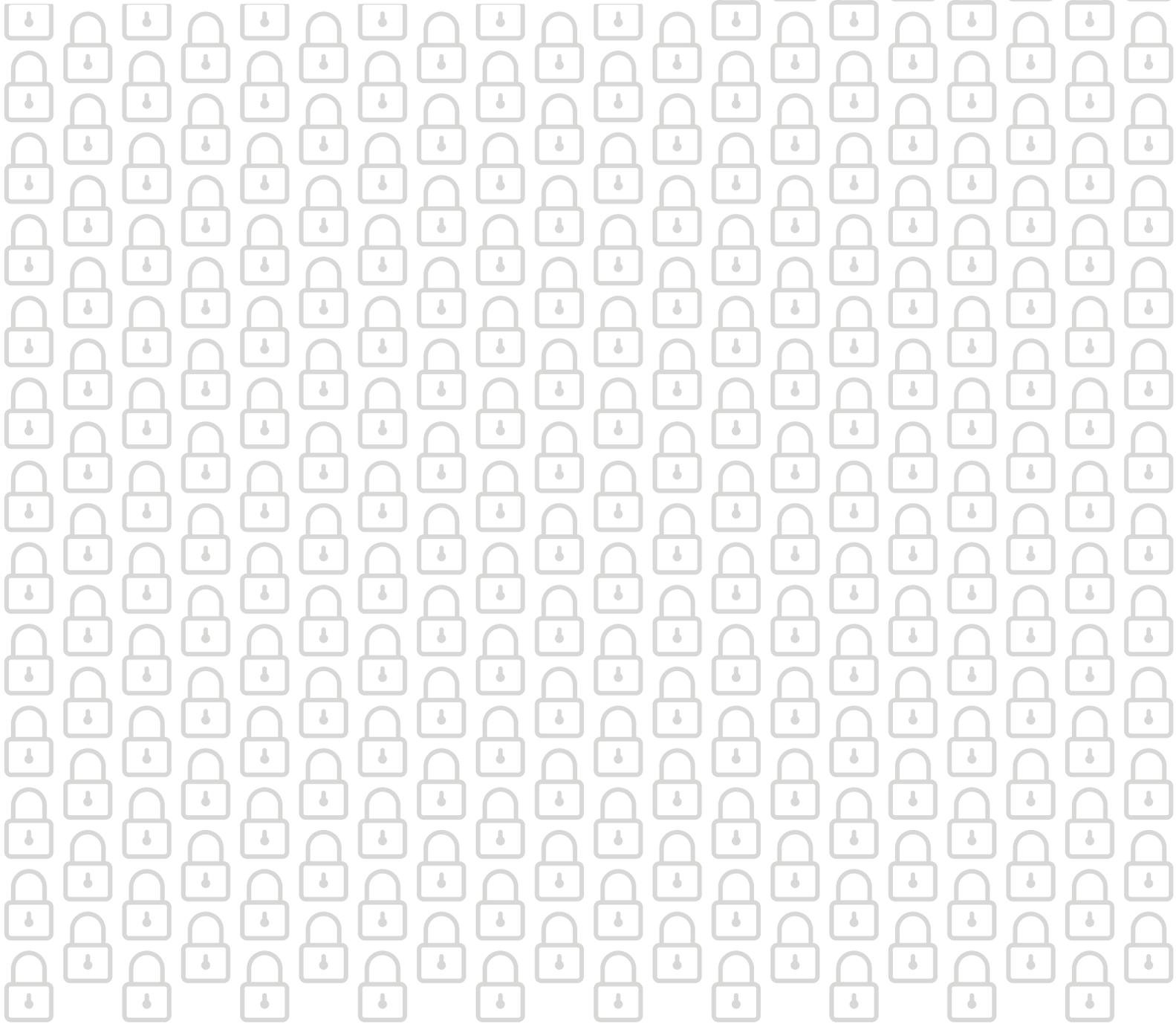




Digital
Rights Foundation



DIGITAL (IN)SECURITY OF JOURNALISTS IN PAKISTAN

ABOUT

Digital Rights Foundation (DRF) is a registered research-based advocacy non-governmental organization in Pakistan. Founded in 2012, DRF focuses on ICTs to support human rights, inclusiveness, democratic processes, and digital governance. DRF works on issues of online free speech, privacy, data protection, surveillance, and online violence against women. DRF opposes any and all sorts of online censorship and violations of human rights both on ground and online.

ACKNOWLEDGMENTS

This report could not have been possible without Shaukat Ali and Naveed Sehar for conducting the first round of surveys; without Obaid Ahmed Khan who helped collate the data; and without the journalists in DRF's Network of Female Journalists on Online Safety who helped disseminate the survey, as well as the journalists who filled it honestly and painstakingly.

The report is authored by Maham Javaid, edited by Shmyla Khan and Nighat Dad, and designed by Hija Kamran.

This work was supported by the Free Press Unlimited, a foundation based in Amsterdam that helps local journalists in war zones and conflict areas to provide their audience with trustworthy news and information.

CONTENTS

- Executive Summary ----- 1
- Introduction ----- 2
- Objectives ----- 4
- Background ----- 5
- Research Methodology ----- 6
- Analysis:
 - 1. Why digital security matters ----- 8
 - 2. The gender lens ----- 11
 - 3. The crimes and criminals ----- 13
- Pointing fingers:
 - 4. How do journalists fall short? ----- 15
 - 4.5. Digital insecurity, mental health and support systems ----- 16
 - 5. How do media organisations fall short? ----- 18
 - 6. How does the government fall short? ----- 21
- 11. Recommendations ----- 23

EXECUTIVE SUMMARY

There has been much delay in Pakistan to recognize that violence, threats and harassment faced online by journalists is a mere reflection of the violence they are exposed to offline. A nationwide survey of working journalists was conducted to ascertain their level of digital insecurity, to record their experiences and to conclude what protections they desired from the journalist community, their media organizations and the government. This report is an analysis of the survey; it contends that media organizations must take responsibility for the digital security of their employees; similarly, the government and the journalist community must also play their role in making online spaces safer for journalists. Special attention has been paid to female journalists who experience violence in digital spaces differently from male journalists. Unless these recommendations are taken seriously, journalism in Pakistan will continue to be dominated by male journalists; self-censorship will continue to increase, and the overall quality of journalism and accountability of public officials will decrease.

INTRODUCTION

Journalism is becoming an increasingly dangerous profession. A century ago, the threats and concerns journalists faced were limited to their physical world; but as the world went online, so did much of its violence.

Today, journalists face digital or online insecurity in various ways which include, but are not limited to, being hacked, threatened, blackmailed, harassed over a sustained period of time, sexually harassed, having your data stolen, being cyber-stalked, receiving malware or phishing emails.

While the state does pay limited attention to the physical security of journalists there has been a delay in understanding the intertwining of digital and physical security. Abductions and murders of journalists are by far the most serious forms of censorship, however as a UNESCO report points out¹, a large proportion of journalists killed in recent years were easy targets because they were exposed by the digital tools they use.

“The threats identified in the UNESCO survey include illegal digital surveillance by intelligence agencies or non-state actors, location tracking and software and hardware exploits without the knowledge of the target. According to a Committee to Protect Journalists (CPJ) research, 38 per cent of journalists murdered in last two decades were threatened [through social media] before they were killed.”² Hence proving that digital security cannot be viewed as something ‘lesser’ than physical security and both need to be considered for the creation of a secure atmosphere for journalists to work in.

Pakistani journalists face various kinds of digital insecurities that need to be recorded, evaluated and dealt with. If ignored, the online threats and harassment against journalists will keep growing, hence creating larger spaces for censorship.

The need for this survey can be surmised from one of the survey’s questions in which respondents were asked if they had ever had their digital security, as defined above, compromised – an overwhelming 66 per cent of journalists confirmed that they had suffered online insecurity.

¹ Henrichsen, Jennifer R; Betz, Michelle; Lisosky, Joanne M. “Building Digital Safety for Journalism. A Survey of Selected Issues” UNESCO - Division for Freedom of Expression and Media Development. 2015.

² “Why Pakistan is fourth most dangerous for media?” The News International. 2016.

12. Have you ever experienced digital insecurity, which includes being hacked, threatened, blackmailed, harassed over a sustained period of time, sexually harassed, having your data stolen, being cyber-stalked, and receiving malware or phishing emails, etc.



OBJECTIVES

The objectives of this report are as follows:

1. To ascertain whether journalists in Pakistan feel secure online and explore the unique experience of journalists in online platforms;
2. To understand what level of training in digital security and privacy Pakistani journalists have received;
3. To ascertain whether the state run Federal Investigation Agency's National Cyber Crime Response centre is effective in making journalists feel secure;
4. To recognise differences in the way male and female journalists experience digital insecurity, and the way they react to online threats/harassment;
5. To propose recommendations in the spirit of making digital spaces, and in turn physical spaces, safer for journalists;
6. Dissemination of report among media houses, journalists and the general public to increase awareness of the specific threats journalists, and specifically women journalists, face;
7. Dissemination of report among policy-makers and legislators to push for digital-specific provisions in the forthcoming journalists' safety bill;
8. Build on existing research done by Digital Rights Foundation on the subject of digital security of journalists.

BACKGROUND

It has been reported that a draft of the Journalist Protection Bill is currently being considered by the Senate Standing Committee on Information, Broadcasting and National Heritage, and is currently being re-drafted. DRF has learnt that this version of the Bill did not include provisions for the digital security of journalists. The reason the bill is being re-drafted, however, has nothing to do with online security – it is because the bill did not constitute for punishments for those who have attacked media houses, DSNG vehicles and media workers.

DRF would like to take this chance to push the creators of the bill to also consider that journalists be protected online, not only for their mental health, quality of work, and to keep censorship at bay, but also because digital insecurity of journalists is closely tied in with physical insecurity of journalists and freedom of the press.

RESEARCH METHODOLOGY

This report is a result of two sets of similar surveys. The first survey was paper-based and it was conducted at the end of a Digital Rights Foundation's advanced 'Empowerment of Women in Media' training retreat in Murree in December 2017. The first question of the survey asked who the respondent had been harassed online by, so the survey does not account for experiences of women who have never suffered online harassment, which comprised 7 per cent of the survey respondents. This first survey was mainly used to collect as a base to design the second survey, and less for the results it tabulated.

The second survey opened the floor not only to women who had never experienced online harassment but to journalists of all genders. The aim was to explore how secure journalists felt on online spaces. The survey was distributed carefully to 15 print, online and television journalists from across Pakistan who then asked their colleagues to fill it out. This was done to ensure that the responses are genuine, and not hastily filled.

The survey was divided in two parts; the first part inquired journalists' understanding of digital security, their online fears and media organizations' attitudes towards online threats. The second part was only addressed to journalists who had experienced online threats or harassment – 32 per cent of total respondents opted out of the second part of the survey since they had never experienced online threats or harassment, hence exposing that the majority of journalists feel insecure online.



Eighty-six per cent of the respondents work for local news organisations, while 12 per cent are freelancers and 4 per cent are based in Pakistan but work for foreign media organizations. The surveys were also divided across journalists who work online (66 per cent), print (48 per cent), television (30 per cent) and radio (4 per cent).

Both parts of the survey ended with a qualitative section where journalists shared their recommendations for what journalists, media organizations and the government could do to increase digital security for journalists.

BREAKDOWN OF PARTICIPANTS BASED ON THEIR AFFILIATION

86% 12% 4%

Local news
organisations

Freelancers

Foreign media
organisations

BREAKDOWN OF PARTICIPANTS BASED ON THE MEDIA

66% 48% 30% 4%

work online

work in print

work in television

work in radio

The Gender Lens

Lastly, it is important to mention that the second survey was divided by gender, after completion. This was done in order to analyse how different genders experience digital insecurity, and also to investigate whether different genders respond to digital violence in different ways. Forty-two percent of the total respondents were male, and 58 per cent were female.

Online harassment can take various forms. One of the more recent and more disturbing forms of harassments are sexual and violent in nature – however it is crucial to remember that online sexual violence is not a consequence of lust or desire, it is also not a consequence of how “attractive” the journalist is, the motivation is simply to silence the journalist by exerting force, power and intimidation.³

To highlight that male and female journalists experience and react to digital security in different manners, this survey will revert to this gender lens in various questions.

³ Ed: Munoz, Elisa Lees. “Violence and Harassment against Women in the News Media”. International Women’s Media Foundation. March 2014.

1. WHY DIGITAL SECURITY MATTERS?

The survey learnt 92 per cent of the survey's respondents believe that online harassment in journalism is either "extremely common" or "common". Only 8 per cent of respondents believe that online harassment is rare or extremely rare.



These basic figures clearly show that a problem persists. Earlier it was believed that fears and scares from the digital could, at times, translate into physical insecurity, and only in such cases would the online violence be taken seriously. Now, however, it is understood that the virtual and physical world are two sides of the same coin, or reflections of each other. "Online violence is real violence," says Bishakha Datta of the Mumbai-based non-profit Point of View. "We need to address online violence because it limits our right to free and full participation, our freedom of expression and our right to safety and to privacy. Just because it's in the virtual realm doesn't make it any less real."

Online violence is a manifestation of violence in the 'real world' and needs to be dealt with as strictly and urgently, but perhaps not with the same tools and weapons. Only 6 per cent of respondents failed to establish any link between digital and physical insecurity. The majority of respondents can see a direct link between physical and digital insecurity and 38 per cent say that the link is only established 'sometimes'.

⁴ "Online violence: Just because it's virtual doesn't mean it's not real." Global Fund for Women.

11. Do you think a journalist's digital insecurity is tied in with their physical insecurity?



56%
Yes



38%
Sometimes



6%
No

In another question, we asked journalists how online insecurity affected their journalism careers. A whopping 45.5 per cent reported that it resulted in self-censorship. This is not a small number – it means that almost 50 per cent of journalists are being coerced into censoring themselves by making them feel unsafe and insecure, and the worst part is that a large proportion of these crimes go unreported and unpunished.

18.2 per cent of respondents said that after experiencing digital insecurity they confined themselves to certain beats, thereby implying a different kind of self-censorship i.e. by not allowing themselves stories that

45.5%

respondents said that online insecurity resulted in self-censorship



seem more controversial. Similarly, 33.3 per cent of respondents said they used social media less after undergoing online insecurity of various types; 15.2 per cent even deactivated their social media accounts out of fear.

Fortunately, there is a segment, comprising 36.4 per cent of the respondents who said that experiencing digital insecurity did not impact their career in any way. From a policy point of view, the goal should be to empower and protect journalists, in digital spaces, so well, that this percentage rises to a 100 per cent.

5. How did the online insecurity/harassment affect your journalism career (You may check more than one box)?

36.4%

Not at all

33.3%

I used social media less

45.5%

Resulted in self-censorship

15.2%

I deactivated my social media accounts

18.2%

I confined myself to certain beats

0%

I considered giving up my profession altogether

2. THE GENDER LENS

Earlier this report established that 66 per cent of all respondents had suffered from at least one form of digital insecurity. If we divide our journalist respondents by gender, we can see that 72 per cent of female journalists said yes to having experienced digital insecurity, while within male journalists, 61 per cent reported to having suffered online insecurity.

Similarly, when respondents were asked if online harassment of journalists was gender specific or gender neutral, 60 per cent of respondents said that harassment was gender specific.

10. Do you think online harassment of journalists is:

60%
Gender Specific ♀

40%
Gender Neutral ♀♂

It is important here to understand that this report is not implying that male journalists are not harassed, or that they harassed far less than women. In fact, some surveys have revealed that “male celebrities are recipients of more abuse overall on Twitter than their female counterparts”. The point the above responses make is that women’s harassment is more likely to be gender-based and that has specific, discriminatory harms rooted in our history. The study pointed out that the harassment targeted at men is not because they are men, as is clearly more frequently the case with women. It’s defining because a lot of harassment is an effort to put women, because they are women, back in their “place.”⁵

⁵ Chemaly, Soraya. “There’s No Comparing Male and Female Harassment Online.” Time Magazine. September, 2014.

As Soraya Chemaly writes in an article for Time Magazine: “The harassment men experience also lacks broader, resonant symbolism. Women are more frequently targeted with gendered slurs and pornographic photo manipulation because the objectification and dehumanization of women is central to normalizing violence against us. Philosophers Martha Nussbaum and Ray Langdon describe in detail how this works: women are thought of and portrayed as things for the use of others. Interchangeable; violable; silent and lacking in agency.”

Chemaly’s hypothesis is put to the test in our survey. When female journalists are asked how the harassment of female and male journalists differs, 71 per cent of them cite that female journalists are more likely to be attacked on their appearance. Similarly, 68 per cent of them also believe that female journalists are attacked more than male journalists on their personal lives.

3. THE CRIMES AND CRIMINALS

Before the report proceeds to explain how digital insecurity affects journalists' mental health, ability to work and increases their physical insecurity, it's important to account for the most common crimes against journalists that occur online, and who carries them out.

The overarching culprits of online threats/harassment are "strangers". Over 90 per cent of respondents said they faced harassment from "strangers". The next categories, "Someone you know/trust", and "Colleagues" were at 15.2 per cent and 12.1 per cent, respectively. The last category, "Law enforcement personnel" have harassed 6.1 per cent of the respondents.

The most common type of threat that respondents experienced was Cyber Stalking – 45.5 per cent of respondents complained about it, followed by 42.4 per cent of respondents having suffered "threats that made them feel insecure". The next two most common crimes included being sent malware/phishing emails, and lastly, having their social media hacked. (A complete list with numbers can be seen below.)

1. What kind of online insecurity/harassment have you experienced (You may check more than one box)?

33.3%

My social media was hacked

42.4%

I received threats that made me feel insecure

9.1%

I've had my data stolen

9.1%

My computer was hacked

15.2%

I was blackmailed

21.2%

Other

36.4%

I was sent malware/phishing emails

21.2%

I was harassed over a sustained period of time

15.2%

I was sexually harassed

45.5%

I was cyber-stalked

The Gender Lens

For both male and female respondents, digital criminals were mostly strangers, with a handful of reports against colleagues and people they knew/trusted. It appears that law enforcement agencies are also equally likely to harass male and female journalists.

However, the nature of the crime against male and female journalists were disparate. In the case of cyber stalking and hacking of social media, male and female journalists remained on equal footing. But it appears that male journalists on the survey did not experienced harassment over a sustained period of time; and their chances of being blackmailed and sexually harassed online were half of those of female journalists.

Nevertheless, a large proportion of male journalists were sent malware/phishing emails, and they were much more likely to have their computer hacked and to have their data stolen. As mentioned before, it's not that male journalists are more secure online than women, it's just the nature of the threats that are different.

It is interesting to note that neither the type of harassments, nor their segregation across gender is particular to Pakistan. Take, for instance, this data from Pew Research Center's 2017 analysis of how harassment differs between males and females: "There are also differences in the types of experiences men and women have had online. Overall, 44% of men and 37% of women have faced some form of online harassment. Men are somewhat more likely than women to have been called offensive names online (30% vs. 23%) or to have received physical threats (12% vs. 8%). By contrast, women – and especially young women – receive sexualized forms of online abuse at much higher rates than men. Some 21% of women ages 18 to 29 have been sexually harassed online, a figure that is more than double that of men in the same age group (9%). Further, 53% of young women say that someone has sent them explicit images they did not ask for (compared with 37% of young men)."

Crime	Female Percentage	Male Percentage
My computer was hacked	0	8.3%
I received threats that made me feel insecure	33.3%	50%
I was harassed over a sustained period of time	23.8%	0%
I was cyberstalked	38%	33.3%
I was sent malware/phishing emails	19%	50%
I was blackmailed	14.2%	8.3%
I was sexually harassed	14.2%	8.3%
My social media was hacked	28.5%	33.3%
I have had my data stolen	4.7%	8.3%
Other	19%	25%

4. HOW DO JOURNALISTS FALL SHORT?

In order to fight digital insecurity, it is important for journalists to report the crimes they experience. The most common response to experiencing online security is to block the harasser on social media – 66.7 per cent of the respondents did that. Thirty-three per cent of respondents did absolutely nothing.

As far as reporting the suspects goes, journalists seem reluctant to do so: 24.2 per cent reported the online threats to bosses, a smaller 18.2 per cent reported to social media websites and an even smaller 9.1 percent reported to the FIA.

This shows that journalists do not feel encouraged or compelled to report their complaints about digital security. There are various reasons for this; the most common of which, at 36.4 percent, is that despite being journalists they do not know how to report the crime/harassment. Another reason for the lack of reporting in this regard is because often the crime/harassment is not considered serious enough by them.

These reasons explain how journalists fall short; given that most journalists do understand that without reporting crimes, it is difficult to create a momentum to curb them. Eighteen per cent of journalists said that they didn't report the crime because it would take up too much of their time.

4. If you didn't report them to anyone, why was that (You may check more than one box)?

24.2%

I didn't think the crime/harassment was serious

24.2%

I was afraid those I'd report to would harass me

12.1%

Reporting the crime required me to travel a long distance

18.2%

Reporting the crime/harassment would take too much time

18.2%

FIA response system is slow and useless

27.3%

I reported them

36.4%

I didn't know how to report the crime/harassment

3%

My organisation's response system is slow and useless

Fortunately, there was a segment of journalists, albeit small, at 27.3 per cent that reported the insecurity they felt. At this point it may also be pertinent to explore that dealing with online surveillance, harassment, threats and blackmailing may be terrifying and reporting the crime may be easier said than done. It would also be pertinent to mention that online harassment comes hand in hand with a host of mental health issues and without adequate support systems, reporting the crime can seem like a tedious, terrifying ordeal.

4.5. Digital insecurity, mental health and support systems

One aspect of digital insecurity that is often ignored is the toll it can have on the victim's mental health. When a person is threatened, blackmailed, stalked, robbed in the physical world, it upsets their mental peace, the same way when a person experiences threats or attacks in cyberspace, even if they don't have scars to show, they are affected.

The survey shows that 63.6 percent of the respondents felt stressed when they were harassed, while 67.6 per cent were annoyed and 54.5 per cent were angry at being attacked online. Slightly more than half the respondents felt afraid, at 51.5 per cent.

Other unfortunate experiences that respondents experienced were alone (15.2 per cent), guilty (3 per cent) and suicidal (6.1 per cent).

The Gender Lens

At this point it might be pertinent to return to our gender lens for a brief moment to analyze if male and female journalists emotionally react to harassment in similar ways. Diving the data across genders reveal that the feelings male journalists experience while facing digital insecurity are not that vastly different from women (see table below) hence implying that mental health services and support systems while facing online threats is a tool both genders should have access to.

EMOTIONS	FEMALE JOURNALISTS %	MALE JOURNALISTS %
Annoyed	57	50
Stressed	66	50
Angry	57	50
Afraid	52	50
Suicidal	9	0
Alone	9	25

In fact, the probability of men feeling “alone” while undergoing online insecurity is much higher than that of women, perhaps because women have the ability to confide in their peer groups. Let’s have a look at that data:

Who did you confide in?	FEMALE JOURNALISTS %	MALE JOURNALISTS %
Friends	66	33
Colleagues	52	17
Family	43	17
No one	14	50

We learn that while journalist across the genders inwardly experience very similar emotions to being harassed, their outward responses differ vastly. Female journalists are a lot more likely to confide in friends, family and colleagues, while data shows that half of the male journalist respondents did not share their concerns with anyone.

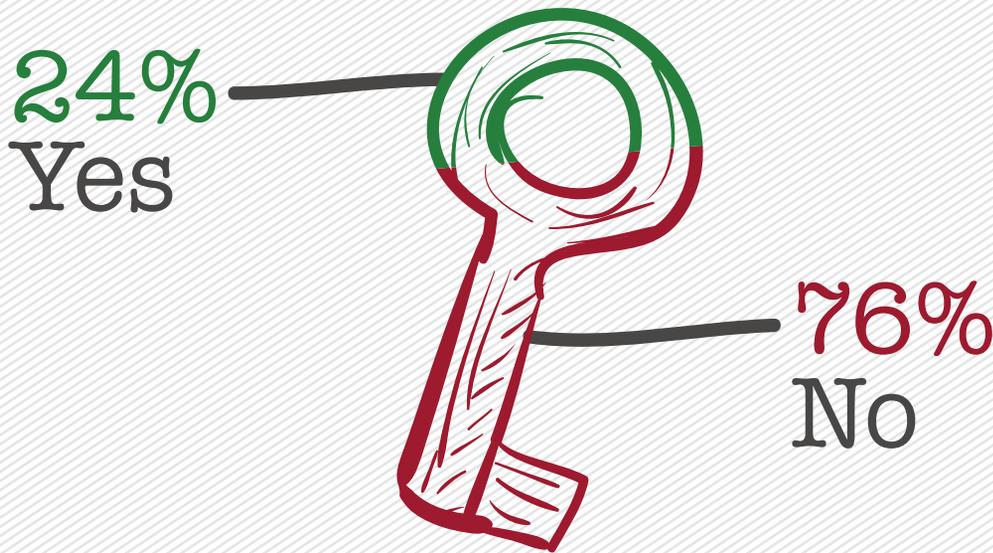
To further understand why that is, we can again turn to the numbers. Upon confiding, 95 per cent of the women found emotional support, whereas only 36 per cent of the man received emotional support. Similarly, 19 per cent of the women were helped by peers to file reports, while this was true for zero per cent of the men. Most interestingly, a larger percentage of men were told to go offline, to quit journalism and were simply ignored, than women. Hence explaining why such a large percentage of male journalists refused to confide in anyone about their digital insecurity

REACTION	FEMALES	MALES
Supported me emotionally	95	36
Helped me file a complaint	19	0
Blamed me	4	9
Asked me to go offline	19	36
Asked me to quit journalism	9	27
Ignored me	0	27

5. HOW DO NEWS ORGANIZATIONS FALL SHORT?

Seventy-six per cent of respondents confirmed that their news organization had never held a training for digital security and privacy. Trainings on digital security and privacy are vital for journalists today since they can help journalists protect themselves against digital threats.

4. Has your news organization ever held a training for digital security and privacy?



According to the European Federation of Journalists, “[j]ournalists face an increasing challenge to secure their communications in a digital world. The protection of confidential source can be easily compromised in a world where surveillance is becoming ubiquitous. Trainings are vital for journalists to protect their sources in a fast-paced digital newsroom, bypass internet censorship and secure their online communications.”⁶

(In 2012, Bytes For All conducted a national survey to ascertain if journalists and bloggers were aware of ways to protect themselves, their data, and their sources online. Data revealed that 90 per cent of respondents had never received any training in digital security. It appears that, the country’s media organizations have been recognizing the need for trainings.)⁷

⁶ “Cyber security training for journalists: Tips and tricks to keep your communications safe.” European Federation of Journalists. 2015

⁷ “Digital Security and Journalists – A SnapShot of Awareness and Practice in Pakistan”. 2012. Bytes for All, Pakistan.

It was a relief to see that the 24 per cent of journalists who did receive training were spread across Online, Radio, Television and Print organizations. It would be disheartening if only Online media organizations were training their employees since digital security and privacy are pertinent to all kinds of journalists regardless of the medium they work with.

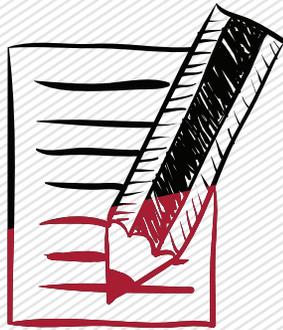
Within this 24 percent, the tool most journalists were introduced to included learning how to set a secure password and online ethics. Only a meagre 8 per cent were taught how to recover lost data, which is a skill 80 per cent of the respondents are interested in learning. Similarly, 62 per cent of the respondents wanted to learn how to report an online crime/harassment to the FIA, but only 24 per cent of trainings were taught this. Further skills and tools that journalists are interested to learn through basic trainings on digital security and privacy will be discussed in the recommendations part of this report.

Another way in which news organizations have failed their employees in the realm of digital security is the absence of policies for reporting online threats/harassment. An overwhelming 60 per cent of the respondents admitted that their media organization has no policy to report or deal with online threats/harassment. Out of the journalists who do have access to a policy to report online crimes to their media organizations, only 18 per cent can take their cases to Human Resources; the rest have to suffice by reporting their digital security problems to their editor, who may or may not have the skills/expertise/training to deal with online threats/harassment.

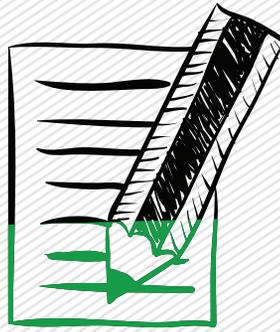
The third way in which media organizations fail their employees is when journalists who can, do report the online insecurity to their employees, 42 per cent of the complainants are provided with no follow up, i.e. their reports are registered but the case ends there. Eighteen per cent of complainants are told to ignore the harasser or crime – this is counterproductive as it discourages journalists from reporting online threats/harassment and it allows blackmailers and harassers to continue their practices with impunity.

It is a pleasure to note that out of the small pocket of media organizations that do have a mechanism of reporting digital insecurity, 40 percent respond to their employees' complaints with digital and psychological support. It shows that within the small pockets where employees are being encouraged to report digital insecurity, media organizations are willing and able to provide much needed support to journalists.

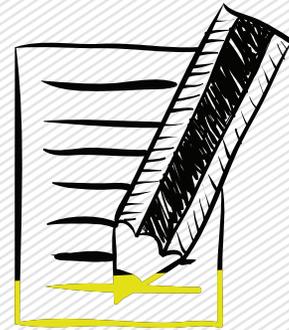
8. When colleagues/or you yourself have reported online insecurity to your media organization, what steps were taken to address it?



42%
There was no
follow-up



40%
The staff is provided
digital and psychological
support



18%
The staff is told
to ignore it

However, the general sense revealed by the qualitative part of the survey is that “media organization should listen to their employees when they report online/digital threats.” A survey respondent writes that “Media organizations and editors should not ignore the matter [when reported].”

The last way media organization’s fail their employees, as revealed by the survey, is by monitoring their own employees. Journalists in the survey raised the issue by citing that “the organizations you work for should not be monitoring your computers”, and by stating that “my online/data security is being breached by our own organization’s IT department”. The survey revealed that in some organizations, the institutions themselves were monitoring employees’ social media, email accounts and browsing history. One respondent said “I’d like to have a guaranteed digital security or employees and their online/personal data within their workspace. We’ve been in a protest against this act of our IT department but it hasn’t been proved to be of much help”.

They also have to no one to report their organization to, which brings us to the failure of the Federal Investigation Agency (FIA)’s National Response Centre for Cyber Crime (NR3C).

6. HOW DOES THE GOVERNMENT FALL SHORT?

The survey reveals that the Federal Investigation Agency (FIA)'s National Response Centre for Cyber Crime (NR3C) has failed on two counts. The first being that while the FIA set up the NR3C almost a decade ago, they have failed to disseminate information about how digital threats and crimes can be reported to them. Data reveals that 62 per cent of journalists who partook in the survey did not know how to report digital insecurity to the FIA. If that is the percentage of journalists who don't know how to access the FIA, one shudders to imagine the amount of ordinary citizens who don't know how to access this online crime-fighting wing, hence rendering it useless to them.

Through the survey we also learnt that many journalists do not know "how and where to report digital threats and crimes", they desire "easy access to FIA's cyber-crime wing (NR3C)", and in their recommendations, have included "prompt and active response from FIA and other security agencies, mostly they don't respond properly".

6. Are you interested in learning (You may check more than one box):

46%

How to set a secure password

62%

How to report an online crime/harassment to FIA

54%

What constitutes as online harassment

58%

How to keep your phone/password protected

56%

How to deal with online harassers

80%

How to recover lost data

60%

How to send a secure email

50%

How to report a harasser to a social media website

50%

Online ethics

10%

I already know all this

The second count against the FIA is that out of all the respondents who face digital insecurity, only 9 per cent reported their cases to the FIA. This number, again, goes to show that the cyber-fighting wing is hardly being used the way it was meant to be. Additionally, apart from the 62 per cent of the respondents who didn't know how to report a crime, 18.2 per cent of the respondents didn't report it to the FIA because they believe "the FIA's response is slow and useless". Lack of reporting is contingent on lack of public confidence in law enforcement, and it is a matter that the FIA needs to take seriously.

4. If you didn't report them to anyone, why was that (You may check more than one box)?

24.2%

I didn't think the crime/harassment was serious

24.2%

I was afraid those I'd report to would harass me

12.1%

Reporting the crime required me to travel a long distance

18.2%

Reporting the crime/harassment would take too much time

18.2%

FIA response system is slow and useless

27.3%

I reported them

36.4%

I didn't know how to report the crime/harassment

3%

My organisation's response system is slow and useless

Lastly, an overwhelming 63.6 per cent of respondents believe that the ideal response to online harassment are "stricter FIA laws" and 72.7 per cent believe that the laws which already exist should be implemented.

RECOMMENDATIONS

In light of the responses from the survey, DRF posits the following recommendations regarding journalist safety:

1. Security is all encompassing

Digital safety and security should be included under the definition of “protection” in the Bill. In the digital age, the internet is a commonly used medium of news reporting and consumption--all major news outlets have a digital component as well. Most journalists use the internet in some form or another: to communicate via email and messaging apps, cultivate sources, disseminate information through social media or publish online. Under this digitized landscape Digital Rights Foundation (DRF) feels that it would be remiss to exclude digital security from the realm of protections guaranteed under the proposed Bill. Digital security intersects with physical security in complex ways, thus it is an aspect that can no longer be ignored. These observations are in line with international best practice and juridical opinion.^[1]

2. Institutionalisation of digital safety of journalists:

Training journalists about digital security is crucial. Journalists should know which of their devices can be tracked, hacked or monitored, and how they can prevent this. These trainings can occur at two levels: at the level of private media houses and at the level of the federal/provincial government.

Journalists should not be sent into conflict zones without proper training and safety equipment, hence, the same way, journalists should not have to navigate the internet without proper training about how to tackle attacks and threats, and the proper equipment/software to do so.

These trainings must include teaching journalist what to do in case they are harassed/attacked/threatened – no journalist should not know how to report a crime. The onus for trainings should rest with media houses and organisations, and should be a continuous process of reinforcement and responsive to emerging threats.

[1] UN General Assembly, “The safety of journalists and the issue of impunity”: report of the Secretary-General”, 6 August 2015, A/70/290, available at: <http://www.refworld.org/docid/55f2cd454.html>

3. Social media protection:

Better communication and channels should be built with social media companies that sometimes harm the interests of journalists.

4. Institutionalisation of reporting mechanism:

It should be made mandatory on media organizations to hear and respond to digital security concerns of journalists. Media houses should immediately be instructed to set up systems and channels where employees can report the various ways they are being harassed, threatened, monitored, and attacked online. Furthermore, there should be a mechanism by which journalists can report media houses that do not respond to their grievances regarding online security.

5. The state must take more responsibility:

The FIA's NR3C are required to accord more resources into ensuring journalists safety and understand the unique challenges that they face. Their responses need to be made more sensitive, timely and effective. Since they are the only federal agency fighting online crime, the responsibility on them is great and they should be provided with better and more resources.

The FIA should fulfill its obligation to submit six-month reports to the senate about how many cases they solve, and how many suspects are convicted. Effectiveness of laws must be checked, and if ineffective, they must be improved. These reports should be public and open to public scrutiny.

6. Lift obstacles on use of encryption:

While policy and regulation are quite murky, the Pakistan Telecommunications Authority (PTA) requires prior approval for the use of VPNs and encryption. This impacts the work that journalists can do.^[2] The UN Special Rapporteur on Freedom of Expression has concluded that encryption and anonymity deserve strong protection and recommended that legislation and regulations protecting journalists also enable access and provide support to technologies to secure and protect their communications.^[3]

^[2] PTA VPN Policy: http://www.ispak.pk/Downloads/PTA_VPN_Policy.pdf

^[3] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye", 22 May 2015, A/HRC/29/32, <http://undocs.org/A/HRC/29/32>, pg. 4.

7. Provisions for Women Journalists:

In a report by Report of the Secretary-General published in 2017,^[4] noted that women journalists face additional threats to security in the gendered threats, harassment, gender-based violence and discrimination at the workplace. Women are less likely “less likely to have the same contractual protection; in addition there are fewer women working in senior and management position [...] They are also less likely to be asked to work on high-profile issues.”^[5] These same concerns were raised through DRF’s own research.^[6] The onus must be placed on media organisations to address these gendered issues, and have functioning mechanisms in place when female journalists experience these issues. Existing laws on workplace harassment, online harassment and gender discrimination need to be implemented specifically keeping in mind the needs of female journalists.

8. Provisions for Freelancers:

Freelancers are the most vulnerable kind of journalists. Redress must be provided about who they can turn to while facing digital insecurity. A freelancers’ union could be created to encourage their online security.

[4] “The safety of journalists and the issue of impunity Report of the Secretary-General”, 4 August 2017, A/72/290,

https://digitallibrary.un.org/record/1304392/files/A_72_290-EN.pdf

[5] Ibid, pg. 3.

[6] “Surveillance of Female Journalist of Pakistan”, Digital Rights Foundation, December 2016,

<http://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female->



Digital
Rights Foundation

www.digitalrightsfoundation.pk

 /DigitalRightsFoundation

 @DigitalRightsPK