Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Ophoff, J., Machaka, T., & Stander. A. (2015). Exploring the impact of cyber incivility in the workplace. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015,* 493-504. Retrieved from. http://Proceedings.InformingScience.org/InSITE2015/InSITE15p493-504Ophoff1565.pdf

Exploring the Impact of Cyber Incivility in the Workplace

Jacques Ophoff, Thabiso Machaka, and Adrie Stander
Department of Information Systems, University of Cape Town, Cape Town, South Africa

jacques.ophoff@uct.ac.za; MCHTHA012@myuct.ac.za; adrie.stander@uct.ac.za

Abstract

The world is an interconnected global village due to the increasing adoption and reliance on technology, but an ugly side of the increased usage of technology has come to light. The issue of harassment and abuse on the internet has led to relatively new issues such as cyber harassment, cyber incivility and cyberbullying.

A case study was conducted within two faculties at the University of Cape Town (UCT). The research objectives were: to find out how staff members in a workplace have experienced cyber incivility, to find out what effects cyber incivility has on employees, to find out what the motivations are for staff participation in cyber incivility, and to find out what policies a workplace should have in place in order to deal with cyber incivility.

The data collected shows that there have been occurrences of cyber harassment and cyber incivility among staff members at UCT. The following effects were found to be consistent with cyber harassment and cyber incivility: decrease in productivity and a toxic working environment. On an individual basis: anger, negative feelings and feelings of inferiority, feeling demotivated, feelings of fear and intimidation, feeling emotional and upset, irritation, loss of self-esteem, stress and wasted time.

Keywords: Cyber incivility, online harassment, organizational policy.

Introduction

The world is an interconnected global village due to the increasing adoption and reliance on technology. The internet is very useful for work, leisure and social activities. There is however a negative side to cyber space. The issue of harassment and abuse on the internet has led to research being conducted on relatively new issues such as cyber harassment, cyber incivility and cyberbullying. Cyber harassment is a personal attack against an individual using any form of technology (Workman, 2010). Cyber incivility is electronic aggression that occurs, specifically in the workplace, using emails (Lim & Teo, 2009). Cyberbullying is a subset of cyber harassment and has been linked mainly with youth when it comes to research (Willard, 2011).

The aim of this research study is to explore the phenomenon of cyber incivility in an organization. The research objectives are to: 1) explore staff experiences of cyber incivility, 2) study the effect of cyber incivility on employees, 3) explore motivations for participating in cyber incivility and 4) suggest effective policies for the organization to deal with cyber incivility.

The layout of the paper is as follows. First a review of literature around cyber harassment, including cyber bullying and cyber incivility is given. Then the research methodology of the study is discussed. The collected data is presented and discussed, leading to a conceptual framework of the identified issues. Lastly the findings are summarized and final conclusions are made.

Literature Review

Cyber harassment is a personal attack against an individual using any form of technology. "These kinds of attacks often disseminate misleading or false information to damage their targets, to interfere with them, or for the purposes of extortion" (Workman, 2010, p.117). The fact that individuals are able to do this anonymously and across geographical borders makes cyber harassment a widespread, increasing concern. However, electronic aggression that occurs specifically in the workplace using emails is termed 'cyber incivility' (Lim & Teo, 2009). Both cyber harassment and cyber incivility have a negative impact on the individuals involved, employee productivity, and the work environment (Workman, 2010). Cyber incivility negatively affects employees' work attitudes, perceptions of their superiors, work performance and leads to intentions to quit. Behaviors or actions linked with cyber incivility include: not replying to emails as one should (in cases of urgency - intentionally delaying a response), making demeaning or derogatory remarks in emails, and not responding to emails at all (Lim & Teo, 2009).

Cyberbullying

Cyberbullying can be a form of cyber harassment and cyber incivility. There are authors who simply define cyberbullying as "bullying communicated through the online mode" (Ybarra, Boyd, Korchmaros, & Oppenheim, 2012.p.53). There is no widely accepted definition of cyberbullying, which accounts for discrepancies in the extent and frequency of cyberbullying found among youth (Kiriakidis & Kavoura, 2010; Willard, 2011). Many authors argue that the characteristics of cyberbullying are a power imbalance, repeated occurrence and the intention to harm (Dinakar, Jones, Havasi, Lieberman, & Picard, 2012). The interpretation of these three characteristics is, however, debated upon. The difference in arguments is due to the fact that the online platform provides a challenge when it comes to using the traditional definition of bullying, and applying it to cyberbullying.

Authors seem to disagree when it comes to the issue of what exactly counts as a power imbalance. Unlike traditional bullying, one cannot conclude that the physically bigger person is the one in a position of power. It is, however, noted that the fact that the perpetrator can remain anonymous suggests a power imbalance (Beckman, Hagquist, & Hellström, 2013). Another factor that constitutes a power imbalance is superior technical ability (Slonje, Smith, & Frisén, 2013).

Including repetition in the definition of cyberbullying can be extremely limiting to a study, and a once-off incident could have effects just as devastating as repeated offenses (Tokunaga, 2010). The other problem is that the technology and platforms used enable the fast spread of the cyberbullying incident, which may be out of the initial perpetrator's hands, but cause a snowball effect nonetheless. The victim may experience the same effects repeatedly (Slonje et al., 2013).

Effects and Impact

The increased use of mobile and computing devices has both negative social and physical effects on youth (Álvarez, Torres, Rodríguez, Padilla, & Rodrigo, 2013; Çetin, Yaman, & Peker, 2011).

Cyberbullying has a negative effect on both the victim and the perpetrator's socio-emotional wellbeing, as well as their psychosocial development (Law, Shapka, Domene, et al., 2012; Kiriakidis & Kavoura, 2010). Emotions that are associated with cyberbullying victims are anger, embarrassment, empathy, fear, pride, relief (when the situation is resolved) and sadness (Xu & Zhu, 2012). Victims also display bad moods (Tokunaga, 2010). The victim is also likely to experience feelings of shame about the incident (Slonje et al., 2013). Cyberbullying victims experience loss of self-esteem, depression, self-inflicted harm and feelings of hopelessness (Lam & Li, 2013). Other symptoms include "difficulties sleeping, despondency, headaches and stomach pains" (Willard, 2011.p.80).

Motivation

Motives for cyberbullying include vengeance, lack of anything else to do and venting frustrations that are not intended for the victim (Slonje et al., 2013). The anonymity provided by cyberbullying seems to be a motivating influence as it relieves the ethical and social consequences on the perpetrator, and encourages those who had not participated in cyberbullying to do so (Calvete et al., 2010; Tokunaga, 2010; Workman, 2010).

Demographics

When it comes to demographics, researchers found that respondents who are the same gender as their superior are more likely to experience cyber incivility (Lim & Teo, 2009). The 'Queen Bee' syndrome is used to explain the increased likelihood of women treating women who are their subordinates in an uncivil manner (Lim & Teo, 2009).

Other authors, however, conclude that gender is not a deciding factor as both males and females are exposed to the same scope of the internet (Beckman et al., 2013; Tokunaga, 2010). The influence of gender differences as a predictor for cyberbullying differs according to the culture and context of each country (Çetin et al., 2011).

Policies to Mitigate Cyber Harassment

With regards to legislature, 45 of the 50 states in the United States have laws that deal with bullying, but not all of these laws address the issue of cyberbullying (Willard, 2011; Valcke et al., 2011).The Singapore Ministry of Education has developed a framework to help aid schools to fight against cyberbullying (Kwan & Skoric, 2013). The Flemish government has developed curriculum goals which promote safe internet use in schools (Valcke et al., 2011). The South African Department of Basic Education's Draft Guidelines also promote cyber safety in schools (Sonhera, Kritzinger, & Loock, 2011).

The need for policies to be developed regarding netiquette (appropriate conduct using electronic communication) is important for organizations to run conducive working environments (Lim & Teo, 2009). As the world becomes more connected over the internet, companies become more reliant on using electronic communication to conduct business across geographical borders (Beckman et al., 2013).

Intervention Strategies

In analyzing intervention strategies, researchers found that zero-tolerance policies are not only ineffective, but detrimental to the school climate (Bauman, Toomey, & Walker, 2013). Non-punitive measures are suggested by some authors due the negative impact punishment could have on the perpetrator. Policies that encourage positive behaviors should be enforced (Bauman et al., 2013; Cassidy et al., 2012). When developing policies, school officials should be aware of the

impact these policies will have on the school environment (Willard, 2011). Policies should be understood by teachers, parents and students (Sonhera et al., 2011).

When it comes to experiencing cyberbullying, victims rarely report cyberbullying incidents to the relevant authority figures, choosing to rather confide in their peers (Tokunaga, 2010; Sonhera, Kritzinger, & Loock, 2011; Huang & Chou, 2013). Ignoring the cyberbullying seems to be the most popular method of dealing with the problem (Fenaughty & Harré, 2013). Willard (2011) concludes that students do not report cyberbullying because they believe the school will either do nothing about the report, or that the situation will escalate.

Cyber Incivility and Cyber Harassment

Electronic aggression occurring in the workplace using emails is termed 'cyber incivility'. Cyber incivility is not considered to be cyberbullying by some authors as the intent for harm cannot be established. Respondents indicate having been victims of cyber incivility at the hands of their supervisors, which indicates a power imbalance. Respondents who are the same gender as their superior are more likely to experience cyber incivility. The 'Queen Bee' syndrome is used to explain the increased likelihood of women treating women who were their subordinates in an uncivil manner (Lim & Teo, 2009).

Cyber incivility negatively affects employees' work attitudes, perceptions of their superiors, work performance, productivity and intentions to quit. Behaviors or actions linked with cyber incivility include not replying to emails as one should (in cases of urgency- intentionally delaying a response), making demeaning or derogatory remarks in emails and not responding to emails at all. The need for policies to be developed regarding netiquette (appropriate conduct using electronic communication) is important (Lim & Teo, 2009). As the world becomes more connected over the internet, companies become more reliant on using electronic communication to conduct business across geographical borders (Beckman et al., 2013).

With cyber harassment, the intent to harm is clearly established. The power differential and repetition that are used by many to characterize cyberbullying, are debatable as being present in cyber harassment in the workplace. Cyber harassment is a personal attack against an individual using any form of technology: "These kinds of attacks often disseminate misleading or false information to damage their targets, to interfere with them, or for the purposes of extortion" (Workman, 2010). The fact that individuals are able to do this anonymously and across geographical borders makes cyber harassment a widespread, increasing concern. Cyber harassment has a negative impact on the individuals involved, employee productivity and the work environment (Workman, 2010).

The themes that have been identified in the literature review were the basis upon which the research questions were formed and guided the case study methodology which is explained next.

Research Methodology

The purpose of this research is exploratory, the research question being: what are the perceptions of cyber incivility within an organization? This is justified since little empirical data has been collected and the issues around cyber incivility are not yet well-understood. In order to investigate the research question a single-site case study was done. The University of Cape Town (UCT), the top ranked university in Africa, was chosen as a case site.

A random sampling method was used, consisting of two departments from different faculties in the university. Departments from different disciplines were chosen to minimize bias. Semi-structured individual interviewing was selected as this method is more personal than a survey. The type of information collected warrants the use of interviews as respondents can be probed

further in order to gain more insight. A purposeful sampling strategy was followed to include both academic and administrative participants, as well as a balance of gender and cultural background. Participants agreed to answer the interview questions, with responses reported anonymously.

An interview protocol was developed through a pilot study and followed for each interview. The protocol, based on studies done by Bhattacherjee (2012) and Dicicco-Bloom & Crabtree (2006), specified the following:

- The purpose of the interview and study is stated to participants before the interview begins. This is done in such a way as not to jeopardize the integrity of the study by leading the participant to form a particular view beforehand.
- All questions are asked in the exact order in which they appear on the questionnaire, and none are skipped.
- Deviation for further exploration into a response is allowed in order to gain insight or understanding should there be confusion.
- Questions are asked in a neutral tone and leading of respondents will not take place.
- Questions are asked in layman terms – no jargon is used.
- Notes regarding observations or points of interest are taken down in addition to taping conversations.
- In order to further probe a response encouragement, silent probing, elaboration and reflecting on the response with the respondent can be employed

In addition to interview data publicly accessible organizational policy documents was obtained from the university website, and analysis of policy items that are directly related to cyber harassment and cyber incivility was done. Gaps emerging from the analysis of these documents are also presented. From the interview and policy document data an inductive approach led to the development of a Conceptual Framework of Cyber Incivility Issues, presented in Figure 1.

The following section provides an analysis of the data that was collected.

Data Analysis and Findings

This section provides an analysis of the data that was collected. Ten interviews were conducted with participants. Each interview was transcribed before being analyzed using the Atlas.ti qualitative data analysis software package.

Each subsection presents data related to the interview questions (listed in the Appendix) that were asked. All the data will be used in the Findings section to answer the research question and achieve the research objective.

Experience of Cyber Incivility

The data shows that there have been occurrences of cyber harassment and cyber incivility among staff members at UCT. Some staff members have had personal experiences, and others have witnessed or heard of cases regarding cyber harassment and cyber incivility. The behaviors that were most common regarding cyber incivility were the delayed receipt of emails, receiving an email in the wrong format and not receiving a response to an email. Receipt of disturbing or offensive images was not intentionally sent to or by any individual- rather, it was the result of malfunctioning spam filters.

Only one respondent had received a threat via electronic communication, and very few had been recipients of demeaning or derogatory remarks in emails. When asked about their own participation in cyber harassment and cyber incivility, all respondents did not consider themselves to be perpetrators. When confronted with the list of behaviors of what constitutes cyber harassment and cyber incivility, respondents still did not consider themselves to be perpetrators, although they had all clearly committed one or more of the 'offenses'.

Responses to Cyber Incivility

Some respondents chose not to respond or react to the situation or incident that had occurred to them. Respondent 9 said that choosing not to respond to an incident of cyber harassment or cyber incivility was an alternative, especially if the incident occurred in a hostile environment: *"If you respond it might, it might escalate things"*. The respondent also explained that *"...and if you don't respond maybe that's the best way for you to calm down, and calm the situation down"*. This was clarified as the respondent went on to explain that they preferred to resolve all issues, regardless of where these issues originated from, by confronting the perpetrator in person.

On the contrary, Respondent 1 preferred to use electronic communication as a means to resolve the situation and did not confront the other party in person: *"I usually phone them, their office and try to get hold of them you know… or get hold of their secretary or somebody that works with them and find out where they are"*.

Effects of Cyber Incivility

All respondents agreed that cyber harassment and cyber incivility can have real effects on not only the individuals involved, but the workplace as well. The following effects were found to be consistent with cyber harassment and cyber incivility: decrease in productivity and a toxic working environment. On an individual basis: anger, negative feelings and feelings of inferiority, feeling demotivated, feelings of fear and intimidation, feeling emotional and upset, irritation, loss of self-esteem, stress and wasted time. These findings are in line with previous research (Xu & Zhu, 2012; Lam & Li, 2013);

Others felt that experiencing cyber harassment and cyber incivility made them more cautious in their dealings with others. Respondent 9 stated that:

> *"I feel, you get a feeling of intimidation you know? Given the language they've used". Respondent 9 went on to say that experiencing something like this made them think twice about the type of communication they send out. So being more conscious of one's own behavior is one of the effects: "That makes me think about the way I write emails to people who are probably b-, under me or maybe students, tutors you see? So that makes me be more careful because I don't want what I'm feeling, I don't want someone else to feel what I'm feeling at that point in time. When someone else writes sort of the same kind of email in the same kind of tone, and you feel like it makes you uncomfortable and, and insecure you cannot, you lose confidence in your work and production. And you start realizing and then you obviously improve the way you, you communicate with other people".*

Respondent 5 explained that they became emotional and upset as a result: *"It gets me emotionally upset… So it did affect me emotionally. I was very upset about that"*. The respondent also reported insomnia as an effect: *"So it did take a strain on me emotionally. And I was very tired after that because I lost sleep"*.

Respondent 10 expressed irritation as an effect of cyber harassment and cyber incivility. The respondent also explained how the working environment can become toxic as a result: *"…create bad blood you know, in a working environment, fairly toxic kind of behavior…"*

Respondent 6 reported anger as being the strongest feeling they associated with cyber harassment. The respondent also stated, similarly to respondent 9, that an incident like that could damage one's self esteem and you could even begin to doubt yourself:

> *"Once you lose your self-esteem you don't trust yourself, if you're doing anything right. So it's not right, because in a workplace you need motivation, somebody has to motivate you to do well. If someone is always on your case, discouraging you, you don't trust yourself even when you're doing something right"*.

Respondent 3 also identified with these feelings of anger: *"We're all angry because one person caused it, because he delayed a response"*.

Cyber harassment and cyber incivility seemed not to affect some respondents as they felt that it all didn't make a difference to them – they just didn't care. Respondent 3 explained that the effects of cyber harassment and cyber incivility could be hard to define as some people are either unaware that they are victims or they completely ignore the situation, while others confront the situation, which makes things worse:

> *"I think this issue of harassment and incivility happens, and in fact on a regular basis. The only thing is that people just choose not to, choose to ignore it. And the second option is that people don't know that this is harassment; don't even know, so they just go along with it. So there are people who know, they choose to ignore it. There are people who know and refuse to ignore it and it often creates bigger conflicts. And then there are those who don't even know they are being harassed- that's the worst part of the whole scenario or the idea that they themselves are even harassing people by making statements"*.

Motivations for Cyber Incivility

Although all the respondents did not identify with being a perpetrator when it comes to cyber harassment and cyber incivility, all gave reasons for the behaviors they had displayed that were consistent with cyber harassment and cyber incivility. The following reasons were given as motivations for participating in cyber harassment and cyber incivility: lack of time and prioritizing, office politics, work pressures. Another reason that came up was insensitivity and an unawareness of other people's feelings. The online platform as a relief for moral behavior was suggested as another reason.

Respondent 9 believed that work hierarchy could play a role in cyber incivility: *"... but you have an environment where people are new, people who are- they have been there for a while, you have people who are below the hierarchy, people who are high in the hierarchy and you can, you can somewhat sometimes be complacent with what you do without realizing the implication, and chances are you're probably bullying someone"*. The respondent went to further explain that office politics also provided some sort of motivation for people to engage in cyber incivility and cyber harassment behaviors: *"First of all some people are bullies but office politics as well, people get upset sometimes"*.

Other respondents felt that the pressure of work was the reason why people participated in cyber incivility. Respondent 10 stated that *"I often think it's the pressure of work... there's so many emails we receive in a day that you may not be able to respond to all of them. And some of them just drop off the radar"*. The respondent went on to say that another reason is that people bring personal issues into the workplace, and this ends up affecting the work relationships: *"If they're personal then it must be because they have personal issues, you know, which means you know that they're sorting out their own social problems using electronic means"*. It is possible that

work pressure is a precedent to the venting of frustration, found by previous research (Slonje et al., 2013).

Respondents who were guilty of the cyber harassment and cyber incivility behaviors either felt guilty and did something about it, or felt that they were justified and didn't do anything about mediating the situation. Respondent 2 felt that with regards to participating in cyber incivility, they were justified as they too had a lot on their plate: *"I'm not excited about it, I'm not unhappy. I just felt I'll answer at the right time, I felt ok this person is bothering me, and I need my space, that's all. It's not that I am happy that I have not responded to the mail, I'm also busy"*. Respondent 4 felt that since their reason for intentionally delaying a response was because they still needed to get all the relevant information, they were perfectly justified.

Policies on Cyber Harassment and Cyber Incivility

The UCT policy documents that were analyzed provided insight into the rules and regulations governing electronic communication and computer usage at UCT. Two of the documents analyzed did not have time stamps, so one cannot know how relevant they still are in terms of the date. One of the policies, The UCT Mediation policy, was last updated in August 2012, but only details what to do should one seek mediation for a conflict or dispute. The Policy and Rules on Internet and Email Use details some activities consistent with cyber harassment and cyber incivility, but the policy was last updated in 2004.

The majority of the respondents either said they had no idea what protocol to follow or they didn't believe there was a protocol in place to handle cyber harassment and cyber incivility at the university. Respondent 9 said: *"I don't really know what it is"*. The respondent did however mention other avenues of dispute resolution that the university has in place- such as the office of the Ombudsman and reporting the incident to the perpetrator's line manager. Respondent 10, who had been at the university for twelve years had the following to say: *"I don't know actually. I don't know. I haven't read it if there's one, or you know the universities always have all kinds of protocols that sometimes nobody really knows about, until it affects you and then you'll go find out"*. This puts into question the practical value of policies, as predicted by previous research (Lim & Teo, 2009).

When asked whether or not they thought the existing protocol was adequate, the respondents had differing opinions. Respondent 3 suggested that since the issue of cyber harassment and cyber incivility had a technological aspect to it, the issue would best be solved by a technological solution. The respondent explained:

> *"There should be an evidence repository of every email I send. And that repository cannot be touched unless I request for it to tender a case- in other words privacy. But then whenever I request for that repository to tender a case, I need it to be considered by whoever is in charge of handling cases like that"*.

The policies are not definite with regard to what one should do when faced with cyber harassment and cyber incivility. For example, what happens if a victim deletes all traces of the abusive material- does the system keep a permanent record or is the onus on the victim to produce evidence? At what point or after how many offenses can one seek help? Are offenses rated by how serious they are and in that case, what is considered serious enough to seek help or report the issue? These kinds of questions are just some of the gaps identified in the UCT policy documents.

Conceptual Framework of Issues

The issues identified above have been captured into the conceptual framework, illustrated in Figure 1. The figure highlights several important areas for research that play a role regarding cyber harassment and cyber incivility.

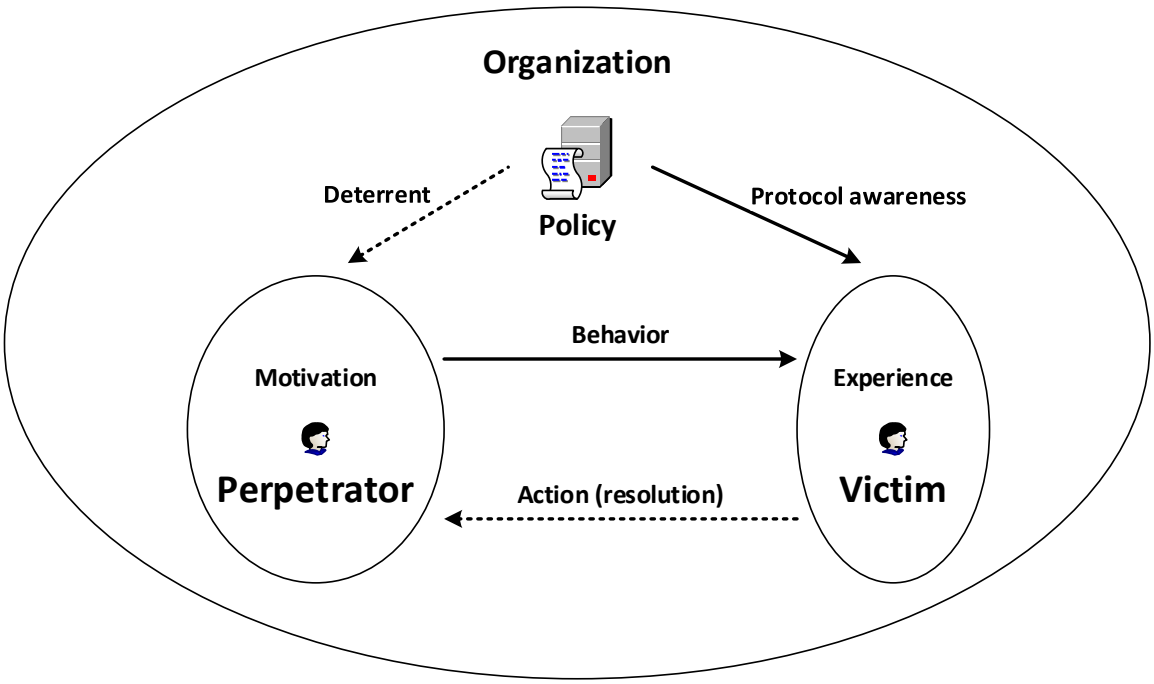


Figure 1: Conceptual Framework of Cyber Incivility Issues

Within the organizational (workplace) context the role of the perpetrator needs to be understood in terms of motivating factors and behaviors of cyber incivility. Only once there is a good understanding of these issues can effective countermeasures be implemented. The role of policy as a deterrent to such behavior should also be investigated.

From the victim's perspective the experience of cyber incivility and the actions this leads to need to be understood. This may require to interdisciplinary research linking with psychology, which is not uncommon in the information systems discipline. From a policy perspective effective means of addressing employee awareness needs to be established, as well as the efficacy of policy (together with technology) to address the underlying issue.

Conclusion

The aim of this research was to find out how staff at UCT has experienced cyber harassment and cyber incivility. The literature review highlighted the importance of studying cyber aggression, as well as highlighting the gaps in literature regarding cyber harassment and cyber incivility in the workplace. The responses from the respondents that were interviewed indicated that cyber harassment and cyber incivility are issues that are currently taking place in at least two faculties at UCT, with the most common experiences relating to cyber incivility specifically. Policy documents were analyzed and gaps were identified – particularly a lack of awareness – with regards to cyber harassment and cyber incivility.

This research was limited to two departments due to time constraints. Future studies can validate and build upon these results by including a broader sample. While this research only focused on cyber incivility an interesting comparison may be drawn with the effects of physical bullying.

Other avenues for further research include looking at cyber harassment and cyber incivility among university students. The prevalence of these phenomena could be analyzed through the use of surveys and questionnaires as respondents might also reveal more because of the anonymity offered by this form of data collection.

References

Álvarez, M., Torres, A., Rodríguez, E., Padilla, S., & Rodrigo, M. J. (2013). Attitudes and parenting dimensions in parents' regulation of Internet use by primary and secondary school children. *Computers & Education, 67*, 69–78.

Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence, 36*(2), 341–50.

Beckman, L., Hagquist, C., & Hellström, L. (2013). Discrepant gender patterns for cyberbullying and traditional bullying – An analysis of Swedish adolescent data. *Computers in Human Behavior, 29*(5), 1896–1903.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. (U. of S. F. S. Commons, Ed.) (2nd ed.). Open Access Textbooks.

Calvete, E., Orue, I., Estévez, A., Villardón, L., & Padilla, P. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior, 26*(5), 1128–1135.

Cassidy, W., Brown, K., & Jackson, M. (2012). "Under the radar": Educators and cyberbullying in schools. *School Psychology International, 33*(5), 520–532.

Çetin, B., Yaman, E., & Peker, A. (2011). Cyber victim and bullying scale: A study of validity and reliability. *Computers & Education, 57*(4), 2261–2271.

Dicicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education, 40*(4), 314–21.

Dinakar, K., Jones, B., Havasi, C., Lieberman, H., & Picard, R. (2012). Common Sense Reasoning for Detection, Prevention, and Mitigation of Cyberbullying. *ACM Transactions on Interactive Intelligent Systems, 2*(3), 1–30.

Fenaughty, J., & Harré, N. (2013). Factors associated with young people's successful resolution of distressing electronic harassment. *Computers & Education, 61*, 242–250.

Huang, Y., & Chou, C. (2013). Revisiting cyberbullying: Perspectives from Taiwanese teachers. *Computers & Education, 63*, 227–239.

Kiriakidis, S., & Kavoura, A. (2010). A review of the literature on harassment through the internet and other electronic means. *Family and Community Health, 33*(2), 82–93.

Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in Human Behavior, 29*(1), 16–25.

Lam, L. T., & Li, Y. (2013). The validation of the E-Victimisation Scale (E-VS) and the E-Bullying Scale (E-BS) for adolescents. *Computers in Human Behavior, 29*(1), 3–7.

Law, D. M., Shapka, J. D., Domene, J. F., & Gagné, M. H. (2012). Are Cyberbullies really bullies? An investigation of reactive and proactive online aggression. *Computers in Human Behavior, 28*(2), 664–672.

Lim, V. K. G., & Teo, T. S. H. (2009). Mind your E-manners: Impact of cyber incivility on employees' work attitude and behavior. *Information & Management, 46*(8), 419–425.

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior, 29*(1), 26–32.

Sonhera, N., Kritzinger, E., & Loock, M. (2011). A proposed cyber threat incident handling framework for schools in South Africa. *SAICSIT '12 Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference*. ACM New York.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior, 26*(3), 277–287.

Valcke, M., De Wever, B., Van Keer, H., & Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers & Education, 57*(1), 1292–1305.

Willard, N. (2011). School response to cyberbullying and sexting: the legal challenges. *Brigham Young University Education and Law Journal, 1*, 75–125.

Workman, M. (2010). A behaviorist perspective on corporate harassment online: Validation of a theoretical model of psychological motives. *Computers & Security, 29*(8), 831–839.

Xu, J., & Zhu, X. (2012). Fast learning for sentiment analysis on bullying. *WISDOM '12 Proceedings of the First International Workshop on Issues of Sentiment Discovery and Opinion Mining* (pp. 1–5). ACM New York.

Ybarra, M. L., Boyd, D., Korchmaros, J. D., & Oppenheim, J. K. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health, 51*(1), 53–58. doi:10.1016/j.jadohealth.2011.12.031

Appendix: Interview Questions

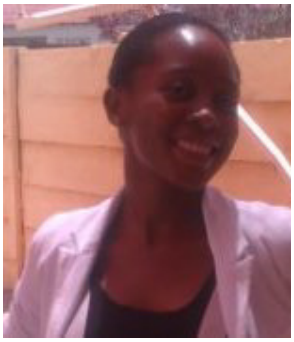
The following questions were used during interviews:

1. What is your position in the organization?
2. How often do you use email and other forms of communication technology in a normal day's work?
3. Have you ever experienced or seen cases of one or more of the following:
    a. Receiving an email where the sender doesn't reply as they should (in cases of urgency, intentionally delaying a response)
    b. Making demeaning or derogatory remarks in emails
    c. Not responding to emails at all
    d. Receiving disturbing or offensive images through emails
    e. Receiving threats through emails
4. How did experiencing this make you feel?
5. Why do you think others participate in these behaviors?
6. Have you ever participated in one or any of the following:
    a. Sending an email where you did not reply as you should have (in cases of urgency, intentionally delaying a response)
    b. Making demeaning or derogatory remarks in emails
    c. Not responding to emails at all
    d. Circulating disturbing or offensive images through emails
    e. Sending threats through emails
7. How did participating in this make you feel or why do you think others participate in this?

8. What did you do about the situation as a:
    a. Participant (receiver)
    b. Participant (sender)
    c. Bystander
9. How do you think the listed actions affect the organizational environment?
10. What is the departmental protocol to follow should one of the above experiences happen to you?
11. Do you think this is adequate?

Biographies

Jacques Ophoff is a Senior Lecturer in the Department of Information Systems at the University of Cape Town (UCT), South Africa. He obtained his doctorate in Information Technology from the Nelson Mandela Metropolitan University, South Africa. Before joining UCT he was an IT Product Manager at an online startup company. His research interests include information security, mobile technologies, and education.



Thabiso Machaka is a graduate IT trainee in the Financial Services industry. She is a graduate of the University of Cape Town, and holds a Bachelor of Commerce (Hons) degree specializing in Information Systems.

Adrie Stander is a Senior Lecturer in the Department of Information Systems at the University of Cape Town. He specializes in digital and computer forensics. His research interests include a wide topic range from Forensic Readiness and Mobile Forensics to Open Source Forensic Tools.