



This is a repository copy of *Predictors of work-related cyberaggression in a random sample of the Swedish working population*.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/208203/>

Version: Accepted Version

---

**Article:**

Farley, S. [orcid.org/0000-0003-0782-4750](https://orcid.org/0000-0003-0782-4750), Cowen Forssell, R. [orcid.org/0000-0002-3332-8163](https://orcid.org/0000-0002-3332-8163), Holm, K. [orcid.org/0000-0002-2077-0243](https://orcid.org/0000-0002-2077-0243) et al. (1 more author) (2024) Predictors of work-related cyberaggression in a random sample of the Swedish working population. *International Journal of Workplace Health Management*, 17 (1). ISSN 1753-8351

<https://doi.org/10.1108/ijwhm-09-2023-0123>

---

This author accepted manuscript is deposited under a Creative Commons Attribution NonCommercial 4.0 International (<http://creativecommons.org/licenses/by-nc/4.0/>) licence. This means that anyone may distribute, adapt, and build upon the work for non-commercial purposes, subject to full attribution. If you wish to use this manuscript for commercial purposes, please contact [permissions@emerald.com](mailto:permissions@emerald.com)

**Reuse**

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial (CC BY-NC) licence. This licence allows you to remix, tweak, and build upon this work non-commercially, and any new works must also acknowledge the authors and be non-commercial. You don't have to license any derivative works on the same terms. More information and the full terms of the licence here: <https://creativecommons.org/licenses/>

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.



[eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk)  
<https://eprints.whiterose.ac.uk/>

# **Predictors of work-related cyberaggression in a random sample of the Swedish working population**

Samuel Farley<sup>1</sup>, Rebecka Cowen Forssell<sup>2</sup>, Kristoffer Holm<sup>2</sup>, and Hanne Berthelsen<sup>2,3</sup>

<sup>1</sup> Sheffield University Management School, University of Sheffield, UK

<sup>2</sup>Centre for Work Life and Evaluation Studies, Malmö University, Sweden

<sup>3</sup> Faculty of Odontology, Malmö University, Sweden

## **Author Note**

Samuel Farley <https://orcid.org/0000-0003-0782-4750>

Rebecka Cowen Forssell <https://orcid.org/0000-0002-2077-0243>

Kristoffer Holm <https://orcid.org/0000-0002-2077-0243>

Hanne Berthelsen <https://orcid.org/0000-0002-4573-4548>

Author email:

[s.j.farley@sheffield.ac.uk](mailto:s.j.farley@sheffield.ac.uk)

[rebecka.forssell@mau.se](mailto:rebecka.forssell@mau.se)

[kristoffer.holm@mau.se](mailto:kristoffer.holm@mau.se)

[hanne.berthelsen@mau.se](mailto:hanne.berthelsen@mau.se)

**Acknowledgements:** The project was financed by AFA Försäkring (Dnr 190182).

## **Abstract**

**Purpose:** With greater numbers of employees using computer-mediated communication, cyberaggression is becoming a more pressing problem for employees and their organizations. However, whilst a growing body of research illustrates its harmful effects, we know less about the factors that drive its occurrence. We therefore sought to identify factors that increase the risk cyberaggression among employees.

**Methodology:** A random sample of the Swedish working population ( $N = 11,556$ ) were surveyed via Statistics Sweden, which produced a final sample of  $N = 2,847$  (response rate = 24.6%).

**Findings:** Logistic regression analysis showed that emotionally demanding work, availability expectations, low perceived work quality, public sector work, and being in a managerial position were related to higher levels of experienced cyberaggression. In addition, exploratory analyses indicated that some of these factors were more strongly related to cyberaggression enacted by organizational insiders compared to organizational outsiders.

**Originality:** Together our findings suggest that situational factors are stronger antecedents of cyberaggression victimization than personal factors. This has implications for organizations, as practical steps can be taken to reduce cyberaggression among employees.

**Keywords:** cyberaggression, general aggression model, antecedents, organizational outsiders, computer-mediated communication.

## 1. Introduction

According to a recent survey, 41% of U.S. adults have experienced some form of online abuse (Pew Research Center, 2021). For some individuals, this abuse is confined to their private lives, however many people experience it in relation to their work (e.g. Posetti et al., 2021). With the increase in virtual working since the COVID-19, there is a need to identify the main causes of work-related cyberaggression. However, somewhat surprisingly, only a few studies have examined antecedents of cyberaggression among employees (Oksanen et al., 2022; Weatherbee, 2007). This is problematic, as we are lacking an understanding of which antecedents are of greater and lesser importance, which prohibits organizations from taking an evidence-based approach to intervention.

In this study, we address the need for such research by using the General Aggression Model (Anderson & Bushman, 2001) to understand the comparative importance of several different predictors of cyberaggression. By examining predictors together in a large random sample of the Swedish working population, we provide generalizable evidence on which factors are most strongly related to work-related cyberaggression. This is important as existing studies tend to examine one or two predictors in isolation, which limits understanding on their relative strength.

We also seek to determine whether the factors that are linked to cyberaggression from organizational insiders are distinct from those linked to cyberaggression from organizational outsiders. Insider initiated aggression is defined as “*any behavior initiated by employees that is intended to harm an individual within their organization or the organization itself and that the target is motivated to avoid*” (Hershcovis et al., 2007, p. 229). In contrast, outsider aggression involves behavior enacted by people from outside of the organization, such as clients, customers, or members of the public. Our study therefore goes beyond existing research by examining differences in predictors across organizational insiders and outsiders.

This is important to understand as it may affect the nature of intervention efforts. For example, employees who are subjected to social media abuse from the public may require different support to those subjected to email abuse by their colleagues. In the following section, we describe the nature of cyberaggression and the theoretical background of the study.

### *1.1 Theoretical Background*

Cyber mistreatment researchers have differentiated several forms of hostile online behavior, including cyberaggression, cyberbullying, trolling, cyber stalking, and cyber incivility (Vranjes et al., 2020). In this article we focus on cyberaggression as a broad form of cyber mistreatment, defined as “*aggression expressed in a communication between two or more people using information and communications technologies (ICTs), wherein at least one person in the communication aggresses against another in order to effect harm*” (Weatherbee & Kelloway, 2006, p.461). Empirical studies show that cyberaggression is distinct from other forms of workplace mistreatment, including cyberbullying (Farley et al., 2016) and face-to-face aggression (Richard et al., 2020). Cyberbullying refers to an ongoing situation whereby a power differential exists between perpetrator and victim (Platts et al., 2023), whereas cyberaggression is more transient and does not necessarily involve unequal power relations (Vranjes et al., 2018). In addition, cyberaggression encompasses behaviors that are more severe in nature, such as written, graphic, or video insults, manipulations of pictures and videos, identity thefts, and violent threats (Oksanen et al., 2022). This differentiates it from cyber incivility, which involves low intensity behaviors, such as e-mails with a rude and discourteous tone (Lim & Teo, 2009).

Media reports and research findings have highlighted the detrimental impact that work-related cyberaggression can exert on employees and organizations. In April 2023,

Nature reported that 39% of climate scientists had experienced cyberaggression in relation to their work, with many reporting that it affected their sleep, productivity, and anxiety levels (Vidal Valero, 2023). In addition, a UK survey of female journalists found that three quarters had experienced cyberaggression, which had prompted a fifth of them to consider leaving the profession (Tobitt, 2023). These reports emphasize the organizational consequences of cyberaggression in the form of productivity losses and staff turnover. Yet, research findings have also highlighted consequences for employees, as cyberaggression has been linked to psychological stress (Oksanen et al., 2022), counterproductive work behavior (Richard et al., 2020), and diminished psychological health (Ford, 2013). However, relatively few studies have sought to examine predictors of work-related cyberaggression. Weatherbee (2007) found that employees who believed that their organization had a clear, enforceable policy concerning the appropriate use of email experienced less cyberaggression. In addition, Oksanen et al. (2022) found that university personnel who were more active users of traditional and social media were more likely to experience cyberaggression than those who used these media to a lesser extent.

To guide our investigation into the predictors of cyberaggression, we adopt the General Aggression Model (GAM; Anderson & Bushman, 2001), which offers a broad framework through which to understand the situational and personal factors that influence aggressive actions. The GAM describes ‘inputs’ as the biological, environmental, psychological, and social factors that influence aggressive behavior. Two types of inputs are distinguished: *situational factors* are the features of an individual’s situational context that contribute to aggression, such as social climate, or job characteristics. In contrast, *personal factors* are the features of the person that influence victimization, such as sex.

Like Kowalski et al (2014), we use the GAM to examine factors related to victimization, rather than enactment. Therefore, whilst we acknowledge that a range of

factors may lead an individual to enact cyber mistreatment, such as low self-control (Zhang et al., 2022), experiencing mistreatment (Ramos Salazar, 2021), and low empathy (Zych et al., 2019), we focus on factors that increase the risk of individuals becoming victimized. In doing so, we primarily examine work-related predictors for two main reasons. First, theory on why cyber mistreatment occurs has argued that it is primarily driven by work-related stressors, such as job characteristics, organizational change, and ineffective leadership (Vranjes et al., 2017). Second, a focus on work environment predictors facilitates the development of evidence on how organizations can intervene to prevent cyberaggression, as factors such as job characteristics and organizational culture are more malleable than individual personality traits. Below, we review existing research to consider the situational and personal factors that may increase one's risk of experiencing work-related cyberaggression. Given the lack of research into cyberaggression, we draw upon studies on related forms of cyber mistreatment to develop our hypotheses.

### *1.2 Situational Factors*

**Role Conflict.** Role conflict involves the extent to which people experience conflicting demands relating to their work tasks (Burr et al., 2019). Theoretically, role conflict increases stress, withdrawal from work, and conflict with others, all of which can lead an individual to be targeted by aggressive actions (Salin & Hoel, 2020). Role conflict has therefore been linked to the occurrence of traditional bullying (Salin & Hoel, 2020) and cyberbullying (Czakert et al., 2021; Vranjes et al., 2018). In addition, role conflict may be more commonly experienced by virtual workers, as lean forms of media (e.g. email) may inhibit clarity about the nature of work tasks (Daft & Lengel, 1986), thereby enhancing the likelihood of cyberaggression.

Hypothesis 1: Employees who report higher levels of role conflict will experience greater levels of cyberaggression.

**Availability Expectations.** Availability expectations refer to the extent to which an employee is expected to be constantly available and accessible outside of work hours (Day et al., 2012). It has been argued that technology provides perpetrators with greater access to targets, which may increase the likelihood of victimization (Farley et al., 2021). Heightened availability also allows perpetrators to abuse targets at times when they are more likely to engage in aggression, such as after consuming alcohol. Indeed, Zhang et al (2022) found that engaging in technology-mediated work during family time was significantly associated with the enactment of cyberbullying behavior. They argued that access to targets outside of working hours enhanced the likelihood of cyberbullying, as perpetrators were unconstrained by bystanders who might support the target.

Hypothesis 2: Employees who report greater expectations of availability over computer-mediated communication will report experiencing more cyberaggression.

**Quality of Work.** Quality of work refers to the employee's experience of the immediate output of their work, such as the product made, or service accomplished (Burr et al., 2019). It comprises the employee's perceived evaluation of whether they find it possible to perform work of a satisfactory quality within their organization, which may be linked to cyberaggression from both insiders and outsiders. Conflict often occurs when organizational outsiders receive a lower quality product or service than they expect. For example, Spencer et al (2023) reported that patients engaged in cyber incivility towards nurses due to unmet expectations. Being unable to deliver quality can also lead to conflict between employees, particularly when employees seek to scapegoat a colleague when errors or mistakes are made.



Hypothesis 3: Employees who report lower quality work will report experiencing more cyberaggression.

**Emotional Demands.** Emotional Demands involve the extent to which an employee must deal with the emotions of others in their work role (Burr et al., 2019). Being responsible for other peoples' emotions is likely to increase cyberaggression exposure, especially when one must cope with anger. Vranjes et al (2017) note that anger stimulates blame and retaliation, which promotes aggression. This is particularly likely in some online environments (e.g. social media platforms) where intense negative emotions are expressed more overtly, as people have less concern about being negatively evaluated (Derks et al., 2008; Vranjes et al., 2017). Prior research has identified that emotional care provision is a predictor of experiencing workplace violence (LeBlanc & Kelloway, 2002), which tends to be enacted by organizational outsiders, such as customers, inmates, or patients (Barling et al., 2009). A similar trend has been reported in relation to cyber mistreatment, as Spencer et al (2023) found that nurses were subjected to cyber incivility from patients, while D'Souza et al (2022) reported cyberaggression towards caregivers from patients' relatives.

Hypothesis 4: Employees who report greater emotional demands will experience more cyberaggression.

**Sector.** Evidence is accumulating that both traditional and cyber forms of bullying occur to a greater extent in the public sector than the private sector (Ikeda et al., 2022; Zapf et al., 2020). Public sector jobs involve high levels of interdependent work, which may increase the opportunity to attack or negatively evaluate someone else's contribution (Zapf et al., 2020). Working with outsiders is common in public sector jobs such as teaching, healthcare, and social work and research indicates that employees in these professions do encounter cyber abuse from outsiders (e.g. Cassidy et al., 2017; D'Souza et al., 2022; Forssell, 2020b;

Kagan et al., 2018). This may occur because outsiders are unconstrained by the sanctions that insiders face for engaging in abusive acts (Farley et al., 2021) and because some online environments allow outsiders to maintain a sense of anonymity, thus heightening the likelihood of abuse (Vranjes et al., 2017).

Hypothesis 5: Public sector workers will experience greater cyberaggression than private sector workers.

### *1.3 Personal Factors*

**Age.** Mowry and Giumetti (2019) summarized existing findings on how age relates to cyber mistreatment, which highlighted a small significant negative relationship between age and cyberbullying in several studies (Forssell, 2020a; Kowalski et al., 2018; Oksanen et al., 2020). Although there have been fewer studies on cyberaggression, Ford (2013) reported a small, significant negative correlation with age. Together, these findings suggest that younger workers are more likely to experience cyberaggression than older workers. One explanation for these findings is that younger employees spend more time online than older employees (Mowry & Giumetti, 2019), which increases the likelihood of experiencing cyberaggression.

Hypothesis 6: Younger workers will report experiencing more cyberaggression than older workers.

**Sex.** Several studies on workplace cyberbullying report that males are exposed to more cyberbullying behavior than females (Forssell, 2016; 2020a; Choi & Park, 2019; Vranjes et al., 2018). A similar pattern of results is observed in studies on cyber incivility (Krishnan, 2016; Wang et al., 2022). It is not clear why men might experience more cyber mistreatment than women, although one possible explanation is that men are involved in more online conflicts than women, and therefore both enact and experience more cyberaggression.

Hypothesis 7: Males will report experiencing more cyberaggression than females.

**Managerial position.** Research consistently reports that managerial staff experience more cyber mistreatment than non-managers (Forssell, 2016; Gardner et al., 2016; Ikeda et al., 2022; Oksanen et al., 2022). This is a curious finding, as managers are typically in positions of power within organizations. However, it has been suggested that disgruntled employees may vent frustrations with their managers on social media websites (Farley et al., 2021). Managers may also face cyberaggression from outsiders by virtue of their role as the face of the organization. For example, Forssell (2020b) highlights the experience of a school leader who was subjected to cyberbullying by dissatisfied parents on a social media website.

Hypothesis 8: Managers will experience more cyberaggression than non-managers.

## **2. Method**

The data were collected using a survey that sought to validate the third version of the Copenhagen Psychosocial Questionnaire (COPSOQ) in Sweden (for full details see Berthelsen et al, 2020). The data were collected between September and November 2018 from a random sample of 11,556 employees via Statistics Sweden (SCB). A total of 3,642 (30.9%) people responded to the cross-sectional survey. However, to be included in the final sample, respondents needed to be 25–65-year-old workers living in Sweden, who had a colleague, and who had worked for at least three months prior to completing the survey. The three-month working criterion was necessary so that participants had sufficient experience of work to provide informed responses to the study measures. The criterion of having a colleague was adopted to ensure that employees could provide an indication of whether they had experienced insider-enacted cyberaggression. Finally, the age range criterion was initially 20-65-year-olds, however the response rate among the 20–24-year-olds was low, and a high proportion of this age group remained in higher education, therefore a decision was made to

exclude this age group from further analyses (Berthelsen et al, 2020). After applying these inclusion criteria, a final sample of  $N = 2,847$  was obtained. Of the 2,847 respondents, 56% were female, their mean age was 47.7 (SD = 10.8), and the most common occupational group was professionals (35%). Most respondents either worked in the private sector (47.1%), or the public sector (44.7%) and the majority worked over 30 hours per week (88.6%). The Regional Ethical Review Board of Sweden approved the study (Dnr 2018–392).

### *2.1 Measures*

**Work-related cyberaggression.** Cyberaggression was measured with a single item from COPSOQ III (Berthelsen et al, 2020; Burr et al., 2019): *'Have you been exposed to work-related harassment on the social media (e.g. Facebook), by e-mail or text messages during the last 12 months?'*. In the COPSOQ III survey (Berthelsen et al, 2020), the item is labelled as a measure of cyberbullying, however given that it makes no reference to repetition or power imbalance, we concluded that it is a more valid measure of cyberaggression. As part of the item validation process, cognitive interviews were held with 36 potential respondents from the target group to clarify how different measures were interpreted by the respondents. The interviews revealed that participants considered whether they had been exposed to severe forms of harassment online when answering the item, but they did not consider low level forms of cyber mistreatment (e.g. cyber incivility). The response options were Yes, daily (100); Yes, weekly (75); Yes, monthly (50); Yes, a few times (25); and No (0). Following exposure to this item, participants then answered a second item, which asked *'If yes, from whom? (You may tick off more than one)'*. The response options for this second item were Colleagues; Manager/superior; Subordinates; and Clients/customers/patients.

Role conflict, quality of work, and emotional demands were operationalised using the Swedish standard version of COPSOQ III (Berthelsen et al, 2020; Burr et al, 2019). The

COPSOQ items have five response options on Likert-type scales, which for statistical analyses were scored 0, 25, 50, 75, 100. Scale scores were computed as means of items (range of 0–100), and the scale score was set to missing if respondents had replied to less than half of the items included in the scale.

**Role Conflict.** Role conflict was measured using a three-item scale. A sample item is *‘Are contradictory demands placed on you at work?’*. The response options were: To a very large extent; To a large extent; Somewhat; To a small extent; and To a very small extent. The Cronbach’s alpha of the scale was 0.71 and higher scores represented greater levels of role conflict.

**Quality of Work.** Quality of work was measured with a two-item scale. A sample item is *‘To what extent do you find it possible to perform your work tasks at a satisfactory quality?’*. The response options were: To a very large extent; To a large extent; Somewhat; To a small extent; and To a very small extent. The Cronbach’s alpha was 0.69 and higher scores indicated perceptions of engaging in higher quality work.

**Emotional demands.** Emotional demands were measured using a three-item scale. A sample item is *‘Do you have to deal with other people’s personal problems as part of your work?’*. The response options were: Always; Often; Sometimes; Seldom; and Never/hardly ever. The Cronbach’s alpha of the measure was 0.86 and higher scores on this variable represented greater emotional demands.

**Availability Expectations.** Availability expectations were measured using two-items from the Swedish Labor Inspection’s 2017 work environment survey (Arbetsmiljön 2017). A sample item is *‘Does your employer expect you to read work-related e-mail during leisure time?’*. The response options were: Always; Often; Sometimes; Seldom; Never/Almost Never. The Cronbach’s alpha of the scale was 0.83 and higher scores indicated greater

availability expectations. The scale score was computed in the same way as the COPSOQ scales.

The demographic factors of sector, sex, and managerial position were all measured using single items. For sector, the response options were 'private', 'public', and 'other'. For sex, the response options were 'male' and 'female'. For managerial position, the response options were 'manager' and 'non-manager'. Age was assessed in two ways, firstly as a continuous variable that was used in the inferential analyses, however it was also assessed using a set of four response options which were 25-35 years, 36-45 years, 46-55 years, 56-65 years. The information gathered from these response options was used to provide descriptive information (see tables 1 and 4).

## *2.2 Data analyses*

The analytical procedure involved three steps. In the first step, descriptive statistics and intercorrelations between the study variables were calculated. In the second step, a binary logistic regression model was estimated to explore the associations between situational factors, personal factors, and exposure to cyberaggression. In the final step, exploratory analyses were conducted to explore differences in predictors for insider- and outsider-instigated cyberaggression.

An initial exploration of the data revealed that the prevalence of cyberaggression in the sample was low, with only 79 respondents (2.8%) reporting some experience of it. Of these, 1 had experienced it daily, 0 experienced it weekly, 4 had experienced it monthly, and 74 had experienced it a few times. Given the lack of variance across the response categories, the responses were collapsed into a single category representing all those who had been exposed to cyberaggression. To test the study hypotheses, the associations between the predictors and cyberaggression were then calculated as odds ratios (ORs) with 95%

confidence intervals (CIs). Traditionally, variables such as age, sex, and sector are usually treated as control variables when examining antecedents of workplace mistreatment. However, in the current study these variables were examined as predictors, which meant that we did not control for any variables in the analyses as there was no theoretical rationale for doing so (Bernierth & Aguinis, 2016). Given the absence of relevant control variables, we computed a single logistic regression model in which all the predictors were entered simultaneously. The work environment predictors in this model mostly came from the COPSOQ questionnaire where scales are scored from 0-100. Therefore, the ORs are shown for 10-point differences in scale scores, as a change of 5-10 points is considered meaningful when working practically with the COPSOQ measures (Pejtersen et al., 2010).

To address the research question of whether the predictors of insider-enacted cyberaggression differ from the predictors of outsider-enacted cyberaggression, we conducted a set of exploratory analyses. We first examined whom the respondents reported as perpetrators of cyberaggression, which revealed that 12 participants (15.2% of targets) experienced it from a manager, 24 (30.4%) experienced it from colleagues, 9 (11.4%) experienced it from a subordinate, and 43 (54%) experienced it from clients, customers, or patients. We then used information on the perpetrators of cyberaggression to create two new variables. These variables represented (1) individuals who had only experienced cyberaggression from organizational insiders (comprising those who had experienced it from managers, colleagues, and subordinates) and (2) individuals who had only experienced cyberaggression from organizational outsiders (i.e. from clients, customers, and patients). Individuals who reported experiencing cyberaggression from both insiders and outsiders were not included in either variable, however only 5 (6.3%) of the 79 cyberaggression targets reported dual exposure. In addition, one respondent did not state the identity of the perpetrator and consequently they were also not included in either variable. In total, 35

(44.3%) of the 79 cyberaggression targets were only exposed to insider-initiated cyberaggression, while 38 (48.1%) of the 79 were only exposed to outsider-initiated cyberaggression.

To understand whether the categorical predictors differed in relation to insider- and outsider initiated cyberaggression, we conducted a series of chi-square tests. These sought to identify whether there were significant predictors of insider-initiated cyberaggression, which were non-significant for outsider-initiated cyberaggression, and vice versa. To understand whether the continuous predictors differed in relation to insider and outsider initiated cyberaggression, we explored a series of spearman's correlations that showed how the predictors related to insider and outsider initiated cyberaggression. Spearman's correlations were adopted instead of Pearson's correlations due to the non-normal distribution of the cyberaggression variables. In the exploratory analyses, the 5 respondents reporting exposure from both insiders and outsiders and the single respondent who did not report perpetrator were excluded. Statistical analyses were conducted using SPSS Statistics version 28.

### **3. Results**

The 12-month prevalence rate for exposure to cyberaggression was 2.8% (n=79), with the results for different subgroups detailed in Table 1. Cyberaggression was more common among public sector employees and managers, with no statistically significant differences in relation to age or sex. Bivariate Spearman's correlations between cyberaggression and the continuous predictor variables of age, role conflict, availability expectations, emotional demands, and quality of work can be seen in Table 2, which shows small significant relationships between cyberaggression and all predictors, apart from age. Spearman's correlations were adopted due to the non-normally distributed cyberaggression variable.

Insert Table 1 Here



Insert Table 2 Here

Logistic regression was used to analyze the relationship between situational factors, personal factors and cyberaggression. Table 3 shows the results of the binary logistic regression analysis. Hypothesis 1 was not supported as role conflict was not significantly related to cyberaggression (OR = .90,  $p = .21$ ). However, both high availability expectations (OR = 1.12,  $p < .05$ ) and low quality of work (OR = .82,  $p < .01$ ) were significantly linked with cyberaggression, which supports hypotheses 2 and 3. In support of hypothesis 4, we found that emotional demands were significantly positively associated with cyberaggression (OR = 1.16,  $p < .05$ ). This result should be interpreted in the way that when holding all other predictor variables constant, the odds of exposure to cyberaggression increased by 16 percent (95% CI 1.02-1.31) for a 10-point increase in emotional demands (on a scale ranging 0-100). Sector was also shown to be a significantly linked to cyberaggression (OR = 2.66,  $p < .01$ ), with employees in the public sector experiencing cyberaggression more often, which provides support for hypothesis 5. Together these results suggest that situational factors play an important role in shaping whether an individual experiences cyberaggression.

Insert Table 3 Here

When considering the personal factors, we found that age (OR = .99,  $p = .34$ ) and sex (OR = 1.35,  $p = .28$ ) were non-significantly associated with cyberaggression, therefore hypotheses 6 and 7 were not supported. However, in support of hypothesis 8, managerial position was significantly linked to cyberaggression (OR = 1.77,  $p < .05$ ), with managers being more likely to experience it than non-managers.

### *3.1 Exploratory analyses*

Table 4 shows that age, sex, and managerial status did not separately influence insider nor outsider initiated cyberaggression. In contrast, public sector employees were exposed to

outsider-initiated cyberaggression  $\chi^2 = (1) 5.80, p < .05$  more often than private sector employees. The same tendency was seen for insider-initiated cyberaggression but did not reach statistical significance ( $p = 0.07$ ). Spearman's correlations were calculated to examine how the continuous predictors were related to insider and outsider cyberaggression (see Table 5). These correlations showed that role conflict, availability expectations, and quality of work were significantly associated with insider-initiated cyberaggression, but not outsider-initiated cyberaggression. In contrast, emotional demands were significantly associated with both insider-initiated and outsider-initiated cyberaggression.

Insert Table 4 Here

Insert Table 5 Here

#### **4. Discussion**

Understanding what makes employees vulnerable to cyberaggression is important given the increase in virtual forms of working since the COVID-19 pandemic. Our findings indicate that employees may be more at risk of cyberaggression when they hold a managerial position, are responsible for the emotions of others, work in the public sector, do not have working conditions where they can produce quality work, and are expected to be constantly available over technology.

Similar to other studies of cyber mistreatment (Forssell, 2016; Ikeda et al., 2022; Oksanen et al., 2022), we found that managers experienced cyberaggression to a greater extent than non-managers. We also found that availability expectations and perceived quality of work are significantly related to cyberaggression. As far as we are aware, these factors do not commonly predict exposure to face-to-face aggression, which means that those responsible for virtual workers need to be aware that these variables may increase the risk of cyberaggression exposure. Interestingly, we found that role conflict was unrelated to

cyberaggression, but existing studies show that this is a prominent antecedent of workplace bullying (Salin & Hoel, 2020). As such, it seems that certain factors are more important predictors of aggression in the offline context than the online context, and vice versa. Nevertheless, working in the public sector and engaging in emotionally demanding work are antecedents of face-to-face aggression (LeBlanc & Kelloway, 2002; Zapf et al., 2020), and they were also significantly associated with cyberaggression in the current study. This highlights the need for theory development on which antecedents have greater weight in the online and offline contexts, as well as which antecedents are important in both contexts.

Our study also explored whether the predictors of cyberaggression varied according to the perpetrator's status as an organizational insider or outsider. We found that role conflict, availability expectations, and quality of work were linked to cyberaggression from insiders, but not outsiders. In contrast, emotional demands were linked to cyberaggression from both sources. These analyses were exploratory and thus should be interpreted with some caution, nevertheless they highlight factors that may be relevant depending on the extent to which employees work with insiders or outsiders. For example, if employees rarely work with organizational outsiders, organizations may be able to minimise the extent to which they experience cyberaggression by providing role clarity, conditions for good quality work, and by limiting availability expectations. Interestingly, we found that there was an almost equal split between those who had experienced cyberaggression from insiders compared to outsiders. This highlights that cyberaggression is not a problem that is confined to one specific source but occurs equally across insiders and outsiders.

#### *4.1 Limitations*

A few limitations should be acknowledged. First, we used a single item to capture exposure to cyberaggression, which may have resulted in lower reliability and a less fine-

grained assessment of the construct (Allen et al., 2022). However, in recent years it has been recognised that single items have considerable advantages, including reducing the burden on participants and providing high levels of face validity (Fisher et al., 2016). As part of the validation of the COPSOQ instrument (Berthelsen et al., 2020), interviews were undertaken with participants to understand their reaction to the cyberaggression item, which corroborated face validity. This study also provided evidence of the criterion validity of the item, as most study hypotheses were supported, which indicates that the relationship between the measure and other variables is generally as expected. Given that single item measures have produced equivalent results to multiple-item scales in meta-analyses (Ang & Eisend, 2018), we felt that the use of a single item in this circumstance was warranted, particularly given its use in a widely distributed national survey. A second limitation concerns the cross-section nature of the study, which means that alternative explanations for the findings should be considered, in that cyberaggression may predict the personal and situational factors explored within the study. Future longitudinal research is therefore needed to determine the direction of causality between these variables, and we also encourage researchers to examine a broader array of antecedents than those examined in this study. We predominantly examined work environment predictors of cyberaggression, however there is a need to examine a broader array of predictors, including personal predictors of cyberaggression enactment and exposure. A third limitation concerns the relatively low number of people who were subjected to cyberaggression, which limited statistical power, particularly for the insider-outsider analyses. The low prevalence rate indicates that cyberaggression is likely to be an uncommon phenomenon, particularly in Swedish workplaces. Nevertheless, our study indicates that certain situational factors could be important determinants of exposure and there is a need to investigate these relationships in larger samples. Finally, it should be noted that imbalanced data sets may lead to biased estimates in logistic regression models. However, such bias has

not been found to be substantial when there are approximately 10 observed outcomes for each predictor variable in the model (Vittinghoff & McCulloch, 2006), which was the case in the present study.

#### *4.2 Practical implications*

Our findings have clear practical implications, as organizations can directly intervene to reduce employees' availability expectations and to increase conditions for high quality of work. Regarding the former, organizations can implement clear boundaries regarding working time that stipulate when an employee is no longer expected to respond to work communications. To further solidify these boundaries, employees could set out of hours emails to emphasize that they are unavailable during non-work hours. Improving the quality of work may be more challenging, as this may depend on uncontrollable factors, such as demand for products and services, or the availability of staff. Nevertheless, public facing organizations such as hospitals and airports often make clear to members of the public that abuse towards staff will not be tolerated using posters, or other communications. These communications could be extended to cover online abuse, such as UEFA's 'real scars' advertising campaign which seeks to reduce the abuse directed toward football players and officials over social media. This makes clear that aggression is not a legitimate response when people feel that they have not received a quality product or service.

#### *4.3 Conclusion*

The COVID-19 pandemic has accelerated the use of virtual working. As a result, organizations need to be aware of factors that may increase the risk of cyberaggression. Our study sheds light on possible risk factors, which has implications for organizations as practical steps can be taken to limit the risk of cyberaggression among employees.

## References

- Allen, M. S., Iliescu, D., & Greiff, S. (2022). Single Item Measures in Psychological Science: A Call to Action. *European Journal of Psychological Assessment*, 38(1), 1-5.  
<https://psycnet.apa.org/doi/10.1027/1015-5759/a000699>
- Anderson, C. A., & Bushman, B. J. (2002). Human aggression. *Annual Review of Psychology*, 53(1), 27-51. <https://doi.org/10.1146/annurev.psych.53.100901.135231>
- Ang, L., & Eisend, M. (2018). Single versus multiple measurement of attitudes: A meta-analysis of advertising studies validates the single-item measure approach. *Journal of Advertising Research*, 58(2), 218-227. <https://psycnet.apa.org/doi/10.2501/JAR-2017-001>
- Arbetsmiljön. (2017). *The Swedish Work Environment Authority. The Work Environment 2017*. The Swedish Work Environment Authority: Stockholm, Sweden, 2018.  
<https://www.av.se/globalassets/filer/statistik/arbetsmiljon-2017/arbetsmiljostatistik-arbetsmiljon-2017-rapport-2018-2.pdf>
- Barling, J., Dupré, K. E., & Kelloway, E. K. (2009). Predicting workplace aggression and violence. *Annual Review of Psychology*, 60, 671-692.  
<https://doi.org/10.1146/annurev.psych.60.110707.163629>
- Bernerth, J. B., & Aguinis, H. (2016). A critical review and best-practice recommendations for control variable usage. *Personnel Psychology*, 69(1), 229-283.  
<https://doi.org/10.1111/peps.12103>
- Berthelsen, H., Westerlund, H., Bergström, G., & Burr, H. (2020). Validation of the Copenhagen psychosocial questionnaire version III and establishment of benchmarks for psychosocial risk Management in Sweden. *International Journal of Environmental Research and Public Health*, 17(9), 3179. <https://doi.org/10.3390/ijerph17093179>

- Burr, H., Berthelsen, H., Moncada, S., Nübling, M., Dupret, E., Demiral, Y., Oudyk, J., Kristensen, T.S., Llorens, C., Navarro, A., Lincke, H.J., Bocéréan, C., Sahan, C., Smith, P., & Pohrt, A. (2019). The third version of the Copenhagen psychosocial questionnaire. *Safety and Health at Work*, 10(4), 482-503.  
<https://doi.org/10.1016/j.shaw.2019.10.002>
- Cassidy, W., Faucher, C., & Jackson, M. (2017). Adversity in university: Cyberbullying and its impacts on students, faculty and administrators. *International Journal of Environmental Research and Public Health*, 14(8), 888.  
<https://doi.org/10.3390/ijerph14080888>
- Choi, J., & Park, M. (2019). Effects of nursing organisational culture on face-to-face bullying and cyberbullying in the workplace. *Journal of Clinical Nursing*, 28(13-14), 2577-2588. <https://doi.org/10.1111/jocn.14843>
- Czakert, J. P., Reif, J., Glazer, S., & Berger, R. (2021). Adaptation and psychometric cross-cultural validation of a workplace cyberbullying questionnaire in Spain and Germany. *Cyberpsychology, Behavior, and Social Networking*, 24(12), 831-838.  
<https://doi.org/10.1089/cyber.2020.0856>
- Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, 32, 554-571.  
<https://doi.org/10.1287/mnsc.32.5.554>
- Day, A., Paquet, S., Scott, N., & Hambley, L. (2012). Perceived information and communication technology (ICT) demands on employee outcomes: the moderating effect of organizational ICT support. *Journal of Occupational Health Psychology*, 17(4), 473. <https://psycnet.apa.org/doi/10.1037/a0029837>

Derks, D., Fischer, A. H., & Bos, A. E. (2008). The role of emotion in computer-mediated communication: A review. *Computers in Human Behavior*, 24(3), 766-785.

<https://doi.org/10.1016/j.chb.2007.04.004>

D'Souza, N., Catley, B., Tappin, D., & Forsyth, D. (2022). 'You live and breathe it...': Exploring experiences of workplace cyberbullying among New Zealand nurses. *Journal of Management & Organization*, 28(2), 329-347.

<https://doi.org/10.1017/jmo.2019.71>

Farley, S., Coyne, I., Axtell, C., & Sprigg, C. (2016). Design, development and validation of a workplace cyberbullying measure, the WCM. *Work & Stress*, 30(4), 293-317.

<https://doi.org/10.1080/02678373.2016.1255998>

Farley, S., Coyne, I., & D'Cruz, P. (2021). Cyberbullying at work: Understanding the influence of technology. In P. D'Cruz, E. Noronha, G. Notelaers, & C. Rayner (Eds.), *Concepts, approaches and methods. Handbooks of workplace bullying, emotional abuse and harassment* (1st ed., pp. 1–31). Singapore: Springer.

[https://doi.org/10.1007/978-981-13-0134-6\\_8](https://doi.org/10.1007/978-981-13-0134-6_8)

Fisher, G. G., Matthews, R. A., & Gibbons, A. M. (2016). Developing and investigating the use of single-item measures in organizational research. *Journal of Occupational Health Psychology*, 21(1), 3-23.

<https://psycnet.apa.org/doi/10.1037/a0039139>

Ford, D. P. (2013). Virtual harassment: media characteristics' role in psychological health. *Journal of Managerial Psychology*, 28(4), 408-428.

<https://doi.org/10.1108/JMP-12-2012-0398>

Forsell, R. (2016). Exploring cyberbullying and face-to-face bullying in working life—Prevalence, targets and expressions. *Computers in Human Behavior*, 58, 454-460.

<https://doi.org/10.1016/j.chb.2016.01.003>



- Forssell, R. C. (2020a). Gender and organisational position: predicting victimisation of cyberbullying behaviour in working life. *International Journal of Human Resource Management*, 31(16), 2045-2064. <https://doi.org/10.1080/09585192.2018.1424018>
- Forssell, R. C. (2020b). Cyberbullying in a boundary blurred working life: Distortion of the private and professional face on social media. *Qualitative research in organizations and management: An international journal*, 15(2), 89-107. <https://doi.org/10.1108/QROM-05-2018-1636>
- Gardner, D., O'Driscoll, M., Cooper-Thomas, H. D., Roche, M., Bentley, T., Catley, B., ... & Trenberth, L. (2016). Predictors of workplace bullying and cyber-bullying in New Zealand. *International Journal of Environmental Research and Public Health*, 13(5), 448. <https://doi.org/10.3390/ijerph13050448>
- Hershcovis, M. S., & Barling, J. (2010). Towards a multi-foci approach to workplace aggression: A meta-analytic review of outcomes from different perpetrators. *Journal of Organizational Behavior*, 31(1), 24-44. <https://doi.org/10.1002/job.621>
- Hershcovis, M. S., Turner, N., Barling, J., Arnold, K. A., Dupré, K. E., Inness, M., LeBlanc, M. M., & Sivanathan, N. (2007). Predicting workplace aggression: A meta-analysis. *Journal of Applied Psychology*, 92(1), 228-238 <https://psycnet.apa.org/doi/10.1037/0021-9010.92.1.228>
- Ikeda, T., Hori, D., Sasaki, H., Komase, Y., Doki, S., Takahashi, T., Oi, Y., Ikeda, Y., Arai, Y., Muroi, K. & Sasahara, S. (2022). Prevalence, characteristics, and psychological outcomes of workplace cyberbullying during the COVID-19 pandemic in Japan: a cross-sectional online survey. *BMC Public Health*, 22(1), 1-18. <https://doi.org/10.1186/s12889-022-13481-6>

- Kagan, M., Orkibi, E., & Zychlinski, E. (2018). 'Wicked', 'deceptive', and 'blood sucking': Cyberbullying against social workers in Israel as claims-making activity. *Qualitative Social Work*, 17(6), 778-794. DOI: 10.1177/1473325017694952
- Krishnan, S. (2016). Electronic warfare: A personality model of cyber incivility. *Computers in Human Behavior*, 64, 537-546. <https://doi.org/10.1016/j.chb.2016.07.031>
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073-1137.  
<https://psycnet.apa.org/doi/10.1037/a0035618>
- Kowalski, R. M., Toth, A., & Morgan, M. (2018). Bullying and cyberbullying in adulthood and the workplace. *The Journal of Social Psychology*, 158(1), 64-81.  
<https://doi.org/10.1080/00224545.2017.1302402>
- LeBlanc, M. M., & Kelloway, E. K. (2002). Predictors and outcomes of workplace violence and aggression. *Journal of Applied Psychology*, 87(3), 444-453.  
<https://psycnet.apa.org/doi/10.1037/0021-9010.87.3.444>
- Lim, V. K., & Teo, T. S. (2009). Mind your E-manners: Impact of cyber incivility on employees' work attitude and behavior. *Information & Management*, 46(8), 419-425.  
<https://doi.org/10.1016/j.im.2009.06.006>
- Mowry, N. L., & Giumetti, G. W. (2019). Cyberbullying in the workplace: Developmental perspectives. In Giumetti GL and Kowalski RM (eds) *Cyberbullying in Schools, Workplaces, and Romantic Partnerships*. New York: Routledge, pp. 118–134

- Oksanen, A., Celuch, M., Latikka, R., Oksa, R., & Savela, N. (2022). Hate and harassment in academia: the rising concern of the online environment. *Higher Education*, 84(3), 541-567. <https://doi.org/10.1007/s10734-021-00787-4>.
- Oksanen, A., Oksa, R., Savela, N., Kaakinen, M., & Ellonen, N. (2020). Cyberbullying victimization at work: Social media identity bubble approach. *Computers in Human Behavior*, 109, 106363.
- Pejtersen, J. H., Bjorner, J. B., & Hasle, P. (2010). Determining minimally important score differences in scales of the Copenhagen Psychosocial Questionnaire. *Scandinavian Journal of Public Health*, 38(3 Suppl), 33-41. <https://doi.org/10.1177/1403494809347024>
- Pew Research Center. (2021). *The state of online harassment*. Pew Research Center. <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>.
- Platts, J., Coyne, I., & Farley, S. (2023). Cyberbullying at work: an extension of traditional bullying or a new threat?. *International Journal of Workplace Health Management*, (16) 2/3, 173-187. <https://doi.org/10.1108/IJWHM-07-2022-0106>
- Posetti, J., Shabbir, N., Maynard, D., Bontcheva, K., & Aboulez, N. (2021). The chilling: Global trends in online violence against women journalists. *New York: United Nations International Children's Emergency Fund (UNICEF)*.
- Ramos Salazar, L. (2021). Cyberbullying victimization as a predictor of cyberbullying perpetration, body image dissatisfaction, healthy eating and dieting behaviors, and life satisfaction. *Journal of Interpersonal Violence*, 36(1-2), 354-380. <https://doi.org/10.1177/0886260517725737>

Richard, E. M., Young, S. F., Walsh, J. J., & Giumetti, G. W. (2020). Cyberaggression in work-related email: Nomological network and links to victims' counterproductive work behavior. *Occupational Health Science*, 4, 161-190.

<https://doi.org/10.1007/s41542-020-00056-3>

Salin, D., & Hoel, H. (2020). Organizational risk factors of workplace bullying. In S. Einarsen, H. Hoel, D. Zapf, & C. Cooper (Eds), *Bullying and harassment in the workplace: Theory, research and practice* (3rd Edition; pp. 305-329). Boca Raton, FL: CRC Press.

Spencer, C., Loehr, K., & Byrd, A. (2023). Patient and Family Perpetrated Cyber-Incivility and Cyber-Aggression Within Healthcare: A Cross-Sectional Descriptive Study. *SAGE Open Nursing*, 9, 23779608231158970.

<https://doi.org/10.1177/23779608231158970>

Tobitt, C. (2023, March 8). Online abuse toll means fifth of women journalists considered leaving industry. *Press Gazette*. <https://pressgazette.co.uk/media-audience-and-business-data/women-in-journalism-online-abuse/>

Vidal Valero, M. (2023, April 6). Death threats, trolling and sexist abuse: climate scientists report online attacks. *Nature Online*. <https://www.nature.com/articles/d41586-023-01018-9> doi: <https://doi.org/10.1038/d41586-023-01018-9>

Vittinghoff, E., & McCulloch, C. E. (2006). Relaxing the Rule of Ten Events per Variable in Logistic and Cox Regression. *American Journal of Epidemiology*, 165(6), 710-718. <https://doi.org/10.1093/aje/kwk052>

Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2017). The dark side of working online: Towards a definition and an Emotion Reaction model of

workplace cyberbullying. *Computers in Human Behavior*, 69, 324-334.

<https://doi.org/10.1016/j.chb.2016.12.055>

Vranjes, I., Baillien, E., Vandebosch, H., Erreygers, S., & De Witte, H. (2018). Kicking someone in cyberspace when they are down: Testing the role of stressor evoked emotions on exposure to workplace cyberbullying. *Work & Stress*, 32(4), 379-399.

<https://doi.org/10.1080/02678373.2018.1437233>

Vranjes, I., Erreygers, S., Vandebosch, H., Baillien, E., & De Witte, H. (2018). Patterns of cybervictimization and emotion regulation in adolescents and adults. *Aggressive Behavior*, 44(6), 647-657.

<https://doi.org/10.1002/ab.21790>

Vranjes, I., Farley, S., & Baillien, E. (2020). Harassment in the digital world: Cyberbullying.

In S. Einarsen, H. Hoel, D. Zapf, & C. Cooper (Eds.), *Bullying and harassment in the workplace: Theory, research and practice* (3rd Edition, pp. 409–433). CRC Press.

Wang, X., Kim, T. Y., & Li, H. (2022). Why and for whom cyber incivility affects task performance? Exploring the intrapersonal processes and a personal boundary condition. *Asia Pacific Journal of Management*, 1-26. <https://doi.org/10.1007/s10490-022-09865-2>

Weatherbee, T. G. (2007). Cyberaggression in the workplace: Construct development, operationalization, and measurement. In *Unpublished doctoral dissertation*. Saint Mary's: University, Halifax.

Weatherbee, T. G., & Kelloway, E. K. (2006). A case of cyberdeviancy: Cyberaggression in the workplace. In E. K. Kelloway, J. Barling, & J. J. Hurrell (Eds.), *Handbook of workplace violence* (pp. 445 –487). Thousand Oaks, CA: Sage Publications.

Zapf, D., Escartín, J., Scheppa-Lahyani, M., Einarsen, S. V., Hoel, H., & Vartia, M. (2020). Empirical findings on prevalence and risk groups of bullying in the workplace. In S. Einarsen, H. Hoel, D. Zapf, & C. Cooper (Eds), *Bullying and harassment in the workplace: Theory, research and practice* (3rd Edition; pp. 106-162). Boca Raton, FL: CRC Press.

Zhang, S., Leidner, D., Cao, X., & Liu, N. (2022). Workplace cyberbullying: A criminological and routine activity perspective. *Journal of Information Technology*, 37(1), 51-79. <https://doi.org/10.1177/02683962211027888>

Zych, I., Baldry, A. C., Farrington, D. P., & Llorent, V. J. (2019). Are children involved in cyberbullying low on empathy? A systematic review and meta-analysis of research on empathy versus different cyberbullying roles. *Aggression and Violent Behavior*, 45, 83-97. <https://doi.org/10.1016/j.avb.2018.03.004>

**Table 1**

Number (*N*) and percentage (%) of individuals exposed to cyberaggression by sex, age, position, and sector.

<b>Group</b>	<b><i>N</i> (%) total sample</b>	<b><i>N</i> (%) exposed to cyberaggression</b>	<b><i>p</i></b>
<b>Sex</b>			
Women	1,597 (56.1%)	45 (2.8%)	.88
Men	1,250 (43.9%)	34 (2.8%)	
<b>Age group</b>			
25-35 years	476 (16.7%)	16 (3.4%)	.80
36-45 years	652 (22.9%)	16 (2.5%)	
46-55 years	905 (31.8%)	26 (2.9%)	
56-65 years	814 (28.6%)	21 (2.6%)	
<b>Managerial Position</b>			
Employee	1,903 (66.8%)	43 (2.3%)	<.01
Manager	930 (32.7%)	36 (3.9%)	
<b>Sector</b>			
Public	1,271 (44.6%)	48 (3.8%)	<.001
Private	1,354 (47.6%)	23 (1.7%)	

**Source(s): Authors' own creation/work**

**Table 2**

Spearman correlations, means and standard deviations for the continuous study variables and cyberaggression

<b>Variable</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
1. Age	-				
2. Role conflict	-.13**	-			
3. Availability expectations	-.05*	.19***	-		
4. Emotional Demands	.01	.36***	.11***	-	
5. Quality of work	.05**	-.49***	-.08***	-.23***	-
6. Cyberaggression (no = 0, yes = 1)	-.01	.05**	.07**	.08**	-.06**
<i>M (SD)</i>	47.74 (10.78)	41.84 (1.93)	28.80 (2.86)	47.69 (2.52)	67.89 (1.82)
<i>N</i>	2,847	2,829	2,813	2,817	2,835

*Note.* \*  $p < .05$ , \*\*  $p < .01$ , \*\*\*  $p < .001$ . M = mean; SD = standard deviation.

**Source(s): Authors' own creation/work**



**Table 3**

Odds ratios (OR) and confidence intervals (CI) for factors predicting exposure to cyberaggression during the last 12 months.

	Exposure to cyberaggression ( <i>N</i> = 79)		
	OR	CI	
Role Conflict	.90	.77	1.06
Availability expectations	1.12*	1.03	1.22
Quality of work	.82**	.71	.94
Emotional demands	1.16*	1.02	1.31
Sector (public)	2.66**	1.47	4.84
Age	.99	.97	1.01
Sex	1.35	.78	2.33
Managerial position	1.77*	1.05	2.99

Nagelkerke R Square .084

*Note.* \*  $p < .05$ , \*\*  $p < .01$ , \*\*\*  $p < .001$ . For the dichotomous predictors sex, managerial position, and sector, the reference levels were male, no managerial position, and private sector. OR shown for 10-point difference in scale scores.

**Source(s): Authors' own creation/work**

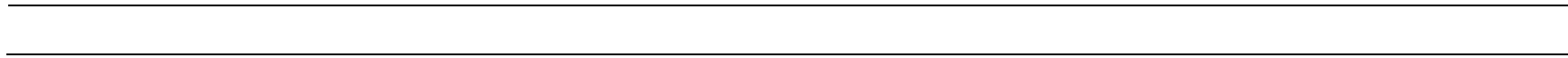
**Table 4**

Number (*N*), percentage (%), and Chi-square of individuals exposed to insider- and outsider- cyberaggression by sex, age, position, and sector.

<b>Group</b>	<b><i>N</i> (%) entire sample</b>	<b><i>N</i> (%) exposed to insider cyberaggression</b>	<b><math>\chi^2</math></b>	<b><i>N</i> (%) exposed to outsider cyberaggression</b>	<b><math>\chi^2</math></b>
<b>Total</b>	2,847	35 (1.23%)		38 (1.34%)	
<b>Sex</b>					
Women	1,597 (56.1%)	21 (1.3%)	0.22	20 (1.3%)	0.19
Men	1,250 (43.9%)	14 (1.1%)		18 (1.4%)	
<b>Age group</b>					
25-35 years	476 (16.7%)	9 (1.9%)	2.23	7 (1.5%)	2.13
36-45 years	652 (22.9%)	8 (1.2%)		5 (0.8%)	
46-55 years	905 (31.8%)	10 (1.1%)		13 (1.4%)	
56-65 years	814 (28.6%)	8 (1.0%)		13 (1.6%)	
<b>Managerial Position</b>					
Employee	1,903 (66.8%)	21 (1.1%)	0.85	21 (1.1%)	2.51
Manager	930 (32.7%)	14 (1.5%)		17 (1.8%)	
<b>Sector</b>					
Public	1,271 (44.6%)	20 (1.6%)	3.28	24 (1.9%)	5.80*
Private	1,354 (47.6%)	11 (0.8%)		11 (0.8%)	

Note: Note: \*  $p < .05$ .

**Source(s): Authors' own creation/work**



**Table 5**

Spearman correlations for exploratory analyses

	<b>Age</b>	<b>Role conflict</b>	<b>Availability expectations</b>	<b>Emotional Demands</b>	<b>Quality of work</b>
Cyberaggression from insiders	-.03	.07**	.06**	.04*	-.07**
Cyberaggression from outsiders	.01	-.01	.03	.06**	-.01

*Note.* \*  $p < .05$ , \*\*  $p < .01$ .

**Source(s):** Authors' own creation/work