



Key populations Uganda

+256773321055

keypopulationug@gmail.com

www.keypopulationsug.org

REPORT ON LGBTI ORGANISATIONS UNDERSTANDING OF DIGITAL AND INFORMATION SECURITY PROTECTION THREATS AND SAFETY PRACTICES



With contributions from

Initiative For The Affected And Infected Persons-IPIA

ARK WLLNESS - HUB

Triumph Uganda

Trans Youth Initiative-TYIU

Trans Alive Initiative Uganda - TAIU

Wave of Legacy Initiative (WALAI)

Lets Walk Uganda (LWU)

Trans Alive Initiative Uganda – TAIU

Kampus Liberty Uganda (KLUG)

Children of The Sun Foundation (COSF)

Happy Family Youth Uganda (HFYUL)

Kuchu Shiners Uganda (KSU)

Friends of The marginalized (FOMU)

Out and Proud Uganda (OAP)

Red Horn Elites Foundation (RHE)

With Support From:



ABOUT KEY POPULATIONS UGANDA.

Key Population Uganda is a youth-led nonprofit support organization for LGBTIQ and Male Refugees LGBTIQ Sex workers focused on sexual health, advocacy, safety and security, community mobilization, and HIV/AIDS awareness and prevention for all LGBTIQ and Male Sex workers.

Our team is consistent, dynamic, and dedicated to serving the LGBTIQ – Male LGBTIQ Refugee Sex workers communities despite the challenges and dangers. We also find pride in working with a number of partners from MSM CSOs, other LGBTIQ organizations, mainstream/general hospitals, volunteers, and individuals.

Key Populations Uganda is committed to serving the needs of minority groups in Uganda. The organization provides life-changing programs for LGBTIQ youths at risk in varying circumstances. We undertake social and educational interventions/activities aimed at educating, sensitizing, and empowering young LGBTIQ people about HIV/AIDS and other STIs. Through promotion of healthy lifestyles with an emphasis on HIV/AIDS education, we offer a youth friendly service through our partners that provides HIV/STIs counseling, testing, sexual reproductive health education and support. In the last three years, we have undertaken key population projects with our partners, where we engage minority groups in awareness of dispelling myths and misconceptions relating to HIV/AIDS, SRH and supporting mechanisms which will allow for a sustained holistic enabling environment.

Key Populations Uganda delivers its mandate through the following approaches:-

Evidence based: Capturing and utilization of information in the implementation of identified strategies.

Focus on Results: Focusing on targeted results and linking the same to resources utilized to measure cost effectiveness.

Human rights and equality: Ensuring all programs are planned with all members of community and implementation is in a dignified manner.

Partnerships strengthening: Advance cooperation & coordination with other CSOs for mutual interests.

Advocacy: Support the cause, speak /write in favour /defending/intercede on behalf of the community including provision of information and tools for empowerment to access health and other social services

Capacity building: Facilitate learning, mobilize resources and create partnerships through organizational development and civil society strengthening.

ABOUT THE CONTRIBUTING ORGANISATIONS.

The Robust Initiative for Promoting Human Rights -TRIUMPH UGANDA.

Triumph Uganda is an independent charity organization founded in 2014 and duly registered with the Government of Uganda in 2016 as a community-led charity organization aspiring to remedy the improprieties caused by inadequate Human Rights respect and knowledge, increase in HIV/AIDS scourge, lack of knowledge on Sexual Health and Reproductive Health (SHRH) and addressing socio-economic drivers of HIV/AIDS among marginalized communities (LGBT, Sex workers. TRIUMPH UGANDA takes pride in championing Human Rights, fighting against the spread of HIV/ AIDS and managing a healthy positive living of the infected Marginalized persons in Uganda with a primary focus on the districts of Eastern Uganda.

Trans Alive Initiative Uganda – TAIU:-

Trans Alive Uganda is a Trans youth women and gender diverse youth led organization that is registered under the laws of Uganda. TAIU exists to achieve justice, equity, quality health and community service provision for Tran’s youth women; Tran’s youth sex workers, gender non conforming youth, gender non conforming youth sex workers and intersex youth in Gulu.

Our main focus is to promote legal gender recognition and acceptance, create safe spaces, improve the current situation and protect rights for trans youth women and gender diverse youth, access to comprehensive healthcare that meets the needs of gender diverse communities, combat stigma and discrimination, enhance access to comprehensive HIV/AIDS and Sexual Reproductive Health services.

Ark Wellness Hub:-

Ark Wellness Hub Uganda Is a registered organization that started in 2018 to comprehensive health and wellness services to LGBT Ugandans often affected by Stigma, Discrimination, and the many forms of marginalization.

Wave of Legacy Initiative (WALAI):-

Wave of legacy alliance initiative (**WALAI**) is a nonprofit and non-government organization focusing on the wellbeing of Lesbians, Gays, and Transgender; It was formed ideally in March 2018 and registered in 2019, to bridge the gap between the main stream organizations and the LGBT persons to enhance accessibility to health and legal services. The aim is to customize services to address lived experiences of younger LGBT persons and younger people living with HIV, as well as promoting their talents.

Lets Walk Uganda (LWU)

Let's Walk Uganda is a national organization which was started in February 2016 in Kikoni, Makerere aimed at providing a variety of quality services to young MSM on a National level. Informed by the issues and experiences raised through our services, we also provide training, shelter and advocacy to enhance the visibility, inclusion and rights of the Young MSM living in Uganda.

Pride for Youth Initiative

Pride for Youth Initiative is a Transgender led organization working on local and National Level was founded in 2018 to mitigate issues of trans youth women, trans youth sex workers, gender non-conforming youth and intersex youth community by bringing them together to fight for their rights through trainings and mobilization of the community on legal rights.

Kampus Liberty Uganda (KLUG)

Kampus Liberty Uganda is a non-profit organization that advocates for the rights of marginalized people in Uganda. We fight for the healthcare rights, sexual health education, and access to justice for the Lesbian, Gay, Bisexual, and Transgender population, Men who have Sex with Men, Male Sex Workers, and people who face discrimination because of their gender identity or sexual orientation.

Children of the Sun Foundation (COSF)

COSF is an NGO in Uganda providing Health, Legal, Economic empowerment, and Shelter services to the vulnerable LGBTIQ+ members in Uganda. COSF Uganda is a youth LGBT led organization whose main objectives are to advocate for human rights, especially the right to health, education and full recognition of the LGBTI in Uganda and also to sensitize the LGBT on prevention of sexually transmitted infections such as HIV/AIDS.

Happy Family Youth Uganda (HFYUL)

Happy Family Youth Uganda is a grass root based organization which was formed in April 2016 and registered under the government of Uganda. It was formed to help the key population members regardless of their race, gender, and social status. With an aim to improve quality of life of the key population (MAPS) through poverty eradication, human rights and health service advocacy.

Kuchu Shiners Uganda (KSU)

Kuchu shiners Uganda is a Transgender sex workers organization which was founded by a group of Transgender sex workers due to so many challenges faced such as criminalization, stigma and discrimination, the existing organizations not really reaching their grass root people when it came to service provision and the need to promote a positive living among the Transgender sex worker persons.

Friends of The marginalized (FOMU)

FOMU is a nonprofit Organization that looks to mobilize all marginalized groups into development with an aim to strengthen their roles and building capacity. Out and Proud Uganda (OAP) OAP is a civil social Organization that works with Key Populations (KPs)/ Marginalized groups such as Sex workers, LGBTIQ and people who inject drugs.

Red Horn Elites Foundation (RHE)

Red Horn Elites Foundation Uganda is a Non Profit, which provides various forms of assistance and support in advocating for Human Rights and Social Justice, Gender identity, Sexuality Awareness, Economic empowerment and Health Education.

Table of Contents:-

| | |
|---|----|
| With contributions from..... | 2 |
| ABOUT KEY POPULATIONS UGANDA..... | 3 |
| ABOUT THE CONTRIBUTING ORGANISATIONS..... | 4 |
| PREFACE:- | 8 |
| PROJECT TEAM | 9 |
| Purpose..... | 10 |
| Design/Methodology/Approach..... | 10 |
| Research limitations/implications | 10 |
| Ethics | 10 |
| Originality/value | 10 |
| Key words | 10 |
| RECOMMENDATIONS | 11 |
| PRESENTATION | 12 |
| CONCLUSION | 26 |
| RECOMMENDATIONS | 26 |
| List of acronyms..... | 27 |

PREFACE:-

This report is intended to determine diverse LGBTIQ Human Rights (Activists) Organizations understanding of digital and information security protection, threats and safety practice. (The risk assessment) Findings will inform better Human Rights Activists engagements basing on evidence generated on existing gaps as well a basis for tailoring digital security training and Management.

The report also intended to support advocacy efforts towards better laws such as access to information Act, (that provides for the right to access public information pursuant to article 41 of the Uganda Constitution) and the Data Protection and Privacy Act) as well as positive changes in the legal and policy environment as it relates to data security and access to information by Human Rights Activists in Uganda.

All the information in this report has been independently verified through interviews with the Organizations about the digital and cyber security awareness and threats.

Through the responses partner LGBTIQ Human Rights Organizations provided basing on the feedback Key Populations Uganda organized workshop trainings with Human Rights Organizations Activists on digital safety and Security.

IVAN FREDRICK KASONKO

EXECUTIVE DIRECTOR,

KEY POPULATIONS UGANDA.

PROJECT TEAM

Editor

Mr Ivan Fredrick

Researchers

Richard Asingwire

Purpose

The purpose of the study was to find out whether there was Organizational awareness on Digital Security among LGBTQI organizations in Urban areas in Uganda.

Design/Methodology/Approach

The study was done both in-person visits to different organizations within the Central and Eastern regions, but also done virtually to those in the Northern and Western regions of the country due to COVID-19 and it used a mixed research paradigm through more quantitative research. A digital questionnaire was designed and sent to the emails of the intended respondents who answered the questions and sent them back. Responses were fed and analyzed using SPSS. Findings were presented in graphs – pie charts, and bar charts for clear display for even ordinary people. Conclusions were reached and recommendations were made.

Research limitations/implications

This research looked at the LGBTQI Organizational Digital Security in Urban areas in Uganda.

Ethics

Consent was obtained from the LGBTQI organizational leaders who were the focused respondents of the study. The consent sheet was attached to the questionnaire and all the respondents agreed to take part in the study by ticking "Yes" to mean that they have agreed willingly to give the information needed.

Originality/value

There no any study that has ever been done in LGBTQI Organizational Digital Security in Urban areas in Uganda. Therefore, the findings are original

Key words

LGBTQI, Digital security, Safety, Digital Management System

Findings

The study Most of the registered LGBTQI organizations have digital security equipment. There are no specific trained personnel employed in the field of the LGBTQI community for the purpose of effectiveness in the organizational Digital Management System, which is meant for the security of LGBTQI organizations. Organizational leaders are the same people who manage digital security systems. There is total LGBTQI organizational digital insecurity. There are limited opportunities for digital management training. There are very few cases of cyber-crimes among LGBTQI organizations in Uganda.

RECOMMENDATIONS

There should be enough training about digital management systems, digital security and cyber-crimes among LGBTQI organizations in Uganda.

These can be at least three times per year. Each LGBTQI organization can train two to five personnel who will form a rich human resource as far as organizational Digital Security is concerned.

Professional personnel should be employed for the purpose of effectiveness in the organizational Digital Management System, which is meant for the security of LGBTQI organizations.

Organizational leaders should be over all supervisors, not the working personnel, on the ground, by themselves.

This will bring effectiveness at work when the one responsible knows that there is someone above him to either give a report or to evaluate his performance.

PRESENTATION

The question of whether LGBTIQ organizations have Digital data security management policies, a big percentage agreed to the question with 66.7%. 33.3 disagreed to the question. Pie chat 1 shows the responses.

Pie chat 1 showing responses to the question of whether LGBTIQ organizations have Digital security management policies.

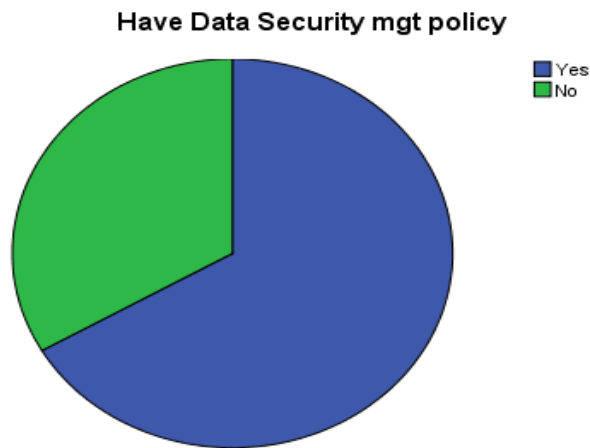


Table 1 showing details of responses to the question of whether LGBTIQ organizations have Digital security management policies.

Have Data Security mgt policy

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------|-----------|---------|---------------|--------------------|
| Valid Yes | 8 | 66.7 | 66.7 | 66.7 |
| No | 4 | 33.3 | 33.3 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of whether organizations have a digital data security management plan in place, 83.3% agreed to the question. 16.7% disagreed to the question. Pie chat 2 showing responses to the question of whether organizations have a digital data security management plan in place.

Have Digital Security mgt Plan

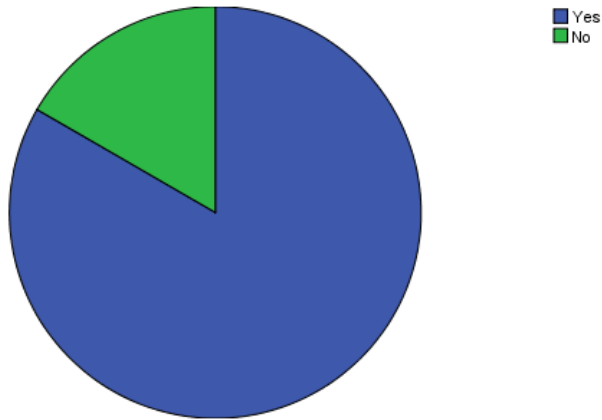


Table 2 showing details of the responses to the question of whether organizations have a digital data security management plan in place.

Have Digital Security mgt Plan

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------|-----------|---------|---------------|--------------------|
| Valid Yes | 10 | 83.3 | 83.3 | 83.3 |
| No | 2 | 16.7 | 16.7 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of whether organizations have ever conducted internal digital security assessments for you and partners, the majority disagreed to the question with 83.3%. 16.7% agreed to the question. Bar 3 shows the responses to the question of whether organizations have ever conducted internal digital security assessments for you and partners.

Have ever conducted internal awareness

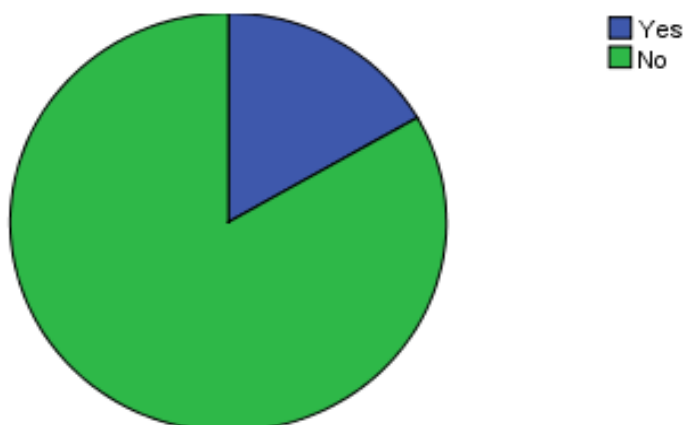


Table 3 showing details of the responses to the question of whether organizations have ever conducted internal digital security assessment for you and partners.

Have ever conducted internal awareness

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------|-----------|---------|---------------|--------------------|
| Valid Yes | 2 | 16.7 | 16.7 | 16.7 |
| No | 10 | 83.3 | 83.3 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of whether organizations have ever conducted or participated in a digital security awareness session, 58.7% agreed to the question. 41.7% disagreed to the question. Pie chart 4 shows the responses to the question of whether organizations have ever conducted or participated in a digital security awareness session.

Have ever participated in Digital Security awareness

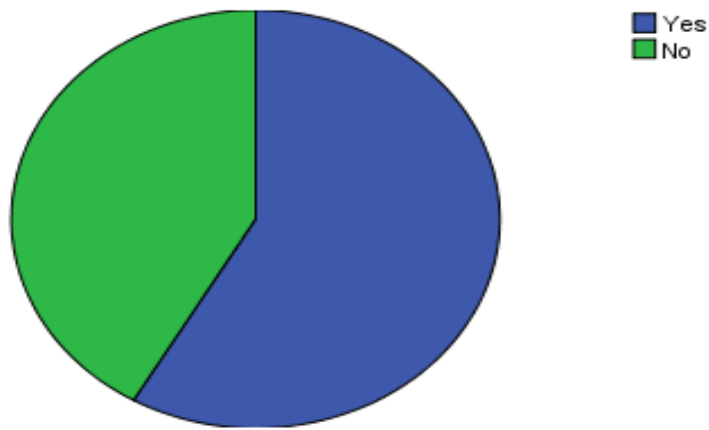


Table 4 showing details of responses to the question of whether organizations have ever conducted or participated in a digital security awareness session.

Have ever participated in Digital Security awareness

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------|-----------|---------|---------------|--------------------|
| Valid Yes | 7 | 58.3 | 58.3 | 58.3 |
| No | 5 | 41.7 | 41.7 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of how many organizational staff have ever been trained in digital security/insecurity and threats, 41.7% answered "None". 50% answered "1-2". 8.3% answered "3-4". Pie chart 5 shows the responses to the question of how many organizational staff have ever been trained and knowledgeable about digital security/insecurity.

Number of staff trained

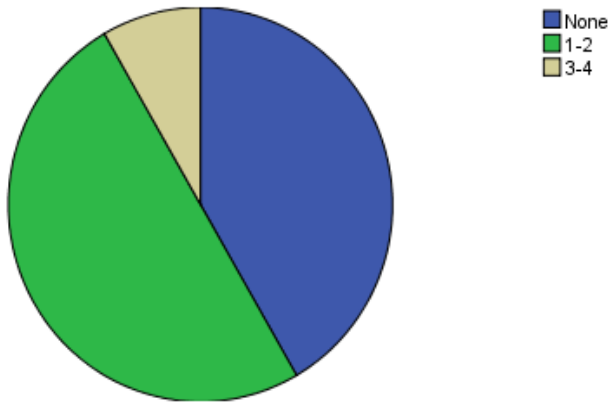


Table 5 showing details of the responses to the question of how many of organizational staffs have ever been trained and knowledgeable of digital security/insecurity.

Number of staff trained

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------------|-----------|---------|---------------|--------------------|
| Valid None | 5 | 41.7 | 41.7 | 41.7 |
| 1-2 | 6 | 50.0 | 50.0 | 91.7 |
| 3-4 | 1 | 8.3 | 8.3 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of whether there was any staff ever reported a digital threat or insecurity in their line of duty, 91.7% disagreed to the question. 8.3% agreed to the question. Pie chart 6 shows the responses to the question of whether there was any staff ever reported a digital threat or insecurity in their line of duty.

Any insecurity reported

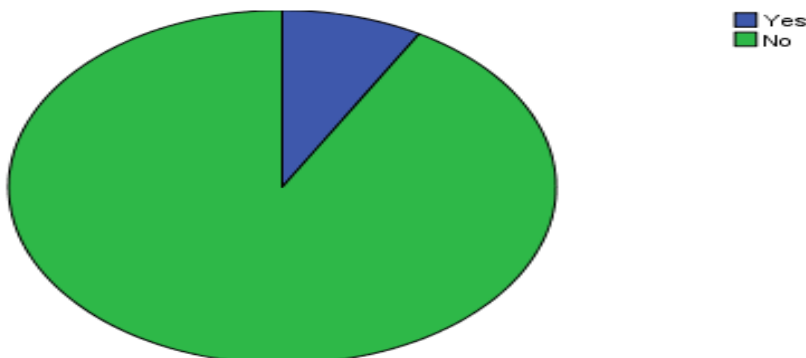


Table 6 showing details of the responses to the question of whether there was any staff ever reported a digital threat or insecurity in their line of duty.

Any insecurity reported

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------|-----------|---------|---------------|--------------------|
| Valid Yes | 1 | 8.3 | 8.3 | 8.3 |
| No | 11 | 91.7 | 91.7 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of which of the given areas was the digital security skills gap most apparent, 41.7% answered “Incident assessment”. 33.3% answered “Digital equipment mgt”. 25.0% answered “Auditing & risk mgt “. Bar chart1 shows the responses to the question of which of the given areas was the digital security skills gap most apparent.

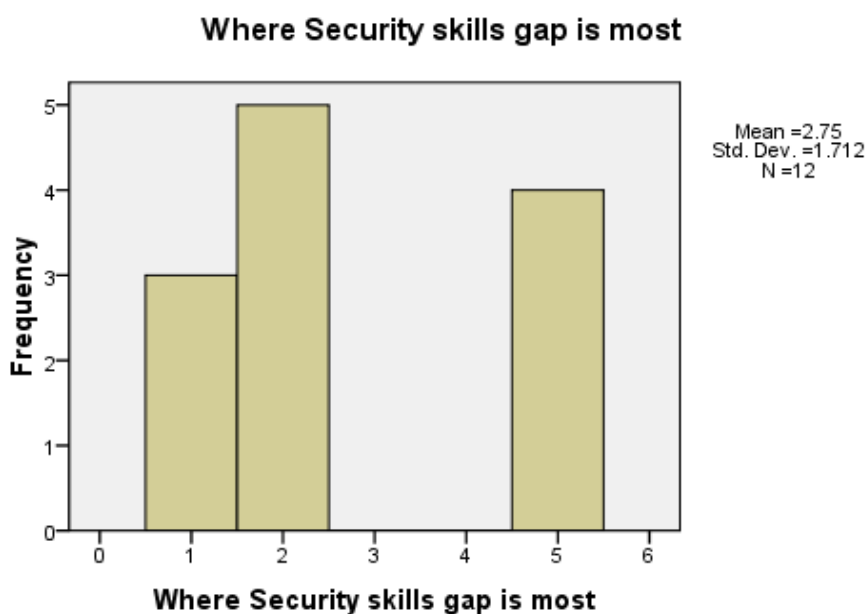


Table 7 showing responses to the question of which of the given areas was the digital security skills gap most apparent.

Where Security skills gap is most

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------------------------|-----------|---------|---------------|--------------------|
| Valid Auditing & risk mgt | 3 | 25.0 | 25.0 | 25.0 |
| Incident assessment | 5 | 41.7 | 41.7 | 66.7 |
| Digital equipment mgt | 4 | 33.3 | 33.3 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of whether organizations had recruited professional digital security officers, 83.3% disagreed to the question. 16.7% agreed to the question. Bar chat 2 shows the responses to the question of whether organizations had recruited professional digital security officers.



Table 8 showing the details of the responses to the question of whether organizations had recruited

We have professional Digital security officer

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|-------|-----------|---------|---------------|--------------------|
| Valid | Yes | 2 | 16.7 | 16.7 | 16.7 |
| | No | 10 | 83.3 | 83.3 | 100.0 |
| | Total | 12 | 100.0 | 100.0 | |

The question of what constraints encountered as organizations when recruiting experienced digital security professionals, 75% answered “Too high expectations”. 25% answered “Lack of solid experience”. Bar chart 3 shows responses to the question of what constraints encountered as organizations when recruiting experienced digital security professionals.



Table 9 showing detailed responses to the question of what constraints encountered as organizations when recruiting experienced digital security professionals.

Constraints when recruiting professionals

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--------------------------------|-----------|---------|---------------|--------------------|
| Valid Lack of solid experience | 3 | 25.0 | 25.0 | 25.0 |
| Too high expectations | 9 | 75.0 | 75.0 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of whether organizations had ever been a victim of cybercrime, 66.7% disagreed to the question. 33.3% agreed to the question. Pie chat 7 shows responses to the question of whether organizations had ever been a victim of cybercrime.

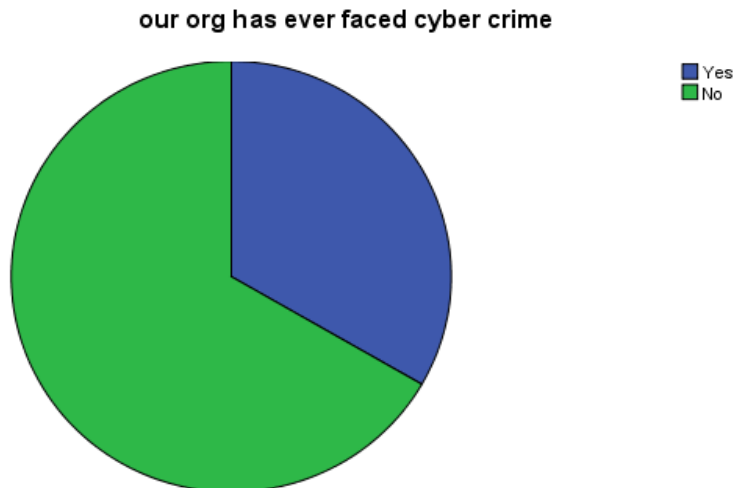


Table 7 showing details to the question of whether organizations had ever been a victim of cybercrime.

our organization has ever faced cyber crime

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------|-----------|---------|---------------|--------------------|
| Valid Yes | 4 | 33.3 | 33.3 | 33.3 |
| No | 8 | 66.7 | 66.7 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of whether organizations had ever been victims of cybercrime, what action followed, 66.7% answered “Didn't report to Police”. 33.7% answered “Reported to the Police but no action”. Bar chat 4 shows responses to the question of whether organizations had ever been victims of cybercrime, what action followed.

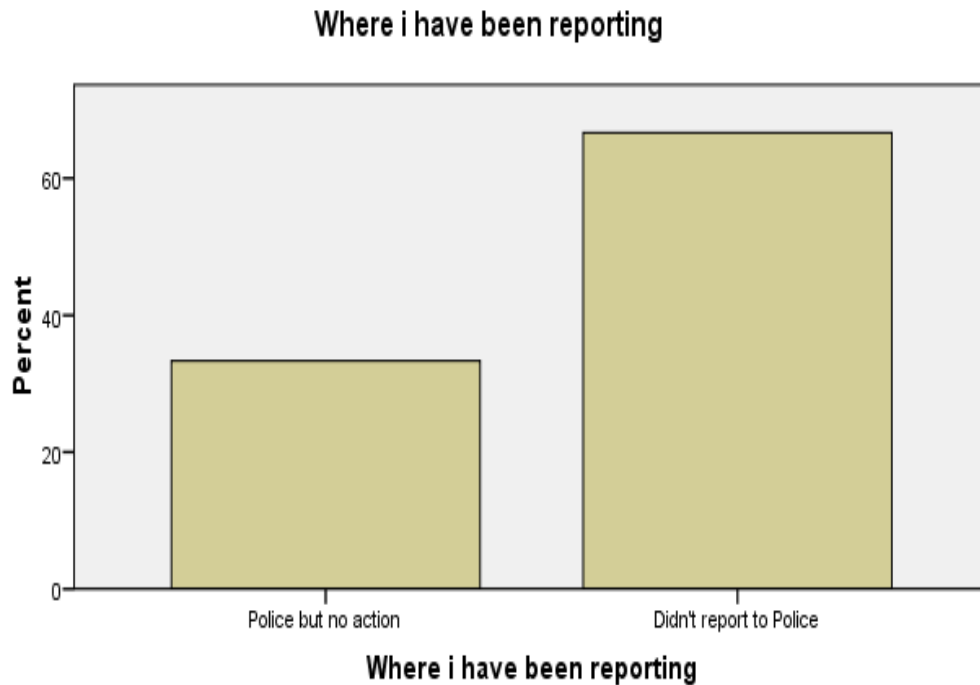


Table 11 showing details of the responses to the question of whether organizations had ever been victims of cybercrime, what action followed.

Where I have been reporting

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------------|-----------|---------|---------------|--------------------|
| Valid Police but no action | 4 | 33.3 | 33.3 | 33.3 |
| Didn't report to Police | 8 | 66.7 | 66.7 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of how organizations’ digital security was managed, 58.3% answered “In-house by In-

charge of policies”. 41.7% answered “I don't know”. Bar chart 5 shows responses to the question of how organizations’ digital security was managed.

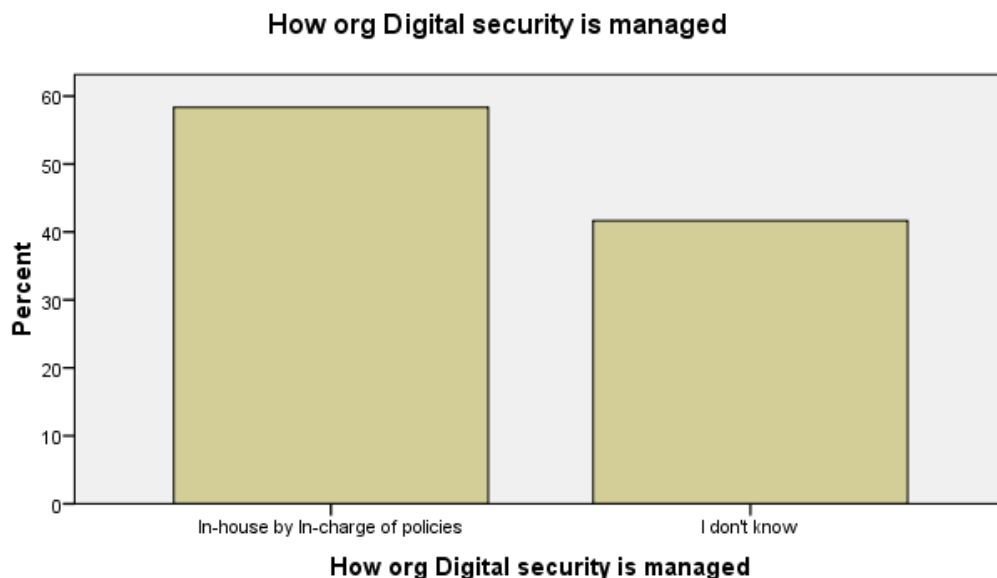


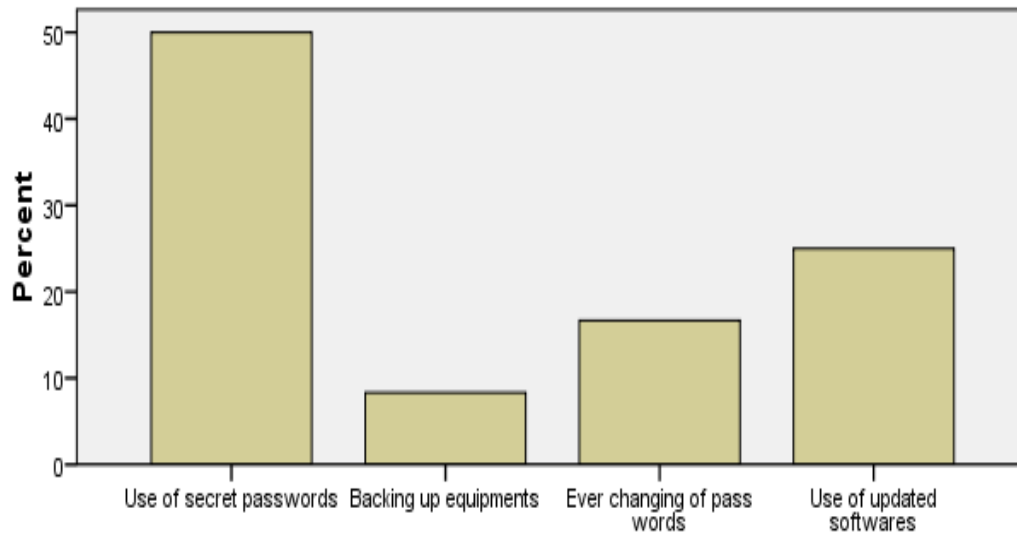
Table 12 showing details of the responses to the question of how organizations’ digital security was managed.

How org Digital security is managed

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|-----------|---------|---------------|--------------------|
| Valid In-house by In-charge of policies | 7 | 58.3 | 58.3 | 58.3 |
| I don't know | 5 | 41.7 | 41.7 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of how organizations managed digital equipment like computers, 50.0% answered “Use of secret passwords”. 25.0% answered “Use of updated software”. 16.7% answered “Ever changing of pass words”. 8.3% answered “Backing up equipment”. Bar chart 6 shows responses to the question of how organizations managed digital equipment like computers.

Management of Digital security equipments



Management of Digital security equipments

Table 13 showing details of the responses to the question of how organizations managed digital equipment like computers.

Management of Digital security equipment

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------------------------------|-----------|---------|---------------|--------------------|
| Valid Use of secret passwords | 6 | 50.0 | 50.0 | 50.0 |
| Backing up equipment | 1 | 8.3 | 8.3 | 58.3 |
| Ever changing of pass words | 2 | 16.7 | 16.7 | 75.0 |
| Use of updated software | 3 | 25.0 | 25.0 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of how often staffs were trained on cyber security risks, 66.7% answered “Yearly”. 25.0% answered “Never”. 8.3% answered “When there is a problem”. Bar chat 7 shows responses to the question of how often staffs were trained on cyber security risks.



Table 14 showing details of the responses to the question of how often staffs were trained on cyber security risks.

How often the staff are trained

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------------------------|-----------|---------|---------------|--------------------|
| Valid Yearly | 8 | 66.7 | 66.7 | 66.7 |
| Never | 3 | 25.0 | 25.0 | 91.7 |
| When there is a problem | 1 | 8.3 | 8.3 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

The question of which gender, among the staff was most affected or at a higher risk of digital insecurity, 50.0% answered “Females”. 33.3% answered “I don’t know”. 16.7% answered “both”. Pie chart 8 shows responses to the question of which gender, among the staff was most affected or at a higher risk of digital insecurity.

staff that is affected by digital insecurity

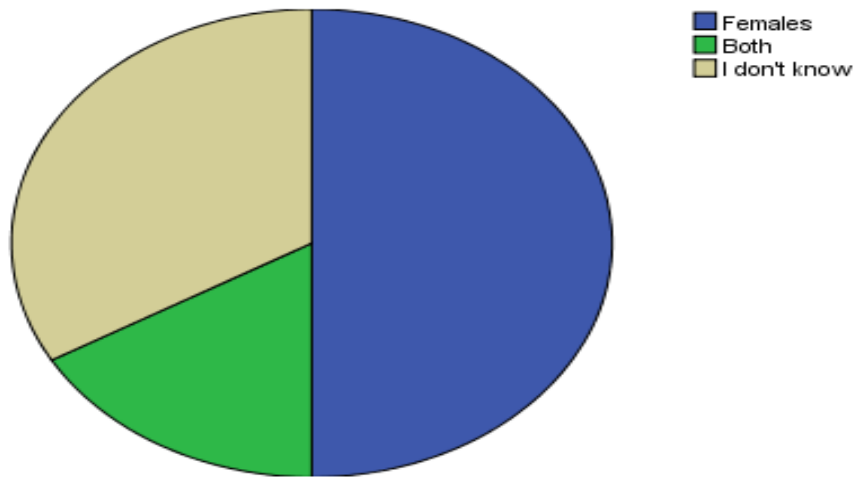


Table 8 showing responses to the question of which gender, among the staff was most affected or at a higher risk of digital insecurity.

Staff that is affected by digital insecurity

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------------|-----------|---------|---------------|--------------------|
| Valid Females | 6 | 50.0 | 50.0 | 50.0 |
| Both | 2 | 16.7 | 16.7 | 66.7 |
| I don't know | 4 | 33.3 | 33.3 | 100.0 |
| Total | 12 | 100.0 | 100.0 | |

CONCLUSION

Most of the registered LGBTQI organizations have little Digital security equipments. There are no specific trained personnel, employed in the field on LGBTQI community, for the purpose of effectiveness in organizational Digital Management System which is meant for the security of LGBTQI organizations. Organizational leaders are the same people who manage the Digital security systems. There is total LGBTQI Organizational Digital insecurity. There are limited opportunities or Digital management trainings. There are very few cases of Cyber crimes among LGBTQI organizations in Uganda.

RECOMMENDATIONS

There should be enough trainings about Digital management system, Digital security and Cyber-crimes among LGBTQI organizations in Uganda.

These can be, at least, three times per year. Each LGBTQI organization can train two to five personnel who will form a rich human resource as far as organizational Digital Security is concerned.

Professional staff should be employed for the purpose of effectiveness in organizational Digital Management System which is meant for the security of LGBTQI organizations.

Organizational leaders should be over all supervisors not the working personnel, on the ground, by themselves.

This will bring effectiveness at work when the one responsible knows that there is someone above him to either give a report or to evaluate his performance.

There is need to equip Organizations with data management systems and digital security equipments for use at their offices.

List of acronyms

ED - Executive Director MBs –

Megabits OTT – Over The Top Tax

LGBTIQ - Lesbian, Gay, Bisexual, Transgender

CCT V- Closed-Circuit Television CSOs – Civil Society Organizations NDPSCA –

Narcotic Drugs and Psychotropic Substances Control Act,

KPs - Key Populations

UPF - Uganda Police Force

MSM – Men who have sex with men

PWUIDs – People Who Use And Inject Drugs

TRIUMPH UGANDA – The Robust Initiative for Promoting Human Rights

HIV – Human Immune Virus

PLHIV – People Living With Human Immune Virus

SRHR- Sexual Reproductive Health Rights

AIDS- Acquired Immune Deficiency Syndrome

HRAPF – Human Rights Awareness And Promotions Forum.