DIGITAL SECURITY SURVEY

August 2017

An Assessment of the Digital Security Posture of HRDs in Uganda

Defenders Protection Initiative
Plot 944, Block 254, Kansanga – Ggaba Road | P. O. Box 35684, Kampala – Uganda
Tel: +256-312-201102 | Email: admin@defendersprotection.org | Web: http://www.defendersprotection.org

Acronyms

Table of Contents

Table of Figures

1 Executive Summary

Information and Communications Technologies are at the core of the operations of nearly every organisation as they support nearly every operation within the organisation. Unscrupulous parties target them to cripple the operations of organisations by attacking their digital assets to either destroy them, deny their rightful owners access, to steal both information and finances.

Civil society in Uganda, just like any other sector, has been a victim of digital security incidents. These incidents have been perpetrated by vendors, employees, criminals, powerful business interests and state actors.

This study to assess the digital security posture of civil society organisations was commissioned by Defenders Protection Initiative (DPI) which has been at the forefront of building the capacity of Human Rights Defenders (HRDs) to create a secure environment for their work including digital security.

This study found that even though DPI and other players have made efforts to sensitise civil society on digital security, there are areas of exposure that have affected and continue to affect the security of CSOs. These areas are in relation to IT governance in CSOs, inadequate finances and IT human resources to manage IT in the organisations and digital security and limited adherence to recommendations made during digital security trainings. As a consequence, a majority of the CSOs have been victims to digital security incidents.

Continued incidents pose a threat to the entire sector because civil society in Uganda does a lot of its work in a collaborative effort on many causes such as human rights, governance issues, land and property rights and others which draw the attention of powerful and sometimes criminal forces. A successful breach on the digital assets (information, IT infrastructure, etc) on one CSO could potentially unravel the security of the entire sector, its beneficiaries and donors. There is therefore a need for CSOs to work together to secure the digital assets. This can be achieved by creating a formal partnership among CSOs where financial resources are pooled to support a team of IT specialists to provide IT support and digital security services to the sector. The IT personnel can be drawn from the already existing IT professionals employed by the sector. This partnership should also make partnerships with the private sector and other international organisations to obtain equipment, skills and infrastructure at subsidised prices so that CSOs with limited resources can have the benefit of very secure systems, skills and training.

Key findings and recommendations

	Key Finding	Recommendations	
		Short Term	**Long Term**
1	More than half of the CSOs do not have an IT Policy, and of the ones that have, 27% of them do not enforce the policies across the organisation.	• Support CSOs to conduct digital security assessments and to create IT policies and procedures.	• Conduct regular reviews on the effectiveness of existing policies and adherence to the policies within the organisations
2	Only 46.8% of the organisations employ full-time IT professionals and over 80% of those that do not cite lack of financial resources to hire a professional	• Provide onsite support to CSOs for IT support and digital security issues. • Train existing IT human resource in various aspects of IT support and digital security.	• Create a pool of IT human resource from the existing IT professionals in civil society to support the entire sector. • Pool the financial resources and find funding for a dedicated IT resource team to support the entire civil society sector.
3	Even though over 75% of the respondents have attended digital security training, there is limited adherence to digital security best practices.	• Conduct a review of IT resources CSOs are currently using and support them to acquire, install and configure the basic requirements such as software licences, BIOS passwords, remote wipe for mobile devices, etc. • Conduct regular user training on various aspects of digital security.	• Create minimum standards for equipment, communication, network requirements and configurations and review adherence to these standards.

	Key Finding	Recommendations	
		Short Term	**Long Term**
4	63.8% of the respondents reported that either their organisations or them as individuals have been victims of digital security incidents with malware infections, online account hijacking and physical breaches being the most frequently reported incidents	• Train staff on digital security and create a security aware culture within organisations. • Procure and install anti-malware solutions on all user devices. • Reinforce physical security measures with well-designed contingency plans, data back up and data encryption to reduce exposure to the consequences of physical breaches.	• Establish a cyber emergency response team (CERT) to respond to incidents, to document them and continuously advice CSOs on emerging digital security trends.

2 Background to the Survey

Defenders Protection Initiative is a non-profit organisation formed with the aim of promoting and protecting human rights by strengthening the capacity of HRDs to mainstream security, safety and protection management in their work. Digital security is one of the security aspects that DPI addresses in its activities. It has been at the forefront of empowering and building the capacity of individual HRDs and organisations with the competence to manage their digital security through digital security assessments, training, emergency response, onsite technical support and the development of digital security strategies and plans.

This work is being done within an environment of increasing numbers and sophistication of digital security incidents and where the civil society and its other stakeholders such as beneficiaries and benefactors in Uganda has been specially targeted by various state and none state actors. Increasingly attacks on and the exposure of a single CSO poses a threat to the entire CSO ecosystem as there is a lot of information sharing and collaboration among CSOs.

CSOs have however endured inadequate resources both financial and human to deal with the various digital security threats. Whereas DPI's efforts have made in-roads in securing the digital assets of many CSOs, its efforts have been hindered by limited technical competence of its trainees and a high staff turnover at CSOs where capacity has been built.

DPI together with a number of CSOs with an interest in securing the information assets of civil society are spearheading the formation of a Digital Security Alliance. It is envisaged that this alliance will pool human, technical and financial resources within the civil society ecosystem to set standards, provide IT support, emergency response and secure the information assets of civil society.

DPI conducted a baseline survey on the digital security posture of civil society in Uganda. The findings of this survey are shared in this report.

3 Objectives of the Survey

The digital security survey was conducted to provide baseline information upon which the Digital Security Alliance (DSA) would identify areas where human resources and technical support would be provided to secure the information assets and infrastructure of civil society. The specific objectives of the survey were:

1. To establish the existence of and compliance to a policy framework that governs IT, digital security and incidence response within CSOs.
2. To establish the availability of human resources with IT competences and the level of digital security training within the organisations and the factors hindering the acquisition of such human resources.
3. To establish if the organisations maintain an inventory of their information and digital assets, resources and infrastructure, how these are accessed and shared within the organisations and other stakeholders.
4. To establish the existence of basic digital security measures implemented within CSOs
5. To understand the nature of the most common digital security incidents affecting CSOs and how CSOs have been responding to these incidents.

The information gathered in this survey will help in mapping action plans for the alliance in building capacity, acquiring and sharing human resources, setting IT and digital security standards and mobilising resources for the wider use of civil society to acquire the appropriate tools for bridging the digital gap within civil society, empowering it and protecting its digital security.

3.1 Methodology

DPI designed a questionnaire based on the objectives of the study. The questionnaire design targeted chief executives or heads of operations at HRD organisations on one hand or heads of IT in these organisations. The questionnaire was sent to all of seven hundred (700) HRDs that have either collaborated or been the beneficiaries of DPI's services in either digital or physical security and other human rights related work. The questionnaires were administered using Google Forms and responses were received using the same platform. Of the 700 questionnaires issued, only forty-five (45) responses were received giving a response rate of 6.43 percent.

The responses were then exported to comma-separated value (CSV) files where the responses were coded and prepared for analysis. Tables and cross-tabulations were generated and correlation analysis conducted using R-project to draw findings for the report.

4 Survey Findings

The survey sought to obtain information on IT and digital security governance within CSOs, their digital security practices and to review the digital security incidents that have occurred in these organisations and their response

4.1 Governance

IT is now a major driver of innovation, operations and delivering services in any organisation. It also however poses a risk to organisations in the event of a digital security incident. The board of directors and executive level management of organisations must provide guidance and leadership on digital security within the organisations they lead.

This leadership is manifested through policy guidelines, procedures and allocating the appropriate resources (human and financial) for IT and digital security for the organisation.

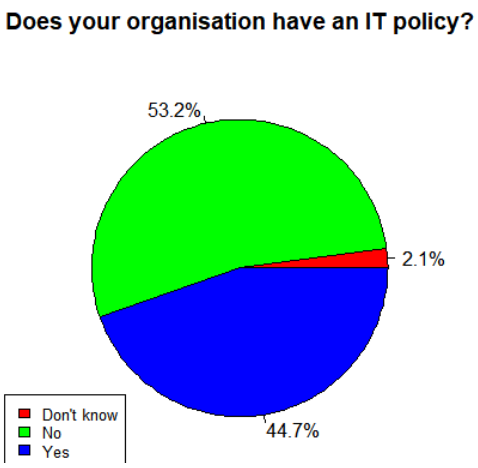

Figure 1: Organisations with IT Policy

In this survey, it was established that only 44.7% of the organisations that responded to this survey have an IT Policy, 90% of which address digital security issues. However, of the organisations that report that they have policy guidelines for their IT, 27.3% reported that the IT policies are not enforced across the entire organisation.

Of all the organisations surveyed, only 34% have ever assessed their digital security. Of the organisations that have an IT policy, only 38% have assessed their digital security and 25% of those without an IT Policy have assessed their digital security.

Less than half (46.8%) of the organisations employ a full-time IT staff and of the organisations with a full-time IT staff member, 81.8% reported that the IT staff member has attended digital security training. The leading reason for organisations not hiring an IT staff member is because there are inadequate financial resources to pay for the services of a full-time IT (69.6%). 21.7% of the organisations without a full-time IT reported that their IT support requirements do not justify hiring a full-time IT staff member. There is a higher likelihood that an organisation with an IT policy will hire a full-time IT (72.7%) as opposed to one without an IT policy (20%).

It is evident from the foregoing findings that executive level engagement in digital security issues within CSOs is limited. There is little policy guidance given to the organisations by their leaders and even where a policy exists, only one third of the organisations with an IT policy have assessed their digital security with the view of identifying risks, mitigating them and drawing contingency plans if there is a digital security incident. This makes these organisations very susceptible to digital security incidents as they are ill-prepared to defend themselves or to face them when they occur.

CSOs are also ill-equipped in terms of financial and human resources to deal with digital security. As the findings show, less than half of them have the human capital to provide IT support services including digital security support and inadequate financial support is most often cited as the reason for this.

4.2 Digital Security Practices

The policy guidelines of an organisation provide a framework within which practices and procedures are implemented within an organisation. In the case of digital security, all related policies guide the practices of the organisation and its staff members on how to ensure the security of the organisation's digital assets and respond to incidents that affect them. Such practices and procedures include management of access to physical and information assets and contingency plans.

This study found that 78.7% of the respondents have attended digital security training. This is an indication that there has been an effort within civil society to sensitise its members about digital security. This training's effectiveness then needs to be measured against the implementation of digital security practices. It is already evident from the previous section that the recommendation that the organisations should assess their digital security posture and make IT policies has not been overly implemented by a large proportion of the CSOs. The table below shows adherence to other recommendations of the digital security trainings.

Table 1: Adherence to Digital Training Recommendations

Recommended Practice	Adherence
Use licensed and updated operating system and application software	68%
Use supported operating system	93.4%
Require authentication to access network resources	74.5%
Use separate accounts on shared computers	78.9%
Change passwords at least 3 times a year	48.9%
Use 2 factor authentication	48.9%
Use different passwords for different services	80.9%

Recommended Practice	Adherence
Lock smart devices with a PIN or Password	74.5
Uses and updates anti-virus solution	87.2%
Maintains an inventory of all devices (PCs, smart devices, printers, routers, etc)	63.8%
Protect PC BIOS with a password	27.7%
Have remote wipe enabled on mobile devices	76.6%
Encrypts at least one of digital devices (PC or smart device)	48.9%
Maintains an inventory of data	38.3%
Backs up data	68.1%
Backs up data at least once a month	75%
Backs up data at least once a week	44.4%

Adherence to the recommendations of various digital security trainings for civil society is mostly a mixed bag as the table above shows.

It is evident that data management is poor within CSOs with only 38.3% of the organisations and individuals maintaining an inventory of the data and only 44.4% maintaining a weekly back up of the data. Only 48.9% of the respondents drawn from civil society encrypt data on at least one of the devices they own. More to that, a paltry 27.7% of the respondents protect the BIOS of their computer with a password. In light of the frequent break-ins on the premises of CSOs and theft of mobile devices such as laptops, mobile phones, tablets and iPads in Uganda, a lot of effort would be made to secure the data kept on these devices.

A large percentage (93.4%) of the respondents use supported operating systems. However, only 68% of them use licenced and updated operating systems and application software. Whereas 87.2% of them use and update their anti-virus solution, the fact that 3 in 10 of the respondents either do not use properly licenced software or do not patch it is a major vulnerability to the digital assets of CSOs. There is a lot of unlicensed software in Uganda sold at very low prices compared to the price of a valid software licence. Organisations with limited resources often opt to procure invalid software licences from the Uganda market. This predisposes them to the risks associated with invalid licences such as the vulnerabilities of unpatched software which are exploited by hackers to break into computer systems.

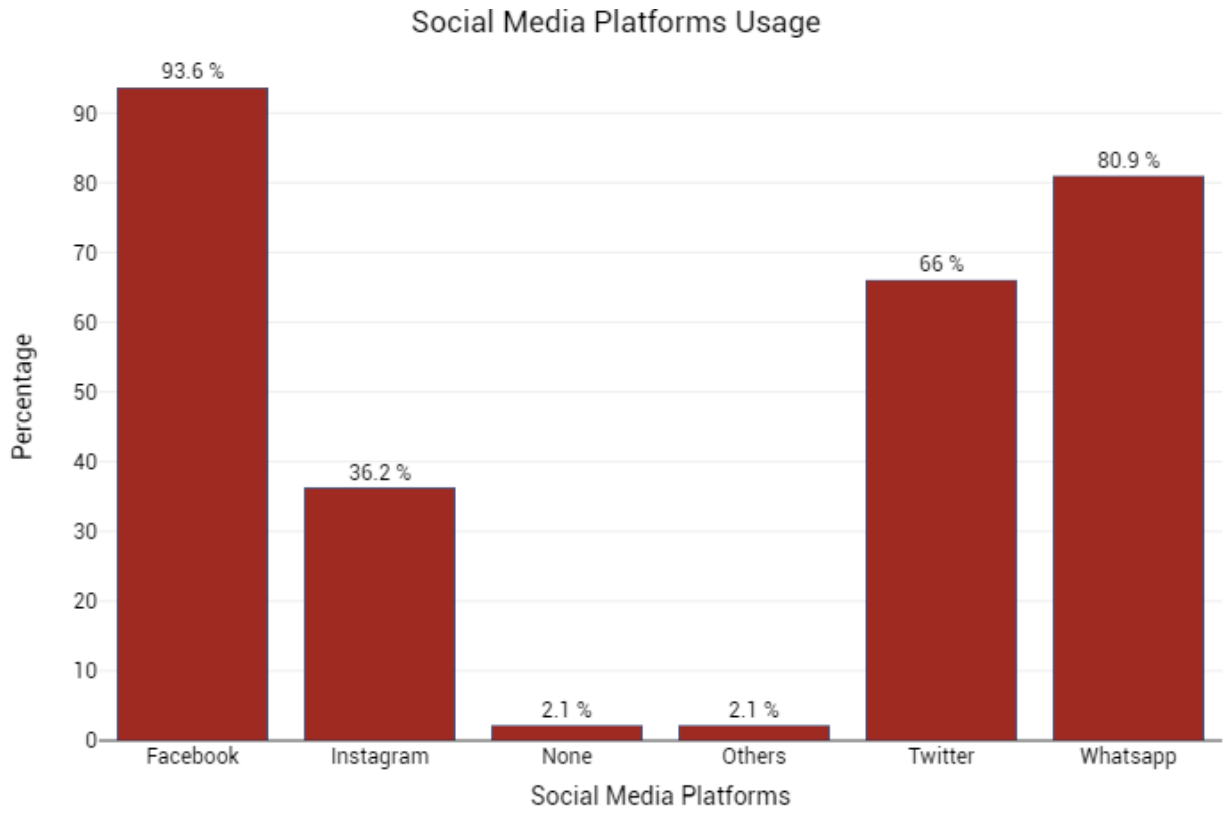

Figure 2: Usage of Social Media Platforms

This study also revealed that nearly all respondents (97.9%) are regular users of social media platforms such as Facebook, Twitter, Instagram, Whatsapp and others. 36.2% of them reported that never log out of their social media accounts on at least one of their devices. Less than half (48.9%) of them use multi-factor authentication on important accounts such as email and social media accounts and the same proportion of the respondents change their passwords at least 3 times a year.

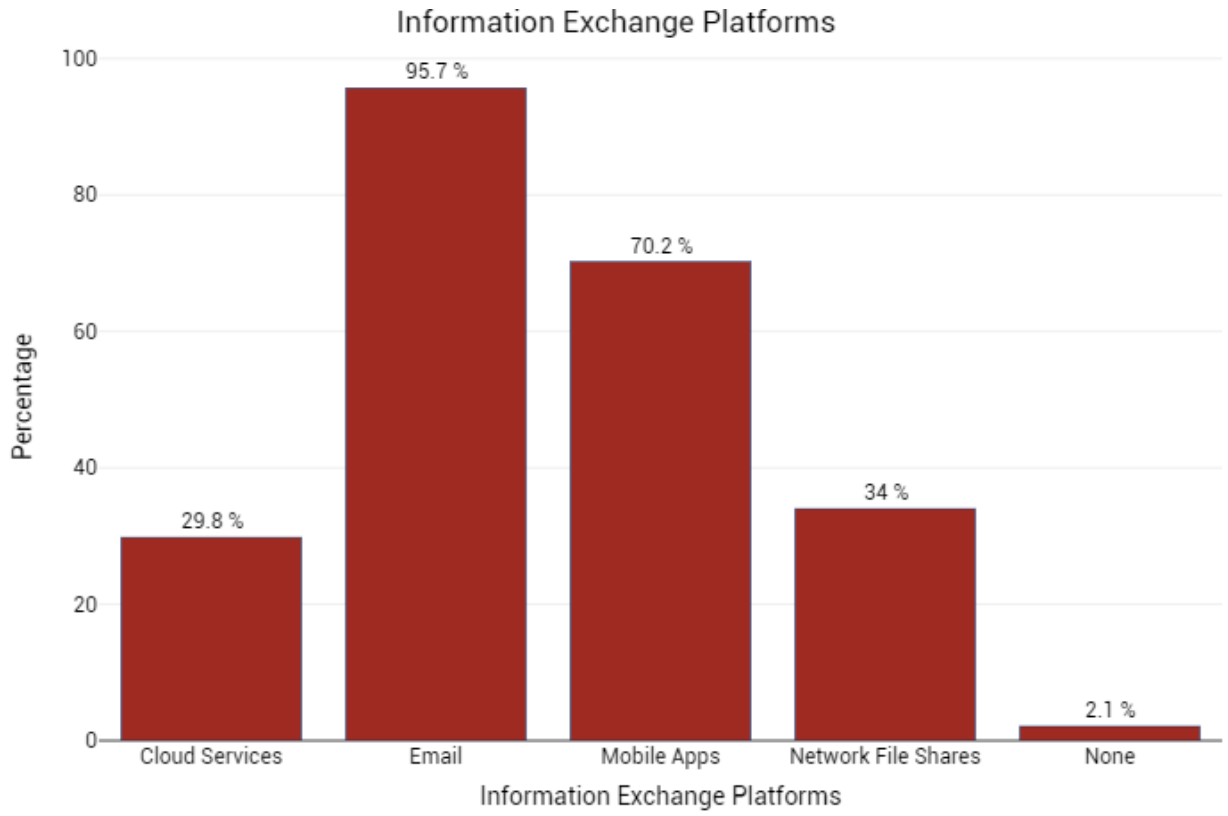

Figure 3: Usage of Information Exchange Platforms

It also revealed that most of the respondents (95.7%) use email as one of the methods for exchanging information while 70.2% of them use social media mobile apps such as Whatsapp and Facebook Messenger.

The survey clearly shows that many of the respondents use their mobile devices to communicate and exchange information many times using social media platforms. However, their practices put the information insecure especially in the event of loss/theft of these devices.

4.3 Incidences and Incidence Management

Civil society like any other sector in Uganda and in the world, has been the victim of digital security incidents. While we have noted in earlier findings that a lot of effort has been made to train CSOs in digital security, civil society continues to be a victim of attacks on its digital assets. 63.8% of the respondents reported that they have individually been victims of digital security incidents or the organisations they belong to have been victims of attacks while 27.7% reported that neither themselves or the organisations they belong to have been victims to attacks.

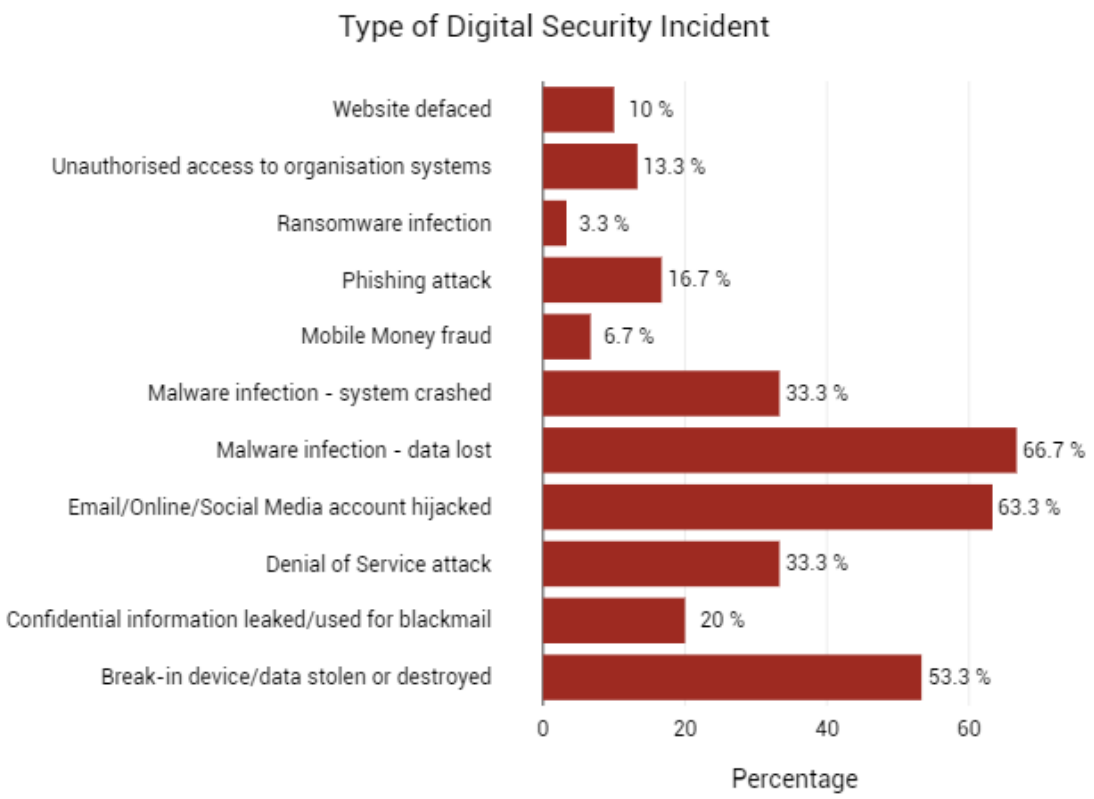

Figure 4: Digital Security Incidents

Of the respondents that reported that either their organisation or the individual respondents had been a victim of a digital security incident, 67% reported that they had been a victim of malware that resulted in the loss of data. They were closely followed by 63% who reported that either their email, social media or other online account had been hijacked. And over half (53%) reported that they their devices were destroyed, lost or data stolen as a consequence of a physical break-in on premises of their organisation or home. Other often reported incidents were denial of service attacks on organisation systems (33%), systems corrupted/crashed because of a malware infection (33%), confidential information leaked or used to blackmail an individual or organisation (20%) and phishing attacks (17%).

Data loss due to malware infections is common place in Uganda. Most of it is spread through USB drives and in some cases by email and over the internet. However, the incidence of accounts being hijacked is worryingly high and exposes a lot of the CSOs' vital information. It also makes many of the stakeholders in civil society including beneficiaries and benefactor's potential victims of phishing attacks. The fact that over half of the respondents also reported loss of data due to physical break-ins also makes their accounts susceptible to hijack. With less than half of the respondents using multi-factor authentication and the same proportion changing their passwords regularly, this may also explain

the high occurrence of account hijacks and data leaks and blackmail experienced by the respondents and the organisations they belong to.

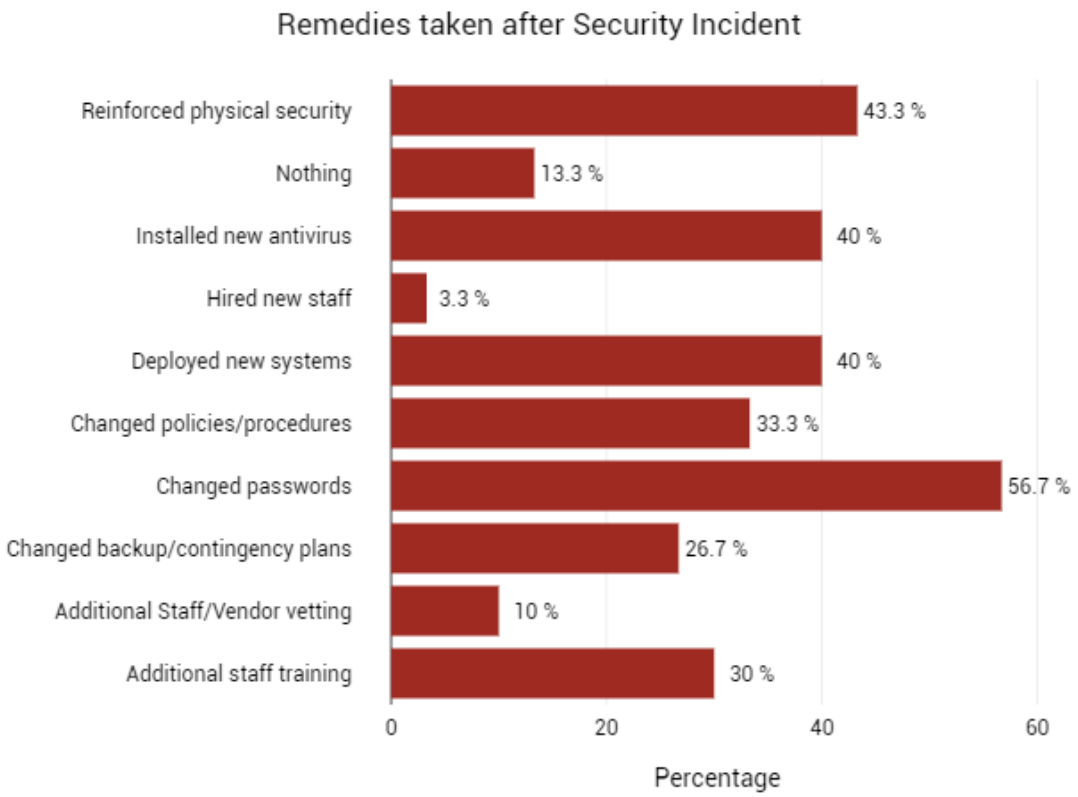

Figure 5: Remedies to Digital Security Incidents

In the aftermath of these security incidents, respondents report that their organisations mostly resorted to technical solutions to prevent re-occurrence of these events such as changing passwords (57%), deploying new (and may be presumably more secure) systems (40%) and installing new anti-virus solutions (40%).

Only 30% reported that the organisations conducted additional staff training, 33% reported that the organisational policies and procedures were changed and 27% reported that contingency and data backup plans were changed. 43% of the respondents said that physical security was reinforced – an indication of how much CSOs have been the victims of burglaries and break-ins in Uganda.

It is evident that CSOs are more likely to resort to technical means of securing their digital assets as opposed to training their staff on how to secure them. The current trends and this is shown by the high incidence of account hijacks among respondents, are that many attackers are taking advantage of human weaknesses to attack systems. This needs to be addressed through more rigorous and frequent staff training.

5 Recommendations and Way Forward

Civil society organisations collaborate over many causes and projects, often exchanging and sharing a lot of information on such issues and governance, property rights, human rights, education, health, etc. However, CSOs have different security management capacities and disparate access to financial and human resources to manage their digital security. However, a breach into the systems of one of the CSOs or their employees poses a threat to the entire civil society as it could be the gateway to a lot of the information CSOs share and the start of phishing and spear-phishing attacks targeting civil society, its beneficiaries and benefactors. It is therefore imperative that strategies are drawn to protect the entire sector from digital security incidents.

Defenders Protection Initiative (DPI) has been at the forefront of building the capacity of human rights defenders (HRDs) and civil society in general to build their physical and digital security mechanisms. It has conducted various training sessions, conducted security assessments, supported organisations to create policies, provided emergency responses and provided security tools such as anti-malware solutions. This though, is still short of securing the digital assets of the civil society sector as some of the challenges that face CSOs require a change in the organisational culture and a concerted effort by the civil society sector.

Securing the civil society sector requires that every player in the sector is secure irrespective of their size and access to resources. This requires a collaborative effort where CSOs pool the human resources available to them. DPI already has a team of well trained and skilled IT professionals that can serve as the core to the digital security infrastructure of CSOs. This team can build the capacity of other IT professionals in the sector from the half of the CSOs that employ full-time IT professionals. This human resource should then be made available to all CSOs to provide IT support and digital security to the sector. These skills should be further enhanced by obtaining technical support from security firms in the private sector and from organisations that specialise in digital security for civil society and human rights defenders. This collaborative effort should be formalised into an alliance with a memorandum of understanding among participating organisations that sets out the nature of their relationship, the financing of the collaboration and the terms and conditions by which IT staff shall be shared.

The alliance should set minimum standards to be met by all its members. These standards should include policies, equipment and infrastructure, network and communications protocols and configurations. The alliance should also institute review and enforcement mechanisms that are binding on members. Financing should be sought to support CSOs with inadequate financial resources to meet these minimum requirements.

The alliance should institute a cyber emergency response team (CERT) or work with another partner to have a CERT available to CSOs. This team will provide effective response to digital security incidents and should also document all incidents affecting the sector with the view of analysing trends and providing up-to-date advice on how CSOs should address emerging threats.

Donors and benefactors of CSOs should be encouraged to factor IT requirements and digital security into funding for programmes and projects. As has been highlighted before, digital security incidents for CSOs also create exposure to the donors as well.