SECURING Civil Society

Exploration of the relationship between civil society organisations and security policies

Research report by

GEM BARRETT

as part of the

Security Policy Generator project

APRIL 2019

Table of Contents

Introduction

Project overview

In October 2018 I undertook a project with the aim of helping civil society organisations (CSOs) to better defend themselves against attacks. Security policies enable CSOs to equip themselves with procedural knowledge and everyday processes that can secure their information assets and the safety of their staff, as well as the privacy of those organisations and individuals with whom they work. These formalised rules cover security decisions on everything from email encryption to office access and are often the core of an organisation's security plan.

While seeking a balance between cost, time and quality, organisations sometimes find themselves having to implement a copy-and-paste security policy that doesn't suit their needs or engage their staff and is, ultimately, unenforceable. Such a situation is brought about through pressure from a range of sources, including partners, funders, or a lack of resources. Though unintentional, this can lead to a false sense of security and risks being taken without the proper information.

Some CSOs take an informal or trust-based approach to organisational security, whether through necessity (e.g. lack of security budget) or preference (e.g. staying nimble). With all of these scenarios in mind, an array of issues around security policies can be identified. It is not the goal of this project to solve all of those issues. However, the research has been planned to ensure that the interview questions are focused yet flexible, and that the participants represent a diverse range of environments and viewpoints.

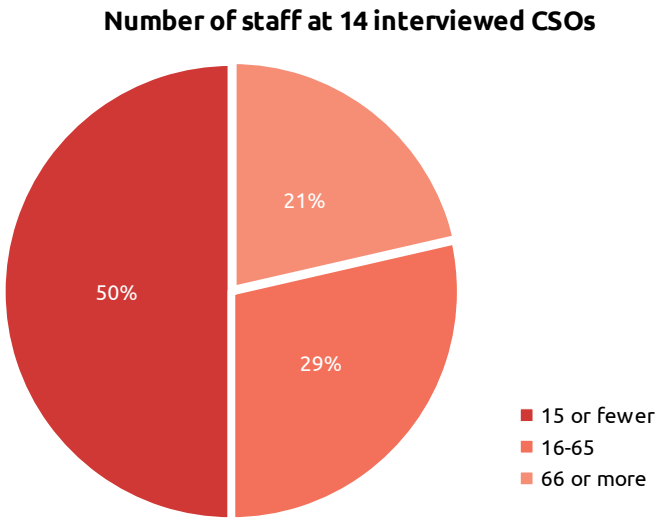
The end goal of the Security Policy Generator project is to build a free, easy-to-use online tool for creating organisational security policies that are relevant, clear and supportable. In addition to providing a custom security policy, the Security Policy Generator will also supply guidance for supporting the policy and an appendix of items for future review. It is envisioned as a supplementary resource to organisations' other security efforts, and so the purpose of this research is twofold. In addition to informing the tool's development, this research will also share insights with the civil society community that can be used to improve our collective resilience.

Research context

As part of the proposal for this project, I identified four main areas of investigation on which to focus during this interview-based research stage;

- The barriers to security policy implementation
- What works and what doesn't when it comes to security policy implementation
- The workarounds and alternative methods in use
- Unique challenges faced in oppressive environments

With these areas in mind, I designed a series of questions for the interviewees, and the ones used in this report can be found in the appendix. To be flexible to varying contexts the questions were arranged such that I could "mix and match" them as the interview progressed and choose the most relevant questions based on the interviewees' responses. The questions were written with room for the interviewee to expand upon beyond a "yes/no" answer, thus facilitating a more exploratory interview. As a result, some of the questions received fewer responses than others and so, for clarity, the number of respondents is shown alongside each question in the appendix.



I sent an outreach email to the Open Technology Fund and Organisational Security mailing lists appealing for interviewees. Although the topic of security policies is sensitive, the response was good and resulted in interviews with 16 people representing 14 organisations. The focus of the mailing lists I had reached out to meant the organisations largely work on internet freedom, digital rights and similar civil society issues; throughout the

rest of this report they will be collectively referred to as CSOs (civil society organisations). Over the course of five weeks, the interviews took place face-to-face, via PGP email and across messaging platforms such as Signal, Jitsi and Google Hangout. Interviewees were scattered across several timezones, with 40% of them[1] having a regional focus while the majority had a broad international scope. On average, the CSOs represented in this research employed 50 members of staff in a mixture of full and part-time roles. Some of these organisations also provided organisational security consultancy to other CSOs, adding another perspective to their responses. To further include a range of viewpoints, I interviewed staff in a variety of roles and aimed to go beyond the white male experience.

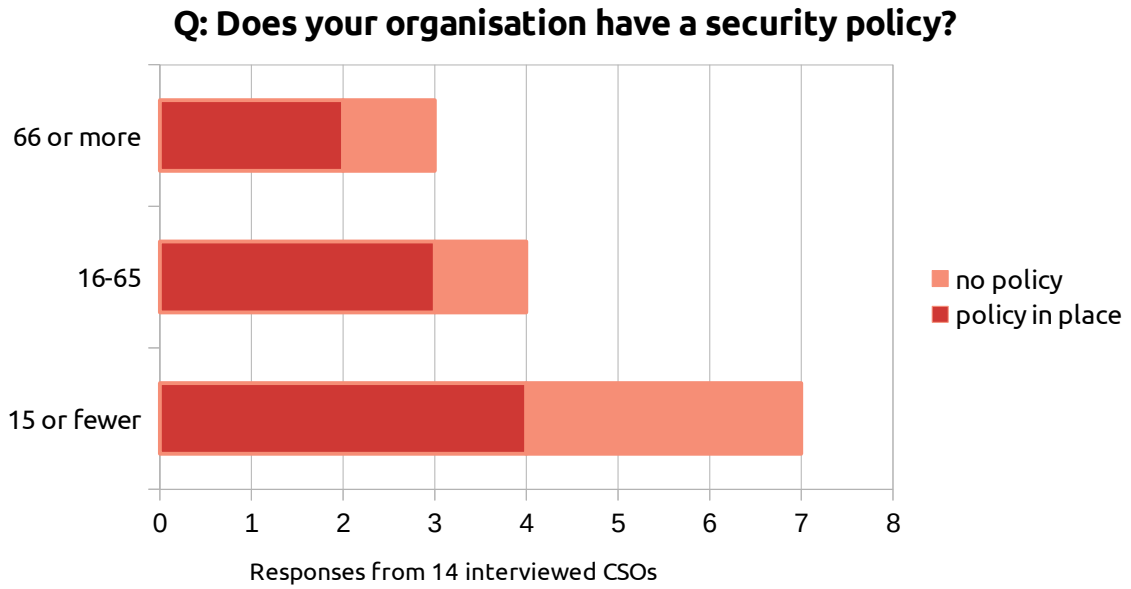
1 Of the 14 organisations interviewed, 4 focus on regional or country-specific focus and 10 on global issues

Security Policy development

Understanding the context[2]

Understanding the relationship CSOs have with security policies begins with examining the development process and so this section will look at the procedures and resources involved, as well as the obstacles and challenges. When designing the questions, it was clear that the interviews all had to start with one question: does their organisation have a formal[3] security policy?

Of the 14 CSOs that I interviewed, 9 said they had a security policy which was either currently in place, or in-progress. Breaking that down to see the relation to organisation size reveals that the medium and large CSOs (16+ staff) were more likely to have a policy in place or in-progress than their counterparts with fewer than 16 staff. Although the smaller CSOs were less likely to have a security policy, over half of those interviewed have one currently in place.



2 Questions used in this section are listed in the appendix as questions *1, 1a, 1b and 1c*
3 By "formal" I mean a set of security rules that are written down and accessible to staff

So why do organisations consider having a security policy in the first place? Interviewees agreed that a security policy helps get everyone on the same page, explains the importance and sets a baseline level of security. Formalising security rules, defining procedures for new hires – often security policy development can simply be writing down all the security practices you do without thinking.

I found that while 22% of those interviewed had had a policy implemented since their launch, an equal number had been prompted by expansion or gaining independence from a larger organisation. A frequent point made in the interviews was that a policy is weak without the support of other security measures. It follows then that the remaining 56% said they had implemented a security policy as part of a larger security prioritisation process. For instance, following a security audit, responding to a funder requirement or hiring security staff.

For nearly 90% of the CSOs interviewed, the development of the security policy had been done by one or more employees, while 22%[4] said they had previously hired an external security consultant. Of those who developed it internally, all had kept the policy's writer in charge of maintaining it – irrespective of the writer being a single IT person, or a team of eight.

The policy building process[5]

The process of developing the security policy focused heavily on collaboration. This came in the form of stakeholder discussions and frequent reviews by the technology team, management and board. In addition, interviewees shared that informal meetings, skill shares and staff retreats all provide opportunities for these feedback sessions. Online security guides such as Security In A Box and other organisations' policies have also proven useful resources for first-time policy writers.

The interviews also revealed that smaller organisations who develop security policies for other CSOs commonly 'dogfood'[6] new changes to their policies. Interviewees were asked about their policy development process for other CSOs, and while the common response focused on threat evalua-

4 One interviewed CSO had had security policies both by an external consultant and developed by internal staff
5 Questions used in this section are listed in the appendix as questions *2, 2a, 2b and 2c*
6 A term used in the technology sector to describe testing out your own products by using it in everyday life

tion, 71% also said that their own security policy forms the base template for their clients' policies. In addition, they found that modularising their own security policy not only makes it easier to use in creating policies for other CSOs, it helps staff to quickly find the relevant content for their scenario, making incident response more efficient.

Threat assessment[7]

Most, but not all, interviewees mentioned working from a risk assessment to build their policy based on mitigating the known risks. They said that their threat evaluation process included some or all of the following aspects:

- Questions to the team: interviewing (in groups or individually) the critical and senior people in order to understand their work context.
- Policy support: identifying focus areas and the training, tools and capacity needed to implement and enforce the security policy.
- Technical analysis: performing network and device analysis, and also determining type and sensitivity of data.

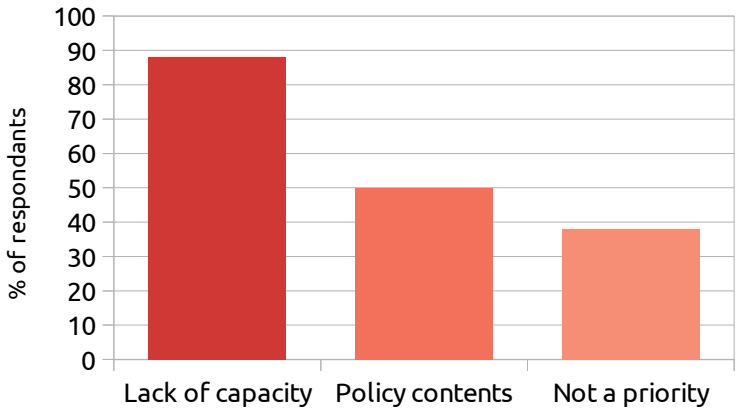
One highly-recommended threat evaluation resource was SAFETAG; a security audit framework created by Internews. The information gathered from this threat modelling process can support the policy in addressing threats individually using relevant scenarios. One interviewee did stress the need to keep the big picture in mind, advocating for policies which include guidance on applicable rules through a decision tree. Checklists were repeatedly brought up as a good way to help staff incorporate the new security measures into their current processes. Strengthening these with several solutions rather than changing habits should be the focus, according to one interviewee. Collaborating on the security policy itself also goes a long way towards creating buy-in. Having a wide range of perspectives is not only useful for designing the policy; staff are more invested in its successful implementation if they have been involved in its construction.

7 Questions used in this section are listed in the appendix as *Q2 and Q2c*

Barriers and challenges[8]

Interviewees both with and without an implemented security policy were asked for their views on the issues around security policies. Specifically, the obstacles to developing a policy and the reasons for choosing not to have one, as well as common problems with the process. Although the financial pressures of neglected security budgets were mentioned as a barrier to implementation, most interviewees pointed to a lack of capacity, rather than funds, as a major obstacle. The amount of time required to develop, implement and maintain a security policy makes it hard to prioritise, especially for small CSOs. Almost 40% of the interviewees said that, for them, a security policy is intentionally not a priority, either because it would make them less flexible or because they are too small to need one. An equal number of respondents mentioned the use of copy-and-paste policies found online, but these template policies are usually geared towards corporate environments and pose the problem of trying to fit a generic policy to a complex and sensitive working context. They can, however, be useful for deciding on policy contents – something that 50% of respondents have had trouble with. Challenges include accessing relevant content, staff disagreements over best practices, keeping it to a manageable length and updating it in a changing environment.

Q: What do you see as the biggest obstacles to implementing a policy?



Most popular responses from 8 interviewees

The interviews also revealed that sometimes the obstacle comes down to the CSO not viewing security as a priority. In some cases, interviewees confirmed that CSOs will create a security policy for fear of exclusion by funders and international partners, but then find that they either cannot or will not enforce it. One interviewee also reported that colleagues had raised concerns about the

8 Questions used in this section are listed in the appendix as Q*3, Q3a and Q10*

slowing of productivity due to the additional security processes. For some CSOs, only a major prompt (such as new management or a security breach) was able to demonstrate the importance of a security policy.

Speaking to five interviewees about their experiences creating security policies for other CSOs, I asked them about the problems they face. They identified two main challenges.

Although the process involves changing structures that rely on insecure practices, some staff would prefer to stick with the status quo. This can make it harder to create a thorough security policy as some elements may be incompatible with a staff member's work environment. Difficulties in researching the unusual software and old hardware in use are exacerbated when staff insist on using tools that are incompatible with modern security measures. For example, staff may prefer to use their old, insecure computer out of convenience or ego rather than be trained in a new system. However, this requires the threat evaluation to consider how that computer interacts with the CSO's sensitive assets and secure systems.

Interviewees also identified that CSO staff frequently have a fear of getting something wrong and this causes the unknown elements, particularly in technical tools, to make small problems seem insurmountable. For example, issues with PGP can seem too intimidating to fix, especially when unfamiliar with the terminology and therefore limited in search terms that can be used to find the solution online.

Security Policy implementation

Introducing the security policy[9]

The process of implementing a policy has been a generally positive experience for all the interviewees, in part thanks to many of them having security-conscious staff. One interviewee did note, however, that in future they would prefer to explain the policy in a group situation, rather than an individual basis as this would help with building a common understanding and contribute to team spirit. I discovered that announcement of the security policy to staff tended to be delivered by email briefing, but accompanying leaflets explaining the policy are an idea being considered by some. In the case of new staff, they are introduced to the security policy as part of the onboarding process, with most of the 8 interviewees telling me that a policy review forms part of a broader introduction to other guidelines within a staff handbook or documents.

Staff reactions to the introduction of a security policy were generally positive, according to those interviewed. Clear benefits, positive engagement and an increase in threat level had all factored into encouraging staff adoption of the policy. However, one interviewee told me that a lack of staff engagement during development had led to their organisation having a partially-enforced policy. This situation can result in staff taking risks based on the expectation that others are adhering to the policy, only to later discover that they are less safe than they thought and have been left vulnerable to unexpected threats.

There were many initial challenges for 6 of the interviewed CSOs when they implemented their security policies. For instance:

- Having so many rules makes it hard to remember them all, and so you have to remind people.
- It can be difficult to discuss enforcement and how to handle violations, with HR department.
- Staff who are resistant to change, whether through fear, habit or ego, can disrupt the implementation of a policy.

9 Questions used in this section are listed in the appendix as *Q4, Q4a, Q4b, Q4c, Q4d, Q5 and Q5c*

- Moving away from proprietary software requires a lot of time spent researching open source alternatives.

- Designing the policy to be accessible to all levels of staff knowledge and ability, without overwhelming the non-technical people or patronising those who are technical.

- Persuading staff to complete set-up processes in a timely manner to avoid gaps in the implementation of the policy.

On the topic of remote staff, interviewees agreed that it can be challenging to implement a policy if it doesn't factor in their different working environment. With two-thirds of the interviewees working alongside remote colleagues, it is clear that creating a policy that includes remote staff members' needs is very important. After all, even if you only have one remote staff member then you're a remote organisation and that brings additional security considerations. Of course, this is simpler to manage if your organisation has had a policy since its launch, like two of the interviewed CSOs. For others, the average age of their security policy ranged from a few months to 5 years, with the average being 2 years.

Integrating the policy[10]

Having security-conscious staff who understand the importance of keeping the CSO secure means that, in some instances, the staff members already follow similar security practices in their personal life, making it easier to adopt them at work too. However, the relationship between work and personal comes to the fore when considering staff discomfort with having a "work profile" [11] installed on their personal smartphones. While it is an option to carry two phones rather than one with two profiles, sometimes it is neither financially possible nor convenient, and so some organisations are giving the choice to their staff instead. Others make the choice between complete separation or side-by-side profiles on their staff members' behalf, with most finding that having work profiles on staff personal devices is more suited to their context than the alternative.

10 Questions used in this section are listed in the appendix as *Q5a, Q5b and Q6a*
11 This refers to the installation of an employer-managed profile on a smartphone, with the aim of providing convenient and remotely-controlled access to work calendars, contacts, emails, etc.

Despite the risks, some people will still choose to ignore security measures, so I asked interviewees which aspects of their security guidelines (in policy or not) they found the most challenging to implement across the organisation or their own workflow. They told me that staff are hesitant to use new tools for fear of getting stuck or breaking them, which could be part of the reason for the slow speed in completing set up procedures too. It's certainly likely to be at the root of causing older staff to resist changing their processes, which can result in their colleagues trusting them less often with sensitive information. Issues such as sending sensitive documents and fixing platform-specific security problems are made much harder when staff use feature phones or an out-of-date insecure operating system for work-related tasks. This can also have an impact on the organisations' position on work profiles or work devices, in addition to incompatibility with required software and specifically-developed security measures.

Many HR policies include rules regarding the personal use of in-office internet, and these can also be seen as security measures. This is a more pertinent issue in countries that have limited bandwidth. Interviewees also reported that it had been difficult to incorporate travel security practices (e.g. enabling travel mode in password managers) into their workflow. Difficulties with enforcing two-factor authentication and password security were noted, as interviewees found that it was easy for staff to work around the rules.

Support and sustainability[12]

When asked further about their enforcement and accountability plan, three types of response stood out. First there are the CSOs that rely on a trust-based approach to enforcement, with staff supported in reporting their own mistakes. Linked to this is the reinforcement from other staff, for example, IT staff reiterating password security during technology training sessions. Interviewees also told me that they've found monthly refresher sessions help to remind staff of the processes. Holding each other accountable is also part of a trust-based approach, and tactics such as refusing to open unencrypted emails assist with this. A different approach to enforcement can be seen with those CSOs who choose to use more technology, such as password managers, to automate most of the security monitoring. For example, this makes it easier to ensure that all staff have two-factor authentication enabled, or that their passwords meet the defined requirements. Meanwhile, some

12 Questions used in this section are listed in the appendix as *Q6, Q6b, Q7, Q7a, Q7b*

organisations have linked their security guidelines very tightly to their IT policy and so it is enforced in the same way. Staff availability also causes issues for enforcement as some interviewees explained that CSOs are hesitant to punish employees for non-compliance due to the shortage of qualified staff. Along with the aforementioned issue of developing procedures with other departments, this can lead to toothless accountability plans with no hope of dealing with security violations.

Interviewees told me that their CSOs have a designated security person or team; someone who they can approach with questions about their security policy. Team size ranged from 1 to 7, with many favoring a streamlined 1 or 2-person security department. For those with a security maintenance plan, annual review-based changes are as popular as updating when new threats or information appear. Changes of government, evolving world situation and a raised profile were all cited as triggers for security policy updates. The ease of updating the policy itself and redistributing it to staff depends on which format it's in. Organisations which use GitHub repositories, or Google Docs are able to create a "live" document with the ability to track changes and facilitate a more collaborative maintenance process. Other organisations avoid relying on the security of another service, and prefer instead to create an encrypted PDF document or physical printed copy.

Alternative practices[13]

Turning to the interviewed organisations who don't use a security policy, I next wanted to look into the alternative methods in use. When it comes to managing their security, 50% of the respondents said that they use a trust model which relies on the staff being security-conscious without guidance. Meanwhile, the other 50% use informal guidelines which are often written down but spread across multiple documents, or may take the form of verbally-agreed rules and processes (for example, physical safety check-ins while travelling). Some of those I interviewed said that they expected staff to ignore formal guides as they have an aversion to official documents. For these reasons, loose communication of the guidance, for instance through checklists, can be useful to overcome that. Onboarding training and staff walkthroughs are also used to support staff in understanding the security processes.

13 Questions used in this section are listed in the appendix as *Q8, Q8a and Q8b*

Enforcement through technology can also be applied to Informal guidelines, for example through Apple software management on Mac and similar tools for upgrade alerts. Other enforcement methods suggested by interviewees include the assignment of individual security measures to specific staff within the organisation, in a way designating them as informal security officers. In addition, staff that don't want to change their habits face having their access to sensitive information restricted in some CSOs.

Security policy contents[14]

I asked 8 of the interviewees about the contents of their policy, whether formal or informal, in order to shed some light on the common elements. Their answers identified 8 content areas.

1. Support:
    - Who the policy applies to. For example, are contractors included or do they work under another policy?
    - Which data is important to protect from loss or unauthorised access. For example, emails, financial documentation and HR files.
    - Information architecture can explain the type and sensitivity of the data which needs protecting. Combined with a traffic light system, this can help staff identify the security level of the data they handle.
    - User roles and responsibilities may be explicitly set out in order to ensure everyone knows the part they play in keeping the CSO secure.
2. Device security
    - Work profiles are a divisive topic as installing a work account on a personal device, such as a phone, is viewed as invasive by some but hailed by others who enjoy the convenience of carrying one device.

14 Question used in this section is listed in the appendix as *Q9*

- Hardware policy can set out the procedures for issuing and destroying computers, phones and other devices.

- Details of any regular security checks. These can help to fix any knowledge gaps the staff may have, perform any outstanding software updates, and generally make sure the device is up to requirements.

- Organisations may pay for a VPN[15] service, and designing guidance for this tool can mean that staff know when it's necessary to use it, the risks and any restrictions on its use.

- Mobile hygiene is an increasingly important topic as so much of our data is held in our phones nowadays. CSOs include this section to educate staff on securing their mobile phones from threats like location tracking, malicious apps and unsolicited Bluetooth connections.

3. Communication security:

    - PGP email guidance can explain how and when it is necessary for staff to encrypt their email, and when it is not. While many organisations help staff with setting up their key, how often it is used is dependent on the sensitivity of the data being communicated.

    - Signal, Whatsapp and Wire are all messaging services which offer some level of encryption and there tends to be a preference towards one in each organisation, although some will leave this choice to individual staff. If prescribing a specific service then advising staff on the use of features like disappearing messages can be very useful.

    - In some cases, organisations will also include access management in their security policy. For example, it can include rules on sharing information with those who use commercial, closed-source systems.

15 Virtual Private Network: a service used to anonymise and encrypt internet traffic

4. Account security:

    - Requiring staff to enable two-factor authentication on their work accounts is becoming standard procedure. In addition, organisations sometimes specify how staff should keep work and private accounts separated.

    - Phone passcodes and account passwords can be the first challenge for an attacker and so requiring staff to use unique, complex ones – and defining what that means – is often a priority.

5. Technical guidance:

    - Tool recommendations are a regular feature of security guidelines, whether they're in a policy or informally communicated, as it makes sense that some commonality is necessary for efficiency. For instance, some CSOs prefer staff to use Thunderbird for its integration with PGP.

    - Instructions to avoid certain services and apps may also be included, and the decision to ban specific tools can come down to security and/or ethical concerns, for example in the case of popular tools from problematic companies such as Google's G Suite, or Facebook's WhatsApp.

6. Data storage:

    - The security of any financial documentation is important, and even more so for CSOs working in countries that have repressive funding regulations. In that case, financial security rules governing how the data is stored and accessed can be beneficial.

    - The encryption of hard disk drives and other storage devices may be dealt with by the IT department in some CSOs, particularly if they provide the hardware already set-up. Where this isn't the case, it can be useful to advise staff on when and how to encrypt their drives.

- When automated data backups are not an option, staff are able to do it manually and setting down a process to follow could help with this. This may also include details of how often the backups should happen, and other settings.

- Purging data often requires more than simply hitting the "delete" button. Requiring staff to empty their computer's trash periodically or archive old emails are examples of rules that can be included here. This can also detail the deletion process for former staff accounts.

7. Travel policy:

    - Public WiFi in airports, cafes and hotels is a convenient facility but it is also insecure, so many organisations advise staff to use a VPN with their connection, or avoid it altogether and use a mobile personal hotspot instead.

    - In some cases there is a threat from 'shoulder-surfing'; a social engineering tactic whereby the malicious actor steals passwords by looking over the victim's shoulder. For this, CSOs sometimes set rules that go beyond the general advice of "be careful entering passwords in public".

    - When organisations believe their staff have a high likelihood of facing snooping border guards or thieves during their travel they generally provide advice on how to secure the work devices. This may include logging out of some or all accounts, or creating fake data in some of them.

8. Incident response:

    - Setting out processes for "what to do in the case of ___" is useful for providing staff with a quick guide to avoid confusion, for example in the wake of a confiscation, receiving a suspected phishing email, or having a tapped phone.

Additional considerations[16]

Once a policy is implemented, scenarios or threats become apparent which then need reviewing before inclusion into the next version. Elements like travel guidance are easy to forget until a staff member has to travel. CSOs may also find themselves with a security policy that doesn't consider their threat model. For instance, foreign authorities such as the NSA aren't relevant to all threat models and if all locally available email providers are insecure, then GMail may be the most secure option for some.

A closer threat to the organisation can be found in the "Always Listening" surveillance devices, both in the office and in the homes of staff. Devices like Amazon Echo, Google Home, smart TVs and internet-connected baby monitors have the ability to record, store and send audio of sensitive work conversations. While widely-acknowledged as a threat, whether through data harvest or data leak, none of the interviewees I spoke to had specific rules regarding this in their security policy. However, half said that they are likely to add it to their existing policy. In addition, 75% of them suggested existing security measures to deal with this threat, such as:

- excluding unnecessary work devices from the office or main internet network.
- leaving devices out of earshot during sensitive conversations.
- disabling Siri, Cortana and other assistants on work phones and laptops.

Capitalist surveillance by the likes of Google and Facebook has found its way into many products, making it hard to avoid them all - especially given the dearth of alternative options. Many of those I spoke to said they use Google's G Suite but advise staff not to place sensitive documents into Google Drive. For some, Google and Facebook are not relevant to their threat model and so they are comfortable with the risk. However, a few organisations I spoke to are beginning to move away from Google Hangouts towards an encrypted option such as Zoom. Interviewees also stated that their CSO's staff were trained on the insecure nature of most communications methods and 75% of them named Signal as a tool they recommend to staff. Understanding the threat and accepting the risk applies to Telegram and WhatsApp in particular; while one organisation bans them from use in work-related conversations, another encourages staff to use it for the end-to-end encryption.

16 Questions used in this section are listed in the appendix as *Q9a, Q9b, Q9c and Q9d*

The protection of staff working under aliases is not a topic that comes up often in relation to security policies, and is usually left ungoverned. Recently, management at a CSO were accused by former staff of misusing anonymity in order to cover up workplace abuses, showing that the use of pseudonyms is a factor to be considered when building a security policy. Although none of the organisations I spoke to about this had specific rules in their policy, many do have staff that use aliases and considerations have been made regarding their protection from exposure by external malicious actors. In addition, there has been a trend in recent years of harassing women and transgender staff online through their employers. While those who work on online harassment issues are keenly aware of the threat, more organisations outside of that work should be considering how they can secure the CSO and staff against harassment tactics by hiring consultants knowledgeable in these areas.

Conclusion

At the start of this project I set out to understand as many viewpoints, acknowledge as many threat models and identify as many solutions as possible. My key findings have been organised around the four research areas I specified at the start of the project: the barriers, the successes, the work-arounds and the edge cases.

64% of the organisations interviewed have a formal security policy.

Reasons for implementing a security policy included expansion and prioritisation of security, while 22% of interviewed CSOs have had a policy since launch. Nearly half of small (<15) CSOs do not have a security policy, with 38% giving their size and current flexibility as reasons for this.

88% of interviewees said capacity was a barrier to implementing a security policy

The time-consuming nature of creating, implementing and supporting a policy makes it hard to prioritise over project work. 50% also named policy contents as a barrier, as disagreements over best practices, the struggle to find relevant resources and creating a straightforward policy all present difficulties. Some turn to online copy-and-paste corporate policies in order to help with these aspects, only to find later that they are ill-fitting and unenforceable.

The process of developing a security policy focuses on threat evaluation, collaboration and modularisation.

Modularising a security policy means that CSOs are able to use their own policy as a baseline template for others. Creating staff buy-in can be done through encouraging their feedback and review of the policy during the development process. Checklists and decision trees also help to efficiently guide staff towards the appropriate security measure for their scenario.

While the introduction of security policies is generally met with approval by staff, the implementation of its measures can throw up some challenges.

Whether through ego or fear of breaking something, staff sometimes refuse to update their processes or technology and this can lead to security implications across the organisation. Similarly, ignoring password specifications, two-factor authentication guidelines and other security lapses can lead to colleagues taking more risks based on assumed compliance. Despite their line of work, CSO staff can at times be less concerned about privacy and more about slowed productivity caused by implementing a security policy.

When it comes to enforcement, there are organisations who rely on trust and self-reporting, while others use technology to monitor compliance.

Organisations successfully share their policies with staff across a range of platforms to suit their preference for ease of updating and redistribution. These updates can be due to changing political situations or part of a regular review schedule.

50% of those without a formal policy rely on a trust-based model to manage their security, while the other half use informal guidelines.

Of these, there was acceptance that some staff avoid official documents and formal guides, meaning that informal communication of the security measures is more effective for some. Checklists and staff walkthroughs are options that can help here.

Security guidelines usually fall into one of the 8 categories identified by interviewees: support, device, communication, account, technical guidance, data storage, travel and incident response

However, there are new threats which are harder to fit into a category. For instance, the “Always Listening” devices recording conversations or Google harvesting data from project files. New human-based security threats also exist, from online harassers externally to abusive management

internally. Ultimately though, the policy contents come down to what the organisation deems a threat at the time, preferably with an eye on the horizon.

One more thing

At the end of each interview, I asked participants whether they had anything else to add on the topic of security policies. Here are some of the points they raised:

- In some countries and languages, the word "policy" is linked negatively to politics and is not ideal for creating buy-in from staff – "rules" or "guidelines" are appropriate alternatives.
- Policies should take into account the relationship and boundaries with partner organisations.
- Security policies should explain its importance to help with staff buy-in.
- Asking staff about their daily processes for completing tasks will help with creating a policy that is easier to integrate into their workflow.
- Support is key to keeping a security policy effective, and not just a document no one reads.
- There will be violations of the security policy; it's best to try and preempt the inevitable ones.
- Personnel management and internal threats are sometimes excluded from policies, when they should be an important consideration.
- The best way to get value for money from a security policy is to keep it updated and accountable, otherwise it's a waste.
- A policy's requirements for support and maintenance should be matched by an appropriate budgeting of staff, money and time to meet the obligations, in order to prevent an unenforceable policy borne of over-commitment and insufficient budget.

Appendix

Interview questions

Responses to the following interview questions were used in the creation of this report. The number of respondents is shown alongside each question.

1. Does your organisation have a formal security policy? (respondents: 16)
    a. Do you know what prompted the creation of the policy? (9)
    b. Was it developed in-house or was an external security professional hired? (11)
    c. Does the person maintain the policy still? (8)
2. What was the process of developing the policy? (6)
    a. Were you or other staff asked for input? (5)
    b. Were there staff meetings to discuss what should go in it? (3)
    c. What is your process for creating security policies for other CSOs? (7)
3. What do you see as the biggest obstacle to implementing a formal security policy? (10)
    a. When helping other organisations to create a security policy, what's usually your biggest challenges? (5)
4. How did the rollout of the security policy go? (3)
    a. How was the policy announced to staff? (2)
    b. What was the initial reaction from staff? (3)
    c. How are new staff introduced to the policy? (8)
    d. What were the initial implementation challenges that you remember? (6)
5. Roughly how long has the policy been in place? (9)

a. Which aspects of the policy were the most challenging to implement across the organisation and/or in your own workflow? (7)

b. How well do you think staff have adapted to the policy? (4)

c. Do you have remote staff? How have they adapted to the policy? (6)

6. How is the policy enforced? (7)

   a. Are staff given work mobile phones or are work profiles installed on their personal phones? (4)

   b. Is there a security person on staff? (3)

7. What is the maintenance plan for the policy? (3)

   a. How often is the policy updated? (8)

   b. Is the policy readily available to staff? (5)

8. Without a security policy, how is security managed at your organisation? (5)

   a. How are the informal guidelines shared with staff? (3)

   b. How are your informal guidelines enforced? (3)

9. What sorts of things do your guidelines/policy cover? (8)

   a. Are there any edge cases that became apparent post-rollout? (3)

   b. Do you have security rules regarding "Always Listening" devices (such as Amazon Echo, Google Home, smart TVs, internet-connected baby monitors)? (4)

   c. Are there any rules regarding the use of Google or Facebook products for work? (4)

   d. Does your organisation make use of pseudonyms to protect staff identities? If so, are there any rules related to this in the security policy? (4)

10. Do you have anything else to add on the topic of security policies? (10)