# Self-promotion with a Chance of Warnings: Exploring Cybersecurity Communication Among Government Institutions on LinkedIn

Alexander J. Wilke
Macromedia University of Applied Sciences
Germany
al.wilke@macromedia.de

Jan M. Nold
Ruhr University Bochum
Germany
jan.nold@ruhr-uni-bochum.de

Oskar Braun
AWARE7 GmbH and Rhine-Waal University of Applied Sciences
Germany
oskar@aware7.de

Florian Meißner
Macromedia University of Applied Sciences
Germany
fl.meissner@macromedia.de

Matteo Große-Kampmann
Rhine-Waal University of Applied Sciences and AWARE7 GmbH
Germany
matteo.grosse-kampmann@hochschule-rhein-waal.de

## ABSTRACT

Knowledge about threats and countermeasures is essential for adequate protection in digital societies. Three government agencies from Germany (Federal Office for Information Security, BSI), the United Kingdom (National Cyber Security Centre, NCSC), and the United States (Cybersecurity and Infrastructure Security Agency, CISA) all have the legal mandate to inform the public about threats and countermeasures. However, no systematic analysis of their communication strategies has been conducted. To close this gap, we conducted an exploratory content analysis. We developed a LinkedIn crawler to download all posts from the three government agencies in 2023. Based on this data set, we did a high-level exploratory analysis of 2,410 posts. We analyzed length, engagement (i.e., number of likes, shares, comments), and media types used as attachments. Afterwards, for March, 188 posts were analyzed using the Protection Motivation Theory (PMT) as a theoretical, analytical framework for risk communication. We find that the NCSC used PMT elements the most and managed to do so while posting the shortest posts in comparison. We furthermore identified thematic differences between the authorities. For example, the NCSC most frequently publishes information on cybersecurity risks without a current reason, while the BSI, like the CISA, frequently communicates on (scientific) publications apart from its self-marketing.

## CCS CONCEPTS

• **Security and privacy → Economics of security and privacy**; **Social aspects of security and privacy**; **Usability in security and privacy**.


*MUM '24, December 1–4, 2024, Stockholm, Sweden*

ACM ISBN 979-8-4007-1283-8/24/12
https://doi.org/10.1145/3701571.3701575

## KEYWORDS

Communication, Risk, Cybercrime, Social Media, Protection Motivation Theory

**ACM Reference Format:**
Alexander J. Wilke, Jan M. Nold, Oskar Braun, Florian Meißner, and Matteo Große-Kampmann. 2024. Self-promotion with a Chance of Warnings: Exploring Cybersecurity Communication Among Government Institutions on LinkedIn. In *International Conference on Mobile and Ubiquitous Multimedia (MUM '24), December 1–4, 2024, Stockholm, Sweden.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3701571.3701575

## 1 INTRODUCTION

The proliferation of digital devices and services presents substantial opportunities for attackers, significantly impacting individuals and businesses. In light of this, there is an increasing imperative for people and organizations to understand cybersecurity risks and take appropriate measures to safeguard themselves. Cyberattacks, data breaches, and other security incidents can result in severe repercussions, from financial losses to erosion of trust in digital infrastructures and critical systems. Public outreach is pivotal in elevating awareness regarding these risks and available protective measures. However, public campaigns have so far proven ineffective [6, 58]. Although media coverage is increasing [2, 9, 13], it fails to accurately portray the technical reality [32]. Such misrepresentations lead, among other things, to relevant risks and countermeasures not being part of the reporting or being questioned by the public [21]. This necessitates addressing technical aspects and sensitizing regular users of digital platforms. Nonetheless, simply raising awareness falls short of ensuring secure behaviors. Effective public communication should raise awareness of pertinent risks and give citizens actionable mitigation guidance [6, 54]. To accomplish this, communication strategies must effectively reach and engage the target audience, rendering information comprehensible and actionable.

Communication in social media on the topic of cybersecurity is an aspect that has been little researched to date [60]. National cybersecurity authorities play a pivotal role in this regard. They are

tasked with informing all stakeholders about IT risks and protective measures. BSI in Germany, the CISA in the USA, and the NCSC in the UK shoulder this responsibility. This study endeavors to scrutinize the communication approaches of these respective authorities and explore divergences in their messaging. Our guiding research question was:

***RQ1:*** *How do different cybersecurity authorities communicate on LinkedIn?*

To further explore the communication of the selected cybersecurity authorities we developed further sub-questions to get a holistic understanding of their communication efforts.

As recent studies have shown, media coverage is often driven by key events, such as the Snowden relevations or cyberattacks on economic actors [2, 9, 13]. These topics discussed in the media as well as on social media form the public reception of cyber threats (see also section 2.1). Therefore we ask:

***RQ1.1:*** *Which topics do the cybersecurity authorities generally communicate about?*

Further research interest in media coverage applies to the portrayal of actors in media coverage [12]. So far, media coverage has mainly focused on hackers as threat actors. In contrast, citizens or the general public remain mainly victims rather than responsible for implementing security measures [44] (see also section 2.1). Therefore we ask:

***RQ1.2:*** *Which cybersecurity threats, victims, and solutions do the various cybersecurity authorities address?*

Numerous studies have applied the Protection Motivation Theory (PMT) to the field of cybersecurity [23, 43, 57, 59]. In particular, personal motivation and the ability to implement the behavior are key elements that can positively influence real behavior change (see also section 2.2). Therefore we ask:

***RQ1.3:*** *To what degree are elements of the PMT (Severity, Vulnerability, Efficacy, Self-Efficacy, Response Costs, Maladaptive Rewards) used?*

To this end, we scrutinized the public communications of these cybersecurity authorities on LinkedIn. Initially, we subjected all postings from these organizations on LinkedIn in 2023 to an automated quantitative analysis. For our analysis, we chose the timespan of one year to cover all special occasions and days, e.g., Christmas, "Change your Password Day" etc. Subsequently, we conducted manual quantitative content analysis on postings throughout March, representing an average month, to discern any significant variances between the authorities. Additionally, we evaluated whether their communication adhered to fundamental risk communication principles as delineated in the PMT. In summary, our paper makes the following contributions:

- **Communication Strategies:** We explore various communication strategies on LinkedIn, focusing on a comprehensive and comparative study of three distinct organizations. We examine whether specific approaches are tailored to different target groups and strategies for communicating the same topics simultaneously. We provide our dataset and analysis scripts to the community for future research.
- **Communication Differences and Effectiveness:** We further investigate how communication varies among the three different government bodies and assess the effectiveness of their communications using the PMT as a framework. The analysis aims to determine how well these messages are crafted to promote secure behavior among the audience.
- **Categorization and Performance of Messages:** We identify different categories of messages, such as humoresque, current affairs, cybersecurity knowledge, and others, and evaluate how well these categories perform. The goal is to understand the impact and effectiveness of each type of message.
- **Recommendations:** We provide recommendations to enhance the effectiveness and correctness of communication in the domain of cybersecurity.

## 2 RELATED WORKS

The following chapter is first dedicated to the current state of research on cybersecurity communication, taking into account related research areas such as human behavior studies (see section 2.1). The theoretical basis for the present study is then presented (see section 2.2).

### 2.1 Research on Cybersecurity Communications

The primary goal of cybersecurity communication must be to make people's behavior more secure [6, 53]. However, studies on human behavior in cybersecurity reveal numerous deficiencies in adopting secure practices [54]. Many individuals do not understand the risks associated with digital devices and service usage. They may be uninformed about relevant countermeasures or doubt their efficacy [21]. Misconceptions are often fuelled by media reports that distort technical realities [32]. Moreover, the abundance of sometimes conflicting information on cybersecurity overwhelms individuals [51]. Simultaneously, it's crucial to avoid overstating cybersecurity risks. Florencio et al. [28] highlight the adverse effects of exaggerated risks propagated by cybersecurity vendors on businesses, while Menges et al. [45] observed trainees becoming despondent and passive when exposed to worst-case online scenarios. Communication science, with few exceptions, has yet to thoroughly engage with cybersecurity, including within the specialized research area of risk and crisis communication. Nonetheless, there has been a notable surge in media coverage about cybersecurity, often catalyzed by significant events prompting heightened public awareness [2, 9, 13]. Notably, online media have emerged as the primary conduit for cybersecurity information dissemination among a significant segment of the populace [19]. However, disparities in demographic profiles, technological affinity, and gender necessitate consideration. An additional research focus centers on scrutinizing media coverage of specific cybersecurity incidents [36], particularly in portraying actors, notably hackers [12]. This examination delves into how media depict these actors and the resultant impact on public opinion formation in the cybersecurity domain. The realm of social media communication on cybersecurity matters was explored by Vogler and Meissner [60], who observed that individuals affected by a data breach at a major ticketing provider predominantly discussed service-related aspects rather than security concerns on Twitter. This trend may signal a lower prioritization of data security topics. Contrarily, Bada et al. [6] found no conclusive

evidence regarding the efficacy of awareness campaigns promoting cybersecurity. The ineffectiveness of such campaigns is attributed to their heavy reliance on fear appeals or their failure to align with the cultural contexts of target audiences [54]. Nurse et al. [48] conducted a literature review on the trustworthy and effective communication of cybersecurity risks. The authors identified several motivational factors that are emphasized, e.g., that users tend to be unmotivated. They also give recommendations e.g., designers of security systems should reduce cognitive effort by individuals in processing security-risk information. Chen [15] differentiates further and analyzes differences and common ground between the human information-processing approach and the mental models approach. The author emphasizes that while both approaches differ, they are closely connected. Researchers and communicators should, therefore, choose approaches and methods carefully based on practical considerations and theoretical rationale. Boase et al. [8] conducted a scoping review that explored whether the mental models' approach is helping to develop more efficient risk communication. They found wide variation in the effectiveness while emphasizing that all reviewed studies reported a positive effect. However, scholarly investigations analyzing the determinants of success or failure in such campaigns and proposing strategies for enhanced cybersecurity communication remain scant. The studies listed show that neither communication on social media about cybersecurity nor by cybersecurity authorities has yet been studied despite its role in raising public awareness. This paper aims to close this research gap (cf. RQ1 - RQ1.2).

As already suggested by Nurse [48], the risk communication perspective seems to offer possible approaches for the effective communication of cybersecurity. Rogers and Pearce [52] define risk communication as a type of communication that employs "persuasion to change the understanding of risk and, as a result, behavior, in light of [...] information about probabilities of harm and methods for reducing the probability of harm. These spontaneous and reactive messages can be delivered frequently (e.g., long-term health communication campaigns), are delivered by technical experts, and are based on what is currently known." However, governmental or administrational risk communication research primarily revolves around public health crises and natural disasters [52]. It is comparably easy to infer protective behavior during extreme events because protection motivation is generally high. However, when it comes to protective behavior before a crisis has even started (i.e., prevention/preparedness), it is often much more challenging to communicate effectively [26]. The same can be assumed for cybersecurity, particularly given that it is a technical and primarily abstract threat to ordinary citizens. This is also supported by large-scale surveys which show little awareness and protective behavior by citizens in the context of cybersecurity [37, 56]. Generally speaking, there still seems to be potential for risk communication by public authorities even when an acute crisis is absent. For instance, Paton et al. [50] found that public risk communication strategies can motivate preparedness measures among citizens. In the same vein, Becker [7] posits that "the timely and effective flow of information between agencies and the public is vital for facilitating and encouraging appropriate protective actions, reducing rumors and fear, maintaining public trust and confidence [...]." At the same time, as Covello [16] problematizes, "many technical, engineering and scientific professionals, together with government and industry authorities [...] lack effective risk communication skills. Leaders, risk managers, and technical experts are frequently insensitive to or unaware of, the information needs of interested and affected parties."

## 2.2 Theoretical Foundation

As stated from a theoretical perspective, exploring risk and crisis communication offers valuable insights applicable to cybersecurity discourse. These frameworks facilitate proactive responses from individuals confronted with risks or emergent situations. This study draws from the Protection Motivation Theory advanced by Floyd, Prentice-Dunn, and Rogers [29], alongside Entman's [25] conceptualization of framing. PMT posits that persuasive messages delineating personal threat scenarios and proposing mitigative actions can catalyze protective behaviors, particularly when users require added motivation to adopt secure practices [10]. Accordingly, PMT stipulates two prerequisites for individuals to undertake protective measures against risks: threat appraisal and coping appraisal, each comprising further dimensions. Threat appraisal involves the perception of threat severity and personal vulnerability. Notably, the fear induced by threat appraisal must outweigh any maladaptive rewards, such as time or cost savings, to incentivize protective action. Conversely, coping appraisal encompasses the perceived efficacy of protective measures, self-efficacy in their implementation, and the perceived costs of such actions [10]. The understanding that these factors are pivotal in persuading individuals to embrace specific security behaviors can inform the development of security communication strategies. PMT is an established theory used in risk communication [22] but also in cybersecurity. In addition, the fact that the theory has been validated many times has encouraged us in our choice of PMT [18, 23, 29]. Prior investigations into PMT in the IT context underscore the significance of self-efficacy in driving desired behaviors [11, 27, 47, 53], prompting an increasing adoption of PMT in information security research [17].

Exemplary study results emphasize using PMT in the context of cybersecurity communication. Anderson and Agarwal [5] developed a conceptual model of conscientious cybercitizens and performed a large-scale study focusing on PMT and its application. They found that psychological ownership is an additional component of PMT in the online security context and highlight the importance of a descriptive norm. Boss et al. [10] analyzed fear appeals and their potential to motivate users towards better online behaviors. The study revealed that for practitioners, it is crucial to understand that a fear appeal requires a persuasive message that addresses maladaptive incentives while enhancing self-efficacy. Crossler et al. [18] analyze whether employees follow "Bring Your Own Device" policies by using PMT as the foundational model. They found compliance was highest among those policies that motivated self-efficacy, threat severity, and response efficacy. Response cost was negatively related to compliance with the policy. However, to the best of our knowledge, it is still unexplored whether and to what extent cybersecurity authorities use elements of PMT in their communication to increase secure behavior (cf. RQ1.3).

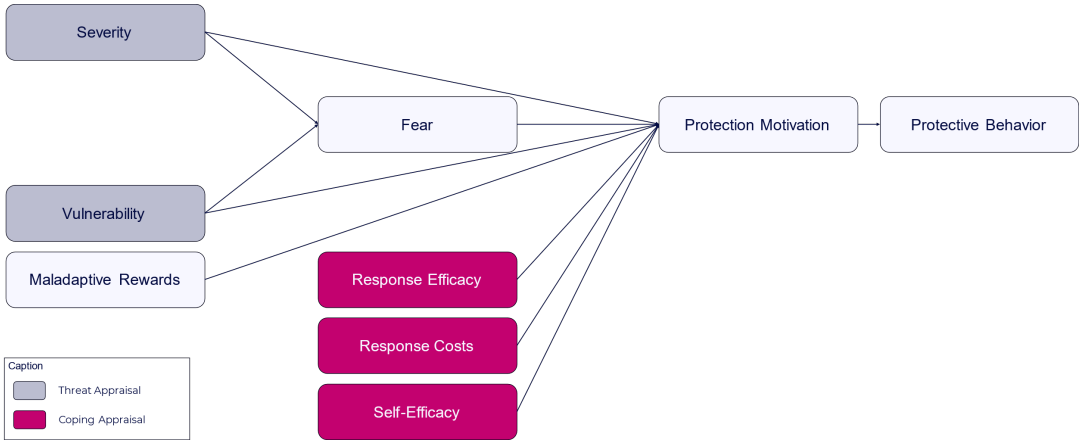



**Figure 1: PMT Model, own illustration based on [10, p. 843]**

Moreover, this study integrates the concept of framing, which is widely employed in communication studies. Entman [25] defines frames as interpretive patterns comprising problem definition, causal interpretation, moral assessment, and action recommendations. Within the context of this study, the problem definition (pertaining to cyber threats) and recommended actions (suggesting specific protective behaviors) are particularly important. We assert that both PMT and framing approaches can be effectively employed in the analysis of cybersecurity communication. In fact, framing theory complements PMT by including a perspective that is more focused on the actual content (specific cyber threats and recommended countermeasures) while PMT focuses on the degree to which the communication content under investigation addresses different dimensions of risk perception and coping. All of these aspects are crucial to answer the research questions outlined above.

## 3 METHOD

This section gives an overview of the methods used in the paper. We start by giving details on the institutions we selected for our analysis and why in section 3.2. Section 3.4 describes our data acquisition approach using LinkedIn. Section 3.5 describes our quantitative analysis of the data and section 3.6 describes the manual content analysis.

### 3.1 Choosing a Social Network

LinkedIn has emerged as a pivotal platform for the dissemination and communication of cybersecurity content and professional content more broadly because it is a career-oriented social network. As a professional networking site with over 850 million members globally [41], LinkedIn facilitates professional networking by enabling users to connect with colleagues, industry peers, and potential employers. This networking capability is particularly valuable in cybersecurity, where staying updated with the latest threats, technologies, and best practices is critical. It also fosters active engagement and communication through comments. Through LinkedIn, cybersecurity professionals can join specialized groups, participate in discussions, and share insights on emerging issues, thereby enhancing their knowledge and staying abreast of industry developments [24].

LinkedIn's publishing platform allows personal users and the whole organization to create and share detailed articles, updates, and multimedia content. This is an effective medium for cybersecurity organizations to disseminate research findings, threat reports, and educational materials. By sharing content on LinkedIn, professionals and organizations can reach a broad audience of peers and stakeholders actively seeking authoritative and relevant information. This targeted dissemination helps build credibility and influence within the cybersecurity community while introducing vulnerability to social engineering attacks [4]. LinkedIn is the most frequently used social network for business contacts in the three countries included in this study. All three organizations whose communication we analyze have many followers on this platform and use it often to communicate and interact with them. Because of these aspects, we chose LinkedIn as the social network we focused on in our studies. We discuss potential limitations and how we mitigated them in section 6.

### 3.2 Selection Process of Institutions

Our study focuses on cybersecurity communication towards citizens and whether communication embeds best practices from the literature, e.g., the different dimensions according to PMT outlined in section 2.2. Therefore, we chose three institutions that put humans first in their mission statements, but each institution does it slightly differently. The NCSC is "making the UK the safest place to live and work online," referencing humans only implicitly [14]. The CISAs mission statement is "We lead the national effort to understand, manage and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day" [1]. CISA is putting Americans at the center of their efforts, and the protection of the systems is a means to safeguard the systems Americans are using every day. Lastly, the BSIs mission is "Gestaltung einer digitalen Welt, der die Menschen vertrauen können. Wir wollen mit unserem Engagement als #TeamBSI die digitale Welt verbessern und Informationssicherheit als Chance für die digitale Transformation etablieren." (Translation: "Shaping a digital world that people

can trust. With our commitment as #TeamBSI, we want to improve the digital world and establish information security as an opportunity for digital transformation.") [35]. The BSI is, therefore, the only institution that addresses "people" in general explicitly without any national constraints. Furthermore, the BSI is already inviting people to join the discussion on social media using "#TeamBSI".

## 3.3 Choosing the Timespan

Focusing on the year 2023 provides a comprehensive view of cybersecurity communication over an entire annual cycle. This approach ensures that the sample is not skewed by seasonal variations, offering a more balanced and accurate evaluation of communication efforts. Significant incidents, such as the MOVEit data breach in the UK [20] ransomware attacks on the NHS [61], the exploitation of Microsoft Exchange Server vulnerabilities in the USA [38], and cyberattacks on critical infrastructures [49], as well as ransomware attacks and geopolitical cyber threats in Germany [3, 55], underscore the importance of this analysis. Analyzing the entire year allows for a more robust understanding of how cybersecurity agencies respond to varied threats, ensuring that findings are representative and reliable.

## 3.4 LinkedIn Crawler

Before starting this study, we needed to obtain all the postings of the respective entities and as much information about them as possible. LinkedIn does not automatically provide a way to retrieve structured information about posts from other organizations. Therefore, we developed our crawler to retrieve structured quantitative information about LinkedIn postings by the organizations we wanted to analyze.

Therefore, we built a LinkedIn crawler with the help of the LinkedIn Community Management API [42] and the Posts API [46]. The crawler's basic idea is that an operator can specify an organization from which we want to retrieve all posts and post information, e.g., the creation date, the URL of the post, the content, media description, and media type. After the operator specifies a URL, the crawler runs and finishes after some time. The crawl returns a serialized JSON, which we convert into an *.xlsx* file for further analysis.

## 3.5 Automated Quantitative Analysis

Running the crawler resulted in three *xlsx* files, one for each agency. The number of likes, comments, and shares was added manually to the files, because the API did not automatically get this information. A measurement summary can be found in section 4.1. Subsequently, the three files were combined into one *csv* file, containing an additional column indicating the source, i.e., agency. The analysis was done in *Spyder IDE 5.5.3* on macOS with custom Python scripts. We used *numpy, pandas, seaborn, statsmodels* and *matplotlib* to compute and visualize results.

## 3.6 Manual Quantitative Content Analysis

In addition to the automated quantitative analysis, an in-depth, manual quantitative content analysis [39] of the postings of each official body was conducted. For this purpose, we selected March as an exemplary month that contained neither external events (e.g., World Password Day in May or Cyber Awareness Month in October) nor events organized by any organizations included in the analysis (e.g., annual conferences).

All identical text and publication date postings were deleted for the manual content analysis. Only the version with the highest interactions (likes or other reactions, shares, and comments) was retained. In the case of the NCSC, all Welsh-language postings were also removed after it was confirmed that they were identical to English-language postings. March was also an average month in terms of the number of postings. The NCSC had 71 postings in March (average of 69), the BSI 44 (average of 54), and the CISA 73 (average of 72). The codebook contains the following content categories: thematic focus, the naming of a risk or damage event, the cyber threat mentioned as well as the victims of the cyber threat, the security measures mentioned, evaluation of the security measures, those responsible for implementing the security measures and finally the elements of the PMT. For example, specific warnings were only coded when warnings were issued for certain singular events or when information was provided about specific cybersecurity measures. Using the example of the recommendations for action, cooperation was coded, among other things, when the article refers to support from other actors. For example, the involvement of experts, cooperation with hackers or companies, and international collaboration were cited as explanations for the coding. One element per post was coded for posts containing several cyber threats, victims, security measures, or persons responsible. The element with the largest share of the total post is coded. If there is no transparent dominant element, only the first is coded. For the PMT elements a category system was developed for the analysis. As suggested by Boss et al. [10] the present study operationalized all dimensions of PMT. They were coded into the following categories: "High", "Ambivalent", "Low", and "Not available". The severity and vulnerability elements could only be coded if a threat was presented, whereas the other elements of the PMT could only be coded if a recommendation for action was given. The framing categories were developed based on an initial review of the material and a theoretical basis, including the classic framing categories of problem definition and recommended action. These categories were already used in another study by Meissner et al. [44], which examined reporting on cybersecurity in German news media. In doing so, the authors want to ensure that the PMT dimensions and the framing categories can be compared with these studies.

In addition, specific threats such as phishing and ransomware or general threats such as security vulnerabilities or cyber-attacks were coded. Recommendations for action in the form of particular security measures, such as security checks, authentication methods, or training, were also coded. Those responsible were coded both for the threats and for implementing the recommendations for action. The study also examined whether the posts discussed potential future risks or actual damages that have occurred. This distinction is crucial as it highlights whether the agencies are focusing on proactive risk management or responding to incidents that have already happened. Risks were coded when posts focused on potential future damages or events, such as predictions or studies on the likelihood of cyber-attacks. In contrast, damages were coded when posts discussed past or ongoing incidents and their impacts. Furthermore, categories aimed at a more precise understanding of

the recommended action, such as comprehensibility, prominence, target group, and unambiguity, were integrated.

One coder analyzed the sample. Therefore, the calculation of intracoder reliability according to Holsti was used. Intracoder reliability measures how well the codes of one encoder match at the beginning and end of the study period [31]. For this purpose, the same material is re-encoded in intervals [31]. According to Holsti, the reliability coefficient results from the number of matching codes at times one and two. Values of one should be aimed for formal categories [30]. Values of over 0.8 for content categories are desirable [30]. The results were very satisfactory, with the coefficient ranging from 0.83 to 1.0, depending on the category.

# 4 RESULTS

In this section we present our results. Section 4.1 gives an overview of our measurement results and contains a quantitative analysis of the postings we crawled. Section 4.2 describes our content analysis of the top postings.

## 4.1 Descriptive and Exploratory Statistical Analysis

We conducted our measurement runs with the tool described in section 3.4 in February and March 2024. The period was long because the authors manually collected some meta-data of the postings (cf. section 3). Our dataset includes all available postings with their respective metrics from the 01st of January 2023 until the 31st of December 2023 of all three government agencies on LinkedIn. In total, we collected 2,410 postings with 392,044 likes and 12,960 comments for all three government agencies. The posts were, in total, shared 65,031 times by users on the social network. The number of followers at the time of our data collection was around[1] 148.000 for BSI, 446.000 for NCSC, and 489.000 for CISA as of May 2024. We are publishing our crawled data and our analysis scripts to contribute to reproducible science[2].

The BSI issued 653 posts over the year. The average length of each post was 776.64 characters (SD 489.01), while the median length was 666.0. The shortest post had zero characters, while the longest contained 3158. The NCSC posted 896 times, with an average length of 247.10 characters (SD 203.75) per post. The median length was 195.0, while the minimal and maximal number of characters was zero and 1816, respectively. The Cybersecurity & Infrastructure Security Agency issued 861 posts over the year, with an average length of 603.88 characters (SD 380.93). The median length was 523.0, while the shortest and longest posts contained zero and 2607 characters, respectively. For comparison, each post's length distribution is shown in Figure 2.

The number of likes, comments and shares per post (i.e., engagement) is depicted in Table 1. For comparison, the distribution of likes is shown in Figure 3. In terms of mean engagement per follower, BSI had 0.0014, NCSC had 0.0003, and CISA had 0.0004 mean likes per follower. This indicates a higher engagement for BSI, getting more likes on average while having the smallest amount of followers. While NCSC had far shorter posts, the number of likes was smaller than CISA and BSI.

[1]LinkedIn is not displaying exact follower counts.
[2]https://github.com/awareseven/agency-comms

To test whether the means of the distribution of the number of likes, shares, comments, and the length of the posts are different, we conducted a Welch-ANOVA test. The results are shown in Table 2. They indicate that the means of the distribution of likes differ between all agencies. This also holds for the length of the posts and the number of comments. Only regarding the mean of the distribution of the number of shares, there was no statistically significant difference between BSI and NCSC, as well as BSI and CISA.

LinkedIn makes it possible to attach different media to a post, i.e., images, videos, or documents. BSI attached documents to 55 posts, 428 images, and 79 videos and posted 91 times without attaching media (i.e., a text only post). NCSC posted one document, 49 images, 98 videos, and 748 times without attaching media. CISA did not post documents but posted 574 images, 54 videos, and 233 times without attaching media. Figure 4a shows the relative fractions for comparison. The distribution of likes for the different media types per agency is shown in Figure 4b.

## 4.2 Analysis of Posts from March

After the removal of duplicates and Welsh-language posts from the NCSC, a total of 188 LinkedIn posts was identified and coded. The BSI in Germany accounted for 44 posts, which represents 23.4% of the total posts analyzed. The CISA in the United States had a more significant share with 73 posts, making up 38.8% of the total. The NCSC in the United Kingdom contributed 71 posts, which constituted 37.8% of the total posts analyzed.

### *4.2.1 Topics Addressed by the Different Cybersecurity Authorities (RQ1.1).*

Concerning the naming of risks (future, potential losses or future, potential loss events), our analysis shows that CISA posts most frequently without mentioning risks or damages, with 84.9% of its posts falling into this category. On the other hand, NCSC reports on risks the most, with 45.1% of its posts discussing potential future threats. BSI also addresses risks, but to a lesser extent than NCSC, with 29.5% of its posts discussing this theme. Posts discussing actual damages (past or current, present damage or past or current, present damage events) are rare across all agencies. BSI does not discuss damages in its posts. Both CISA and NCSC mention damages in only 1.4% of their posts.

The thematic analysis of the LinkedIn posts shows that all three agencies predominantly use the platform for self-promotion or public relations (Fig. 5). This trend is most pronounced in CISA's communications, where 56.2% of the posts are dedicated to self-marketing. The BSI follows with 38.6% of its posts focusing on self-marketing. Similarly, the NCSC has 36.6% of its posts dedicated to self-promotional content.

Interestingly, the NCSC is the only agency that frequently posts about general security topics without specific references. A significant 46.5% of its posts fall into this category, including general information on cyber risks and corresponding countermeasures. In contrast, particular warnings about threats are rarely issued by any of the agencies on LinkedIn. The BSI mentioned specific warnings in only 2.3% of its posts, CISA in 1.4%, and NCSC in 4.2%. The BSI's posts are particularly varied, often covering various topics. Besides

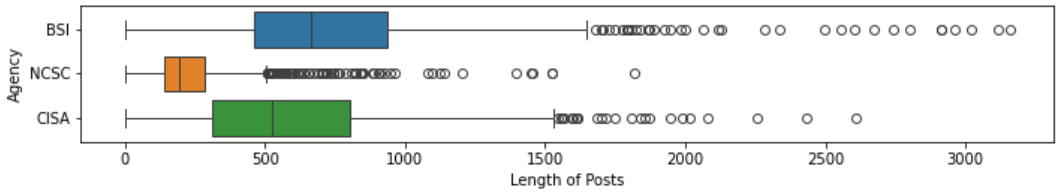



**Figure 2: Distribution of post length for the three agencies.**

**Table 1: Summary statistics (mean, standard deviation, median, min, and max) of the number of likes, comments, and shares for the posts for each agency.**

| | **Likes** | | | | **Comments** | | | | **Shares** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Mean* | *SD.* | *Med.* | *Min, Max* | *Mean* | *SD.* | *Med.* | *Min, Max* | *Mean* | *SD.* | *Med.* | *Min, Max* |
| BSI | 202.16 | 245.75 | 129 | (6, 2752) | 8.98 | 12.7 | 4 | (0, 102) | 25.86 | 41.95 | 13 | (0, 389) |
| NCSC | 121.7 | 216.39 | 49 | (0, 2410) | 3.28 | 7.12 | 1 | (0, 59) | 24.71 | 48.84 | 9 | (0, 438) |
| CISA | 175.35 | 217.85 | 110 | (0, 2156) | 5.82 | 18.04 | 2 | (0, 414) | 30.19 | 48.64 | 13 | (0 , 470) |

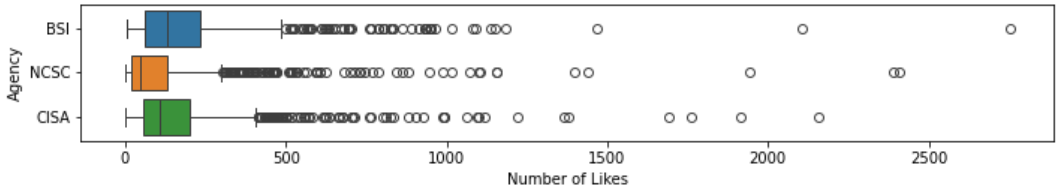



**Figure 3: Distribution of likes per agency.**

**Table 2: Welch-ANOVA between each pair of agencies for the number of likes, shares, and comments, and the length of posts. Bold values indicate statistically significant results assuming a 5% significance level.**

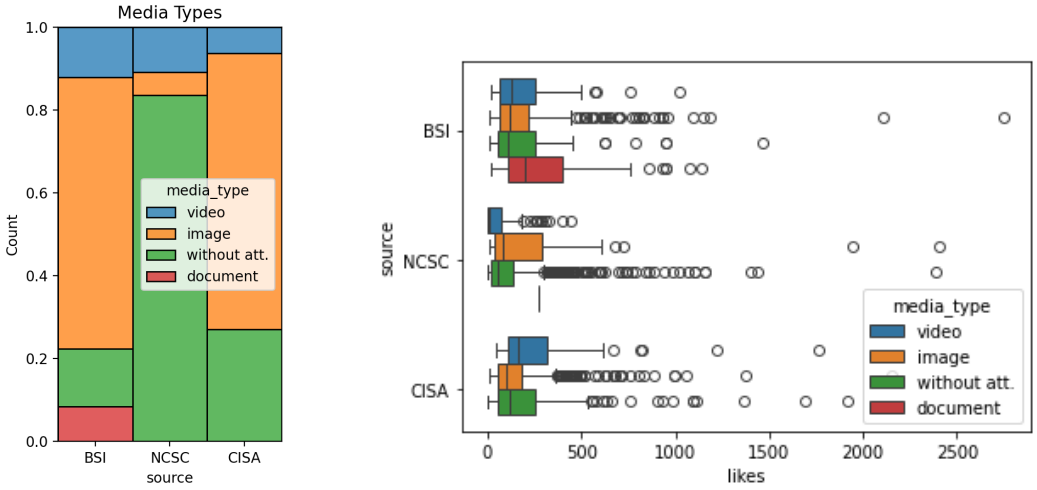
| Agency-Pair | Likes | Shares | Comments | Length |
|---|---|---|---|---|
| BSI vs NCSC | **F = 44.71, p < 0.01** | $F = 0.25$, $p = 0.61$ | **F = 106.0, p < 0.01** | **F = 679.56, p < 0.01** |
| BSI vs CISA | **F = 4.88, p = 0.027** | $F = 3.47$, $p = 0.06$ | **F = 27.59, p < 0.01** | **F = 55.80, p < 0.01** |
| CISA vs NCSC | **F = 26.81, p < 0.01** | **F = 5.55, p = 0.018** | **F = 5.43, p = 0.019** | **F = 592.45, p < 0.01** |

self-marketing, BSI frequently shares (scientific) publications aimed at the IT security community.

We also evaluated whether certain topics evoke higher engagement with the postings. The data indicates that specific warnings generate a particularly high level of engagement. General information on risks and safety measures without specific reference also receives above-average engagement, with a mean value of 198.78 compared to the average mean value of 189.58. Similarly, (scientific) publications intended for the specialist community exhibit above-average engagement, with a mean value of 192.70 against the same average mean value of 189.58. The statistical analysis, represented by 'n = 188, F(6) = 2.389; p < 0.030,' reveals statistically significant differences between the mean values of the six groups. The F-value of 2.389 and the p-value of less than 0.030 confirm that these differences are unlikely due to chance and are indeed significant. However, it is important to approach these findings cautiously, particularly given the low number of cases in certain categories, such as specific warnings (n = 5). The small sample size in this category limits the robustness of these conclusions and suggests a need for further investigation with a larger dataset.

#### *4.2.2 Threats, Victims, and Solutions Mentioned by the Different Cybersecurity Authorities (RQ1.2).*

Analyzing the depiction of cyber threats in the posts reveals significant differences among the agencies. CISA and BSI seldom mention specific cyber threats, with CISA not addressing threats in 86.3% of its posts and BSI in 70.5%. Although NCSC also has a high proportion of posts that do not address threats, at 57.7%, it mentions cyber-attacks in 36.6% of its posts. BSI addresses a variety of threats, although less frequently. For instance, it mentions security vulnerabilities in 9.1% of its posts, ransomware in 2.3%, phishing in 4.5%, and other threats in 6.8%. In terms of depicting victims of cyber




**(a) Media types attached to posts for the three agencies.**

**(b) Distribution of likes for the different media types and agencies.**

**Figure 4: Relative amount of attachment media types per agency (a) and distribution of likes per media type and agency (b).**

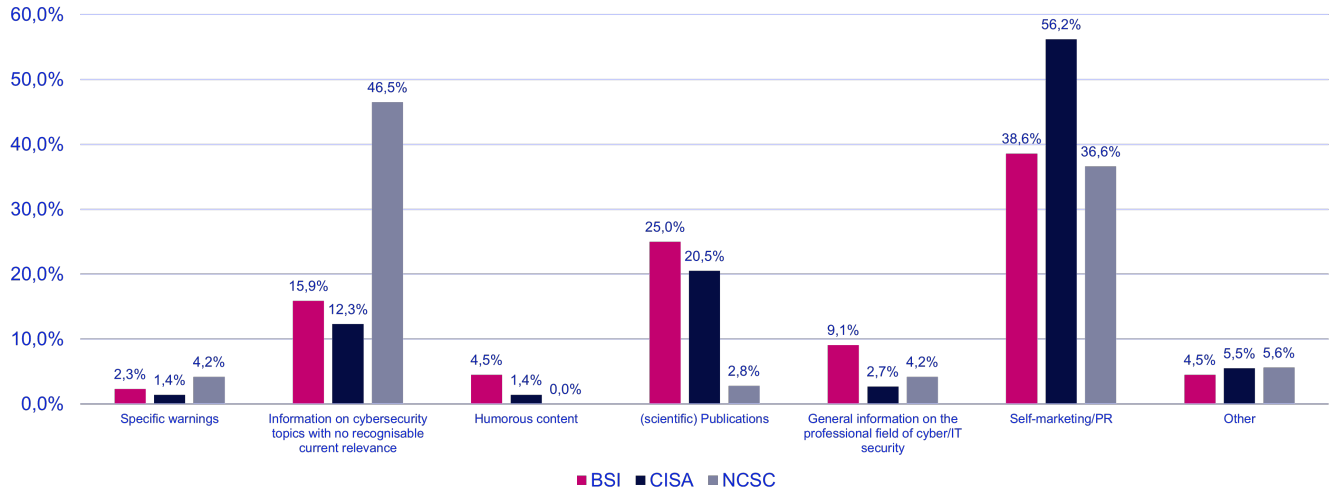



**Figure 5: Thematic focus per cybersecurity authority, own illustration**

threats, NCSC most frequently identifies the victims, focusing on economic actors such as SMEs (Fig. 6). Specifically, 15.5% of NCSC's posts mention businesses, while 28.2% mention SMEs. BSI, in contrast, more often portrays users as victims, with 15.9% of its posts addressing this. Conversely, CISA and BSI mention victims less frequently in their posts than the NCSC. 86.3% of CISA's posts and 70.5% of BSI's posts do not mention victims. In comparison, 53.5% of NCSC posts do not mention victims.

The portrayal of responsible parties for implementing cybersecurity measures also reflects the depiction of victims. NCSC frequently names economic actors responsible for cybersecurity, with 15.7% of its posts mentioning economic actors and 28.6% mentioning SMEs. This indicates that NCSC identifies these groups as victims and emphasizes their role in implementing cybersecurity measures. BSI again highlights users as responsible, with 15.9% of its posts focusing on this group. This mirrors BSI's depiction of users as victims, suggesting a holistic approach that encompasses both protection and responsibility at the individual level. Both the CISA and the BSI mention the responsible parties the least frequently. 82.2% of CISA posts, 65.9% of BSI posts and 50.0% of NCSC posts do not mention who is responsible for implementing cybersecurity measures. However, both the CISA and the BSI occasionally mention experts as being responsible, with 2.3% of the BSI posts and 2.7% of the CISA posts discussing this aspect.

The recommendations for action were specific cybersecurity measures mentioned within the postings. Regarding the depiction

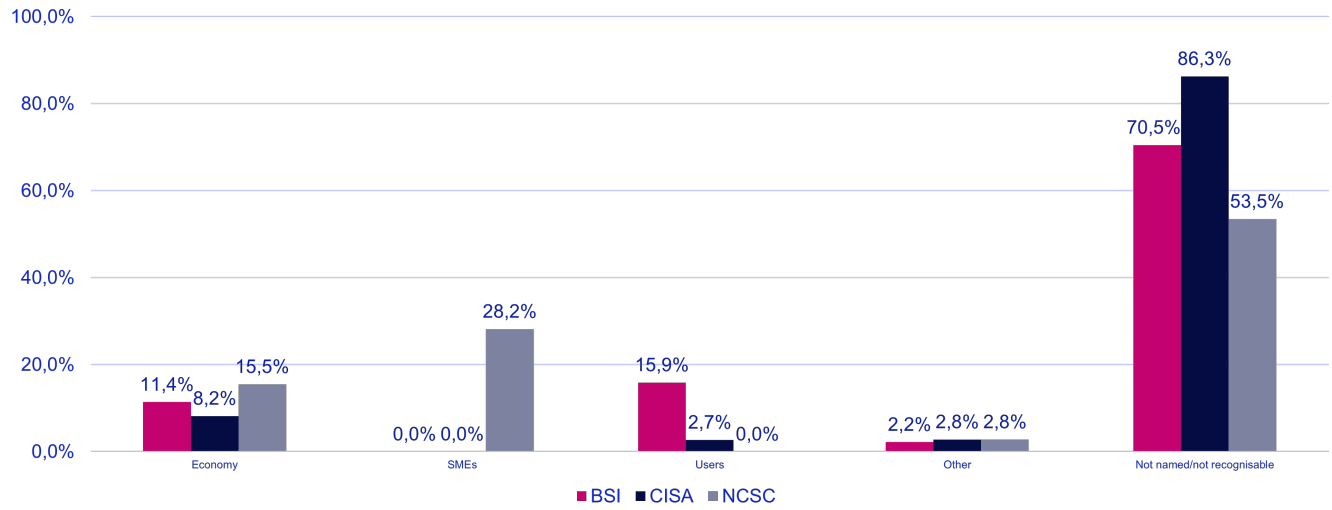



**Figure 6: Naming of victims per cybersecurity authority, own illustration**

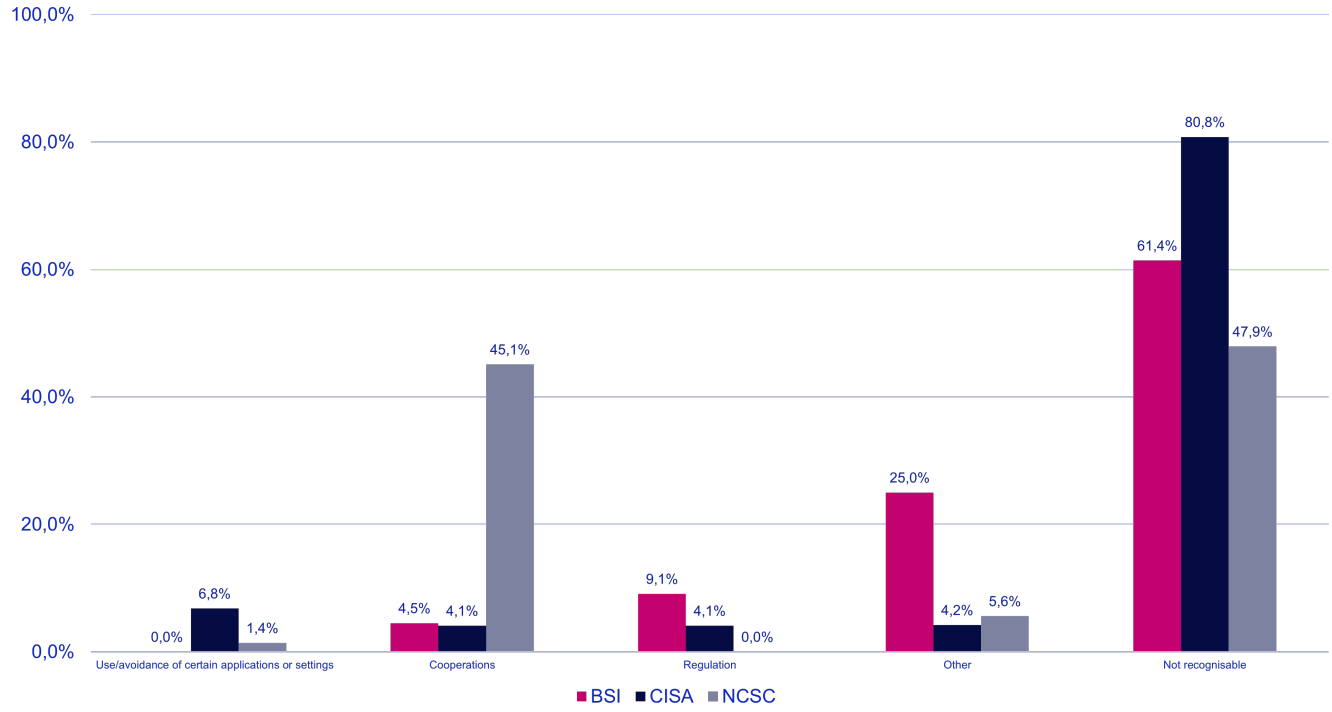



**Figure 7: Mention of cybersecurity measures per cybersecurity authority, own illustration**

of cybersecurity measures, NCSC posts most frequently about specific measures, with 45.1% of its posts focusing on cooperation (Fig. 7). Cooperation was defined as support from other actors, such as experts, external investigations, cooperation with hackers or companies, vulnerability analyzes, or international collaborations. This significant focus on cooperation reflects NCSC's initiatives to foster collaboration and support among businesses, particularly SMEs.

When CISA does recommend measures, it most often advises on the use or avoidance of specific applications or settings, with 6.8% of its posts focusing on this. BSI emphasizes regulations in its posts, with 9.1% addressing this topic. However, both CISA and BSI rarely

discuss specific cybersecurity measures, with 80.8% of CISA's posts and 61.4% of BSI's posts not addressing this.

*4.2.3 Usage of PMT Elements by the Different Cybersecurity Authorities (RQ1.3).*
The analysis also incorporated PMT elements to assess the motivational aspects in the posts. PMT dimensions include maladaptive rewards, response costs, threat severity, vulnerability, response efficacy, and self-efficacy. These dimensions help to understand how agencies try to motivate recipients to engage in protective behavior (Fig. 8).

For BSI, maladaptive rewards were not mentioned in 43.2% of the posts. High response costs were noted in 2.3% of posts, while 29.5% had no mention of this dimension. The severity of threats was mentioned as high in 1.4% of the posts, with 28.1% not addressing severity at all. High vulnerability was mentioned in 11.4% of the posts, and 18.2% did not mention vulnerability. Response efficacy was highlighted as high in 6.8% of the posts, while 34.1% did not mention it. High self-efficacy was noted in 11.4% of the posts, with 29.5% not addressing this aspect.

For CISA, maladaptive rewards were not mentioned in 19.2% of the posts. Low response costs were noted in 2.7% of the posts, and 15.1% did not mention response costs. The severity of threats was highlighted as high in 13.6% of the posts, with 1.5% not addressing severity. High vulnerability was mentioned in 5.5% of the posts, and 9.6% did not mention it. Response efficacy was noted as high in 9.6% of the posts, and 9.6% did not mention it. High self-efficacy was noted in 2.7% of the posts, with 16.4% not addressing this dimension.

For NCSC, maladaptive rewards were not mentioned in 52.1% of the posts. High response costs were noted in 1.4% of the posts, while low response costs were mentioned in 36.6% and 8.5% did not mention them. The severity of threats was highlighted as high in 21.1% of the posts, with 28.2% not addressing severity. High vulnerability was mentioned in 31.0% of the posts, and 18.3% did not mention it. Response efficacy was noted as high in 39.4% of the posts, while 12.7% did not address it. High self-efficacy was noted in 25.4% of the posts, with 26.8% not addressing this aspect.

# 5 DISCUSSION

Our empirical study contributes to the scarce research on cybersecurity communications on social media and the communication of cybersecurity authorities.

## 5.1 Cybersecurity Authorities and their Mandate to Increase Public Cybersecurity Awareness

We have found that all cybersecurity authorities stick to their mission statements. However, the respective cybersecurity authorities focus on individual aspects of the mission statement. For example, the NCSC focuses on the aspect that it wants to make the UK the safest place to work. This is reflected in the strong focus on economic players. In particular in specific offers and assistance for SMEs to better protect themselves against cybersecurity threats. CISA intends to create a secure infrastructure that people in the U.S. can rely on. It is, therefore, hardly surprising that citizens are hardly addressed with LinkedIn communication. Rather, it seems to be about empowering actors responsible for the aforementioned infrastructures to establish and maintain secure infrastructures. However, it is striking that more than half of all contributions are used for self-marketing. This may be because CISA wants to communicate its positions and statements, which indirectly also contain tips for establishing secure structures but are not aimed at specific players. With its mission statement, the BSI addresses the general public and economic players and sees itself as an enabler of secure digital transformation. This approach is also reflected in the organization's LinkedIn communication, as business players and citizens are the most frequently mentioned stakeholders. Regarding the topics addressed, there is also a mix of publications for the specialist community and general advice on protecting yourself from risks. The results presented make it clear that the social media communication of the cybersecurity authorities examined differs significantly from the media coverage on the topic of cybersecurity that has been examined more frequently to date. The thematic focus (RQ1.1.), which on LinkedIn is strongly on self-marketing and general information on cybersecurity topics without any recognizable current reference, is less characterized by current events than in the media coverage [2, 9, 13]. However, there is also a difference to previous studies within media coverage with regard to the portrayal of those responsible for implementing cybersecurity measures. The focus is much more on companies or economic actors than on private individuals [12, 44]. As a study [40] has shown, LinkedIn per se is suitable for efficiently supporting knowledge building. However, LinkedIn is primarily a business network. In other words, people act in their professional context, differentiating it from other social networks. Therefore, LinkedIn seems less suitable for addressing the general population and more suitable for the business sector.

## 5.2 Communication Practices by Cybersecurity Authorities

Our study also provides insights from a risk and crisis communication perspective. It shows that all agencies primarily communicate about risks rather than damage that has already occurred. This underlines the focus on a preventative communication approach and empowering their target groups to protect themselves effectively against cyber threats. This way, the cybersecurity authorities are communicating in line with the definition of risk communication described in section 2.1. Moreover, our analysis of the PMT dimensions suggests that the effectiveness of communication might vary. As previous studies have shown, it is self-efficacy in particular (see, e.g., Boss et al. [10] or Crossler [17, 18]) that has a major influence on the motivation to protect. Using this knowledge, it can be assumed that the communication of the NCSC is most likely to trigger protection motivation and thus encourage people to adopt safer behavior. Slightly more than 20% of the NCSC contributions contain a strongly pronounced threat severity, and even more than 25% contain strongly pronounced self-efficacy elements. The figure for vulnerability is almost 30%, and response efficacy is described as high in almost 40%. At the same time, the countermeasures were presented as having low response costs in 36.6% of the contributions. As slightly less than half (47.9%) did not allow the PMT elements to be coded, these values are also particularly high compared to the other authorities. Therefore, it is expected that the latter two

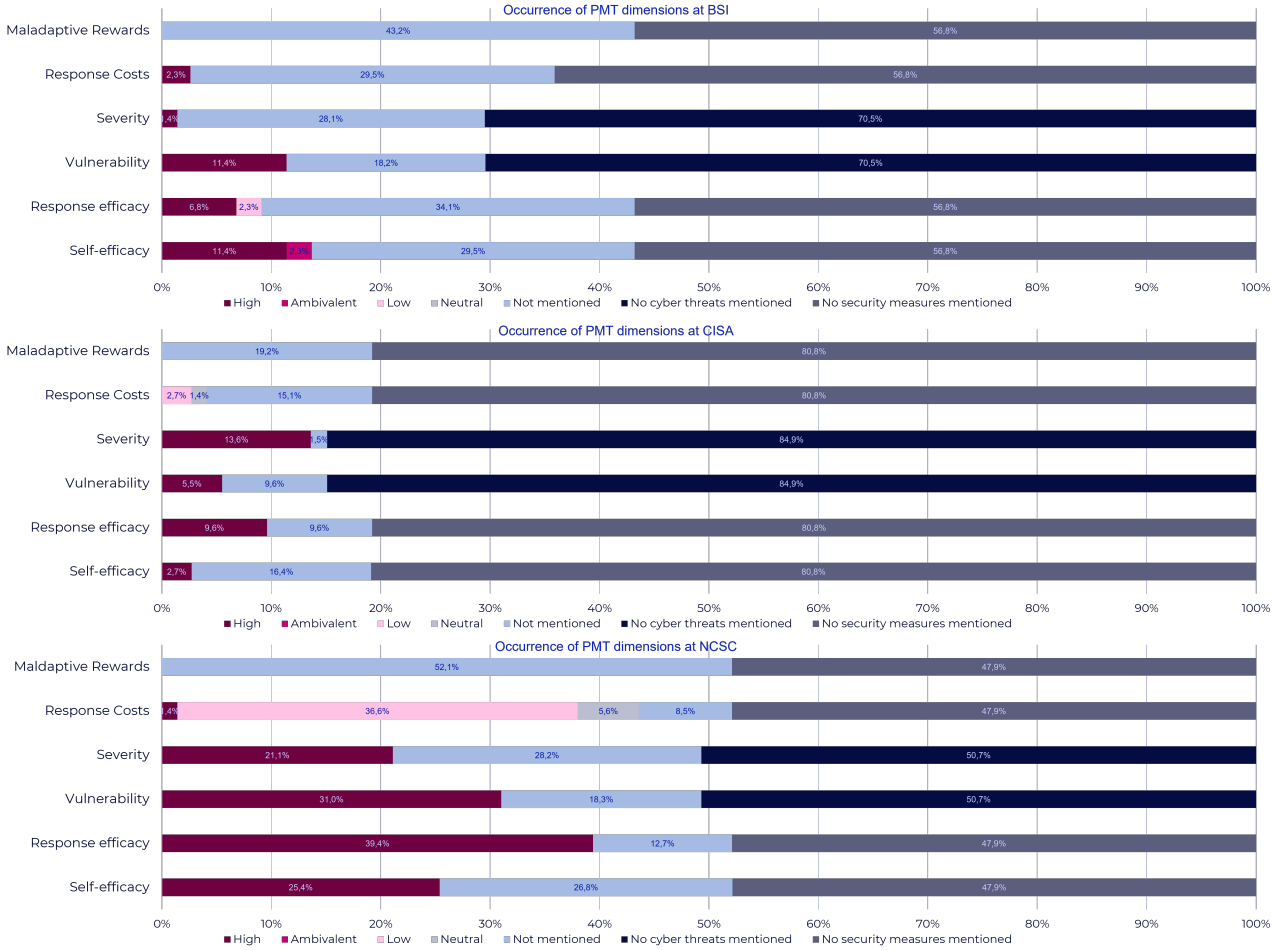



**Figure 8: Occurrence of PMT dimensions per cybersecurity authority, own illustration**

cybersecurity authorities have a significantly weaker effect on the recipients' motivation to protect themselves. As outlined, the NCSC makes the greatest use of the theoretical guidelines for PMT. It is striking that this is achieved even though the posts are the shortest on average. At the same time, user engagement is also lowest in the NCSC posts. The NCSC has the lowest average likes (median likes 121.7), shares (median shares 24.71) and comments (median comments 3.28). The reasons for this warrant further research on the relationship between different types of messaging and social media engagement. Our study is the first to contribute comparative data on cybersecurity authorities' social media communication and offers insights on different risk communication aspects.

## 5.3 Recommended Actions for Cybersecurity Authorities

Based on our findings, we have formulated some specific recommendations for the communication of cybersecurity authorities on LinkedIn. Among other things, these relate to the fit between the topics discussed and the target group on LinkedIn. LinkedIn is primarily a social business network, so this should be considered when choosing topics. It is expected that posts for business professionals, in particular, can have a greater impact than posts aimed at the general public. Social networks such as Facebook or Instagram are expected to have a better chance of raising awareness among the general public and motivating them to behave accordingly. Therefore, cybersecurity authorities should analyze their followers to offer tailored communication content. This applies to LinkedIn as well as other social networks.

By incorporating all PMT dimensions, these agencies can enhance communication, promote protective behaviors, and improve cybersecurity awareness. Next to threat appraisal, coping appraisal has to be included in the communication.We can see from our manual content analysis in section 4.2 that the focus of each agency should be less on engagement with the post but rather on concrete warnings and safety measures as well as the costs of an incident to reduce the risks that are described. However, each agency must walk a tightrope as they are publicly funded but still need to follow the reach paradigms of LinkedIn. Agencies should ensure that they

increase the quality of their postings regarding PMT to increase persuasive messages that potentially invoke better security decisions in their followers and a general audience.

In addition, a general observation was made as part of the manual quantitative content analysis. This concerns the wording and language of the postings. Some of the information was very technical. This makes it difficult to understand, especially for people without an IT background, and makes useful information less accessible. Social media managers should be careful with the wording, to ensure that information is understandable for a wide audience.

## 6 LIMITATIONS & FUTURE WORK

One limitation is that we only selected one sample month for the manual quantitative content analysis. A comparison of several months and even years could be a useful expansion stage. Considering correlations of specific kinds of posts with other variables would be interesting. For example: *Do the thematic focuses of the authorities correlate with the mentioning of cybersecurity measures? Do posts containing more PMT dimensions lead to higher engagement of the users?* Another limitation is that the three authorities we investigated are from Germany, the UK, and the USA, and thus, these results might contain a cultural bias. However, we believe that our results can be generalized for other organizations with cultural backgrounds or compositions of society. Another shortcoming of our approach is that we did not examine the reception of the posted content and only analyzed one platform. We randomly checked whether the content on LinkedIn was similar to content on other networks. This was partly the case (cf. [34] and [33]). Therefore, we argue that the general postings are not tailored to different audiences. We will address the exceptional shortcomings in future work by evaluating the communication and the reception.

To tackle further limitations future work could focus on privacy communication rather than security communication, as our approach and dataset did not analyze this dimension. Furthermore, a follow-up study should also include a reception analysis so that we gain an understanding of how the messages are understood by stakeholders and the general public. Another interesting future analysis could be the analysis of the comments under each posting. Such an analysis could foster an understanding of how comments add to a constructive argument about topics of cybersecurity. Furthermore, such an analysis could gain an understanding of the effectiveness of each communication strategy.

## 7 CONCLUSION

We found that there are major differences within the communication of the three cybersecurity authorities. NCSC and BSI discuss potential threats within their posts whereas CISA communicated mainly for self-promotion purposes. We also found clear differences in the representation of victims and those responsible for the implementation of measures, which can be strongly derived from the respective mission statements. Based on these results, we recommend tailoring the topics to the needs of the respective target group on the various social media platforms. This can increase the chances that recipients will take notice of the content and be sensitized to the topics in the long term. Another important aspect of going beyond awareness-raising and triggering a protection motivation or even protection behavior can be to incorporate theoretical models, such as PMT, into the creation of communication content. For future research it is imperative to evaluate how communication affects the perception of users. In this way, communication on the increasingly important topic of cybersecurity can be further improved. In view of the increasing number of cybersecurity incidents, this is absolutely essential in order to better protect both society and economic players.

## ACKNOWLEDGMENTS

The authors gratefully acknowledge funding from the *Federal Ministry of Education and Research* (16KIS1647, 16KIS1648, 16KIS1646K "DigiFit"; 16KIS1628K "UbiTrans").

## REFERENCES

[1] Cybersecurity & Infrastructure Security Agency. 2024. About CISA. https://web.archive.org/web/20240531053024/https://www.cisa.gov/about
[2] Mahdi R. Alagheband, Atefeh Mashatan, and Morteza Zihayat. 2020. Time-Based Gap Analysis of Cybersecurity Trends in Academic and Digital Media. *ACM Transactions on Management Information Systems* 11, 4 (2020), 1–20. https://doi.org/10.1145/3389684
[3] Fabian Albrecht. 2023. Bundesamt bestätigt Cyberangriffe auf deutsche Einrichtungen. https://web.archive.org/web/20230210025043/https://www.zeit.de/digital/2023-02/ransomeware-cyberattacken-bundesamt-fuer-sicherheit-in-der-informationstechnik
[4] Mohammed Khaled N Alotaibi. 2020. Employees' interest in professional advancement on LinkedIn increases susceptibility to cyber-social engineering: An empirical test. In *Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings 14*. Springer, 85–96.
[5] Catherine L Anderson and Ritu Agarwal. 2010. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly* (2010), 613–643.
[6] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. 2019. Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? *International Conference on Cyber Security for Sustainable Society (2015)* (2019). https://doi.org/10.48550/ARXIV.1901.02672
[7] Steven M Becker. 2004. Emergency communication and information issues in terrorist events involving radioactive materials. *Biosecurity and bioterrorism: biodefense strategy, practice, and science* 2, 3 (2004), 195–207.
[8] Nick Boase, Mathew White, William Gaze, and Clare Redshaw. 2017. Evaluating the mental models approach to developing a risk communication: a scoping review of the evidence. *Risk analysis* 37, 11 (2017), 2132–2149.
[9] Max. Boholm. 2021. Twenty-Five Years of Cyber Threats in the News: A Study of Swedish Newspaper Coverage (1995–2019). *Journal of Cybersecurity* 7, 1 (2021). https://doi.org/10.1093/cybsec/tyab016
[10] Scott R Boss, Dennis F Galletta, Paul Benjamin Lowry, Gregory D Moody, and Peter Polak. 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly* 39, 4 (2015), 837–864.
[11] Dawn Branley-Bell, Lynne Coventry, Matt Dixon, Adam Joinson, and Pamela Briggs. 2022. Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies* (2022), 1–10. https://doi.org/10.1155/2022/2693080 Edited by Zheng Yan.
[12] Christine Buse and Florian Meissner. 2019. Much Ado about Hacking? How News Media in Germany, the United Kingdom, and the United States Report Cyber Threats. (2019). https://www.giga-net.org/2019symposiumPapers/26_Buse_Meissner_Much-Ado-About-Hacking.pdf
[13] Christine Buse and Florian Meissner. 2023. So bleiben Sie sicher im Cyberspace .... Die Darstellung von Cybersicherheit in deutschen Online-Medien. (2023).
[14] National Cyber Security Center. 2024. About the NCSC. https://web.archive.org/web/20240524083548/https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
[15] Jing Chen. 2020. Risk communication in cyberspace: A brief review of the information-processing and mental models approaches. *Current opinion in psychology* 36 (2020), 135–140.
[16] Vincent T. Covello. 2022. *The Critical Role of Risk, High Concern, and Crisis Communication*. 1–9. https://doi.org/10.1002/9781119081753.ch1
[17] Robert E. Crossler and France Bélanger. 2014. An extended perspective on individual security behaviors. *ACM SIGMIS Database: The DATABASE for Advances in*

*Information Systems* 45, 4 (2014), 51–71. https://doi.org/10.1145/2691517.2691521
[18] Robert E Crossler, James H Long, Tina M Loraas, and Brad S Trinkle. 2014. Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems* 28, 1 (2014), 209–226.
[19] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. (2018), 1–12. https://doi.org/10.1145/3173574.3173575 Edited by Regan L. Mandryk, Mark Hancock, Mark Perry, and Anna L. Cox.
[20] Wes Davis. 2023. MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023. https://web.archive.org/web/20240402202811/https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business
[21] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. 401–415. https://doi.org/10.1109/EuroSP.2019.00037
[22] Amanda J. Dillard, Rebecca A. Ferrer, Peter A. Ubel, and Angela Fagerlin. 2012. Risk perception measures' associations with behavior intentions, affect, and cognition following colon cancer screening messages. *Health Psychology* 31, 1 (2012), 106–113. https://doi.org/10.1037/a0024787
[23] Cassandra E. Dodge, Nathan Fisk, George W. Burruss, Richard K. Moule, and Chae M. Jaynes. 2023. What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology and Public Policy* 22, 4 (2023), 849–868. https://doi.org/10.1111/1745-9133.12641
[24] Judith Donath. 2007. Signals in social supernets. *Journal of computer-mediated communication* 13, 1 (2007), 231–251.
[25] Robert M. Entman. 1993. Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication* 43, 4 (1993), 51–58.
[26] Mats Eriksson. 2024. A Multi-motive Risk Communication Model for "Making" Crisis Preparedness. *Risk and Crisis Communication in Europe: Towards Integrating Theory and Practice in Unstable and Turbulent Times* (2024).
[27] Deborah L. Feltz and Erman Öncü. 2014. Self-Confidence and Self-Efficacy. *Routledge Companion to Sport and Exercise Psychology: Global Perspectives and Fundamental Concepts* (2014), 417–429. https://books.google.de/books?id=_zYsAwAAQBAJ Edited by A.G. Papaioannou and D. Hackfort, ISSP Key Issues in Sport and Exercise Psychology.
[28] Dinei Florêncio, Cormac Herley, and Adam Shostack. 2014. FUD: a plea for intolerance. *Commun. ACM* 57, 6 (jun 2014), 31–33. https://doi.org/10.1145/2602323
[29] Donna L. Floyd, Steven Prentice-Dunn, and Ronald W. Rogers. 2000. A Meta-analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology* 30, 2 (2000), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x
[30] Benjamin Fretwurst. 2015. Reliabilität und Validität von Inhaltsanalysen: Mit Erläuterungen zur Berechnung des Reliabilitätskoeffizienten 'Lotus' mit SPSS. *Qualitätskriterien in der Inhaltsanalyse* (2015), 176–203.
[31] Werner Früh. 2015. *Inhaltsanalyse: Theorie und praxis*. Vol. 2501. utb.
[32] Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L. Mazurek. 2019. The Effect of Entertainment Media on Mental Models of Computer Security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 79–95. https://www.usenix.org/conference/soups2019/presentation/fulton
[33] Bundesamt für Sicherheit in der Informationstechnik. 2024. Facebook Post BSI. https://web.archive.org/web/20240531130836/https://www.facebook.com/bsi.fuer.buerger/posts/pfbid0kingdqi49ddigcqe6tEAp3jY9Uhg7RPMD141hyM5KJWQFuv8KFgDwynt8SgaMdQ2l
[34] Bundesamt für Sicherheit in der Informationstechnik. 2024. LinkedIn Post BSI. https://web.archive.org/web/20240531130734/https://www.linkedin.com/feed/update/urn:li:ugcPost:7143926527129223168/
[35] Bundesamt für Sicherheit in der Informationstechnik. 2024. Warum BSI? https://web.archive.org/web/20240316113601/https://www.bsi.bund.de/DE/Karriere/Warum_BSI/warum_BSI.html
[36] Eva-Maria Griesbacher and Martin Griesbacher. 2020. Cybersecurity im medialen Diskurs. *HMD Praxis der Wirtschaftsinformatik* 57, 3 (June 2020), 584–596. https://doi.org/10.1365/s40702-020-00618-7
[37] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. 2022. Digital Security–A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups. *arXiv preprint arXiv:2212.12964* (2022).
[38] Ionut Ilascu. 2024. Microsoft still unsure how hackers stole MSA key in 2023 Exchange attack. https://web.archive.org/web/20240527174521/https://www.bleepingcomputer.com/news/security/microsoft-still-unsure-how-hackers-stole-msa-key-in-2023-exchange-attack/
[39] K. Krippendorff. 2018. *Content Analysis: An Introduction to Its Methodology*. SAGE Publications. https://books.google.de/books?id=nE1aDwAAQBAJ
[40] Xuguang Li, Andrew Cox, and Zefeng Wang. 2018. How do social network sites support product users' knowledge construction? A study of LinkedIn. *Online Information Review* 42, 3 (2018), 304–323.
[41] LinkedIn. 2024. About LinkedIn. https://web.archive.org/web/20240415051223/https://about.linkedin.com/
[42] LinkedIn. 2024. Community Management API. https://web.archive.org/web/20240521001346/https://developer.linkedin.com/product-catalog/marketing/community-management-api Accessed on April 12th, 2024.
[43] Yannic Meier, Johanna Schäwel, Elias Kyewski, and Nicole C. Krämer. 2020. Applying Protection Motivation Theory to Predict Facebook Users' Withdrawal and Disclosure Intentions. In *International Conference on Social Media and Society* (Toronto, ON, Canada) *(SMSociety'20)*. Association for Computing Machinery, New York, NY, USA, 21––29. https://doi.org/10.1145/3400806.3400810
[44] Florian Meissner, Jan Magnus Nold, Martina Angela Sasse, Rebecca Panskus, and Alexander Wilke. 2024. Encryption doesn't matter': Pitfalls in cybersecurity communications. forthcoming.
[45] Uta Menges, Jonas Hielscher, Laura Kocksch, Annette Kluge, and M. Angela Sasse. 2023. Caring Not Scaring - An Evaluation of a Workshop to Train Apprentices as Security Champions. In *EuroUSEC '23*. Association for Computing Machinery, United States, 237–252. https://doi.org/10.1145/3617072.3617099 The 2023 European Symposium on Usable Security, EuroUSEC 2023 ; Conference date: 16-10-2023 Through 17-10-2023.
[46] Microsoft. 2024. Posts API. https://web.archive.org/web/20240428155927/https://learn.microsoft.com/en-us/linkedin/marketing/community-management/shares/posts-api?view=li-lms-2024-04
[47] Florence Mwagwabi and Jhee Hee Jiow. 2021. Compliance with Security Guidelines in Teenagers: The Conflicting Role of Peer Influence and Personal Norms. *Australasian Journal of Information Systems* 25 (2021). https://doi.org/10.3127/ajis.v25i0.2953
[48] Jason RC Nurse, Sadie Creese, Michael Goldsmith, and Koen Lamberts. 2011. Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. IEEE, 60–68.
[49] Office of the Director of National Intelligence. 2024. Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024. https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf
[50] Douglas Paton, Bruce Parkes, Michele Daly, and Leigh Smith. 2008. Fighting the flu: Developing sustained community resilience and preparedness. *Health Promotion Practice* 9, 4_suppl (2008), 45S–53S.
[51] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.
[52] M Brooke Rogers and Julia M Pearce. 2016. The psychology of crisis communication. *The handbook of international crisis communication research* (2016), 34–44.
[53] Martina Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2023. Rebooting IT Security Awareness - How Organisations Can Encourage and Sustain Secure Behaviours. (2023), 284–265. https://doi.org/10.1007/978-3-031-25460-4_14
[54] Martina Angela Sasse, Jonas Hielscher, Jennifer Friedauer, Uta Menges, and Maximilian Peiffer. 2022. Warum IT-Sicherheit in Organisationen einen Neustart braucht. *Cyber-Sicherheit ist Chefinnen- und Chefsache!* (2022). https://www.researchgate.net/publication/358277373_Warum_IT-Sicherheit_in_Organisationen_einen_Neustart_braucht
[55] Der Spiegel. 2023. Ransomware legt IT-Dienstleister von mehr als 70 Kommunen lahm. https://web.archive.org/web/20240316161434/https://www.spiegel.de/netzwelt/web/suedwestfalen-it-ransomware-legt-dienstleister-von-mehr-als-70-kommunen-lahm-a-dd75ebff-e3d0-4589-803f-c6a8b0faadc4
[56] Roland A. Stürz, Christian Stumpf, Antonia Schlude, Ulrike Mendel, and Danilo Harles. 2023. bidt-Digitalbarometer.international. https://doi.org/10.35067/xypq-kn68
[57] René van 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
[58] Tommy van Steen, Emma Norris, Kirsty Atha, and Adam Joinson. 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity* 6, 1 (2020). https://doi.org/10.1093/cybsec/tyaa019 arXiv:https://academic.oup.com/cybersecurity/article-pdf/6/1/tyaa019/34893191/tyaa019.pdf
[59] Anthony Vance, David Eargle, Kirk Ouimet, and Detmar Straub. 2013. Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment. In *2013 46th Hawaii International Conference on System Sciences*. 2988–2997. https://doi.org/10.1109/HICSS.2013.196
[60] Daniel Vogler and Florian Meissner. 2020. How Users Tweet about a Cyber Attack: An Explorative Study Using Machine Learning and Social Network Analysis. *Journal of Digital Media & Policy* 11, 2 (2020), 195–214. https://doi.org/10.1386/jdmp_00016_1

[61] Jess Warren. 2023. Cyber attack on hospitals impacts 1,130 operations. https://web.archive.org/web/20240712065058/https://www.bbc.com/news/articles/c5114k2zg08o