CIPESA

DATA ANALYSIS REPORT FOR ORGANIZATIONAL CYBERSECURITY ASSESSMENT

08th 07 2024
Evidence and Methods Lab
Plot 13, Kenneth Dale Lane
Kampala Uganda
T: +256783474784
E:hello@evidenceandmethodslab.org
W: www.evideceandmethodslab.org

Table Of Contents

Background

In the rapidly evolving digital landscape, cybersecurity has become a critical concern for organizations worldwide, particularly for civil society organizations (CSOs) that often operate with limited resources and face increased targeting by cyber threats. The Collaboration on International ICT Policy for East and Southern Africa (CIPESA), supported by the East West Management Institute (EWMI) in collaboration with Chapter Four, aims to address these challenges by developing and implementing a CSO Compliance Index for the Regulatory Framework and Digital Security. This initiative seeks to evaluate the cybersecurity readiness of organizations across various thematic areas of operation.

Through this initiative, a comprehensive study was commissioned, and a specialized tool was administered to a diverse range of CSOs, including NGOs, community-based organizations (CBOs), and media establishments. The primary objective of this study was to assess the level of CSOs' compliance with regulatory frameworks and their adoption of digital security tools and methods, ultimately enhancing civil society operations.

Introduction

This report presents the findings of the cybersecurity assessment survey conducted among local civil society organizations in Uganda, as specified in the Terms of Reference (ToR) provided by CIPESA. The survey covered a broad range of themes critical to cybersecurity, including operational security, documentation and policy, internal data risks, staff training and support, staff offboarding processes, travel security, data security, website security, office security, messaging and collaboration, legal risks, device security, software security, and password management and authorization.

The primary objective of this assessment was to develop a Cybersecurity Compliance and Readiness Index for Digital Security. By systematically evaluating their practices and policies, we aim to highlight areas of strength and identify key areas for improvement. This report offers a detailed analysis of the survey results, providing insights and recommendations to help organizations bolster their cybersecurity posture.

The following sections delve into each theme, presenting the data collected, analysing the current state of cybersecurity readiness, and suggesting steps to enhance overall security. Through this report, we aspire to empower local civil society organizations to adopt robust cybersecurity measures, ensuring their resilience against the growing spectrum of cyber threats.

Methodological Approach in Cybersecurity Assessment Analysis

In addressing the cybersecurity readiness of civil society organizations (CSOs), we undertook a comprehensive methodological approach that began with meticulous data cleaning and preparation. This initial phase involved removing irrelevant or incorrect data entries, handling missing values through imputation or exclusion, correcting errors, and eliminating duplicates. Additionally, the data was transformed into suitable formats for analysis through normalization, aggregation, and encoding. We employed a series of tools like MS Excel and Stata to ensure the dataset's accuracy and reliability, and to achieve a high level of data integrity.

Following data cleaning, we engaged in a detailed data analysis phase to explore the dataset's characteristics and generate insightful findings. This included conducting Exploratory Data Analysis (EDA) using Stata for data manipulation, descriptive statistics and data visualization with MS Excel.

The final phase involved reporting the analysis results, focusing on effective communication to stakeholders. We created clear and informative visualizations using MS Excel, Tableau and other design software to convey the findings effectively. A detailed report was prepared, emphasizing key insights and actionable recommendations to enhance the cybersecurity measures of the CSOs. This report was tailored to be comprehensible to audiences with varying levels of data literacy, ensuring the critical information was accessible and practical for decision-making.

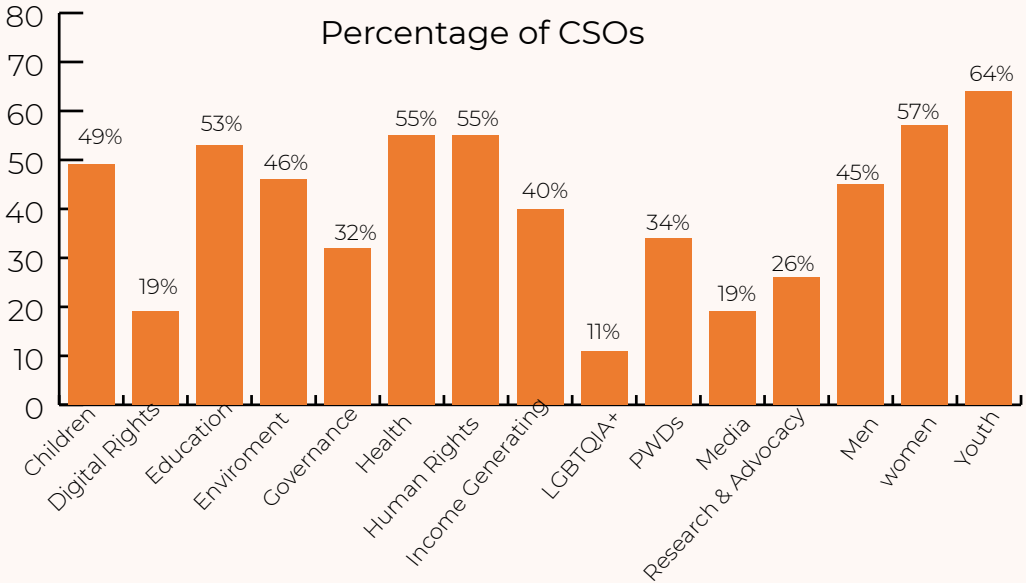
By following this structured methodological approach, we provided a thorough and insightful analysis of the cybersecurity readiness of local CSOs. This process ensured that data was accurately prepared, rigorously analysed, and effectively communicated, ultimately aiding these organizations in bolstering their cybersecurity posture and protecting their operations and data from evolving cyber threats.

Report Findings

The section below provides a comprehensive overview of the cybersecurity practices and concerns within the surveyed organizations. The insights highlight areas of strength and opportunities for improvement based on the descriptive analysis of the survey data.

Organizations' Analysis

The cybersecurity assessment survey included a diverse array of civil society organizations (CSOs) operating in various thematic areas.



The data reveals, a significant portion, 64%, of the participating CSOs focused on youths, 57% focused on women, 55% on Health and Human rights respectively, 53% on education while 49% of CSOs focused on Children affairs, 46% focused on Environment, land and excavation. Only 11% of the CSOs reported to be focused on LGBTQIA+, 19% focused on Digital Rights.

The findings reveal that the areas which created additional risk largely included, Advocacy 65.6%, Communication 52.5%, and Partnerships 50.6% while other areas like Grant making created the least additional risk 17.8%.

Major threats to organizations' cybersecurity by thematic area of operation

The table below presents the nature of threats that present concern to the CSOs based on the thematic area in which they operate.

From the findings, state-sponsored attacks were a major concern for organizations undertaking work in areas of LGBTQIA+ (53%) and Governance (38%) while ransomware attacks are a significant threat for organizations working in areas of Digital Rights (53%) and Media (41%) which highlights the critical need for robust cybersecurity measures in these areas where information dissemination and advocacy are paramount.

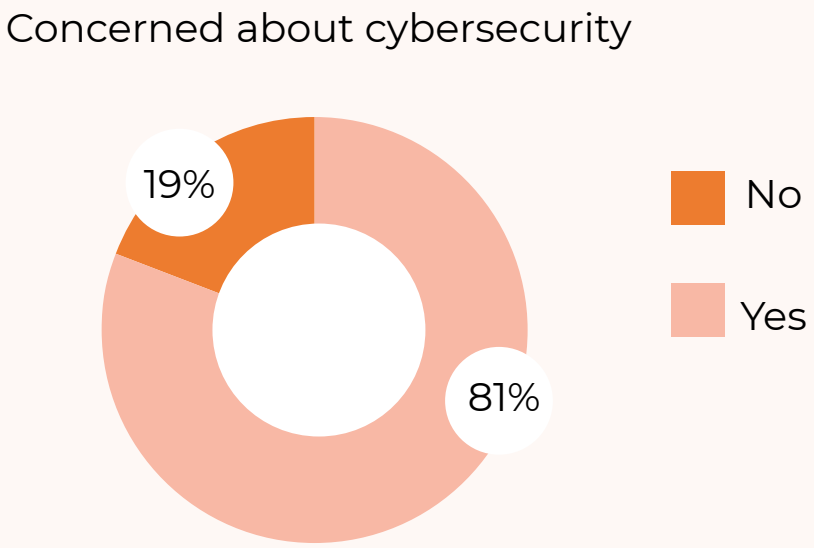
Lack of organizational cybersecurity programs was registered as a prevalent issue amongst organizations working in areas of LGBTQIA+ (84%) and Media (84%) which expressed the highest levels of concern. Phishing attacks were notably concerning for organizations working in areas of Governance (57%) and Human Rights (59%), indicating a need for better awareness and protective measures against such attacks. Risky hybrid or remote work environments posed significant challenges for Digital Rights (65%) and Media (62%) organizations, reflecting the increased vulnerabilities that come with remote working conditions, while social engineering tactics were a significant concern for Digital Rights (51%) and Men affairs (48%) organizations.

The findings reveal the diversity in the cybersecurity challenges faced by CSOs necessitating tailored strategies to be developed to address the issues faced by the different organizations that participated in the survey.

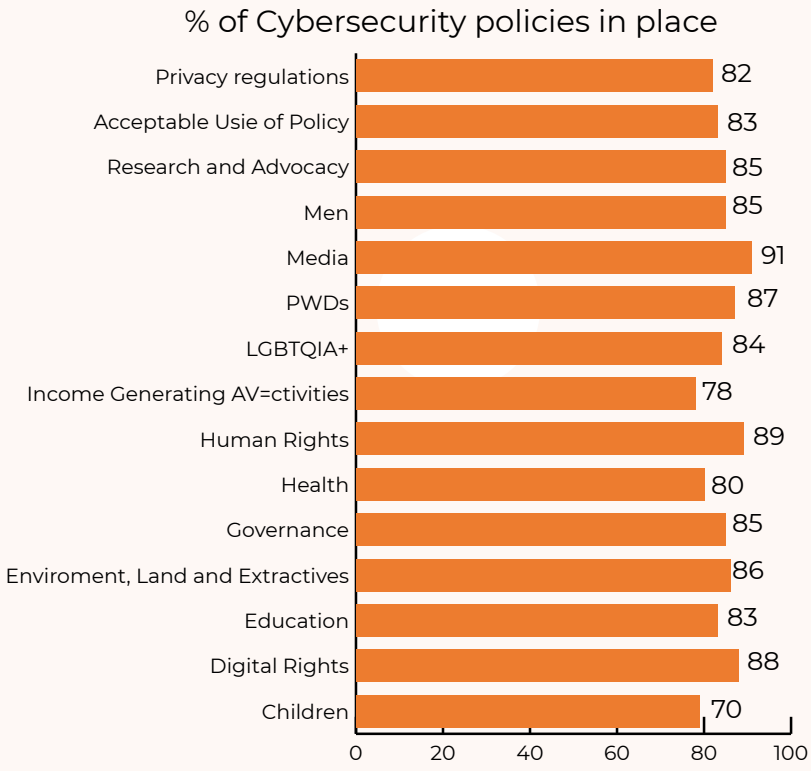
Themes	Major threats to organizations' cybersecurity					
	State-Sponsored Attacks	Ransomware Attacks	Lack of organization cybersecurity program	Phishing	Risky Hybrid or Remote Work Environments	Social Engineering
Children	21%	25%	71%	51%	46%	31%
Digital Rights	34%	53%	82%	56%	65%	51%
Education	20%	29%	78%	54%	51%	36%
Environment, Land and Extractives	31%	37%	78%	59%	54%	39%
Governance	38%	39%	81%	57%	57%	44%
Health	23%	26%	75%	49%	44%	32%
Human Rights	33%	33%	80%	59%	52%	40%
Income Generating Activities (IGAs)	22%	22%	72%	42%	42%	31%
LGBTQIA+	53%	39%	84%	47%	63%	45%
Marginalized population (Elderly, PWDs)	30%	36%	80%	54%	56%	45%
Media	37%	41%	84%	56%	62%	47%
Men	28%	43%	77%	59%	61%	48%
Research and Advocacy	30%	43%	76%	55%	53%	46%
Women	24%	34%	77%	56%	50%	39%
Youth	23%	31%	76%	56%	47%	36%

Operational Security

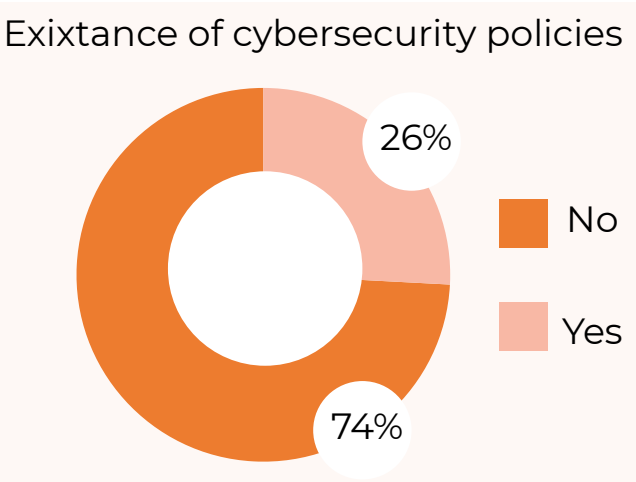
The survey revealed significant concerns regarding cybersecurity threats among the participating civil society organizations (CSOs). When asked, "Do you have any concerns about threats to your organization's cybersecurity?" an overwhelming majority, 81%, affirmed their worries, highlighting the pervasive anxiety about digital security within the sector. In contrast, only 19% of respondents indicated that they did not have any concerns about cybersecurity threats.



The figure below reveals that the majority of CSOs doing media (91%) related work exhibited highest concern about cybersecurity, followed by CSOs focused on Digital rights 88%, Marginalized population 87%, Environment, land and Extractives 86%, Research and Advocacy 85% and CSOs focused on Men 85%. The CSOs focused on Income Generating Activities 78% exhibited the least concern among CSOs by thematic areas, followed by CSOs focused on children.

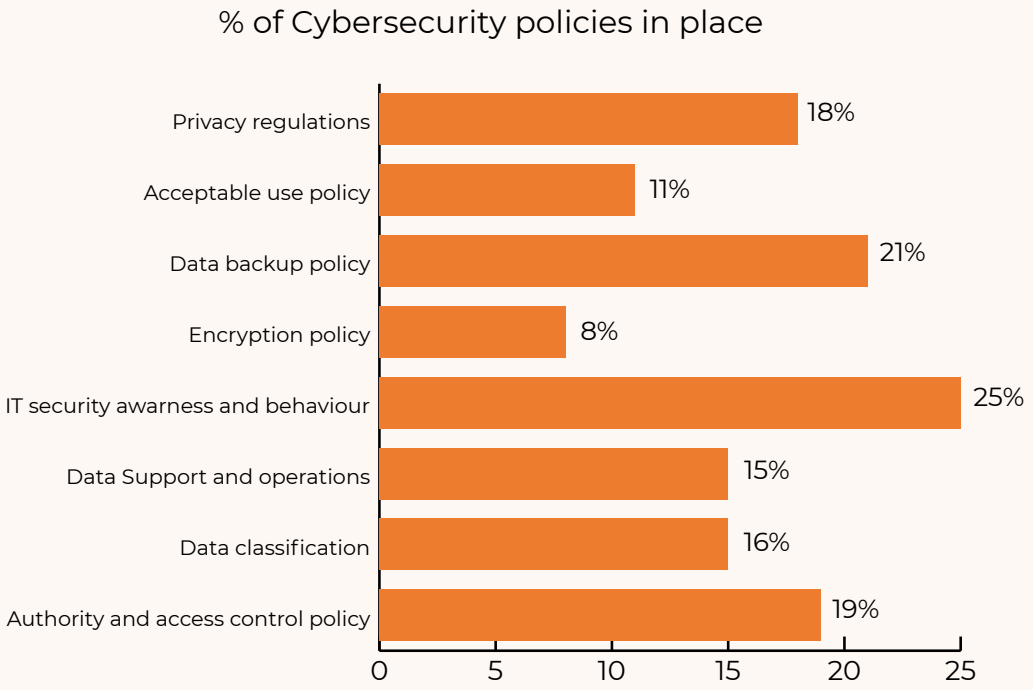


The survey revealed significant concerns about cybersecurity threats among organizations. A majority (81%) expressed concerns, with the most common threats identified being state attacks (26%), ransomware (30%), and general cybersecurity issues (76%), phishing 51%, Risky Hybrid or remote work environments 42% and social Engineering 34%.



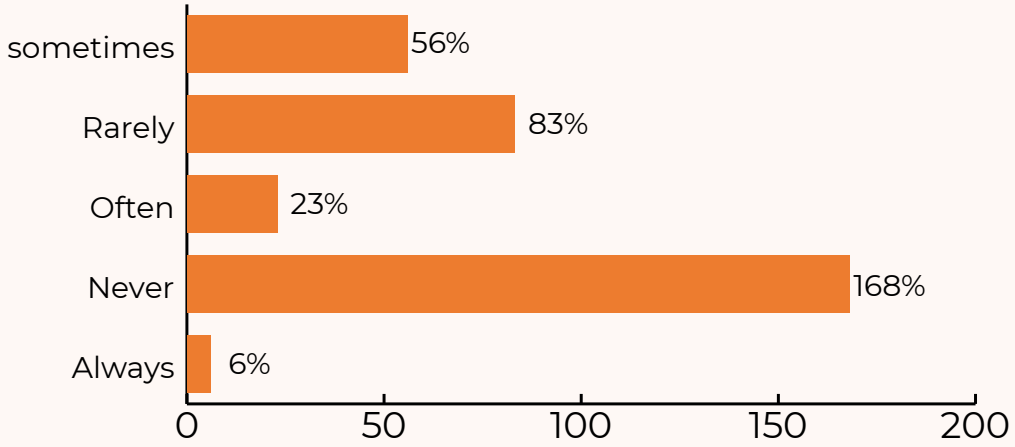
Documentation and Policy

Most organizations lack formal cybersecurity policies, with 73.89% not having any in place. Among those that do, the approach to formulating policies varied, with 57.46% not having any written policies and 21.69% discussing policies without documenting them. IT security awareness and behaviour were the most common policies in the CSOs 25%, Data backup policy 21%, Authority and access control policies were the most common (19%), and Privacy regulations policy 18%.



Regular review and updating of these policies were rare, with 50% never doing so. Employee adherence to security policies was also low, with only 3.83% always following them, while 33.92% never did.

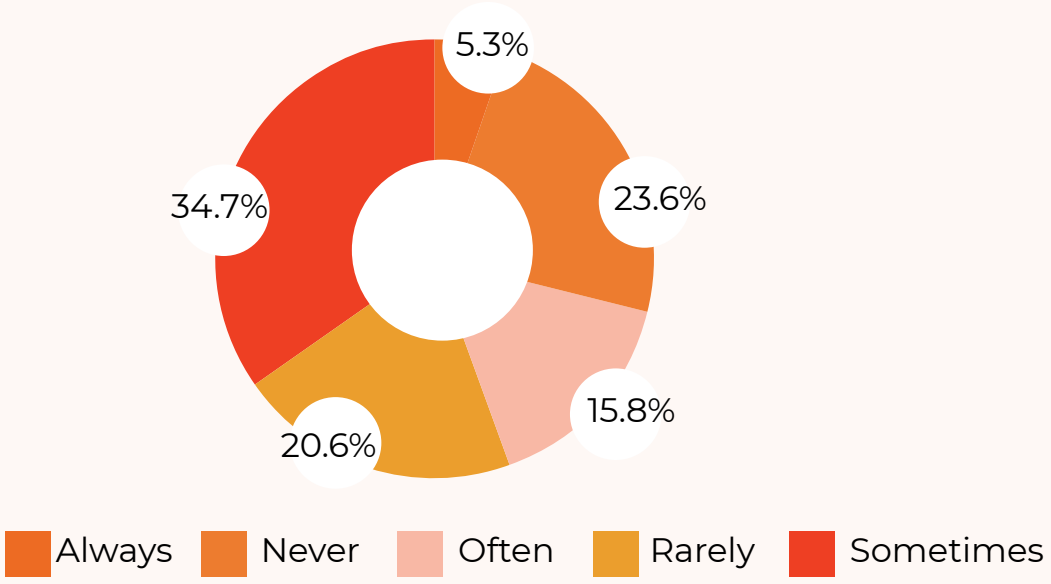
Review period and updating of cybersecurity policies?



Internal Risks (Intentional or Unintentional)

Cybersecurity concerns were identified with varying frequency; 34.72% sometimes and 20.56% rarely. Satisfaction with staff understanding of cybersecurity risks was low, with 28.33% very dissatisfied and 25.56% somewhat dissatisfied. IT support was present in 42.22% of organizations, but 29.44% had no IT support at all.

In the Past year, how frequently have you identified cybersecurity concers within your organization

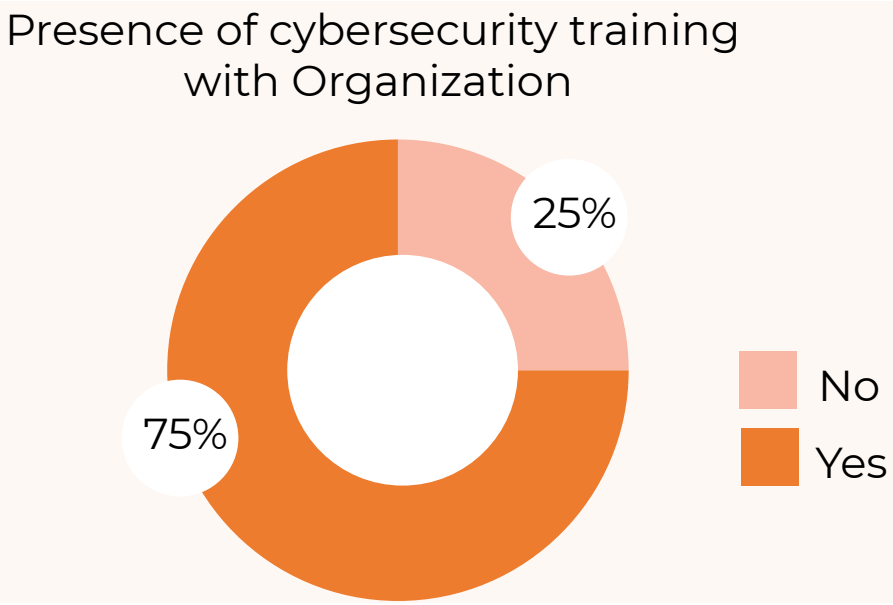


Staff Training and Support

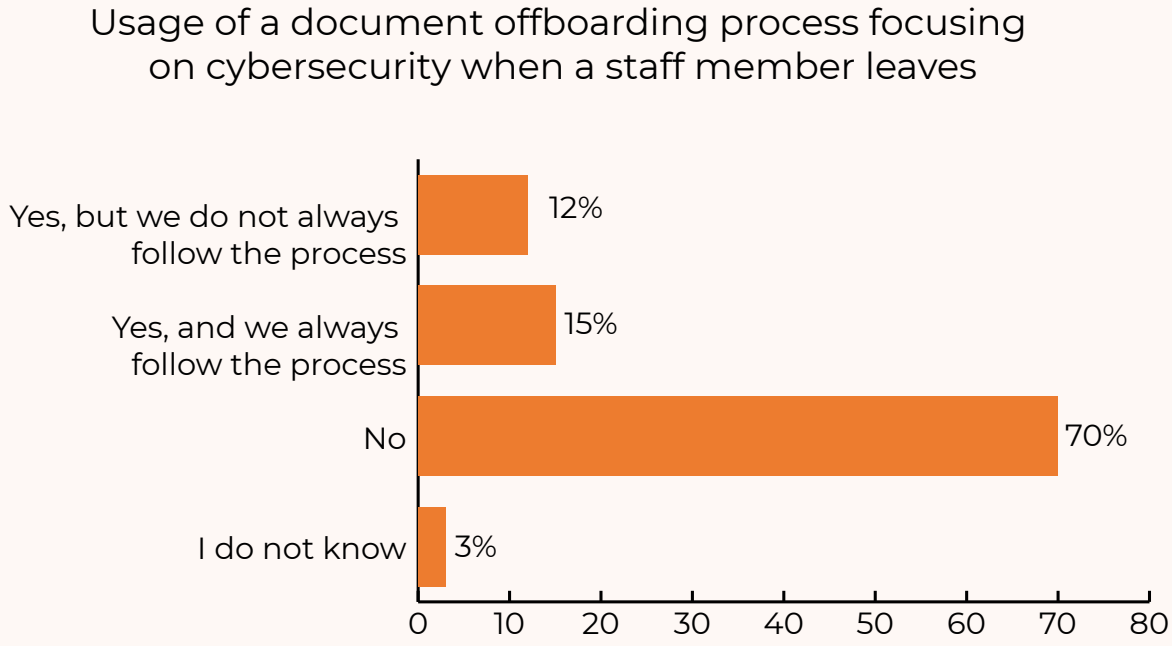
A large majority (74.72%) of organizations did not provide cybersecurity training. Among those that did, training was primarily offered to staff (28.89%) and infrequently to volunteers (7.22%). Training was most often provided only after a threat occurred (13.99%) or never (55.65%). Cybersecurity

training during onboarding was also limited, with 68.21% of organizations not providing it.

Staff Offboarding Processes



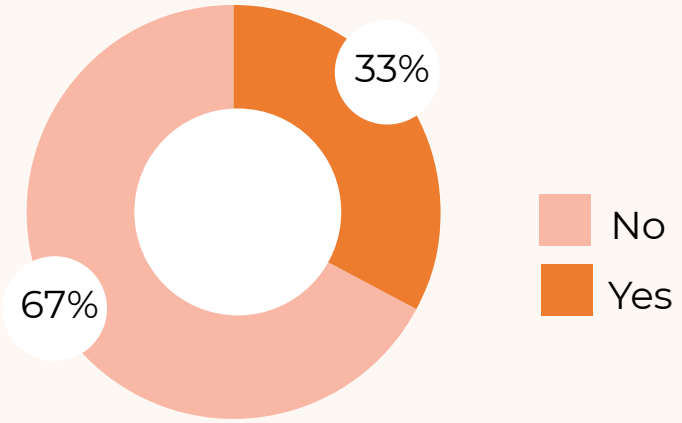
Documented offboarding processes specific to cybersecurity were largely absent, with 69.72% not having any. Exit interviews that include discussions about security were rarely conducted, with 52.5% not conducting them at all.



Travel Security

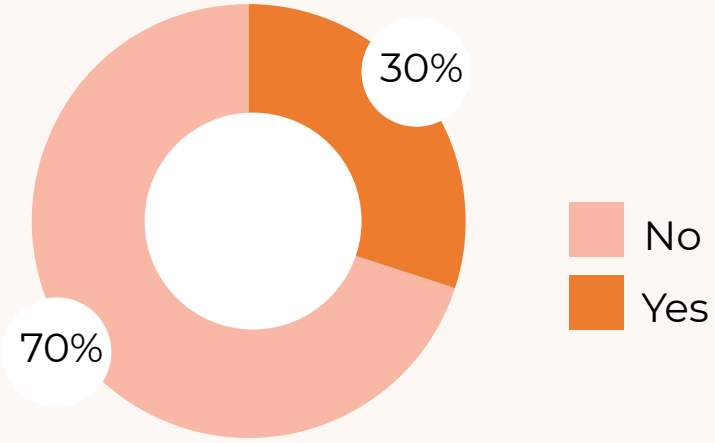
Security-related policies for travel were lacking in 66.94% of organizations. Adherence to existing travel security policies was low, with 55.87% never following them. Physical security risks were covered more frequently (26.67%) than cybersecurity risks (9.72%).

Presence of security-related policies for travel



Data Security

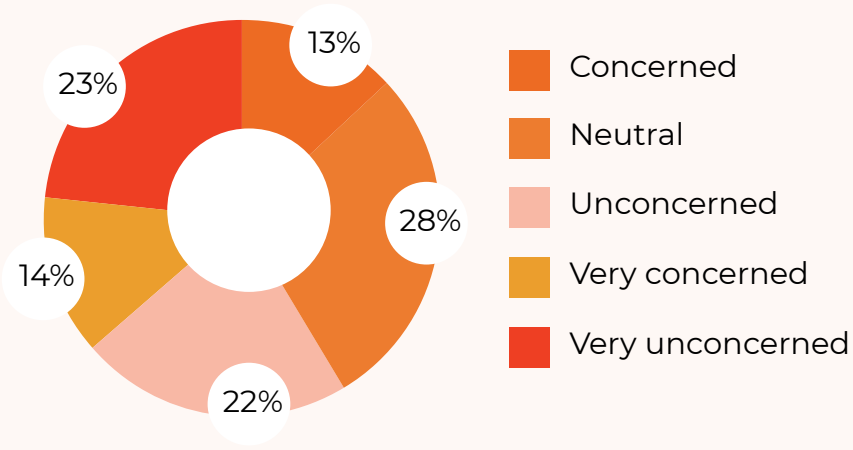
Data retention policies were not present in 70% of organizations, and data categorization by sensitivity was absent in 57.5%. Control over access to sensitive data was inconsistent, with only 34.72% restricting access to authorized staff. Regular data backups were done manually by 53.1% of organizations, while 29.2% did not back up data regularly, only 22.5% said they automated backups.



Website Security

A significant portion of organizations (38.06%) did not have a website. Among those that did, concerns about becoming a target for harmful activities were mixed; 27.6% were concerned, while 22.85% were very concerned. Website hacking or defacement in the past five years was reported by 13.17%, and 33.23% shared information that could upset powerful groups. Regular website backups were not performed by 28.18%.

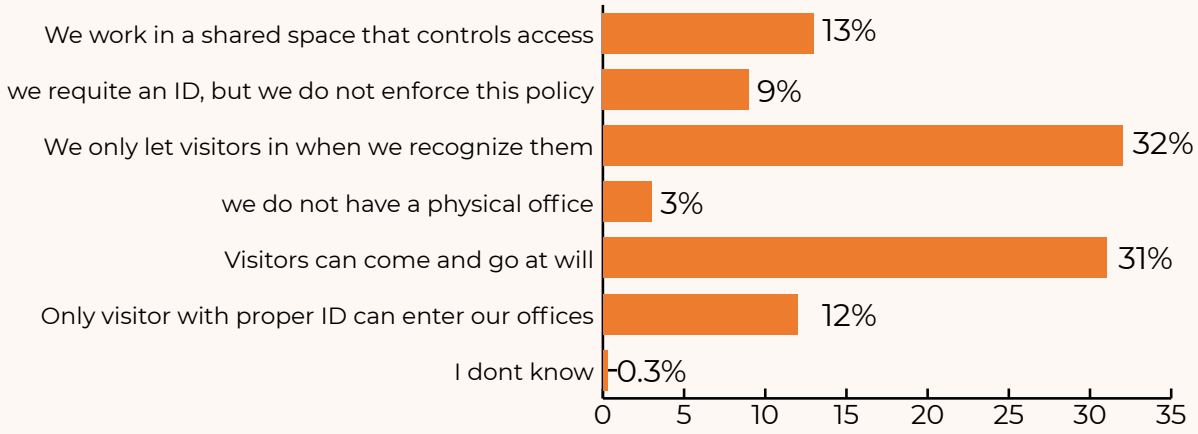
Level of concern for website being a target for people who want to harm the organization



Office Security

Control over office access varied, with 31.39% allowing visitors to come and go at will, and only 11.94% requiring proper ID. Security systems were mostly absent, with 76.67% not having any. Rules for disposing of printed information were also lacking in 54.17% of organizations. End-of-day office procedures were verbal in 53.12% of cases, while 24.33% did not know of any processes.

How does your organization control who enters your office

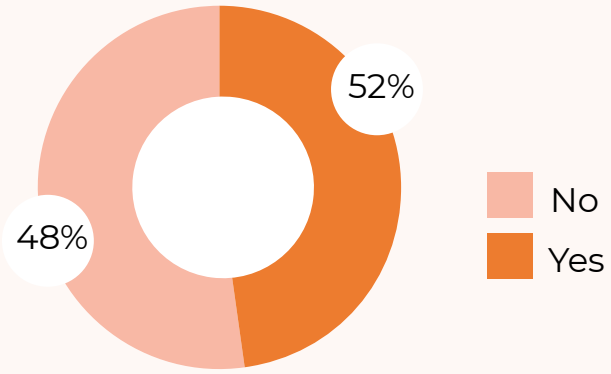


Messaging and Collaboration

Using personal devices and email accounts for work was most popular at 61.7%. About 43.9% of the CSOs said their staff used work emails for communication and 42.2% said Secure messaging and collaboration tools were underutilized.

Processes for working on sensitive topics were present in 52.22% of organizations, with 31.83% having a dedicated workflow.

Availability of a process for working on senstive topics



Legal Risks

Concerns about potential legal requests for internal documents were high, with 30% being concerned and 27.22% very concerned.

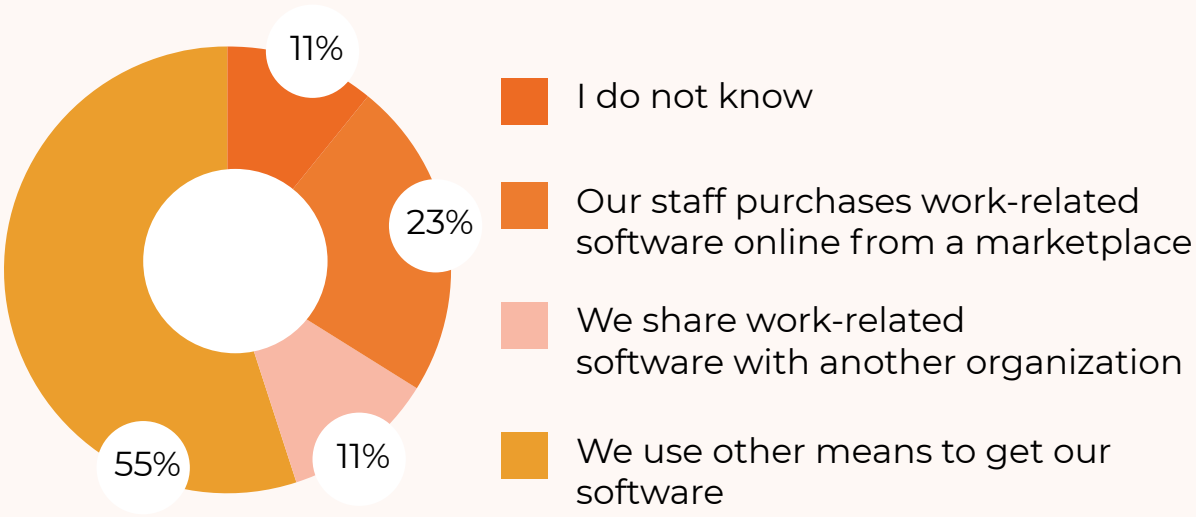
Device Security and Compartmentalization

Personal email usage for work-related tasks was common, with 39.17% of all staff and 43.33% of some staff doing so.

Software Security

Work-related software was commonly obtained through means other than purchases, with 54.44% using various methods. Downloading pirated software was reported by 52.5%, either often or sometimes. Policies on downloading software onto work devices were unclear, with 46% permitting it and 41.94% not allowing it.

How does your staff get work-relates software?



Cybersecurity Index

The International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) 2020[1] [1]evaluates countries based on legal measures, technical measures, organizational measures, capacity building, and international cooperation and highlights significant advancements in cybersecurity globally, with 64% of countries adopting a national cybersecurity strategy and over 70% conducting awareness campaigns.

Africa shows varied progress, with Ghana ranking third due to its strong CERT ecosystem and consistent capacity building. Uganda has made strides in improving its cybersecurity framework, especially amid the increased digital reliance during the COVID-19 pandemic. The country has focused on enhancing legal, organizational measures, and capacity-building initiatives, though challenges remain in protecting critical infrastructure and expanding cybersecurity skills training, which is crucial for the cybersecurity performance of Civil Society Organizations (CSOs) (UNRIC2[2]) (Citi News3[3]).

Based on the findings from the cybersecurity assessment survey, we developed a scoring system for rating the cybersecurity readiness of different organizations based on the survey data. We created a weighted scoring model across all performance measures and this was aggregated to estimate the Cybersecurity Index. Across the performance measures, we developed scores based on the responses made, where good performances were ranked highest (i.e., 2, 1.5 or 1) and the relatively good responses were also awarded a positive score (i.e., between 0-1). The best scores when aggregated sum up to 100 thus the Cybersecurity Index lies between 0-100. A 4-point scale was developed to rate the index as Poor 0-25%, Fair 26% - 50%, Good 51% - 75% and Excellent 75%.

The Cybersecurity Index was derived from the 20 areas of risk which included Operational security, Documentation and policy, Internal risk, Staff training, Staff offboarding, Travel security, Data security, Website security, Office security, Messaging collaboration, Legal risk, Device security, Software security, Data encryption, Account security, Updates, Operational security, Third party, VPN, and Associated risk.

From the performance areas the CSOs cybersecurity readiness was estimated at 38%

Cybersecurity performance areas

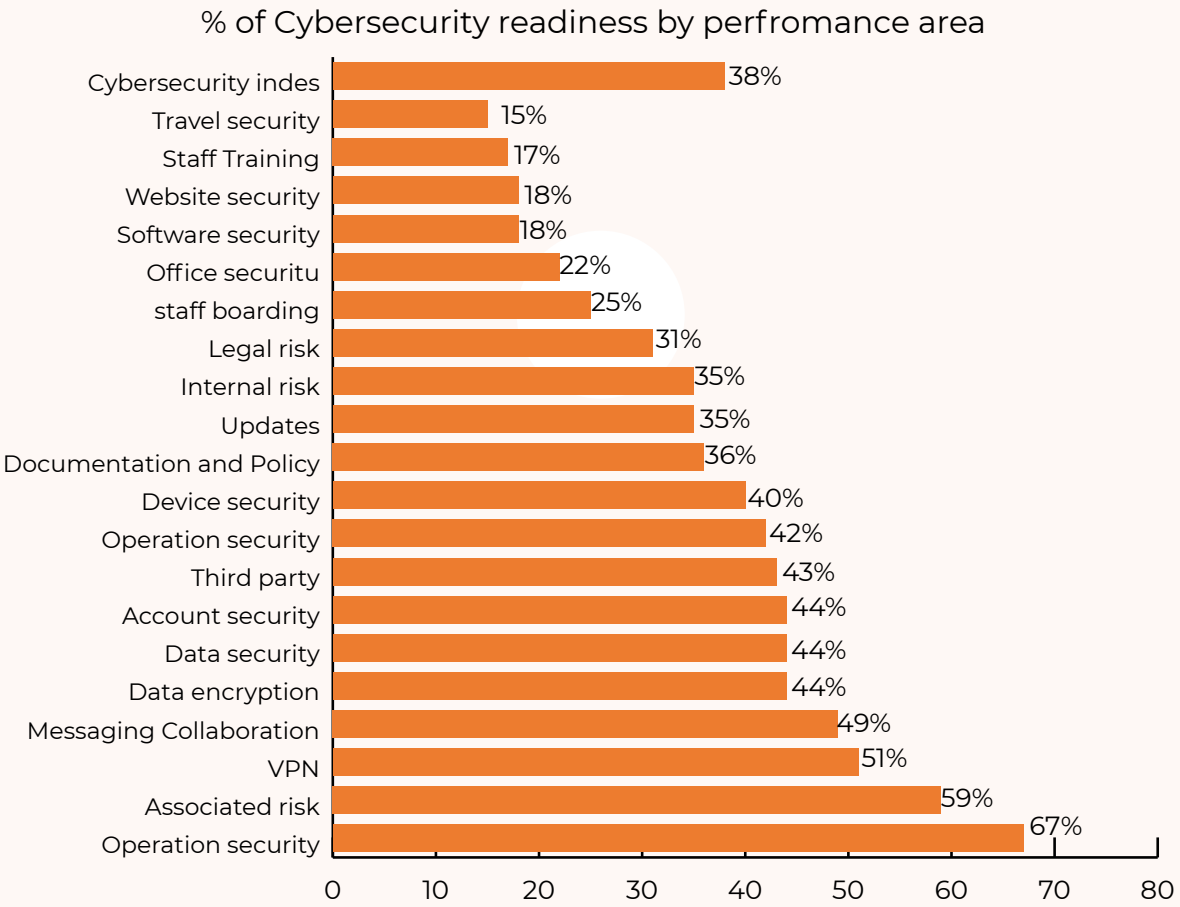
This assessment revealed that along the performance measures, Associated risks had the highest score regards to readiness of CSOs to Cybersecurity 67%, followed by Associated risk 59%, VPN 51%.

Worst ratings were recorded in travel security 15%, staff training 17%, Website security 18%, Software security 18%, office security 22%, Staff offboarding 25%.

1 https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

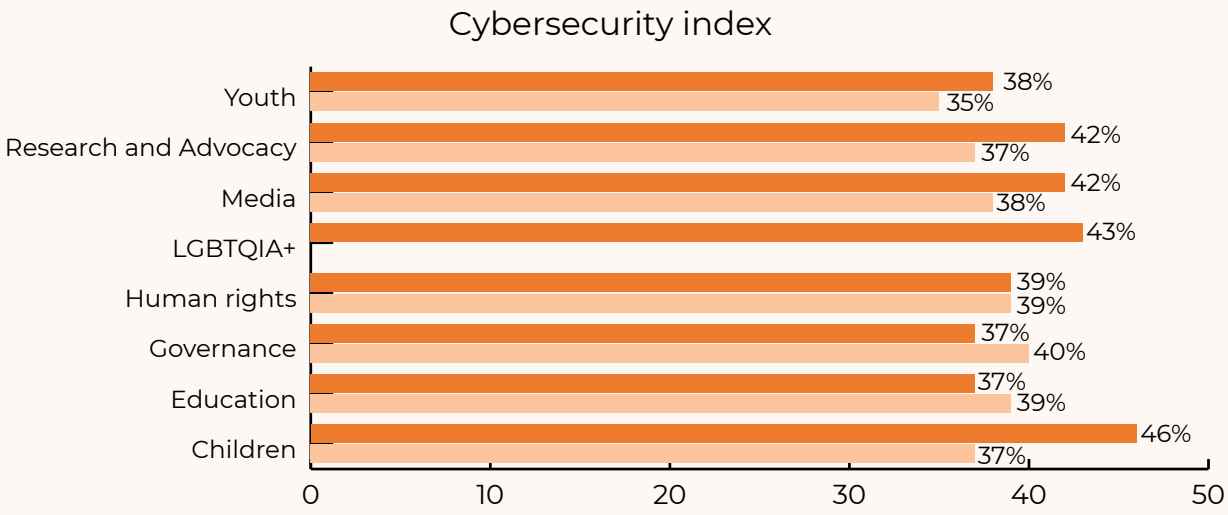
2 https://unric.org/en/itu-releases-fourth-edition-of-the-global-cybersecurity-index/

3 https://citinewsroom.com/2021/07/ghana-ranked-third-in-africa-on-global-cybersecurity-index/



Cybersecurity by thematic areas

Overall, the Cybersecurity Index rating was estimated at 38% among the CSOs that participated in the assessment. This was below average. Best performing CSOs were in Digital rights 46%, LGBTQIA+ 43%, Media 42%, Research and Advocacy 42%. The worst performing CSOs were focused to women 35%. All CSOs rated fair in cybersecurity readiness index i.e., the scores were between 25 and 50%.



Thematic Analysis of Cybersecurity Risks Among Civil Society Organizations

A thematic analysis was undertaken to assess the cybersecurity risks across different thematic areas of operation for Civil Society Organizations (CSOs) that participated in the survey. From this analysis, the risk areas were analysed alongside the various research themes.

The findings revealed that, operational Security related risks concerns were higher among organizations focused on Digital Rights (60%) and Media (58%) compared to others like Children (51%) and Youth (52%). On the other hand, **documentation and Policy** related risks were notably lower across all themes, with Digital Rights organizations at the higher end (23%) and Women-focused organizations at the lower end (15%).

Internal Risks were more significant for organizations undertaking work in areas of Digital Rights (47%) and LGBTQIA+ (45%), while those working in other areas like Income Generating Activities (29%) showed less concern. Whereas **the Legal Risk** was particularly high for organizations working in areas of LGBTQIA+ (63%) and Governance (55%).

Staff Training was a more appreciated and adopted arrangement amongst organizations working in the areas of Digital Rights (38%) and Media (31%) as compared to CSOs working in other areas like Women affairs (16%) and Youth (20%).

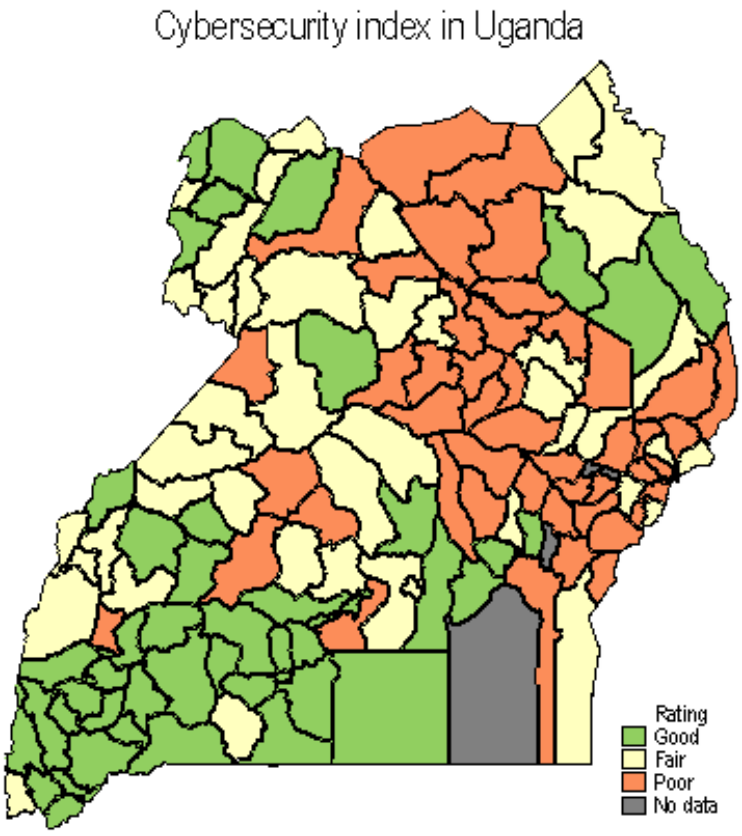
Travel Security was more adopted for CSOs undertaking work in areas of Digital Rights (28%) and Media (26%). The analysis also reveals that **Data Security** was largely considered a priority for organizations undertaking work in areas of Digital Rights (55%) and LGBTQIA+ (53%) as compared to organizations working on women affairs (38%) and Environment, Land and Extractives (40%). Similarly, **Website Security** and **Office Security** followed similar trends, with Media and Digital Rights organizations reporting higher security measures as compared to CSOs operation in other areas. **Device Security** and **Software Security** showed moderate concern, with Digital Rights and Media again reporting higher security measures.

Data Encryption and **Account Security** were more noted to be more critical areas for organizations working in areas of Digital Rights at (51% and 35% respectively) compared to other areas. **Updates** and **Third-Party Risks** were uniformly moderate across all themes, with slight variations. **VPN Usage** was higher among Digital Rights (53%) and Media (60%) organisations.

Overall, the **Cyber Risk Index** indicated that CSOs whose thematic areas of operations are, Digital Rights (46%), Media (42%), and LGBTQIA+ (43%) faced higher cybersecurity risks compared to those working in other thematic areas like Children (37%) and Youth (38%). This comprehensive assessment highlights the need for tailored cybersecurity strategies across different CSO thematic areas to ensure robust protection against cyber threats. The detailed risk analysis matrix by theme is detailed in the table below.

Cybersecurity risk levels by thematic areas

Variable	Children	Digital Rights	Education	Environment, Land and Extractives	Governance	Health	Human Rights	Income Generating Activities (IGAs)	LGBTQIA+	Marginalized population (Elderly, PWDs)	Media	Men	Research and Advocacy	Women	Youth
Operational security	51%	60%	52%	52%	55%	52%	55%	52%	58%	54%	58%	53%	56%	51%	52%
Documentation and policy	17%	23%	17%	16%	20%	18%	20%	19%	25%	18%	27%	18%	23%	15%	18%
Internal risk	30%	47%	32%	31%	33%	30%	33%	29%	45%	32%	41%	31%	36%	28%	32%
Staff training	18%	38%	22%	21%	27%	21%	25%	24%	34%	21%	31%	20%	28%	16%	20%
Staff offboarding	17%	23%	21%	19%	19%	18%	18%	20%	26%	18%	19%	18%	22%	14%	18%
Travel security	14%	28%	17%	16%	22%	16%	19%	16%	25%	16%	26%	17%	19%	13%	17%
Data security	41%	55%	45%	40%	49%	41%	44%	46%	53%	40%	49%	40%	51%	38%	44%
Website security	44%	50%	45%	44%	47%	44%	47%	45%	50%	45%	48%	44%	49%	45%	45%
Office security	38%	46%	41%	38%	45%	39%	40%	39%	42%	38%	43%	35%	45%	36%	40%
Messaging collaboration	60%	63%	59%	60%	59%	60%	59%	58%	61%	59%	65%	57%	62%	56%	60%
Legal risk	40%	54%	43%	46%	55%	41%	49%	48%	63%	46%	52%	43%	50%	39%	42%
Device security	15%	13%	15%	13%	15%	17%	13%	19%	16%	20%	7%	15%	16%	16%	15%
Software security	41%	48%	43%	45%	43%	43%	45%	45%	48%	44%	45%	40%	46%	42%	43%
Data encryption	33%	51%	37%	36%	40%	34%	36%	38%	39%	33%	48%	31%	40%	30%	36%
Account security	24%	35%	24%	24%	25%	24%	26%	27%	35%	25%	29%	21%	29%	20%	24%
Updates	42%	51%	43%	41%	46%	42%	44%	44%	37%	43%	49%	45%	49%	40%	44%
Operational security	35%	43%	36%	33%	38%	36%	37%	39%	41%	35%	40%	32%	38%	31%	37%
Third party	35%	43%	37%	34%	35%	36%	35%	37%	37%	33%	38%	33%	37%	33%	36%
VPN	51%	53%	49%	49%	49%	48%	49%	46%	59%	49%	60%	50%	54%	47%	49%
Associated risk	67%	64%	70%	66%	62%	69%	65%	69%	56%	68%	55%	70%	64%	70%	68%
Cyber Risk index	37%	46%	39%	37%	40%	37%	39%	39%	43%	38%	42%	37%	42%	35%	38%



Cybersecurity index/rating by district

The district level cybersecurity readiness assessment was compiled based on the districts of operation of the CSOs that participated in the survey. The scoring system that was adopted for rating the cybersecurity readiness of different organizations above was adopted for the different districts.

The map below presents a visual representation of the distribution of cybersecurity ratings across the districts of Uganda as per the findings from the cybersecurity assessment survey. The ratings adopted the 4-point scale that was developed above to rate the index as; Poor 0-25%, Fair 26% - 50%, Good 51% - 75% and Excellent 75%. The map reveals that the majority of CSOs operating in South Western Uganda have a better cybersecurity readiness rating in comparison to the other regions while the districts in the Northern and Eastern regions have worse cybersecurity readiness ratings.

The district specific ratings have been profiled in the table below.

Annex 1: Cybersecurity Index rating by district.

District	Rating	District	Rating	District	Rating	District	Rating	District	Rating
Abim	43%	Gulu	35%	Kiboga	29%	Mayuge	32%	Pallisa	23%
Adjumani	44%	Hoima	35%	Kibuku	25%	Mbale	34%	Rakai	40%
Agago	28%	Ibanda	48%	Kikuube	39%	Mbarara	50%	Rubanda	54%
Alebtong	29%	Iganga	53%	Kiruhura	62%	Mitooma	46%	Rubirizi	51%
Amolatar	27%	Isingiro	61%	Kiryandongo	44%	Mityana	34%	Rukiga	51%
Amudat	32%	Jinja	45%	Kisoro	40%	Moroto	47%	Rukungiri	54%
Amuria	38%	Kaabong	42%	Kitagwenda	30%	Moyo	41%	Rwampara	47%

Amuru	23%	Kabale	52%	Kitgum	24%	Mpigi	31%	Serere	30%
Apac	31%	Kabarole	37%	Koboko	46%	Mubende	31%	Sheema	52%
Arua	43%	Kaberamaido	32%	Kole	35%	Mukono	54%	Sironko	29%
Budaka	24%	Kagadi	39%	Kotido	40%	Nabilatuk	35%	Soroti	32%
Bududa	28%	Kakumiro	32%	Kumi	33%	Nakapiripirit	30%	Ssembabule	52%
Bugiri	18%	Kalaki	23%	Kwania	30%	Nakaseke	39%	Terego	44%
Buhweju	55%	Kalangala	50%	Kween	29%	Nakasongola	37%	Tororo	30%
Buikwe	53%	Kaliro	22%	Kyankwanzi	28%	Namayingo	33%	Wakiso	36%
Bukedea	23%	Kalungu	47%	Kyegegwa	46%	Namisindwa	32%	Yumbe	50%
Bukomansimbi	46%	Kampala	42%	Kyenjojo	56%	Namutumba	32%	Zombo	41%
Bukwo	37%	Kamuli	31%	Kyotera	44%	Napak	46%		
Bulambuli	30%	Kamwenge	41%	Lamwo	26%	Nebbi	38%		
Buliisa	30%	Kanungu	47%	Lira	31%	Ngora	34%		
Bundibugyo	36%	Kapchorwa	35%	Luuka	34%	Ntoroko	43%		
Bunyangabu	37%	Kapelebyong	31%	Luwero	52%	Ntungamo	44%		
Bushenyi	50%	Karenga	33%	Lwengo	43%	Nwoya	41%		
Busia	25%	Kassanda	35%	Lyantonde	58%	Obongi	40%		
Butaleja	29%	Kasese	41%	Madi Okollo	37%	Omoro	27%		
Butambala	57%	Katakwi	30%	Manafwa	25%	Otuke	27%		
Buyende	27%	Kayunga	21%	Maracha	39%	Oyam	34%		
Dokolo	30%	Kazo	65%	Masaka	48%	Pader	27%		
Gomba	58%	Kibaale	43%	Masindi	39%	Pakwach	41%		

Annex 2: Data Analysis Annex

Operational security

		freq.	Percent
Do you have any concerns about threats to your organisation's cybersecurity?	No	68	18.89
	Yes	292	81.11
What major threats to your organization's cybersecurity do you have concerns about?	State attack	91	25.28
	Ransomware	68	18.89
	Cybersecurity	130	36.11
	Phishing	17	4.72
	Risky hybrid	7	1.94
	Social engineering	4	1.11
	Other		
10. Which operational areas of your organization's work do you believe create additional risk?	Communication	189	52.5
	Advocacy	236	65.56
	Research	159	44.17
	Grant making	64	17.78
	Partnerships	182	50.56
	No additional risks	22	6.11
	Never thought about it	47	13.06
	Other		
12. How interested are your employees in cybersecurity strengthening?	Very disinterested	27	7.5
	Disinterested	3	0.83
	Neutral	30	8.33
	Interested	118	32.78
	Very interested	182	50.56
13. What is the general mood when cybersecurity comes up in conversation within your organization?	We are bored	3	0.83
	We are confused	57	15.83
	We are excited	188	52.22
	We are stressed and anxious	74	20.56
	We never talk about cybersecurity	38	10.56

14. How often do you consider cybersecurity when making decisions about internal workflow and processes?	Always	43	11.94
	Never	47	13.06
	Often	46	12.78
	Rarely	111	30.83
	Sometimes	113	31.39
15. How does your organization pay for cybersecurity?	Cybersecurity has its own line item in our budget line	8	2.22
	Cybersecurity is part of our operations budget	36	10
	We do not have a consistent way to pay for cybersecurity		
	We raise funds for cybersecurity	19	5.28
	Others specify		
	External partner	1	0.28
	I don't know	4	1.11
	No budget	13	3.61
	Our organization security plan and risk assessment is expired. Since the passage of the anti-homosexuality act, we haven't updated it to bring it up to speed with the new realities	1	0.28
	We currently pay for laptop anti-virus	1	0.28
	We don't have funds for cyber security	1	0.28
	We get it from partners	1	0.28
	We have less risks to cyber security thus we've never thought of paying it	1	0.28
17. How would you best describe your approach to cybersecurity?	I don't know	23	6.39
	We have a staff person who manages cybersecurity	70	19.44
	We have a third-party consultant who manages cybersecurity	55	15.28
	We haven't thought about cybersecurity much within our organization	212	58.89

Documentation and policy

			Freq.	Percent		
18. Does your organization have cybersecurity policies?	No		266	73.89		
	Yes		94	26.11		
19. What is your organization's approach to formulating cybersecurity policies?	We discuss policies but do not write them down		77	21.69		
	We do not have a policy		204	57.46		
	We have a formal written policy		74	20.85		
20. What cybersecurity policies does your organization have in place?	Authority and access control policy		70	19.44		
	Data classification		56	15.56		
	Data support and operations		55	15.28		
	IT security awareness and behaviour		91	25.28		
	Encryption policy		29	8.06		
	Data backup policy		74	20.56		
	Acceptable Use Policy		38	10.56		
	Privacy regulations		64	17.78		
	Other					
22. How often does your organization review and update the cybersecurity policies?	Always		6	1.79		
	Never		168	50		
	Often		23	6.85		
	Rarely		83	24.7		
	Sometimes		56	16.67		
	Obs		Mean	Std. Dev.	Min	Max
23. When was the last time your organization updated or reviewed your security policies? In months		168	10.9	15.5	1	120
24. How often do you believe your employees are following your security policies?	Always		13	3.83	3.83	
	Never		115	33.92	37.76	
	Often		38	11.21	48.97	
	Rarely		89	26.25	75.22	
	Sometimes		84	24.78	100	

D. Internal risks (Intentional or unintentional)

		Freq.	Percent
25. In the past year, how frequently have you identified cybersecurity concerns within your organization?	Always	19	5.28
	Never	85	23.61
	Often	57	15.83
	Rarely	74	20.56
	Sometimes	125	34.72
26. How satisfied are you with your staff's understanding of the cybersecurity risks to your organization?	Very dissatisfied	102	28.33
	Somewhat dissatisfied	92	25.56
	Neither dissatisfied nor satisfied	76	21.11
	Somewhat satisfied	68	18.89
	Very satisfied	22	6.11
27. Is anyone on your staff focused on information technology (IT)for your organization?	I don't know	3	0.83
	No, we do not have any IT support	106	29.44
	No, we use a volunteer	40	11.11
	No, we use an outside IT provider/ consultant	59	16.39
	Yes, we have at least one staff member focused on IT	152	42.22

Staff training and Support

		Freq.	Percent
28. Do you currently provide cybersecurity training within your organization?	No	269	74.72
	Yes	91	25.28
29. Which groups within your organization do you currently provide cybersecurity training to?	Staff only	104	28.9
	Volunteers	44	12.2
	Interns	28	7.8
	Contractors	7	1.9
	None	215	59.7
	Other		
31. How often does your organization provide cybersecurity training to these groups?	After a threat occurs	47	13.99
	Never	187	55.65
	Once a month or more frequently	17	5.06
	Once a quarter	28	8.33
	Once a year	39	11.61
	Only during onboarding	18	5.36

32. Does your organization provide cybersecurity training to new employees (onboarding)?	I don't know	6	1.73
	No	236	68.21
	Yes	60	17.34
	Yes, but only to some staff members	44	12.72

F. Staff offboarding processes

		Freq.	Percent
33. Does your organization use a documented offboarding process that speci	I don't know	12	3.33
	No	251	69.72
	Yes, and we always follow the process	53	14.72
	Yes, but we do not always follow the process	44	12.22
34. Does your organization conduct exit interviews that include a discussion of security (an honest conversation with the staff member about vulnerabilities and areas of improvement they've noticed) prior to an employee leaving?	I don't know	21	5.83
	We always conduct exit interviews about security	35	9.72
	We do not conduct exit interviews	189	52.5
	We do not conduct exit interviews about security	61	16.94
	We sometimes conduct exit interviews about security	54	15

G. Travel Security

		Freq.	Percent
35. Does your organization have security-related policies in place for travel?	No	241	66.94
	Yes	119	33.06
36. How often does your organization follow the cybersecurity related policies in place for travel?	Always	7	2.01
	Never	195	55.9
	Often	25	7.2
	Rarely	58	16.6
	Sometimes	64	18.3
37. What risks are covered in your travel security-related policy?	Physical security	96	26.7
	Cybersecurity	35	9.7
	We do not have a security related policy	236	65.6

H. Data Security

		Freq.	Percent

38. Does your organization have a data retention policy (a policy that controls how much sensitive information you store, how long, and where)?	No	252	70
	Yes	108	30
39. Does your organization categorize the data you store by sensitivity/risk?	No	207	57.5
	Yes	153	42.5
40. Does your organization control who has access to the data you store based on its sensitivity/risk?	I don't know	12	3.33
	No, anyone in our organization can access sensitive data	22	6.11
	No, we do not organize our data by its sensitivity	124	34.44
	Yes, only authorized staff members can access sensitive data	125	34.72
	Yes, only particular staff members can access sensitive data	77	21.39
41. What is your process for keeping a regularly updated backup of your organization's most important data?	We use automated backups ourselves	81	22.5
	We manually back up our data ourselves	191	53.1
	We use an outside contractor/IT professional to back up our data	28	7.8
	We do not back up our data regularly	105	29.2
	I don't know	19	5.3

I. Website Security

		Freq.	Percent
42. Does your organization have a website?	No	137	38.06
	Yes	223	61.94
43. How concerned are you that your website will become a target for people who want to harm your organization?	Concerned	93	27.6
	Neutral	74	21.96
	Unconcerned	48	14.24
	Very concerned	77	22.85
	Very unconcerned	45	13.35
44. Has anyone ever hacked or defaced your website in the past five years?	I don't know	49	14.67
	No	241	72.16
	Yes	44	13.17
45. Does your organization share information of public interest on your website that could upset powerful groups?	No	223	66.77
	Yes	111	33.23

46. How often does your organization share information of public interest on your website that could upset powerful groups?	Always	19	5.67
	Never	159	47.46
	Often	20	5.97
	Rarely	61	18.21
	Sometimes	76	22.69
47. If someone hacked your website, what types of information could they get?	I don't know	106	32.12
	Only publicly available information	147	44.55
	Publicly available information and sensitive private information (addresses, payment records, etc.)	30	9.09
	Publicly available information and unpublished information (draft blogposts, press releases, etc.)	47	14.24
48. What is your process for keeping a regularly updated backup of your website?	I don't know	76	23.03
	We do not back up our website regularly	93	28.18
	We manually back up our website ourselves	59	17.88
	We use an outside contractor/IT professional to back up our website	44	13.33
	We use automated backups ourselves	58	17.58
49. Which of the following versions of your website does your organization have?	Both	9	2.73
	HTTP	41	12.42
	HTTPS	147	44.55
	HTTPS but my browser says "insecure"	16	4.85
	I don't know	117	35.45

J. Office Security

		Freq.	Percent
50. How does your organization control who enters your offices?	I don't know	1	0.28
	Only visitors with proper ID can enter our offices	43	11.94
	Visitors can come and go at will	113	31.39
	We don't have a physical office	11	3.06
	We only let visitors in when we recognize them	114	31.67
	We require an ID, but we don't enforce this policy	31	8.61
	We work in a shared space that controls access	47	13.06

51. Does your organization have an alarm system or cameras in your offices?	I don't know	9	2.5
	We have an alarm system that only makes warning noises	5	1.39
	We have an alarm system that will capture the time and date when it goes off	7	1.94
	We have no security system	276	76.67
	We have some form of an alarm system in our office	16	4.44
	We have some form of video monitoring for our office	47	13.06
52. Do you have rules governing the disposal of printed information?	No	195	54.17
	Yes	165	45.83
53. What are the rules governing the disposal of printed information?	I don't know	36	10.4
	Other, Specify	67	19.36
	We don't have particular rules on what gets shredded or disposed off	160	46.24
	We have a single shredder, and staff are instructed to shred all paper	54	15.61
	We keep shredders closer than garbage cans and shred all printed information	29	8.38
55. Do you have a process for closing up at the end of the day in all your offices?	No	137	38.06
	Yes	223	61.94
56. What is your process for closing up at the end of the day in all your offices?	We have a verbal procedure that includes storing devices and clearing off desks, as well as a special process for the last person out of the office.	179	53.12
	I don't know	82	24.33
	We have a written checklist that includes storing devices and clearing off desks, as well as a special process for the last person out of the office.	57	16.91
	Other		
	At leisure	1	0.3
	Don't have	11	0.3
	Every one turns off laptop and go home	1	0.3
	Leave the laptop on the table	1	0.3
	Power is turned off at the end of the day	1	0.3
	Staff leave after office time	1	0.3
	WE JUST LOCK THE OFFICE	1	0.3

K. Messaging and Collaboration

		Freq.	Percent
58. How does your organization collaborate or message with each other privately and securely?	We use secure messaging and collaboration tools (Signal, Wire, Semaphor, etc.).	152	57.8
	We use our personal devices and personal email accounts	222	61.7
	We use work email on our personal devices	158	43.9
	We don't use any special tools to collaborate securely	50	13.9
	I don't know	19	5.3
59. Does your organization have a process for working on sensitive topics?	No	172	47.78
	Yes	188	52.22
60. What is your organization's process for working on sensitive topics?	I don't know	16	4.51
	Some members of our staff have a different workflow, but we have nonofficial process	74	20.85
	We don't have a process for working on sensitive topics	101	28.45
	We don't work on sensitive topics	51	14.37
	We have a dedicated workflow when working on sensitive topics	113	31.83

L. Legal Risks

		Freq.	Percent
61. How concerned are you about potential legal requests for your organization's internal documents?	Concerned	108	30
	Neutral	72	20
	Unconcerned	39	10.83
	Very concerned	98	27.22
	Very unconcerned	43	11.94

M. Device Security and Compartmentalization

		Freq.	Percent
62. Do members of your staff use their personal email for work-related tasks?	My organization doesn't know	8	2.22
	No, our staff members do not	55	15.28
	Yes, all staff members do	141	39.17
	Yes, some staff members do	156	43.33

N. Software Security

		Freq.	Percent
63. How does your staff get work-related software?	I don't know	39	10.83
	Our staff purchases work-related software online from a marketplace (app store, retailer, etc.)	84	23.33
	We share work-related software with another organization	41	11.39
	We use other means to get our software	196	54.44
64. Does your staff download pirated personal or work-related software?	I don't know	63	17.5
	No, our staff only downloads software from an approved source	108	30
	Yes, our staff often downloads pirated personal/work-related software	98	27.22
	Yes, our staff sometimes downloads pirated personal/work-related software	91	25.28
65. Is your staff permitted to download any software onto work devices?	I don't know	41	11.39
	No, our staff is not permitted to download any software	151	41.94
	Yes, our staff is permitted to download any software	168	46.67

O. Data Encryption

		Freq.	Percent
66. Does your organization encrypt backups and/or external media (hard drives, USB drives, etc.)?	I don't know	23	6.39
	No	185	51.39
	Yes	152	42.22
67. Do you have a process for acquiring, maintaining, and disposing of hardware and devices that includes security procedures (for example, erasing devices between uses)?	I don't know	29	8.06
	No	234	65
	Yes	97	26.94

P. Account Security: Password Management and Authentication

		Freq.	Percent
67. Do members of your organization use a password manager?	I don't know	20	5.56
	No, our staff members do not	174	48.33
	Yes, all staff members do	79	21.94
	Yes, some staff members do	87	24.17

69. Do members of your organization store their existing passwords in the password manager, use it to generate new passwords, or both?	Both	67	18.61
	Generate new passwords	20	5.56
	I don't know	46	12.78
	Store existing passwords	45	12.5
	We don't use a password manager	182	50.56
70. To log in to your email and other services, do members of your organization use two-factor/multi-factor authentication, such as Okta, DUO Security, Google Authenticator, Authy, or RSA ID?			
	I don't know	44	12.22
	No, our staff members do not	117	32.5
	Yes, all staff members do	57	15.83
	Yes, some staff members do	142	39.44

Q. Updates

		Freq.	Percent
71. How does your organization make sure that critical systems (computers, servers, etc.) receive the latest security updates in a timely manner?	An outside contractor/IT provider installs updates on a regular/standard schedule	59	16.39
	I don't know	14	3.89
	Our internal IT department installs updates on a regular/standard schedule	76	21.11
	We do not have a policy for system updates	81	22.5
	We do not install system updates regularly	89	24.72
	We make installing updates the responsibility of each individual user	41	11.39

R. Operational Continuity

		Freq.	Percent
72. Do you have a contingency plan in case your main method of communication (e.g., email) becomes unreliable?	I don't know	18	5
	We do not have a contingency plan for this situation	219	60.83
	We have a contingency plan, but it's not written down	84	23.33
	We have a written contingency plan	39	10.83
73. How would you continue your organization's operations in case an emergency prevents access to your physical office or online systems (such as a natural disaster)?	I don't know	18	5
	We do not have a contingency plan for such a situation	207	57.5
	We have a verbal agreement but no documented policy	83	23.06
	We have a written remote work policy	52	14.44

74. How would your organization recover from fire, flood, theft, or other incidents?	I don't know	23	6.39
	This would be catastrophic because we do not have any backups of our data	129	35.83
	We could start over because our data is stored in the cloud	71	19.72
	We could start over because we have full copies of the data on our devices stored locally (off-line)	65	18.06
	We have some printed documents and materials that we might be able to use	72	20

S. Third-Party Services

		Freq.	Percent
75. Are you actively keeping track of the external online services (e.g., social media, GitHub, etc.) that your organization uses?	I don't know	20	5.56
	We do not have a list	164	45.56
	We have a list that is written down but not updated	38	10.56
	We have a verbal list but nothing written down	57	15.83
	We have an updated list that is written down	81	22.5
76. Do you have guidelines or documentation within your organization on how to use external online services safely?	I don't know	18	5
	We do not have any guidelines for using these services	203	56.39
	We have a verbal understanding but no written policy	84	23.33
	We have written guidelines for external services	55	15.28
77. Do you use non-business platforms (e.g., Facebook Messenger, WeTransfer, Instagram, etc.) to share or receive sensitive information?	I don't know	24	6.67
	We often share or receive sensitive information via non-business platforms	94	26.11
	We rarely share or receive sensitive information via non-business platforms	172	47.78
	We sometimes share or receive sensitive information via non-business platforms	70	19.44
78. When you upgrade or stop using a service, is there a process for turning it off or deleting accounts?	I don't know	26	7.22
	We do not have a process	238	66.11
	We have a verbal process but nothing written	58	16.11
	We have a written process	38	10.56

T. VPN

		Freq.	Percent
79. Do members of your organization use a VPN (virtual private network) when connecting to a public network?	I don't know	16	4.44
	No, our staff members do not	79	21.94
	Yes, all staff members do	67	18.61
	Yes, most staff members do	58	16.11
	Yes, some staff members do	140	38.89

U. Associated Risks

		Freq.	Percent
80. Has anyone at your organization experienced "doxing," or the release of private information online in a targeted manner?	I don't know	46	12.78
	No, none has had their private information released online	268	74.44
	Yes, one or more staff members have had their private information released online	46	12.78
81. Has anyone at your organization been the target of online impersonation or a fake account that spreads misleading or discrediting information?	I don't know	39	10.83
	No, none has been impersonated online	239	66.39
	Yes, one or more staff members have been impersonated online	82	22.78
82. Has your organization had a major hacking incident in the past five years?	I don't know	30	8.33
	No	255	70.83
	Yes	75	20.83
83. Has anyone at your organization experienced online harassment or any abusive language or behaviour directed at a member of your team?	I don't know	37	10.28
	No, none has been harassed online	199	55.28
	Yes, one or more staff members have been harassed online	124	34.44

Annex 3: Cybersecurity Index rating guide

Performance area	Maximum score
Operational security	8.5
Documentation and policy	6
Internal risk	4.5
Staff training	6
Staff offboarding	4
Travel security	5
Data security	7
Website security	9
Office security	9

Messaging collaboration	5.5
Legal risk	2
Device security	2
Software security	4.5
Data encryption	3
Account security	4
Updates	2
Operational security	4
Third party	6
VPN	2
Associated risk	6

The scores are distributed across the different attributes under the performance area.

CYBERSECURITY ASSESSMENT