ADISI - CAMEROUN

Digital Defenders Partnership

DIGITAL SECURITY

REPORT ON THE DIGITAL SECURITY ASSESSMENT OF CSOS AND MEDIA IN THE ENGLISH-SPEAKING REGIONS OF CAMEROON

Headquarters : Douala- Cameroon
3rd floor Aziccul building, Feu Rouge Bessengue
Phone : (+237) 243 526 139
Email : adisi@adisicameroun.org
Facebook : @ Adisi-Cameroon
Twitter : @AdisiCameroun
Website : www.adisicameroun.org - www.datacameroon.com

Hivos people unlimited

NED National Endowment for Democracy
Supporting freedom around the world

TABLE OF CONTENTS

LIST OF TABLES

LIST OF GRAPHICS

INTRODUCTION

In the modern world, technology has become so entwined with our lives that we rarely pause to consider its implications. It becomes difficult to imagine life without our devices, and even more challenging to consider our work without associated software and apps, video calling, the cloud, emails, servers and the various accounts that help us to connect with our activities, colleagues and relatives. If technology is a powerful enabler, it is crucial to consider how this ever-present fact of life can put us, our organizations, and our work, at risk.

Civil society and media Organizations rely greatly on the use of information technology for both their operations and innovative strategic program initiatives. In a sense, they are no different than any small, medium or large-scale enterprise with regard to computing. Keeping information confidential and free from integrity and privacy challenges as well as ensuring their systems are available are as important to these organizations as they are to any other entity and because of this they need to ensure they are protecting themselves, staff and systems against cyber security vulnerabilities.

To fulfill the duty of care obligations and protect staff from physical and psychological harm, organizations must mitigate risks related to their digital presence and activities. When organizations are starting a new project or entering a new region, both context analyses and risk assessments should therefore include digital security vulnerabilities and threats.

Every type of program attracts different risks. Emergency response programs may be more sensitive to blackmail, fraud or safeguarding threats. Advocacy and human rights campaigns may be targeted by various groups, seeking to damage the organization, or to collect personal information on beneficiaries and staff. Development projects are also vulnerable to the diversion of resources and corruption. Even internally, civil society organizations and media organizations use a range of technologies for their various operations, from communications to data gathering to implementation monitoring that can be interrupted at different stages by external or internal actors.
This project will discuss results from a field work conducted with 60 civil society organizations and 30 media organizations from 2 regions in Cameroon, including what type of cyber security programs, staffing, controls, and assessments are being employed, planned or considered.

I.PROJECT CONCEPT

The project is entitled “Digital security for media and civil society organizations in crisis areas in Cameroon” developed, implemented and supervised by the ADISI-Cameroon with headquarters in at Feu Rouge, AZICCUL building, Bessengue Douala.

The project aims to strengthen the digital security system of Civil Society Organizations and media in these North West and South west regions of Cameroon.

In order to collect data to analyze the state of the digital system of organizations selected, a questionnaire and an evaluation form was developed for field work with a digital security expert in selected media and Civil Society Organizations in the two regions

A.THE OBJECTIVES OF THE PROJECT

1.Main Objective

Strengthen the digital / digital system of journalists, their writing as well as civil society organizations in the crisis regions.

2.Secondary Objectives

Assess the digital security situation among media and non-governmental organizations based in Bamenda North-West and South-West;

Strengthen the digital system of the press and large non-profit organizations government based in North-West and South-West;

Train journalists and non-governmental organizations based in North-West and South-West on digital security.

II.ORGANIZATION OF THE FIELD WORK

The project targets 10 media organizations and 20 civil society organizations in Northwest and southwest regions, half from each region.
A 29-question questionnaire was created and circulated to selected media organizations, as well as civil society organizations. The questions in questionnaire the was elaborate to enhance comprehension as much as possible, and recipients were also briefed ahead of time and given enough time to fill so that it would not disturb their workday.
The questionnaire allowed for respondents to complete one per organization. Participants were not asked to provide any identifying information so as to keep the responses anonymous. A timeframe of 3 weeks was provided to allow participants to complete the questionnaire at their convenience. 30 questionnaires were completed.

A.ACTIVITIES PRIOR TO THE FIELD WORK

•The host organization made contacts with focal points in the 2 regions and these focal points forwarded a list of media and civil society organizations in their respective regions. The full list of 30 organizations was established and approved for data collection.

• A questionnaire of 29 questions and an evaluation form was developed and approved by the host organization.

•A field work plan was for the both regions was drawn and approved.

•The questionnaires were forwarded through mail to all 30 organizations to fill.

•The evaluation forms were printed and calls made to book meetings with organization representatives.

B. ACTIVITIES DURING THE FIELD WORK

Physical evaluation at all organizations with the expert and a representative of the host organization.

• Organizations that were not reachable on the field were replaced with others within the same region.

III. THE COLLECTION TOOLS USED AND REASON FOR CHOOSING IT

The following methods were used to collect data for the project; administration of questionnaires and conducting interviews.

A.ADMINISTRATION OF QUESTIONNAIRES

A questionnaire of 29 questions that covers 3 major areas; personnel, equipment and data transfer, was developed to collect data during this phase of digital systems assessment. This method of data collection was chosen because it allows data collection plan to be carefully structures and formulated with precision, thereby giving time for respondents to take these questionnaires at a convenient time and think about the answers at their own pace.

The questionnaires were sent through emails but the response rate was very low, so during the field evaluation, the questionnaires were administered and it was all filled.

B. CONDUCTING INTERVIEWS

The second method of data collection was the field interview. This has helped to uncover rich, deep insight and learn information that they may have missed otherwise. Also, the presence of an interviewer can give the respondents additional comfort while answering the questionnaire and ensure correct interpretation of the questions and significantly improve the response rate.

IV. THE DIFFERENT ORGANIZATIONS AND MEDIA ENCOUNTERED BY REGION

Through the decent field, we have reached a total of 30 organizations, as have 15 Southwest including 10 civil society organization and 05 media and also 15 in the northwest including 10 civil society organization and 05 media. The following tables give more details

Table 1 : Civil society organization and media NorthWest Region

MEDIA ORGANIZATIONS		
	Name of Organization	**Region**
1)	CameroonCommunity media Network	NorthWest
2)	Ndefcam Radio	NorthWest
3)	Liengu'sDiary	NorthWest
4)	The Guardian Post	NorthWest
5)	Chamers Media and Communications Consults	NorthWest
CIVIL SOCIETY ORGANIZATIONS		
1)	Global Initiative for Digital Inclusion and Communication	NorthWest
2)	Community Participation in SustainableDevelopment	NorthWest
3)	Mandela VoluntaryFoundation	NorthWest
4)	YouthOutreach Program	NorthWest
5)	Comunity impact for Africa (CIFA)	NorthWest
6)	Refugeewelfare association Cameroon	NorthWest
7)	Hope Alive Association	NorthWest
8)	Regional center for the welfare of ageing people in Cameroon	NorthWest
9)	African girls development Organisation	NorthWest
10)	Sustainablewomens Organisation	NorthWest

Table 2 : Civil society organization and media SouthWest Region

MEDIA ORGANIZATIONS		
1)	HI TV	SouthWest
2)	Mediafrique	SouthWest
3)	CBC Radio	SouthWest
4)	THE ADVOCATE	SouthWest
5)	Legacydevelopment tv	SouthWest
CIVIL SOCIETY ORGANIZATIONS		
1)	Hope for a bettertomorrow	SouthWest
2)	Reach Out	SouthWest
3)	HUMAN IS RIGHT	SouthWest
4)	SHF CAMEROON	SouthWest
5)	CEYOFE	SouthWest
6)	MIVEG	SouthWest
7)	DAREM	SouthWest
8)	Train up a Child	SouthWest
9)	Lukmef	SouthWest
10)	CHRDA	SouthWest

V. DATA PRESENTATION AND COMPUTATION

In the assessment phase, the data collection targeted 30 organizations, 10 media and 20 civil society organizations, thus 5 media and 10 civil society organizations in the North West; 5 media and 10 civil society organizations in the South West. The main goal of the data collection was to be able to access the digital security situation among media and non-governmental organizations based in North-West and South-West Regions of Cameroon.

A.DIGITAL SECURITY QUESTIONNAIRE

This document was divided into 3 sections, addressing ; personnel, equipment and data transfer.

1.Personnel

In this section, it was about evaluating how the respondent interacts with basic digital devices and the use of security features on them. All 30 respondents answered this section giving a 100% response rate

The key objectives here were:

- To assess if respondents are versed with mobile and computer devices.
- To rate respondents' understanding and use of basic security features on these devices.

To achieve the objectives above objectives, the following questions were answered

Table 3 : Evaluation of staff interaction with basic digital devices and the use of security features

Question	YES	NO	TOTAL RESPONDENTS
Have a personal computer	28 (93.33%)	2 (3.67%)	30
Have a smart phone	29 (96.67%)	1 (3.33%)	30
Have computer password	24 (80%)	6 (20%)	30
Computer has an antivirus	28 (93.33%)	2 (3.67%)	30

2.EQUIPMENT

This section provided the opportunity to examine how respondents use storage equipment as individuals and within the organization. All 30 respondents answered this section giving a 100% response rate.

The key objectives here were:

- **To know if respondents use personal and/or organizational storage devices.**
- To assess the level of security in securing data

To achieve the objectives above objectives, the following questions were answered.

Table 4 :Use of storage equipment as individuals and within the organization

QUESTION	YES		NO		TOTAL RESPONDENTS
Is your office networked with a network cable?	3 (10%)		27 (90%)		30
Does your organization have a website?	25 (83.33%)		5 (16.67%)		30
Is there a website that you are restricted from accessing by your office?	2 (6.67%)		28 (93.33%)		30
How do you move data from one staff to another	Flash disc drive	Wireless access to share group	WhatsApp	Network Workgroups	
	25 (83.33%)	2 (6.67%)	6 (20%)	1 (3.33%)	30

3.DATA TRANSFER

We were able to discover through this section, how information within the organization passes from one end user to another. All 30 respondents answered this section giving a 100% response rate.
The key objectives here were:
•To know how staffs within the organization move data from one person to another

Table5 :Transferring information within the organization from one end user to another

QUESTION	YES		NO		TOTAL RESPONDENTS
Is your office networked with a network cable?	3 (10%)		27 (90%)		30
Does your organization have a website?	25 (83.33%)		5 (16.67%)		30
Is there a website that you are restricted from accessing by your office?	2 (6.67%)		28 (93.33%)		30
How do you move data from one staff to another	Flash disc drive	Wireless access to share group	WhatsApp	Network Workgroups	
	25 (83.33%)	2 (6.67%)	6 (20%)	1 (3.33%)	30

•To know if staffs are restricted from accessing certain information by organization policy.
To achieve the objectives above objectives, the following questions were answered.
Table 5 : Transferring information within the organization from one end user to another

B.THE EVALUATION FORM

This document is divided into 5 sections distributed as continuations: identify, protect, detect, respond and recover.

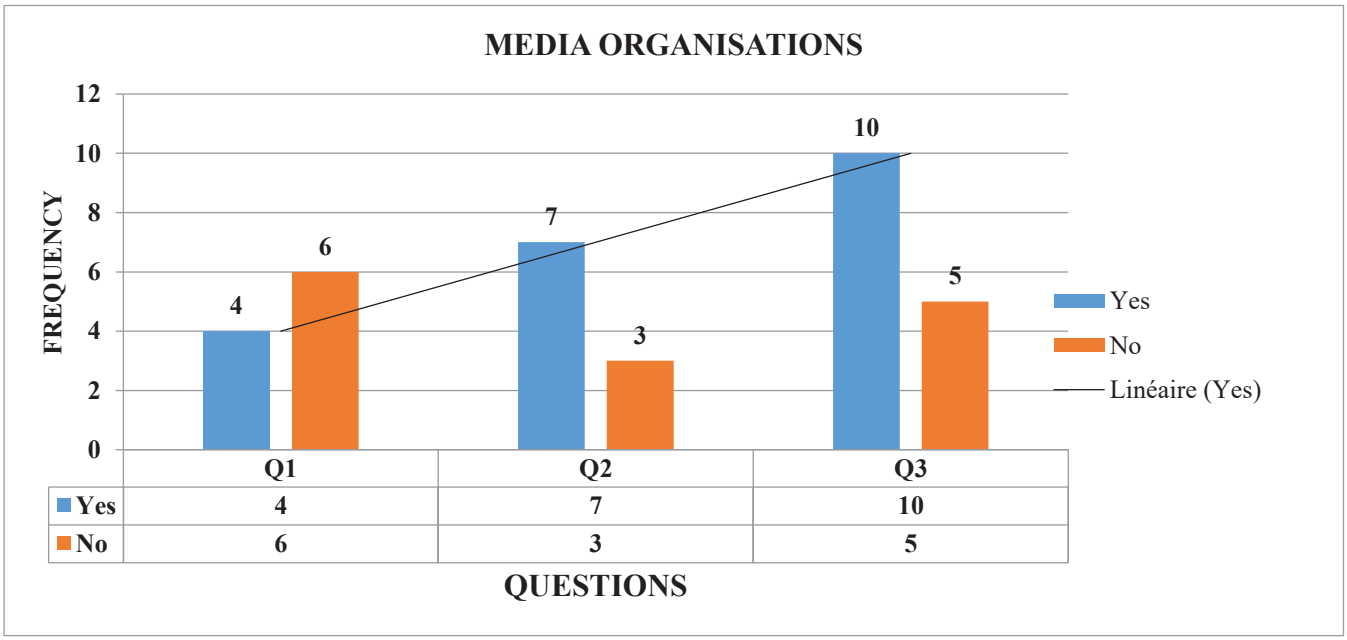
1.Identify

This section made it possible to study the structures and practices in place to identify cyberthreats. The evaluation addresses; who is responsible for cyber security and who can address it, what systems are in place and what software the systems use. This helps us identify the potential source of a security breach.
The main objective: to study the structures and practices in place to identify cyberthreats.

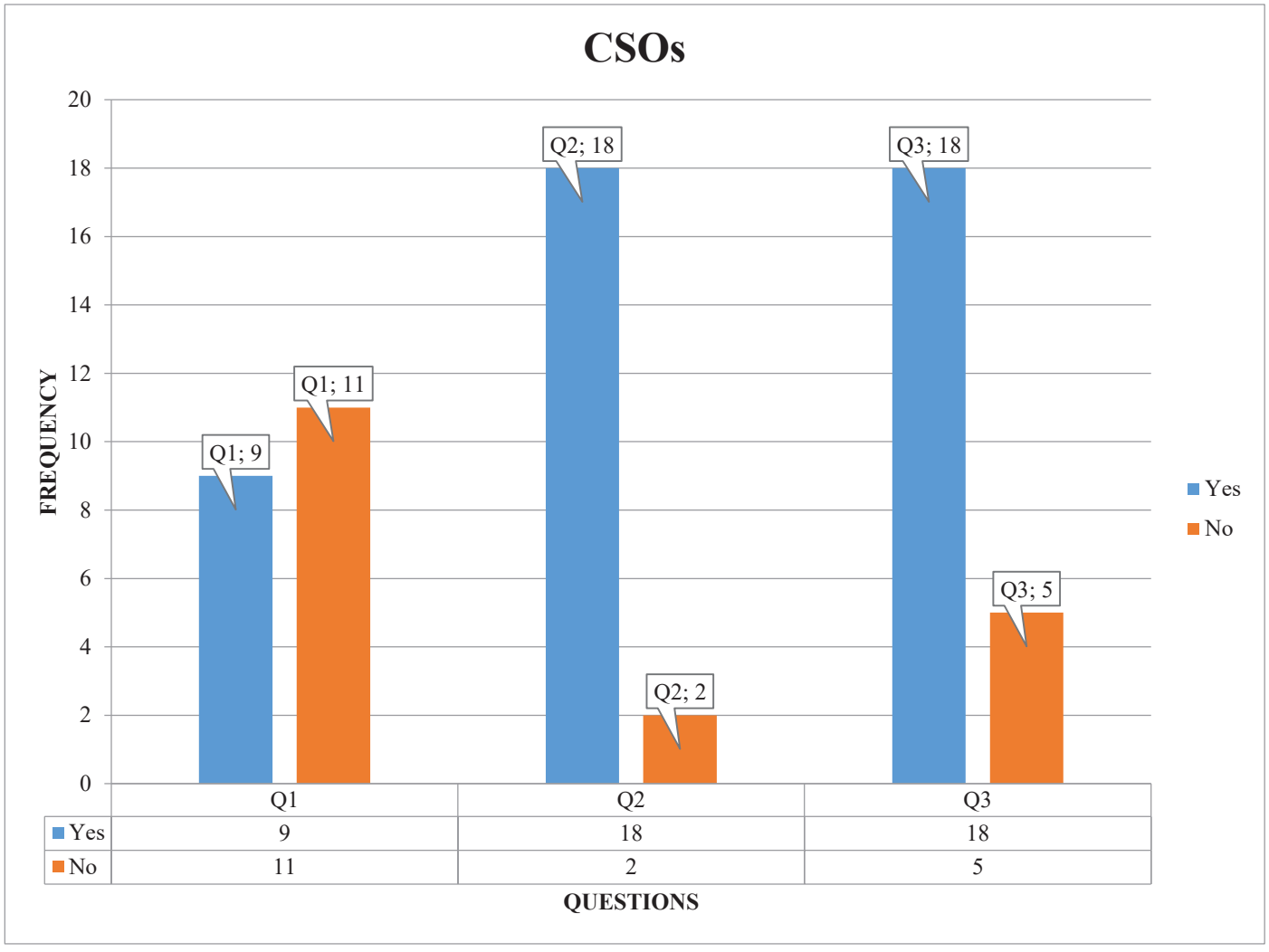
Table 6 : Study on the structures and practices in place to identify cyber threats

CODE	Question	MEDIA		TOTAL RESPONDENTS	CSOs		TOTAL RESPONDENTS
		YES	NO		YES	NO	
Q1	do you have any staff in charge of cybersecurity?	4 (40%)	6 (60%)	10	9 (45%)	11 (55%)	20
Q2	do you contract a consultant out of the organisation for cybersecurity issues?	7 (70%)	3 (30%)	10	18 (90%)	2 (10%)	20
Q3	is your operating system supported ?	10 (100%)	0 (0%)	10	18 (90%)	2 (10%)	20

Graphic 1: Study on the structures and practices in place to identify cyber threats (Media organisations)



Graphic 2 : Study on the structures and practices in place to identify cyber threats (CSOs)



2.Protect

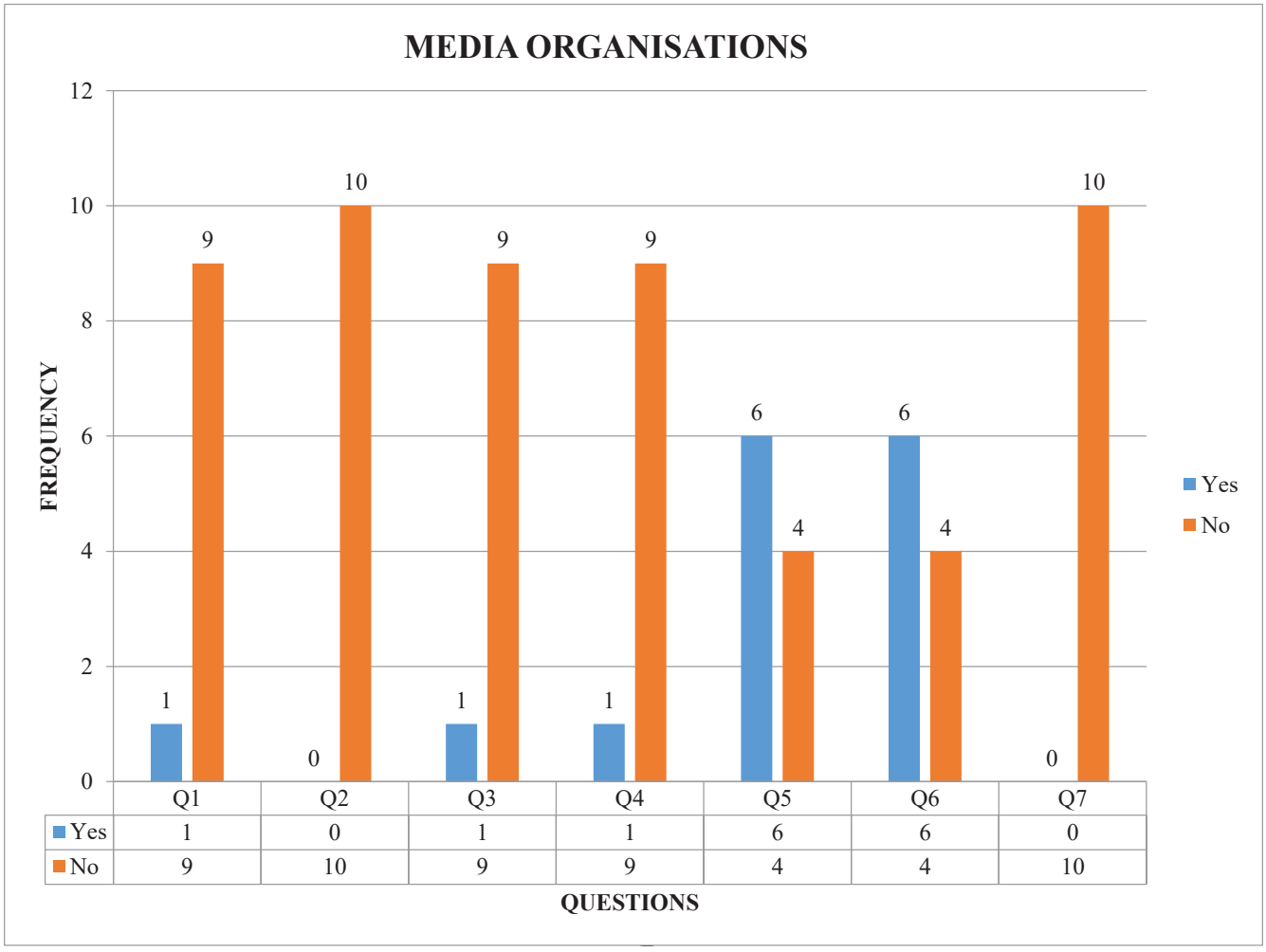
This allowed us to discover the basic practices in place to protect systems and information. He walked us through the specific ways we protect data. User Identities, passwords, data encryption, data segregation, system patching and employee training are a means of determining who is accessing what data at what time.

The main objective of this section is to protect data and systems using best practices.

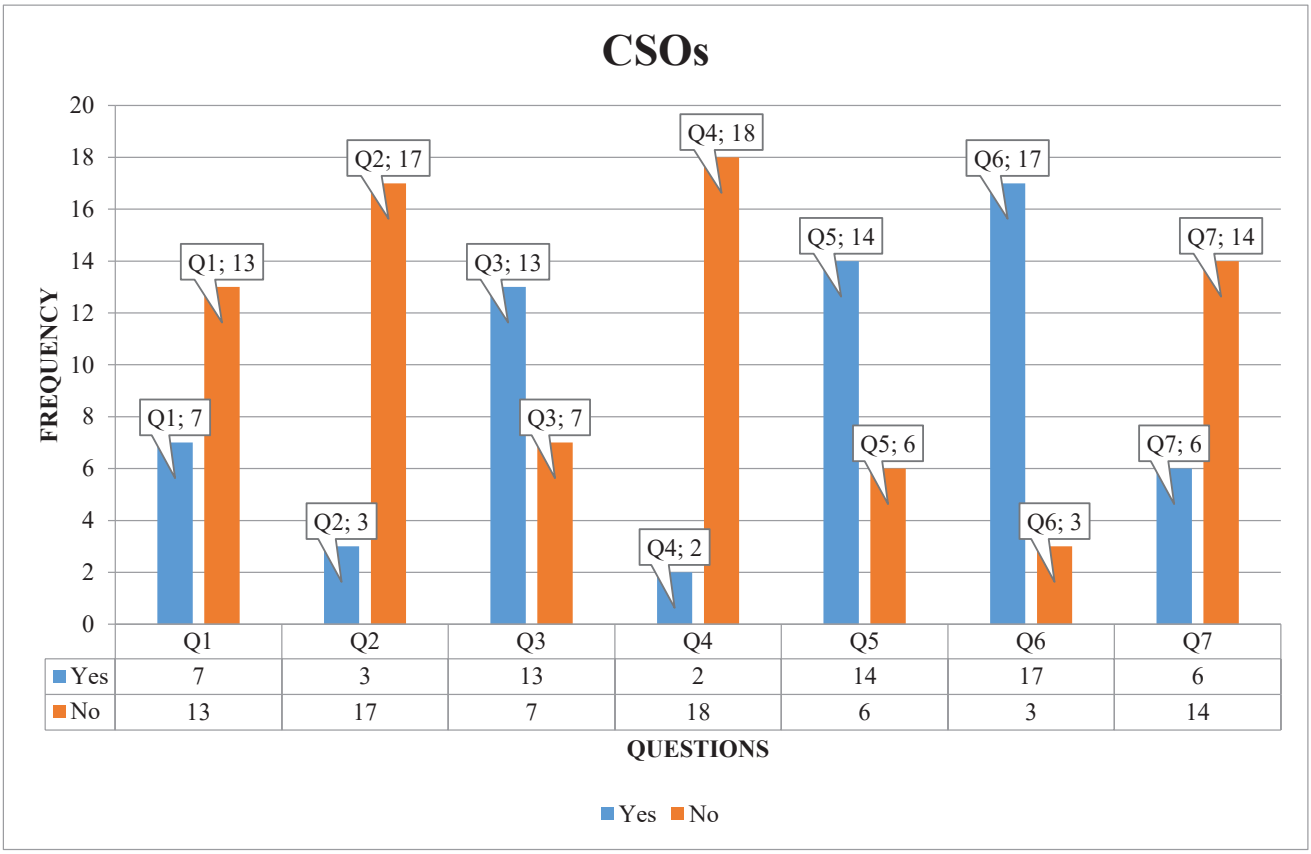
Table 7 : Study of the basic practices in place to protect systems and information.

CODE	Questions	MEDIA		TOTAL RESPONDENTS	CSOs		TOTAL RESPONDENTS
		YES	NO		YES	NO	
Q1	DO you lock your system after inactivity ?	1 (10%)	9 (90%)	10	7 (35%)	13 (65%)	20
Q2	Do you have a password policy sdocument ?	0 (0%)	10 (100%)	10	3 (15%)	17 (85%)	20
Q3	Do you encrypt data ?	1 (10%)	9 (90%)	10	13 (65%)	7 (35%)	20
Q4	Do you seggregate data ?	1 (10%)	9 (90%)	10	2 (10%)	18 (90%)	20
Q5	Do you access files remotely ?	6 (60%)	4 (40%)	10	14 (70%)	6 (30%)	20
Q6	Do you use firewalls ?	6 (60%)	4 (40%)	10	17 (85%)	3 (15%)	20
Q7	Have you had any previous training on digital information management or cyber securuty before?	0 (0%)	10 (100%)	10	6 (30%)	14 (70%)	20

Graphic 3 : Study of the basic practices in place to protect systems and information (Media organisations).



Graphic 4 : Study of the basic practices in place to protect systems and information (CSOs).



3. Detect

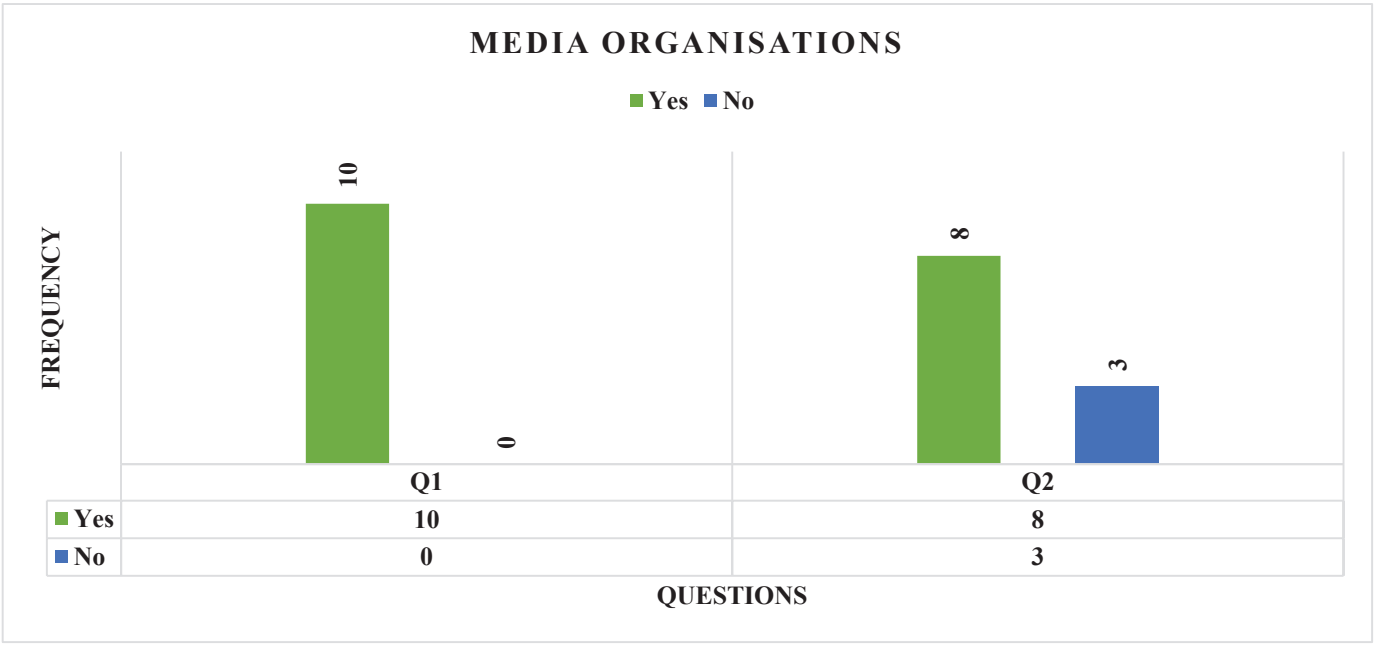
This section allowed us to assess the different tools used to identify someone or something malicious. Detection is the process to recognize if something is going wrong on your network and, if possible, stopping it. This also gives an insight on how these organizations use detection tools to determine the impact of a threat.

The main objective here is to identify something or someone malicious.

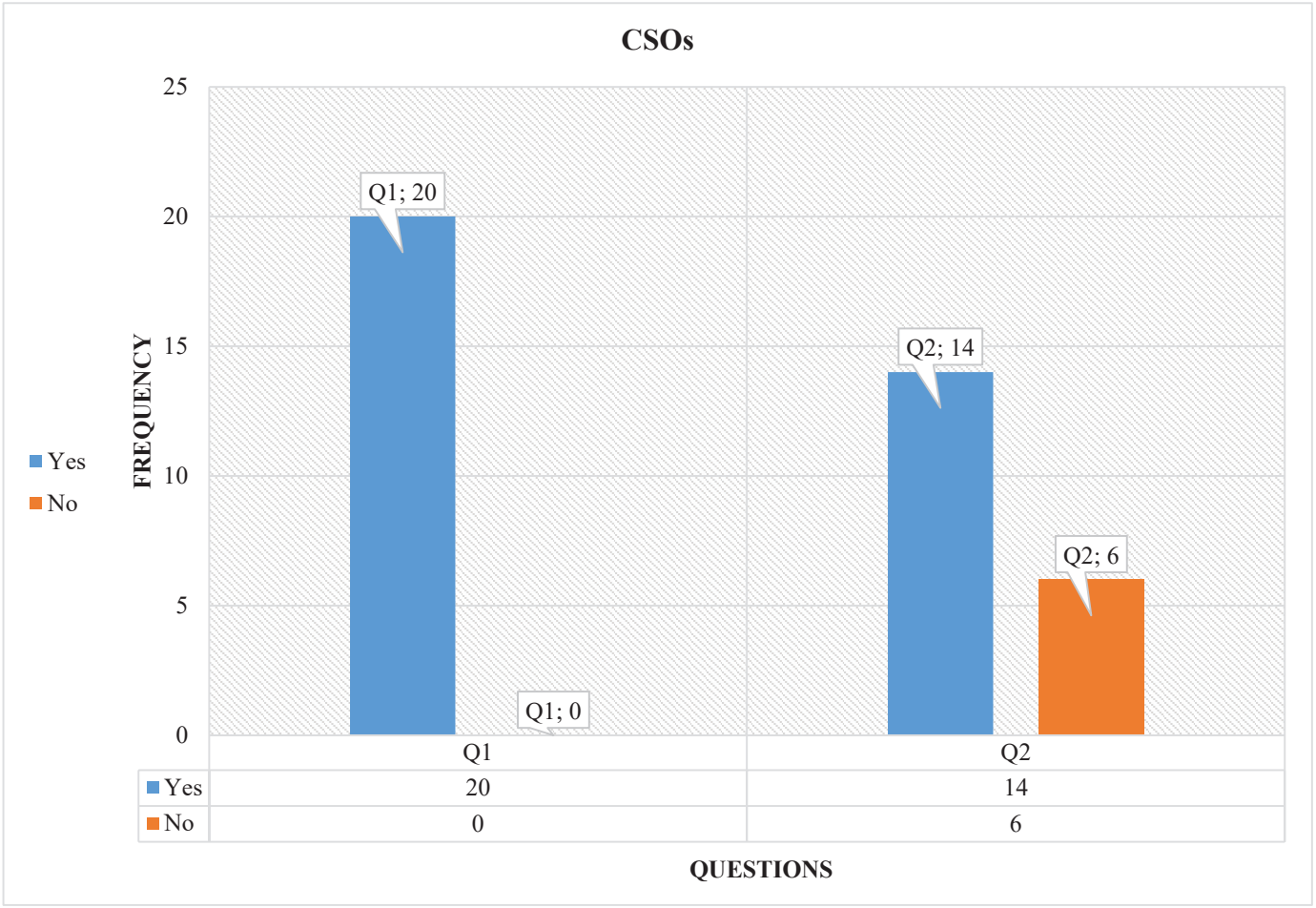
Table 8 : Evaluation of the various tools used to identify someone or something malicious

CODE	Questions	MEDIA			CSOs		
		YES	NO	TOTAL RESPONDENTS	YES	NO	TOTAL RESPONDENTS
Q1	do you have an antivirus?	10 (100%)	0 (0%)	10	20 (100%)	0 (0%)	20
Q2	do you have an antimalware?	8 (80%)	2 (20%)	10	14 (70%)	6 (30%)	20

Graphic 5 : Evaluation of the various tools used to identify someone or something malicious (Media)



Graphic 6 : Evaluation of the various tools used to identify someone or something malicious (CSOs)



4. Respond

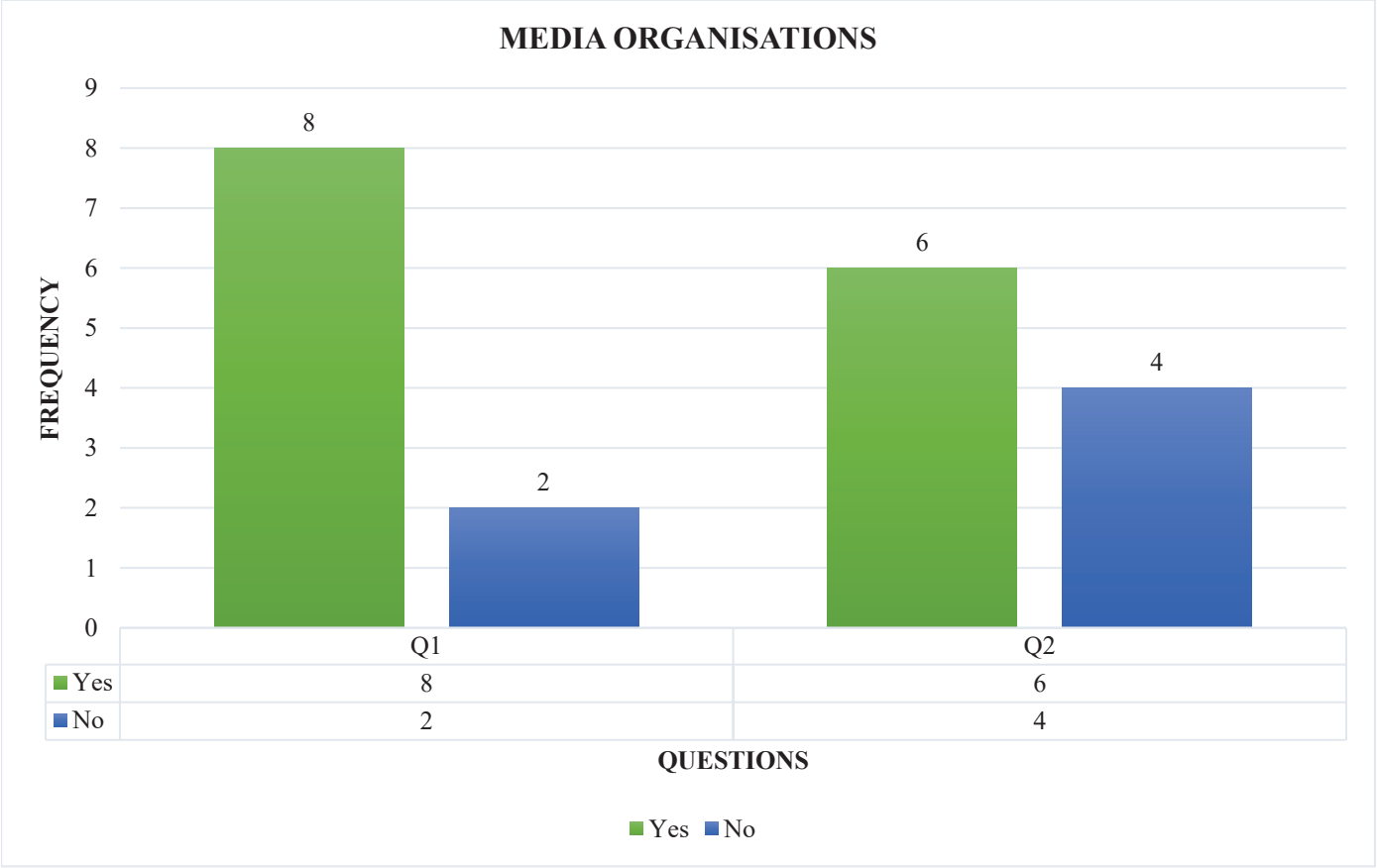
In this section, we evaluated how to handle a data breach when it actually occurs. IT security incident response and recovery are an area with which organizations may struggle. Smaller organizations generally do not have the time to create elaborate plans and to test, so there's a need to plan in a fashion that works for a particular organization.

The main objective: to evaluate the procedure to deal with a breach when it occurs.

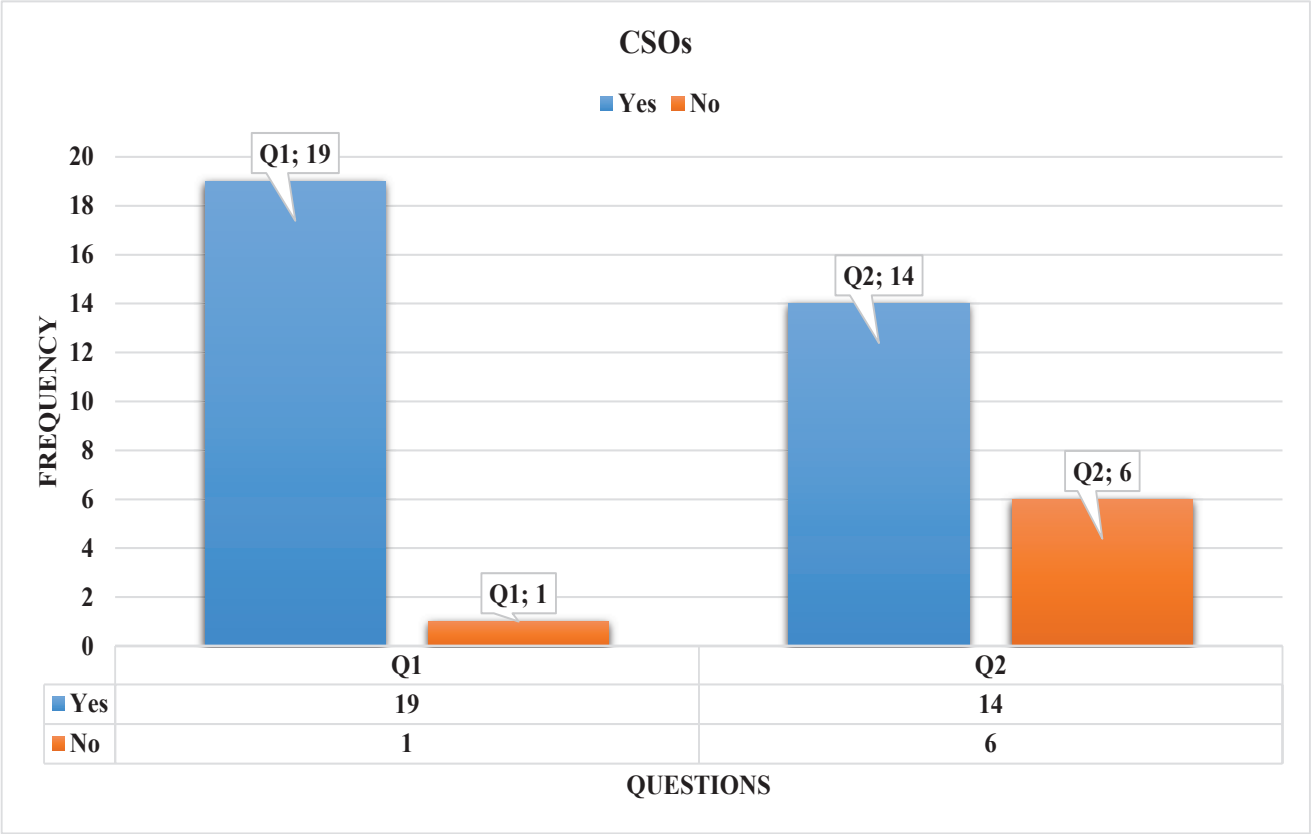
Table 9 : Evaluation of the management of a data breach when it actually occurs

CODE	Questions	MEDIA		TOTAL RESPONDENTS	CSOs		TOTAL RESPONDENTS
		YES	NO		YES	NO	
Q1	Do you back up data?	8 (80%)	2 (20%)	10	19 (95%)	1 (5%)	20
Q2	Have you had any situation where you lost data or faced any cyber security threat?	6 (40%)	4 (60%)	10	14 (70%)	6 (30%)	20

Graphic 7 : Evaluation of the management of a data breach when it actually occurs (Media)



Graphic 8 : Evaluation of the management of a data breach when it actually occurs (CSOs)



4. Respond

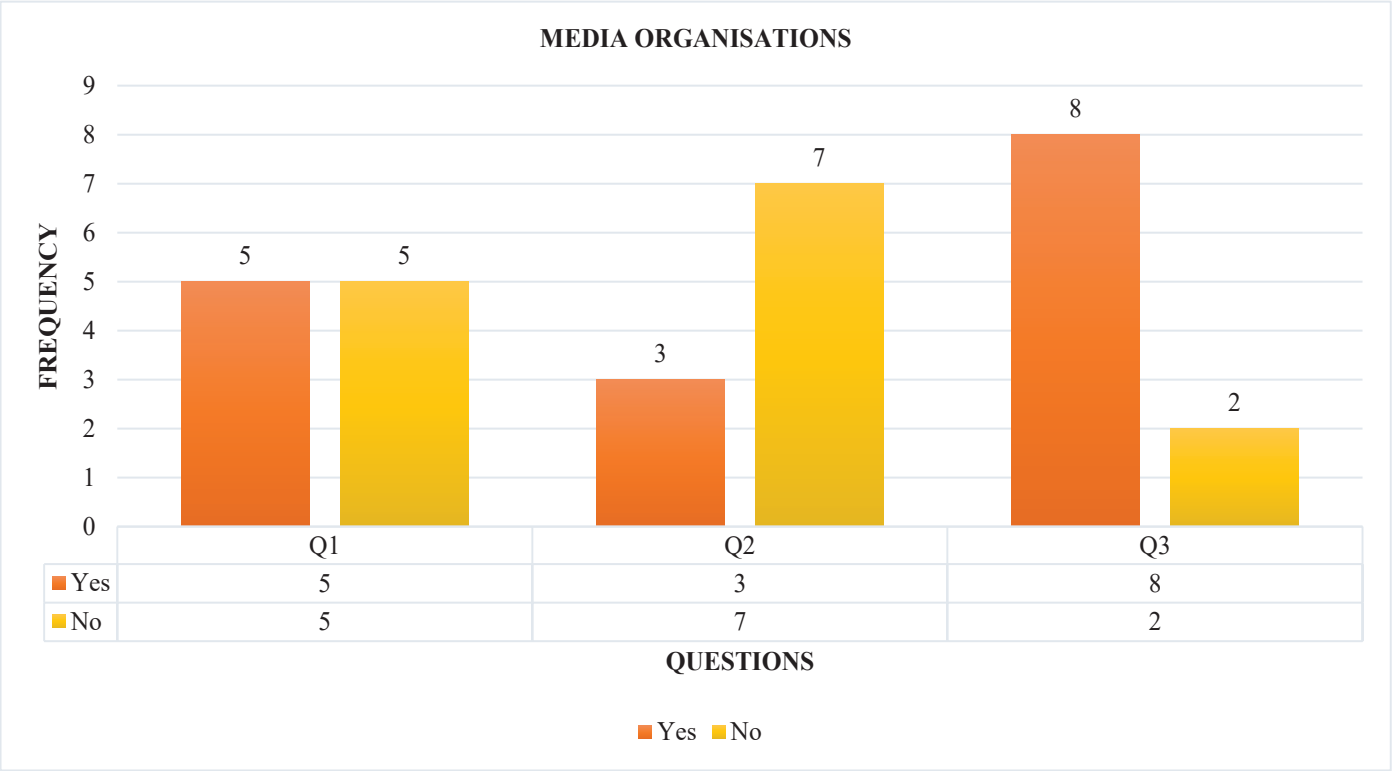
In this section, we evaluated how to handle a data breach when it actually occurs. IT security incident response and recovery are an area with which organizations may struggle. Smaller organizations generally do not have the time to create elaborate plans and to test, so there's a need to plan in a fashion that works for a particular organization.

The main objective: to evaluate the procedure to deal with a breach when it occurs.

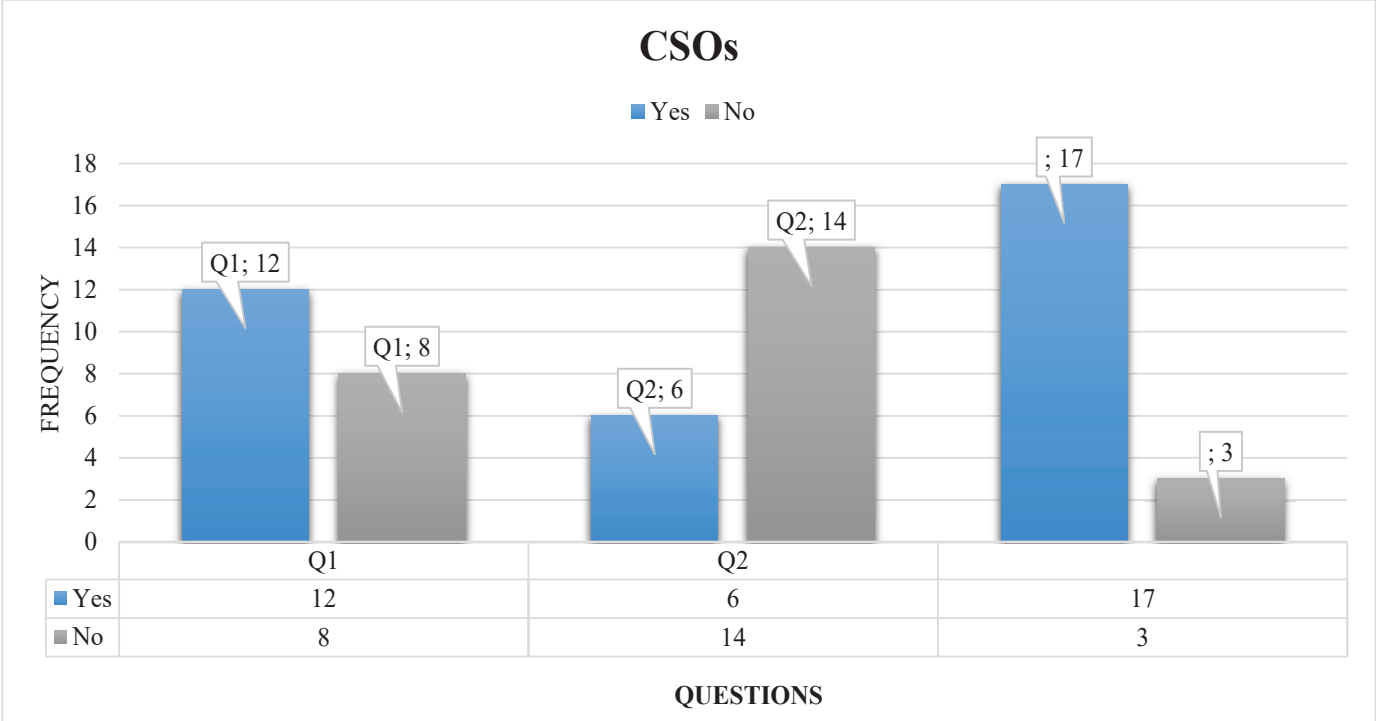
Table 10 : Study of ways to restore the organization's operations to normal after a digital security breach.

CODE	Questions	MEDIA		TOTAL RESPONDENTS	CSOs		TOTAL RESPONDENTS
		YES	NO		YES	NO	
Q1	do you have a legal contact as a resouce in case of a cyber attack?	5 (50%)	5 (50%)	10	12 (60%)	8 (40%)	20
Q2	do you have a cyber security consulting firm as a resource in case of a cyber attack?	3 (30%)	7 (70%)	10	6 (30%)	14 (70%)	20
Q3	do you have the judicial police as a resource in case of cyber attack?	8 (80%)	2 (20%)	10	17 (85%)	3 (15%)	20

Graphic 9 :Study of ways to restore the organization's operations to normal after a digital security breach (Media)



Graphic 10 : Study of ways to restore the organization's operations to normal after a digital security breach (CSOs)



VI.PRESENTATION OF RESULTS

The key take-away from the short cyber security audit demonstrates that there is ample opportunity and a critical need for media and civil society organizations to improve their approach to securing their assets, information, staff and systems.

Of the nearly half of the respondents who said they did not have a staff person or department fully assigned to tackling cyber security, only 11% responded that they have a plan in place to create.

This is a very low percent when in technology services; cyber security is currently viewed as a strategic priority. The reasons can be many, including budget constraints, since there may be restrictions on using donor funds for overhead projects, such as cyber security, instead of programmatic efforts which contribute to the core value they provide to their donors and constituent communities.

Regarding staff training on cyber security issues, 80% of the organizations said they have never had any training, followed by 20% who did. On the evaluation of staff in charge of cyber security, only 40% of the media organizations had while 60% had no staff in charge of cyber security. For civil society organizations, 45% had a staff in charge of cyber security while 55% did not have. This margin below average is because of the less value placed on digital security concerns across these sectors and the lack of sensitization among media and civil society executives.

Of the 10 media organizations that were evaluated, 7 had external consultant they go to in case of any digital security issue while 3 saw no need for an external consultant. Within the civil society organizations, 18 had external consultants while 2 had none. The massive reliance on external consultants for digital security issues is due to the less value these organizations place on digital security and because of lack of expert knowledge in this area.

From the evaluation, it was discovered that most of the operating systems used in both media and civil society organizations are supported systems, that is, they get updates from the system providers. This system are mostly windows 7 and above. All the media organizations had supported systems while 90% of the civil society organizations had supported systems. The 10% used Windows XP and Microsoft stopped sending updates for XP and earlier versions. The 10% was ignorant of the security exposure of their operating system.

It was also seen that only 1% of media organizations lock their systems after inactivity and 90% did not, likewise, only 35% of the civil society organizations lock their systems or configure their systems to lock after inactivity. From the evaluation, it was noticed that there was low use of password and other digital security policy documents, 0% for media organizations and 15% for civil society organizations. The low consideration of protective measures to possible areas of vulnerabilities is greatly due to lack of training in information handling and cyber security. None of the media organizations have had previous training in information handling while only 30% of civil society organizations have gone through some prior training. This actually brings to reality the need for further evaluation and training in these sector as suggested in the recommendation section.

All media and civil society organizations had antivirus installed on their computers. For media organizations, 80% had antimalware installed while 70% of civil society organizations had antimalware on their systems. Even with the high level of antivirus and antimalware installations, less than 20 of the total organizations evaluated update their antivirus and antimalware regularly and it was also noticed that most of these programs where free versions that offered very little protection.

All the organizations were evaluated on how they recover after a cyber-attack in terms of availability of resources. Three primary resources were identified; Legal firm or person, cyber security consultant and judicial police. 50% of media organizations said they have a legal person, 30% said they work with cyber security consultants and 80% have the judicial arm of the police as one of their resource.

For civil society organizations, 60% said they work with a legal firm, 30% work with cyber security firms and 85% had the judicial police as one of their resources.

VII.DIFFICULTIES ENCOUNTERED DURING THE ACTIVITY

i. The regions where the project was carried out has a history of social, economic and security crises which is still active thus the organizations that were considered are only those found in areas that are considered accessible and safe;

ii. The location of some organizations was not easy to get as the field work team was not versed with the entire region;

iii. Team had to go through strict security checks at regular intervals in the target regions;

iv. Some organizations were resistant to give out information because of the security situation in the host regions;

v. Most respondents refused to snap pictures with the team on the field in order to remain anonymous;

vi. Some organizations were not reachable and had to be replaced.

CONCLUSION

Ultimately, ddigital security is a valuable part of our everyday life and within an organizational setting, its application is inalienable. A permanent review, even reinforcement at the personal and organizational level is therefore important to achieve a holistic defense against cyberthreats.

This project aims to contribute to strengthening the digital security of media and civil society organizations in the North West and South West regions, following the assessment of their condition. Therefore, the results of the evaluation phase are proof that the stated objectives have already been reached at almost 40%. Thus, there is need for further research in these areas to further investigate vulnerability possibilities and best practices how organizations can protect and respond to digital security threats.

Media and civil society Organizations do employ the basic tools to help protect their technology and the digital environment of their staff, including both perimeter protection and endpoint security. The more advanced tools which permit for logging of events to be centralized and analyzed, even with artificial intelligence are not possible in many of the organizations discussed in this paper.

There are however opportunities to further protect the digital environment of an organization, without large capital purchases. Behavioral research and approaches provide an opportunity to help provide protection for organizations, without large purchases; however, this would require staff- level focus. If humans using computer systems are given the tools and information they need, taught meaningful and responsible use, and trusted to behave appropriately with respect to cyber security, desired outcomes may be obtained without security procedures being perceived as troublesome or onerous. It's well known that despite technical cyber security efforts, the employee remains the most vulnerable target for cyber-criminals.

Therefore, providing more education to staff may not require a large capital purchase but could yield substantial benefits.

Media organizations pay little attention to digital issues compared to civil society organizations, yet the activities they do on a daily basis are all the more fueled or controlled by the digital tool. Many media and civil society organizations are reluctant to explore new technologies due to the initial efforts required to train their staff and adapt their processes. However, when wisely incorporated into our activities, innovation can make programming both safer and more effective in the long term.

This report on gives a surface view into possible digital security threats to the sample organization and a need for these organizations to put in place structures, policies and tools to be better equipped against breaches. However, to truly understand the concept of digital threats and information management in depth, a more elaborate digital security analysis needs to be done, which will involve extensive training of digital security tools and the hierarchical movement of information within organization.

RECOMMENDATIONS

Media and civil society organizations have the opportunity to focus on their cybersecurity approaches, perhaps without a big budget and limited spending.

Cyber-hygiene controls, which include a set of practices and behaviors designed to minimize the impact of possible breaches, such as segmentation of duties, segmentation of privileges, access policies, and the like are free to adopt and implement. The primary limitations to their implementation are awareness, training, and discipline.

There are a number of incremental efforts and techniques that can be implemented despite constraints that may be helpful. Some of these to consider are:

1) For those organizations who are hosting web applications or publicly available websites in the cloud or on-premises, referring to the Open Web Application Security Project (OWASP). The OWASP provides guidelines, articles, and methodologies freely for organizations to employ.

2) Ensuring that IT systems are updated routinely for operating system updates, and employing adequate end-point protection software.

3) Create a cyber security awareness program that allows staff to be continually educated on steps they can take to contribute to securing their access to systems.

4) If the organization has an enterprise risk management program, it should include cyber security concerns.

5) Develop a plan for what steps you should take if and when the possibility of a serious security concerns arises.

6) When developing or using Android or iOS device applications, only download from trusted sources that are verifiable and link to trusted websites.

7) Make the best use of existing hardware, software and firewall capabilities, such as enabling Geo-IP filtering.

8) Even if CSO and Media cannot get certified, follow one of the recognized security frameworks such as ISO 27001, COBIT, NIST Cyber security Framework or NIST 800-53a. The NIST documents offer much backed cyber security research that is freely available.

9) Consider if it is possible to add cyber security coverage to the organizations existing insurance policy.

10) Given that the overwhelming method used by organizations to recover from ransom ware was from backup restore, it would be prudent to ensure that backups are routinely tested and working properly. Keeping redundant backups would be advised.

11) Performing at least one disaster recovery drill per year within an IT department or cyber security consultancy firm would provide a documented track record that proves the system works and put into place a routine for system administrators in case such an attack occurs.

12) An increase in cyber-hygiene and improvements to endpoint security can be accomplished by mapping the network and controlling access based on need. Mapping and need-only access policies are free and can be simple to implement. Testing the endpoint device security, as the last line of defense should be done quarterly as a spot check to ensure devices are protected.

13) Conduct a risk assessment at regular intervals the organizations assets and apply controls applied where applicable.

14) Provide security awareness training to all staff on induction and communicate security updates at regular intervals.

15) Document security policies, procedures, internal processes and technical work instructions.

16) Implement regular vulnerability scanning and monitoring

17) Plan, document and implement a patching policy for all hardware and applications.

The project training modules should cover Context analysis and actor mapping, risk assessment, Digital security, Security strategies (Acceptance, protection and deterrence), Security plan, Standard Operating Procedures (How staff will mitigate the threats identified in the risk assessment) and physical data security.

REPORT ON THE DIGITAL SECURITY ASSESSMENT OF CSOS AND MEDIA IN THE ENGLISH-SPEAKING REGIONS OF CAMEROON

AOIS - CAMEROON

Digital Defenders Partnership

Hivos people unlimited

NED National Endowment for Democracy
Supporting freedom around the world