect. Further, it has been discovered that the *perceived ease of use* has a positive effect on security behavior [44]. However, the concept of impracticability is contingent on the audience's computer literacy as well as their willingness and ability to learn new computer skills. Nonetheless, the suggestions should include not just *what to do* but also *how to accomplish it.*

3.4.2 Convenience. People always intend to achieve their primary task, and in this process, security often becomes a secondary concern [19]. So, applying the suggestions should not be taxing or noticeably obstruct and slow down the primary responsibility of the audience. Otherwise, the audience will find ways to get around the suggestions [34]. Moreover, this is significant since the *perceived cost of compliance* has a detrimental effect on security behavior [44]. This also implies that the suggestions should facilitate achieving the primary concern of the audience both smoothly and securely.

3.5 Content Presentation

3.5.1 Clarity. Clarity should be in both the purpose and content [4]. Otherwise, the message conveyed could get misunderstood or misinterpreted. For this purpose, it is suggested to consider a specific goal at a time and to use exact, appropriate, and concrete vocabulary. Further, the vocabulary and phrases used to present content should be appropriate to the audience (i.e., avoid ambiguous words, complex words, and jargon). Using familiar words in the text helps the learners in different ways, for instance, it improves reading speed, lessens cognitive load to understand the text, and enhances the recall of information [28]. After all, no one complains about the content being too simple to understand while a poster relying on a specific term, e.g. phishing, might not have the desired effect if the reader does not know what phishing means [39].

3.5.2 Conciseness. The content should be brief, to the point, and comprehensible for the audience [4]. This can be performed by including only what the audience needs to know but not what would be nice to know. Its significance in a poster design, where space for content is limited, is extremely high. After all, there is always a possibility to include detailed information in the provided weblink for the interested audience.

3.5.3 Well-structured. The content structure influences the learner's ability to comprehend and recall the information conveyed [33] [49]. So, it should be well organized and structured. Theoretically, there are different ways to organize or sequence content elements, for instance, the problem followed by its solution, simple to complex concept, familiar to unfamiliar concept, and most to least important information [49]. However, which option would be appropriate to learn cybersecurity concepts may require further investigation. Based on the observation of several CSA contents, a potentially viable structure for the overall content could be in the sequence similar to Entman's [24] message-framing process, i.e., *what is the problem, how to identify it/ its characteristics*, and *what solution fits.* And when listing the problem characteristics and protection measures, they can be arranged in the sequence of from the most important to the least important.

3.5.4 Uses multi representation. The content should use various representations to complement each other, for example, a graph or image to complement the text, and reinforce the main message by highlighting them. This richer representation using different cues improves the understandability and memorability of the message [53] [16] and, at the same time, accessibility for different types of audiences, for example, differently abled audiences. Additionally, a memorable message has proven to lead to behavior change.

3.5.5 Understandability of the main message. The audience should be able to understand the main message in a very short span of time in order to attract their attention. In general, average human attention dwindled to only 8 seconds in 2013 [46]. So, any message (or goal) taking a relatively long time to understand has to face the dwindling attention and interest of the audience. This may lead to a situation where the audience gets completely uninterested in learning about it. To improve the main message's understandability, sub-properties listed for the topic and content presentation could help.

3.5.6 Localized. Localization is about attempting to remove the cultural barriers that may exist, which is important for CSA [54]. The content should be adapted to the audience type, for specific countries, regions, cultures, or groups. Along with language translation, use, for example, suitable terminologies, images, cases, and examples that the audience can relate to. Localization improves user experience, and that will lead to a better understanding. Eliminate things that the audience could not relate to or require mapping to relate and understand as far as possible. Localization should consider, for example,

- Performing accurate translation of all information into the target language.
- Adapting graphics to the preferences of the target audience.
- Adapting layout and design so text can properly be displayed.
- Converting elements such as units of measurement and currency to local requisites.
- Using correct formats of phone number, address, and dates.

3.6 Style and Formatting

3.6.1 Visibility of overall message. The main message (or take-home message) on a poster should be readable from a reasonable distance. There does not exist any defined rule on how far the message should be visible primarily because visibility is influenced by the dimension of a poster as well as where it is placed.

3.6.2 Placement of the main message. The main message of a poster should be placed so that it does not get lost, among other details. Based on design conventions, placing the priority content at the front and center [47] of a poster improves its visual prominence.

3.6.3 Color used. Appropriate color and color contrast should be used for a poster design. Answering what color will be suitable for a poster is dependent on a variety of factors, for example, color symbolism (e.g., blue color often symbolizes serenity, stability, inspiration, or wisdom in various cultures), color conventions for scientific purposes (e.g., red color is used to symbolizes stop, bad, danger, warning, enemy, and unsafe), official colors of an organization (e.g., white and blue are the official colors of the United Nations), and consideration for health issues (e.g., individuals may face difficulty distinguishing certain colors due to color vision deficiency). Further, creating a complementary contrast in the color of content and background improves their visibility [35], i.e., the text is easily visible and readable from a distance. This complementary contrast can be determined by using the *color wheel*. The *color theory* can greatly help with these issues.

3.6.4 Typography used. A poster's text should be easily readable. Making the audience spend extra time to read text is highly discouraging. When selecting an appropriate typeface, it is suggested to ensure the legibility and readability of the text [35]. For example,

- A poster should select a typeface that works well in multiple sizes and weights to maintain readability in different-sized posters.
- A poster should avoid fancy or artistic fonts that could reduce its readability.
- A poster should use decisively contrasting typefaces to enhance its readability if multiple typefaces have to be used.
- A poster should use mixed or lower case rather than upper case characters [55].
- A poster should use boldface and italic, only if necessary. Underline should be reserved for identifying links.
- A poster should avoid reverse type (for example, white text on a dark background).
- A poster should appropriately space the elements among themselves.

3.6.5 Image used. Including an appropriate image that complements the text on a poster is worth many words. It improves the *information richness* [16] and *memorability* [31] of the contents. Furthermore, the memorability of an image depends on various factors, for example, images with people in them are the most memorable [31]. Similarly, positioning an image in the middle of a poster will make it visible from a distance and help attract the audience's attention.

3.6.6 Logo used. The logo of the organization that has designed and distributed the poster should be included on its top or bottom, from where the logo is noticeable to the audience. This visual imagery will serve to inform the audience who is the source or messenger of the information. People tend to determine the seriousness of a message based on its source or messenger [41]. Posters distributed by an organization with a reputation for cybersecurity or is authorized for the purpose will have a strong influence on the audience and motivate them to take it seriously [15].

4 ANALYSIS OF THE ELICITED PROPERTIES

We used an online assessment to determine the degree to which CSA posters designed and distributed by various organizations conform to the elicited properties. In order to carry out the assessment, a Google Form was created. Each poster was displayed with the set of properties and the participants had to assess to what extent the poster satisfies the given properties in terms of a five-point Likert scale (Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree). The evaluation was performed by the five members from partner organizations contributing/participating in the project. The analysis used 117 posters from organizations like ENISA [23], EUROPOL [25], Cyber Safe Work [58], Global Knowledge [38], SANS Institute [30], and INFOSEC Institute [29] that are available for free. The posters covered security issues and concerns like phishing and social engineering protection, security hygiene, unattended device protection, online child safety, data protection, email protection, malware protection, password protection, and privacy protection. All the posters evaluated in this study were in English. While we collected also posters in other languages, we did not include them in the study for the sake of comparability. In total, we received valid submissions for 95 posters. Due to some unknown issues in Google Form, submissions for some posters did not register in its spreadsheet.

The intention behind this analysis is never to show whose posters are superior or inferior in quality; rather realize the disparity, if any exists, between the academic recommendations and real-life practice in poster design. At the same time, this analysis provides a tentative idea on the relevancy of each property based on how many posters and to what extent they conform to the property.

Among the elicited properties, although all of them are important, a few of them have been excluded from the analysis due to practical difficulties to assess them. These excluded properties are as follows:

- Since it was not clear for all posters who the intended audience was, it was difficult to analyze its topic's relevancy.
- All the posters contained the organization's logos, so this obviously has not been analyzed in the assessment.
- Even though localization is essential to improve the effectiveness of CSA posters (and in general), this study did not evaluate it mainly because of these reasons: i) posters available in multiple languages had no other changes except a translation of the awareness text (it was not a complete localization), ii) a very few posters were available in multiple languages, and iii) presumably because reviewers are from different locations, that would also make reviews inconsistent as we could be reviewing different translations and other adjustments.
- Since the color contrast of background and text is analyzed during the typography analysis, color used has not been analyzed. Moreover, going through the color theory to determine appropriate colors was not easy for the participants.

Figure 2 presents the number of posters that conform to each property. Posters for which at least three participants (out of five) have said *agreed* or *strongly agreed* they conform to the given property have been considered to be conforming whereas the remaining are not conforming.

4.1 Discussion of Findings

Overall, all the elicited properties have significance in the CSA poster design and its quality assessment. This is evident from the outcome of the analysis shown in Figure 2, wherein in a worst-case scenario, only a little more than 50% of the posters conform to each property.

Interestingly, we found some disparity between academic recommendations and real-life practice in poster design. Almost 50% of the posters did not meet one or multiple of the criteria mentioned. The top five properties that are mostly not conformed are *Well-structured*, *Use of image*, *Positive*, *Complete*, and *Clarity* in descending order.

Particularly, posters with one-liner messages have an issue of *Complete*, *Well-structured*, and *Clarity*. Obviously, when there is no text there is no *Well-structured*. Similarly, posters with excessively lengthy text and those discussing multiple issues at the same time have an issue of *Clarity*. These imply that the posters should have only enough information that needs to be known by the audience, if possible, to act safely and securely. Indeed, putting just a catchy slogan on the poster will help in attracting attention and is easy to remember, however, something without a clear call for action is

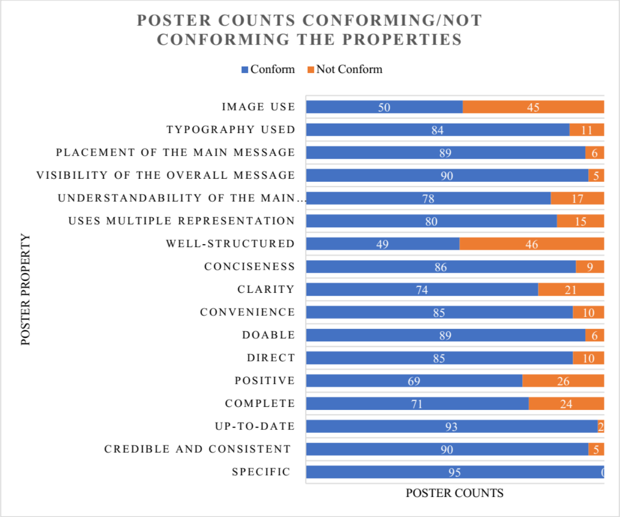

Figure 2: Number of Posters Conforming and Not Conforming to the Individual Properties

questionable since behavior change also requires telling the audience what they need to do [13]. Similarly, posters with excessively lengthy text will be demotivating for the audience to read, understand, and practice in everyday life. Instead, these lengthy posters can use an option like providing a link from where to get detailed information for the interested audience. Obviously, determining how much and what information to include in a poster is a challenging endeavor and could depend on the audience type. A simple rule could be to concentrate on must-haves.

Next, many posters had either plain backgrounds or abstract/unrelatable images on them. The use of images on a poster is to contribute meaningfully to the message conveyed. However, in many posters, the images used do not seem to achieve that. This could be possibly due to the limited understanding of the cybersecurity issue by the responsible graphic designer. Therefore, it is suggested to the graphic designer to have a basic understanding of the cybersecurity issue before s/he works on it. S/he must realize the image is not simply to make the poster attractive but at the same time convey or support the message included in the textual form.

Likewise, many posters emphasized what not to do. Knowing them is definitely useful, but this may not be effective for a long-term behavior change, essentially when such suggestions can obstruct the audience's primary concern. For example, the recommendation "*do not use a weak password*" is true but this does not provide the right alternative. Rather this can be recommended as "*use a password with a combination of alphanumeric and special characters*" or "*use a 2-factor authentication method*" that conveys the same intent.

Last but not least, the meaning of properties like *Understandability of the main message*, *Doable*, *Convenience*, and *Clarity*, differ for each individual. They are dependent on the audience's ability (such as security expertise and experience). For example, the same recommendation could be doable for an individual with security knowledge and experience, whereas undoable for a naïve person. Similarly, an image that could make sense to one individual would make no sense to another. So, while defining them for usable meaning, one should consider the target audience's ability to understand and effectively apply them.

5 CONCLUSIONS

The ultimate goal of CSA is to change people's security knowledge, attitude, and behavior by putting what they have learned into practice. In order to raise people's CSA, security messages are communicated to them using diverse channels. Among them, a poster is one of the simplest and most commonly used channels. Moreover, most people are familiar with the usage of posters in many fields besides CSA. Despite these all, very little effort has been made to produce a more uniform and effective poster for CSA purposes. Further, there does not exist any study that targets systematizing the approaches used for CSA poster design and its quality assessment. Therefore, this study aims to address these issues of non-uniformity in CSA poster design, and also systematize the approach used for its design and quality assessment.

In order to do so, this study used a nonsystematic LR followed by an online assessment. The LR has been utilized to elicit the list of properties that can guide the design of CSA posters as well as act as criteria to be considered when performing a poster's quality assessment. An online assessment has been used to analyze 95 CSA posters from various organizations mainly to assess how much they conform to the elicited properties. The assessment was done in terms of a five-point Likert scale. The aim of this assessment was never to investigate the posters' superiority or inferiority, but to verify how much the elicited properties are in practice. There were two main benefits of this assessment. Firstly, it provided the practical relevancy of the properties, and secondly, it helped to examine the disparity in academia and in practice, if there is any.

The LR resulted in six properties and their respective twenty-one sub-properties. These properties and sub-properties are as follows: *Topic* (Specific, Relevant), *Information Quality* (Credible and consistent, Complete, Up to date), *Message Framing* (Direct, Positive), *Suggestions Quality* (Doable, Convenience), *Content Presentation* (Clarity, Conciseness, Well-Structured, Uses multi representation, Understandability of the main message, Localized), and *Style and Formatting* (Visibility of overall message, Placement of the main message, Color used, Typography used, Image used, Logo used). Interestingly, apart from the last property, the remaining are equally important to all other communication channels. However, one would expect that different properties vary across the different communication channels, e.g. while a poster needs to focus on one topic with a certain level of detail, an awareness video could cover the same topic in more detail, or different topics within the same video. Mostly, because the receiver of the awareness message will most likely spend more time on the video, even if the poster is very engaging.

Similarly, the assessment established the relevancy of all the listed properties. Even in a worst-case scenario, more than 50% of the posters conform to each property. Further, the assessment revealed a level of disparity between theoretical recommendations for a poster design and what is in practice. Some properties like *Well-structured*, *Use of image*, *Positive*, *Complete*, and *Clarity* were least conformed by the posters. This disparity could have occurred due to the existing culture in poster design that is largely influenced by fields like marketing (advertisement), where the focus is more on visual appeal. Therefore, there is a need to have a clear distinction between the poster design for CSA purposes and others. This requires a proper guide for CSA poster design and its quality assessment. Moreover, the designer (different from the CSA professional) also needs to have an adequate understanding of the security issues along with experience in designing to produce an effective CSA poster.

The main limitation of this study is the few numbers of participants in the assessment, which is statistically insignificant. However, this happened due to the nature of the assessment, where the participants were required to have a level of consensus on the meaning of each property. The assessment also did not analyze a few properties due to technical difficulties or difficulties of objectivity.

6 ACKNOWLEDGMENTS

This work has financially been supported by the CyberSec4Europe project (Proposal No. 830929). This paper is an extended and revised version of a section of the deliverable report D3.19 [12] from CyberSec4Europe's WP3: Blueprint Design and Common Research

ACKNOWLEDGMENTS

The authors would like to thank Outi-Marja Latvala (VTT, Finland) and Eda Marchetti (CNR, Italy) for reviewing and providing feedback on the deliverable report submitted to the CyberSec4Europe which was the foundation for this paper.

REFERENCES

[1] Mubashir Aslam Arain, Rima Tarraf, and Armghan Ahmad. 2019. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *Journal of Multidisciplinary Healthcare* 2019, 12 (2019), 73–81. https://doi.org/10.2147/JMDH.S183275

[2] Maria Bada and Jason R.C. Nurse. 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information Computer Security* 27, 3 (2019), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

[3] Maria Bada, Angela M. Sasse, and Jason R.C. Nurse. 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. In *International Conference on Cyber Security for Sustainable Society*. Coventry, UK.

[4] John Baird and Jim Stull. 1979. *The Seven C's of Communication*. Prentice Hall„ Englewood Cliffs, NJ, USA.

[5] Renévan Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies* 123 (2019), 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

[6] Mohammed Boujettif and Yongge Wang. 2010. Constructivist Approach to Information Security Awareness in the Middle East. In *International Conference on Broadband, Wireless Computing, Communication and Applications*. Fukuoka, Japan.

[7] John Braithwaite and Toni Makkai. 1994. Trust and compliance. *Policing and Society* 4, 1 (May 1994), 1–12. https://doi.org/10.1080/10439463.1994.9964679

[8] Jan-Willem H. Bullée, Lorena Montoya, Wolter Pieters, Marianne Junger, and Pieter H. Hartel. 2015. The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology* 11 (2015), 97—-115. https://doi.org/10.1007/s11292-014-9222-7

[9] Albert Caballero. 2017. Security Education, Training, and Awareness. In *Computer and Information Security Handbook* (3rd ed.), John R. Vacca (Ed.). Morgan Kaufmann, Burlington, MA, USA, Chapter 33, 497–505. https://doi.org/10.1016/B978-0-12-803843-7.00033-8

[10] Ronald C.Dodge Jr.and Curtis Carver and Aaron J.Ferguson. 2007. Phishing for user security awareness. *Computers Security* 26, 1 (2007), 73–80. https://doi.org/10.1016/j.cose.2006.10.009

[11] Sunil Chaudhary, Vasileios Gkioulos, and David Goodman. 2021. *D9.11 SME cybersecurity awareness program 2.* Technical Report. Brussel, Belgium.

[12] Sunil Chaudhary, Sebastian Pape, Marko Kompara, Georgios Kavallieratos, and Vasileios Gkioulos. 2022. *D3.19 Guidelines for Enhancement of Societal Security Awareness.* Technical Report. Brussels, Belgium.

[13] Ann Christiano and Annie Neimand. 2017. *Stop Raising Awareness Already.* Retrieved 30 March 2022 from https://ssir.org/articles/entry/stop_raising_awareness_already#

[14] David A. Cook. 2019. Systematic and Nonsystematic Reviews: Choosing an Approach. In *Healthcare Simulation Research: A Practical Guide*, Debra Nestel, Joshua Hui, Kevin Kunkler, Mark W. Scerbo, and Aaron W. Calhoun (Eds.). Springer, Cham, Switzerland, 55–60. https://doi.org/10.1007/978-3-030-26837-4_8

[15] Lynne Coventry, Pam Briggs, John Blythe, and Minh Tran. 2014. *Using behavioural insights to improve the public's use of cyber security best practices.* Technical Report. London, UK.

[16] Richard L. Daft and Robert H. Lengel. 1983. *Information Richness: A New Approach to Managerial Behavior and Organization Design.* Technical Report. USA.

[17] Linda Darling-Hammond, Lisa Flook, Channa Cook-Harvey, Brigid Barron, and David Osher. 2019. Implications for educational practice of the science of learning and development. *Applied Developmental Science* 24, 2 (2019), 91–140. https://doi.org/10.1080/10888691.2018.1537791

[18] Hans de Bruijn and Marijn Janssen. 2017. Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly* 34, 1 (2017), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

[19] Rachna Dhamija, J.D. Tygar, and Marti Hearst. 2006. Why phishing works. In *SIGCHI Conference on Human Factors in Computing Systems.* ACM, Montreal, Canada, 581-–590. https://doi.org/10.1145/1124772.1124861

[20] Paul Dolan, Michael Hallsworth, David Halpern, Dominic King, Robert Metcalfe, and Ivo Vlaev. 2012. Influencing behaviour: The mindspace way. *Journal of Economic Psychology* 33, 1 (2012), 264–277. https://doi.org/10.1016/j.joep.2011.10.009

[21] ENISA. 2010. *The new users' guide: How to raise information security awareness.* Technical Report. Athens, Greece.

[22] ENISA. 2021. *ENISA Threat Landscape 2021.* Technical Report. Athens, Greece.

[23] ENISA. 2022. *Material.* https://www.enisa.europa.eu/media/multimedia/material

[24] Robert M. Entman. 1993. Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication* 43, 4 (1993), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

[25] EUROPOL. 2022. *Public Awareness and Prevention Guides.* https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides

[26] Steven Furnell and Ismini Vasileiou. 2017. Security education and awareness: just let them burn? *Network Security* 2017, 12 (2017), 5–9. https://doi.org/10.1016/S1353-4858(17)30122-8

[27] Urs E. Gattiker. 2006. Can an early warning system for home users and SMEs make a difference? A field study. In *Critical Information Infrastructures Security (LNCS, Vol. 4347)*, Javier Lopez (Ed.). Springer-Verlag Berlin, Heidelberg, Samos, Greece, 112–127.

[28] Shawn M. Glynn. 1983. Cognitive Processes Involved in Text Learning. In *Annual Meeting of the American Educational Research Association.* Montreal, Canada.

[29] InfoSec Institute. 2022. *Top 20 security awareness posters with messages that STICK.* https://resources.infosecinstitute.com/topic/top-20-security-awareness-posters-messages-stick/

[30] SANS Institute. 2022. *Posters.* https://www.sans.org/security-awareness-training/resources/posters

[31] Phillip Isola, Devi Parikh, Antonio Torralba, and Aude Oliva. 2012. Understanding the Intrinsic Memorability of Images. *Journal of Vision* 12, 9 (2012). https://doi.org/10.1167/12.9.1082

[32] Stacy Jansen. 2017. *Bias within systematic and non-systematic literature reviews: the case of the Balanced Scorecard (Master's thesis).* Master's thesis. University of Twente, Enschede, Netherlands.

[33] Robert F. Lorch Jr. and Elizabeth Pugzles Lorch. 1985. Topic Structure Representation and Text Recall. *Journal of Educational Psychology* 77, 2 (1985), 137–148. https://doi.org/10.1037/0022-0663.77.2.137

[34] M. E. Kabay, Bridgitt Robertson, Mani Akella, and D.T. Lang. 2012. Using Social Psychology to Implement Security Policies. In *Computer Security Handbook* (6th ed.), Seymour Bosworth, Michel E. Kabay, and Eric Whyne (Eds.). John Wiley Sons, Hoboken, NJ, USA, Chapter 50, 50.1–50.25. https://doi.org/10.1002/9781118820650.ch50

[35] Paul Kahn and Krzysztof Lenk. 1998. Design: principles of typography for user interface design. *Interactions* 5, 6 (1998), 15—-29. https://doi.org/10.1145/287821.287825

[36] Mitchell Kajzer, Charles R. Crowell, Angela Ferreira, John DArcy, Dirk VanBruggen, and Aaron Striegel. 2013. Poster: Memorability of Computer Security Posters as Affected by Message Type. In *Symposium on Usable Privacy and Security (SOUPS).* Newcastle, UK.

[37] Sokratis K. Katsikas. 2000. Health care management and information system security: Awareness, training or education? *International Journal of Medical Informatics* 60 (2000), 129–135. https://doi.org/10.1016/S1386-5056(00)00112-X

[38] Global Knowledge. 2022. *Cybersecurity Awareness Posters.* https://www.globalknowledge.com/us-en/topics/cybersecurity/cybersecurity-awareness-posters/#gref

[39] Hennie Kruger, Lynette Drevin, and Tjaart Steyn. 2010. A vocabulary test to assess information security awareness. *Information Management Computer Security* 18, 5 (2010), 316–327. https://doi.org/10.1108/09685221011095236

[40] Hennie A. Kruger and Wayne D. Kearney. 2006. A prototype for assessing information security awareness. *Computers Security* 25, 4 (2006), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

[41] Harold D. Lasswell. 1948. The structure and function of communication in society. In *The Communication of Ideas* (1st ed.), Lyman Bryson (Ed.). Harper and Row, New York, USA, 37–51.

[42] Regina E. Lundgren and Andrea H. McMakin. 2018. *Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks* (6th ed.). Wiley-IEEE Press.

[43] Durairaj Maheswaran and Joan Meyers-Levy. 1990. The Influence of Message Framing and Issue Involvement. *Journal of Marketing Research* 27, 3 (1990), 361–367. https://doi.org/10.2307/3172593

[44] Peter Mayer, Alexandra Kunz, and Melanie Volkamer. 2017. Reliable Behavioural Factors in the Information Security Context. In *SIGCHI Conference on Human Factors in Computing Systems*. ACM, Reggio Calabria, Italy, 1–10. https://doi.org/10.1145/3098954.3098986

[45] Carrie McCoy and Rebecca Thurmond Flower. 2004. You are the key to security: establishing a successful security awareness program. In *32nd Annual ACM SIGUCCS Conference on User Services*. Baltimore, MD, USA.

[46] Microsoft. 2015. *Attention spans.* Technical Report. Canada.

[47] Jakob Nielsen. 2010. *Horizontal Attention Leans Left (Early Research).* https://www.nngroup.com/articles/horizontal-attention-original-research/

[48] Oyelami Julius Olusegun and Norafida Binti Ithnin. 2013. *People Are the Answer to Security: Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization.* Retrieved 30 March 2022 from https://arxiv.org/abs/1309.0188

[49] James Van Patten, Chun-I Chao, and Charles M. Reigeluth. 1986. A Review of Strategies for Sequencing and Synthesizing Instruction. *Review of Educational Research* 56, 4 (1986), 437–471. https://doi.org/10.3102/00346543056004437

[50] Postermywall. 2022. *8,720+ customizable design templates for marketing.* Retrieved 10 April 2022 from https://www.postermywall.com/index.php/posters/search?s=marketing

[51] PosterPresentations.com. 2022. *Free Research Poster PowerPoint Templates.* Retrieved 10 April 2022 from https://www.posterpresentations.com/free-poster-templates.html

[52] Tobias Reynolds-Tylus. 2019. Psychological Reactance and Persuasive Health Communication: A Review of the Literature. *Frontiers in Communication* 4, 56 (2019), 1–12. https://doi.org/10.3389/fcomm.2019.00056

[53] R.S.Shaw, Charlie C.Chen, Albert L.Harris, and Hui-Jou Huang. 2009. The impact of information richness on information security awareness training effectiveness. *Computers Education* 52, 1 (2009), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

[54] TerraNova Security. 2022. *Why Localized Security Awareness Training Matters.* https://terranovasecurity.com/why-localized-security-awareness-training-matters/

[55] Miles A. Tinker and Donald G. Paterson. 1928. Influence of type form on speed of reading. *Journal of Applied Psychology* 12, 4 (1928), 359—-368. https://doi.org/10.1037/h0073699

[56] Mark Wilson and Joan Hash. 2003. *Building an Information Technology Security Awareness and Training Program.* Technical Report. Gaithersburg, MD, USA.

[57] Michael Wolf, Dwight A. haworth, and Leah Pietron. 2011. Measuring An Information Security Awareness Program. *Review of Business Information Systems* 53, 3 (2011), 9–21. https://doi.org/10.19030/rbis.v15i3.5398

[58] Cyber Safe Work. 2022. *Security Awareness for a Culture of Security.* https://cybersafework.com/free-security-posters/