CIVIL SOCIETY ORGANIZATIONS' CYBER RESILIENCE

LEAVING NO CIVIL SOCIETY ORGANIZATION BEHIND IN CYBER RESILIENCE

UNITED NATIONS UNIVERSITY
Institute in Macau

AUTHORS

Christy Un, Mamello Thinyane & Debora Christine

DISCLAIMER

This publication aims to provide accurate information regarding the subject matter covered. The views and opinions expressed in this publication are those of the authors. They do not purport to represent the official views and opinions of the United Nations University, the United Nations, or any associated organisations.

ACKNOWLEDGEMENTS

This work is supported by the Science and Technology Development Fund of Macau (FDCT) under Grant No. 0016/2019/A

CONTACT

Any questions or comments should be addressed to Mamello Thinyane, United Nations University, Casa Silva Mendes, Estrada do Engenheiro Trigo No. 4, Macau SAR
Email: mamello@unu.edu

SMART CITIZEN CYBER RESILIENCE PROJECT

This report is produced as part of the a project that aims to enhance the resilience of citizens in smart digital futures. It recognizes civil society stakeholders as significant actors in the co-production of national and global cyber resilience.

https://cs.unu.edu/smart-citizens-cyber-resilience

UNITED NATIONS UNIVERSITY

The United Nations University institute in Macau is a research institute at the intersections of information and communication technologies and international development. It conducts policy-relevant research and generates solutions, addressing key issues expressed in the UN 2030 Agenda for Sustainable Development.

RECOMMENDED CITATION

Un, C., Thinyane, M. and Christine, D. (2021) "Civil Society Organizations' Cyber Resilience - leaving no civil society organization behind in cyber resilience", United Nations University

ISBN: 978-92-808-9131-7

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digital technologies have become increasingly integral to the effective functioning of societies worldwide. These technologies provide the critical infrastructure that supports operations across different domains at different levels. Digital technologies also support the resilience of societies to deal with stresses, shocks, and disasters, as has been evidenced during the COVID-19 pandemic. For example, despite the lockdown measures worldwide, schools continued providing lessons online, businesses and organisations shifted to virtual operations, and governments digitised their services.

As far as Civil Society Organisations (CSOs) are concerned, studies show an increasing reliance on digital technologies for their mission and operations. For CSOs, the COVID-19 pandemic catalysed new forms of civic mobilisation, which has seen organisations shifting to digital organising and increasing their collaboration with various stakeholders in emergency relief and informal activism.

However, digital technologies can have constraining and adverse impacts on the CSOs, for example, by increasing CSOs' exposure to new and advanced cyber risks, such as disinformation campaigns and advanced persistent threats (APT) attacks. Under this evolving threat landscape, CSOs remain ill-positioned and under-resourced to mitigate these risks, making them more susceptible to cyber risks relative to the public and private sectors.

This situation underscores the need for cyber resilience, the capability to prepare for, absorb, recover from, and adapt to significant cyber threats which are multi-dimensional, emanating from the social, technological, environmental or personal environments. Cyber resilience needs to be considered at the systemic level in terms of the ability of different sectors of society, including citizens and CSOs, to cooperate and interact to deal with adverse cyber incidents.

This report observes how CSOs worldwide operate in a context of limited resources and capacity for cyber resilience, increasingly complex regulatory and compliance environment, as well as an evolving cybersecurity risk environment. In general, CSOs continue to experience marginalisation within the cybersecurity domain as far as threat intelligence reporting, direct technical support for incident handling, and capacity-building is concerned. As a result, most CSOs adopt ad-hoc and haphazard cybersecurity management practices, further perpetuating their precarity and vulnerability.

Further, this report details an investigation of the cyber resilience posture of CSOs in the local context of Macau SAR - China and finds that the organisations are similarly operating in the context of increased cybersecurity vulnerability and limited resources and capacity for cyber resilience, which has been exacerbated by the COVID-19 pandemic.

The report recommends that **civil society organisations:**

- undertake cyber resilience management training for senior management
- adopt appropriate cyber resilience management models
- allocate and prioritise funding for cybersecurity
- undertake targeted organisation-wide cybersecurity capacity-building
- leverage external support and partnerships for cybersecurity.

As far as the **private sector** is concerned, the report recommends that they:

- define clear Service Level Agreements (SLAs) for CSOs with specific cybersecurity commitments
- provide context-sensitive and informed solutions to CSOs.

Finally, the project recommends for the **governments** (especially in their role as funders) to:

- prioritise cybersecurity in CSOs' funding instruments
- strengthen the local cybersecurity ecosystem to provide specific support for CSOs
- provide cybersecurity capacity-building for CSOs
- develop locally relevant cybersecurity resources for CSOs
- strengthen cybersecurity threat intelligence research and communication.

INTRODUCTION

Digital technologies have become increasingly integral to the effective functioning of societies worldwide. These technologies provide the critical infrastructure that supports operations across different domains (e.g., health, education, governance) and at different levels from the micro (i.e., individual) to macro (i.e., national). Digital technologies play an essential role in achieving sustainable development worldwide; this has been recognised through the framing of Information and Communication Technologies (ICTs) as an explicit means of implementation within the United Nations Sustainable Development Goals agenda, under SDG 17 "Partnership for the goals". Across the world, countries have also drawn up national development strategies that recognise and position ICTs as a critical enabler for the achievement of the local development goals.

The essential role of ICTs to support societal functioning has poignantly been illustrated during the ongoing global COVID-19 pandemic. From the pandemic onset, ICTs supported research and facilitated communication, dialogue, and information-sharing between and within countries. With the spread of the pandemic and the institution of lockdown measures worldwide, ICTs have enabled countries to deploy COVID-19 tracking and monitoring systems. They have, more importantly, enabled society to continue functioning – for families and friends to remain in contact, for schooling and education to continue online, and for business and meetings to be virtualised.

The COVID-19 pandemic, which has had a fundamental and lasting impact worldwide, is but one of the many global risks recognised by the World Economic Forum (WEF) in the latest Global Risk Report as significant – both in terms of likelihood and impact [1]. The other imminent risks noted in the WEF report include climate action failure, debt crises, natural environment damage, and technology-related risks. According to the report, technological risks, including digital power concentration, digital inequality, and cybersecurity failure, remain top likely risks in the short-term and medium-term.

Digital power concentration is due to the widening digital divide between and within countries worldwide because of digital dependency, automation, information suppression and manipulation, and gaps in regulation and capabilities that are outpaced by digitalisation speed [1]. Digital inequality is expected to be exacerbated by the reduced policy-making capacity and decreased public spending following the knock-on effects of COVID-19. The most impactful technology-related risk identified by the report is IT infrastructure breakdown, which ranks the 10th most impactful risk overall [1].

It is essential to recognise that although the global risks are identified and located within specific domains (e.g., economic, societal, technology), the impacts of the risks emanating from one domain can cascade into other domains through complex dynamics and non-deterministic pathways. The Global Risk Report notes these intricate dependencies and complexity by observing that digital inequality is expected to increase the risk of livelihood crises and social cohesion erosion, which are ranked among the highest impact and likelihood risks of the next decade. A further example of these complex risk dependencies is that, with COVID-19, what started as a disease outbreak within the health domain evolved to become a multisectoral disaster that has impacted economies, societies, and the environment. Another example of these complex dependencies is how the pandemic inspired and triggered a slew of cybersecurity threats, including social engineering, misinformation, and disinformation attacks.

Worldwide, there are efforts to deal with this evolving global risk landscape by formulating frameworks, strategies, action plans, and programmes for disaster risk management and mitigation. These efforts are primarily framed around enhancing resilience – the capability to maintain operations and functioning in the context of stresses, shocks, and disasters. As far as technological risks are concerned, the goal of cyber resilience is to enhance the capability to prepare for, absorb, recover from, and adapt to significant cyber threats which are multi-dimensional, emanating from the social, technological, environmental, or personal environments.

Societal cyber resilience needs to be considered at the systemic level in terms of the ability of different sectors of society to cooperate and interact to deal with adverse cyber incidents [1]. Research has shown that there is better coordination and cooperation between the government and private sector stakeholders (who are usually also critical infrastructure owners) towards national cyber resilience than with civil society stakeholders [2]. There remains a need to strengthen the cooperation with and integrate civil society stakeholders in national cybersecurity dialogues. With the continued marginalisation of civil society in these dialogues, the efforts towards national cyber resilience are not only hampered, but critical sectors of society remain in a position of continued and increased vulnerability.

As far as Civil Society Organisations (CSOs) are concerned, studies show an increasing reliance on digital technology for their missions and operations. Globally, 71% of Non-Governmental Organisations (NGOs) regularly send email updates to supporters and donors, and half of them (51%) increased spending on technology in 2019 [3]. More prominently, Asia witnessed the highest rate of increase (56%) in NGO spending on technology in the same year [3].

The digitalisation of CSOs' functioning has been empowering - technologies have impacted the ways CSOs engage with their partners and clients and how they run their operations [6]. However, digital technologies have also been bivalent, with constraining and adverse effects on the CSOs, for example, by increasing CSOs' exposure to cyber risks. Therefore, while the use of technology in organisations is increasingly vital, there is a strong motivation for planned and strategic technology adoption in organisations, skills training, technology spending and investment, and mitigation of associated risks [7].

In this report, Civil Society Organisations (CSOs) are defined broadly to include groups with hybrid organisational characteristics in the forms of civil society or volunteer-run associations, social movements, and the non-profit sector. This expanded framing of CSOs builds upon their fluid organisational forms - many CSOs evolve, varying in their relationships to the state and degrees of participation by constituents [4]. Hence, CSOs include, according to The World Bank's definition, 'the wide array of non-governmental and not-for-profit organisations that have a presence in public life, express the interests and values of their members and others, based on ethical, cultural, political, scientific, religious or philanthropic considerations' [5].

Despite the cyberspace being multi-dimensional and multi-layered (i.e., comprising the physical, logical or technical, and social layers), research has found that the predominant framing of cybersecurity issues, in large part, has neglected the social layer, which is the most vulnerable dimension to cyber threats [8]. The lack of awareness and capability to identify cyber threats and be resilient against adverse cyber incidents, such as social engineering attacks and disinformation, have impacted CSOs and remain the leading causes of CSOs' vulnerability to cyber risks. Although cyber threats against CSOs are often of low technical sophistication, recent uses of aggressive zero-day exploits against politically vulnerable organisations and journalists suggest that threat actors are likely to employ more advanced tools, techniques, and procedures (TTPs), as the target organisations' cybersecurity posture improves [9].

Under this evolving threat landscape, CSOs remain ill-positioned and under-resourced, making them more susceptible to risks from adverse cyber incidents relative to the public and private sectors. For example, in the UK, where the senior management of charities have placed a higher priority on cybersecurity over the years, over a quarter of charities still experienced cyber-attacks in 2019 [10]. The ongoing COVID-19 pandemic has also brought increased cyberattacks against organisations, for example, through phishing emails related to the pandemic [11]. The attacks have been exacerbated by the fact that remote working has expanded organisations' attack surfaces due to the increased use of personal devices [12].

CYBER RESILIENCE OF CIVIL SOCIETY ORGANISATIONS WORLDWIDE

Despite the differences in the profiles and the operating contexts of CSOs worldwide, they largely share the following similar characteristics as far as their cyber resilience position and posture are concerned.

LIMITED RESOURCES AND CAPACITY FOR CYBER RESILIENCE

Worldwide, CSOs are characterised by their lack of financial resources, inadequate technical capacity, including skilled IT staff, limited awareness of compliance risks, and limited ability to engage in long-term strategic and contingency planning [4]. CSOs are generally under pressure from the public and funders to stay mission-oriented in their budget allocation, and as a result, they tend to minimise overhead costs, especially for IT and cybersecurity-related expenditure [13].

CSOs' position is exacerbated by the under-prioritisation of cybersecurity in funding instruments. When investment in cybersecurity generates diminishing returns for CSOs, as a result of their below-average internal technology and management capacity, they remain disincentivised to make any further investments beyond a basic level of cybersecurity unless funders prioritise cybersecurity with a separate or earmarked budget [14]. There has been growing interest from the public and private grant-makers in recent years to support cybersecurity expenditure. This includes small emergency funds such as the Digital Defenders Partnership funding [15], project-based funding, and funding from traditional international development funders such as USAID [9]. On average, non-profits spend about 5.7% of their total budgets on information technology, compared to 3.3% of total revenue investment from private-sector firms [16]; however, this works out to relative

underinvestment in cybersecurity since the total budget of CSOs is smaller and based on fundraising and donor support [14]. Moreover, only 20% of non-profits worldwide regularly review technology investments, even though such reviews and evaluations would add to organisational effectiveness in using technology resources [16].

According to the 2017 CohnReznick Not-for-Profit Governance and Financial Management Survey undertaken in the United States, although cybersecurity has become more concerning for organisations, only 51% of respondents reported having conducted cybersecurity assessments, and only 38% have performed vulnerability assessments or penetration testing [17].

Beyond the limited financial resources, which subsequently impacts the rest of the organisation's operations, CSOs also have limited capability for cyber resilience in terms of the availability of qualified personnel to manage IT and cybersecurity. On average, small CSOs have one IT staff, and the ratio of IT to non-technical personnel is significantly worse than in larger organisations [9].

These findings on the cyber vulnerability of the CSOs worldwide, due to limited resources and reduced cyber resilience capability, are congruent with the findings from this research, which are discussed later in this report, on the cyber resilience situation of local CSOs.

COMPLEX REGULATORY AND COMPLIANCE ENVIRONMENT

Globally, CSOs operate in diverse legal and regulatory environments with varying demands for compliance. However, there is a growing demand worldwide for CSOs to comply with requirements associated with ICT use for processing sensitive and confidential personal data. As CSOs collect and store valuable data from different stakeholders, ranging from donors to their service users, failure to comply with data protection regulations has immense ramifications on organisational reputation and existence, especially when CSOs mobilise resources and receive support from the public [4].

In general, CSOs have limited ICT and cybersecurity capacities and limited avenues for receiving tailored guidance and assistance to comply with the legal and regulatory requirements. As a result, many CSOs find themselves in either of the two extreme positions of non-compliance or over-compliance due to excessive reliance on external services providers detached from their operational context and lacking the nuanced understanding of CSOs' situation.

The complexity of the compliance requirements associated with data processing and retention places CSOs in a position of needing better context-specific security controls, training, and guidance. Illustratively, CSOs operating under the European Union General Data Protection Regulation (GDPR), one of the most stringent data protection regulations worldwide, were found to have faced more challenges and received less guidance and funding towards GDPR compliance, compared to small and medium-sized enterprises [18].

AD-HOC AND HAPHAZARD CYBERSECURITY MANAGEMENT

Information technology and cybersecurity management among CSOs are generally undertaken through an ad-hoc and haphazard approach due to the lack of dedicated resourcing and personnel.

Recent studies have highlighted the importance of top management to instill cybersecurity culture in organisations. Top management participation in information security initiatives is shown to have a significant impact on both organisational culture and staff beliefs – their attitudes, subjective norms, and perceived behavioural control – and on compliance with internal security policies [19]. The organisations' top management can bring relevant perspectives, skills, information, and organisational mechanisms, such as performance evaluation and communication processes, to change staff perception, attitudes and behaviour around cybersecurity [20]. Similarly, the likelihood for internal compliance depends significantly on organisational leadership's ability to encourage cooperation between staff and adherence to planned and structured security processes within the organisation [21].

However, as noted previously, cybersecurity management is often under prioritised and underinvested in CSOs [13]. According to a report from the Institute for Critical Infrastructure Technology (ICIT), 47% of the international NGOs or non-profit organisations surveyed did not have cybersecurity frameworks in place. For the 51% of the organisations that did, 56% of them employed an internally developed framework, and only 32% utilised the industry-standard NIST cybersecurity framework [22].

On the other hand, CSOs mainly depend on the use of commodity off-the-shelf ICT tools and services that may not be tailored to their specific context and situation, risk profiles, or intended users [23]. For example, for CSOs that process sensitive personally identifiable information, there is a need to employ relevant data protection controls, including encryption, in handling the data. Indicatively, research has found that only 41% of NGOs worldwide employ encryption technology to protect their data and communications [3]. Further findings from a survey of civil society IT practices also show that older and outdated security tools, including antivirus software, are more widely employed than current and updated cybersecurity tools [9].

EVOLVING CYBERSECURITY RISK ENVIRONMENT

CSOs take up critical societal roles and serve various communities. Worldwide, they employ around 54 million full-time equivalent workers and are supported by a global volunteer workforce of over 350 million [24]. In recent years, the operating environment of the CSOs has evolved, with more organisations being "forced" to adopt digital technologies in their operations; this has been particularly true with regards to dealing with the ongoing COVID-19 pandemic. The pandemic has catalysed new forms of civic mobilisation worldwide, which has seen CSOs shifting to digital organising and increasing their collaboration with various stakeholders in emergency relief and informal activism [25]. Against this backdrop of the pervasiveness of technology in their operations, CSOs are at a more critical juncture – as their reliance on digital technologies grows, recovery costs from potential adverse incidents increase correspondingly [14].

The global cybersecurity environment within which CSOs operate is also constantly changing and evolving; daily, there are new cybersecurity threats, new tactics, techniques, and procedures (TTPs) that the threat actors are employing. Targeted digital threats, ranging from malware attacks to defacements of websites, not only bring financial burden and undermine organisational efficiency, but they also pose a considerable risk to both organisational existence and individual safety [26].

Increasingly, sophisticated, well-resourced, and capable adversaries, such as nation-state actors and advanced persistent threat (APT) actors, are targeting CSOs in pursuit of furthering their national and political interests. According to the statistics on nation-state activities against individual or organisation account holders tracked by Microsoft, NGOs were the most targeted (32%) industry sector, followed by professional services that provide consultancy and contract services (31%) in the period from July 2019 through June 2020 [27].

This evolving cybersecurity risk environment requires organisations to always keep abreast new developments and for their systems to constantly adapt to deal with the new risks within the environment.

MARGINALISATION WITHIN THE CYBERSECURITY DOMAIN

Given the importance of cyber resilience for CSOs' functioning and CSOs' centrality to the provision of public services, CSOs' cybersecurity should be seen and understood as contributing to the public good. Instead, the dominant narrative on cybersecurity is captured by the consolidated interests of the public and private sectors – linked to protecting national critical infrastructures and ensuring business operational continuity, respectively [28]. As a result, the civil society stakeholders remain relatively neglected in the realm of cybersecurity.

Research has found that the voices of CSOs have been marginalised in commercial threat reporting and that the understatement of the impact of adverse cyber events on civil society has led to insufficient prioritisation of threats to civil society by both funders and policymakers [29]. Incentivised by structural interests to profit from private reporting and costly protection services, commercial cybersecurity firms have disproportionately prioritised high-end threats to high-profile victims by high-profile threat actors [29]. For example, the recent coverage on the SolarWinds breach serves as a reminder of how the backdoor compromise of the SolarWinds Orion network management application, which has impacted the 18,000 organisations that installed the software with malicious code, overly focused on the Fortune 500 companies and the US government agencies that were attacked, while 18% of the cyberattack victims were think tanks or NGOs [12], [30]. This situation puts CSOs at great harm when their threat landscape is not prioritised within the cybersecurity domain and when cybersecurity is underprovided as a public good [29].

The lack of support to enhance the cybersecurity of CSOs worldwide is evident. At the national level, there are Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) globally that provide technical assistance in response to computer security incidents and product vulnerabilities. However, some of this support does not consider the context of CSOs and tends to be technically advanced to be adopted effectively by organisations with low technical expertise. Currently, several organisations offer tailored and varied support to CSOs, for example, through training and technology development assistance. For example, the Civil society CERT (CiviCERT) is one example of an international network with a particular focus on civil society and online activism cases [31]; Digital First Aid Kit (DFAK) [32] provides a free resource to help politically vulnerable organisations and activists protect themselves against the most common digital threats. Another prominent example is Citizen's Lab, an interdisciplinary academic laboratory researching information controls, such as network surveillance, that impact the openness and security of the Internet and human rights. Nonetheless, such efforts are still insufficient and limited, relative to the support available to both the public and private sectors. Moreover, much of the assistance to CSOs is concentrated on analysis, advocacy, and emergency response. Meanwhile, direct technical assistance addressing threats specific to CSOs and long-term capacity-building on cybersecurity are rare [9].

LOCAL CYBERSECURITY LANDSCAPE

The global situation of CSOs highlights the generally precarious and vulnerable position that they find themselves in. However, CSOs must also contend with local dynamics that shape their overall cyber resilience posture.

CYBER THREATS

According to the data from the Macau Computer Emergency Response Team Coordination Centre (MOCERT), a significant proportion of cyber threats in Macau are attributed to phishing attacks (37%) and active attacks (32%) [33]. There are also noticeable concerns amongst the Macau public regarding Internet privacy and fake news - 57% of Macau netizens thought Internet privacy was assured, and 85% indicated that they had come across fake information online in 2020 [34]. Alarmingly, during the ongoing pandemic, local companies have also experienced a drastic increase in cybersecurity risks - Macau's Cybersecurity Incident Alert and Response Centre reportedly received around 1,600 cybersecurity risk alerts per day on average in 2020 [35].

Recent cyberattack incidents reported in Macau point to the increasing vulnerability of different sectors of society. One major cyber incident reported in 2020 is the cyber-attack against the Health Bureau that resulted in the interruption of the service for supplying masks to residents [36]. Another significant incident is the ransomware attack against the Macau Portuguese School (EPM), which highlighted the negative impact of adverse cyber incidents and how they affect and disrupt the regular operations of institutions and organisations. This case further highlighted the importance of cybersecurity capability and cybersecurity support ecosystem for enabling an effective response to cyber threats [37].

Invariably, the level of media reporting on local cybersecurity incidents does not

represent the near absence of cyber threats to the local institutions and organisations, specifically to the civil society organisations. The reporting, or lack thereof, is compounded by the potential lack of situational awareness of cybersecurity vulnerabilities and compromises by the potentially affected organisations due to limited cybersecurity capabilities.

COMPLIANCE ENVIRONMENT

Regarding the compliance requirements that the local organisations need to adhere to, the Macau cybersecurity legal landscape is constituted of, but not limited to, the following cybersecurity-related legislation: the Personal Data Protection Act (2005) [38]; the Law on Combating Computer Crime [39], which was enacted in 2009 and revised in 2020; and the Macau Cybersecurity Law (2019) [40].

However, beyond the local legislation and regulation, there are also international compliance requirements associated with the processing of personal information of citizens from other jurisdictions – one such prominent regulation is the European Union General Data Protection Regulation (2016) [41] which spells out stipulations and requirements for processing European citizens' data.

The Personal Data Protection Act

The principal legal instrument governing data protection in Macau is the Personal Data Protection Act (PDPA), which came into effect in 2006 and took reference from the EU's 1995 Data Protection Directive (Directive 95/46/EC) [42]. This Act applies to entities that, directly or indirectly, collect, process, or transfer personal data in Macau.

To supervise and coordinate the public implementation of and compliance with the PDPA, the Office for Personal Data Protection (GPDP) was established.

The legislation sets out clear definitions of the types of personal data protected and the stakeholders involved in handling personal data. Further, it makes provisions for protecting personal data and spells out the responsibilities of the key stakeholders, the rights of the data subjects, and the associated sanctions and penalties for non-compliance.

With the sheer amount of personal and sensitive data collected, processed, and stored by CSOs, the PDPA is highly relevant to their day-to-day work. Recognising the importance of making CSOs aware of the legal compliance context, the GPDP serves as the main public entity that guides CSOs through the publication of guidelines, educational workshops, and supervision of the Act's implementation. In addition, the respect and protection of data privacy rights are also briefly mentioned in the Social Welfare Bureau's Social Service Facilities' Regular Funding Budget Guidelines [43], which is followed by all CSOs whose operations are funded through the Social Welfare Bureau funds. These guidelines reference the PDPA and highlight the importance of informing relevant parties of the purpose of data collection, the possibility of data transfer, and obtaining data subjects' consent when necessary, during the collection and processing of data.

Law on Combating Computer Crime

The Law on Combating Computer Crime was enacted in 2009 to regulate and define computer crime and establish an electronic evidence collection regime. This law has recently been amended in 2020 to consider the technological advances over the last decade.

The latest amendments have strengthened the regime to combat computer crime by expressly adding two new crimes – the use of illegal broadcasting stations (Article 9-A) outside of the legal conditions or contrary to the competent authority's specifications, and the illegitimate exposure of a severe computer security vulnerability (Article 9-B) [44].

In coordination with the Macau Cybersecurity Law, the Law on Combating Computer Crime provides greater criminal protection to critical infrastructure operators and better protects the privacy rights of individuals and organisations, including CSOs.

Macau Cybersecurity Law

The Macau Cybersecurity Law (MCSL) came into effect in December 2019 and sets out regulations to protect information networks, computer systems, and data of critical information infrastructure operators, which are defined as assets, information networks, and computer systems vital for the normal functioning of society and that serve the interests, order, public safety, and social well-being of the society.

CSOs are currently not considered critical infrastructure operators and are not subjected to heavy fines and penalties under the Macau Cybersecurity Law. The day-to-day reliance of vulnerable groups on CSOs' services and the evolving nature of the law suggest that it is essential for CSOs to be well-prepared and aware of potential adverse cyber events and possible future compliance requirements.

European Union General Data Protection Regulation (GDPR)

The GDPR came into force in 2018 and carries implications for data protection in the local Macau context, as the legislation applies to entities established within or outside the EU processing EU citizens' personal data.

This legislation is known to be one of the most stringent data privacy regulations worldwide. Besides its comprehensive coverage, what makes the GDPR different are the heavy fines imposed for violators, the strict new rules defining consent and data protection principles, the new organisational obligations to ensure "appropriate technical and organisational measures" in handling data securely, and the new privacy rights for data subjects [45].

Although the stringent protection afforded by the GDPR mainly apply to data subjects residing in the EU and has fewer implications for CSOs which provide services primarily to local citizens, the legislation has "great reference value" and "plays an important guiding role in the protection of personal data" [46].

CYBERSECURITY SUPPORT

Direct Technical Assistance

Macau's official cybersecurity service provider is the Macau Computer Emergency Response Team Coordination Centre (MOCERT), a non-profit service initiated in 2009 and funded by Macau New Technologies Incubation Centre (MANETIC). MOCERT was established to provide computer security incident handling support, promote information security awareness, coordinate with stakeholders on both international and local levels, and produce research for Internet users and local enterprises [47]. In recent years, the centre has strengthened its incidents handling capability by launching a Cyber Threat Intelligence (MOCERT-CTI) System to automatically obtain threat intelligence from trusted parties and open sources [33].

There is, however, limited capacity to provide technical assistance tailored to the specific needs and situations of CSOs. Without such dedicated technical support for incident handling and response, the over 10,000 loosely formed and organised citizen associations and CSOs operating in Macau remain in a position of precarity [48]. While private-sector IT and cybersecurity companies in Macau could provide cybersecurity services to CSOs, the associated service costs may prove prohibitive for organisations with limited financial resources.

Capacity-building

The Macau government recognises the significance of integrating cybersecurity capacity-building within its development plans. As a result, it has supported efforts to develop local cybersecurity talent through education and training. For example, the Science and Technology Development Fund of Macau (FDCT) organised Certification Training Session on Certified Information Security Professionals (CISP) as well as a cybersecurity technology exchange tour for participants from critical information infrastructure operators [49], [50].

Following the recent enactment of the Macau Cybersecurity Law, local security authorities conducted their first-ever major cybersecurity attack drill, which involved cooperation with the Judiciary Police and 15 other entities, including critical infrastructure operators and public utility companies [51]. Other similar capacity-building efforts include cybersecurity workshops and training co-organised by the Macau Young Entrepreneur Incubation Centre, Alibaba, and Deloitte [52].

While these measures amount to an essential first step to engage wider societal stakeholders, there remains an opportunity to better engage CSOs, both as recipients and providers of cybersecurity capacity-building, towards the co-production of societal cyber resilience.

Cybersecurity funding for CSOs

In general, and congruent with the global situation, there is a lack of awareness and investment in cybersecurity by local funders and CSOs. Notably, the Social Service Facilities' Regular Funding Budget Guidelines does not mention investment in cybersecurity or digital technology, except for the procurement and disposal of fixed property from public departments, private donors, and individual organisations. Furthermore, cybersecurity is not indicated in the section on organisational management mechanisms, which cover the management of organisations operations, human resources, finance, and reputation, except for a call for organisations to establish a guideline on the use and protection of sensitive data.

Overall, there is limited support for CSOs within the local context as far as direct technical assistance, capacity-building, and targeted funding instruments are concerned.

LOCAL ORGANISATIONS' CYBER RESILIENCE POSTURE

Through a series of interviews and questionnaires with the local CSOs (see Appendix for details), their internal cyber resilience position and posture was found to be vulnerable, as far as increased exposure to potential cyber risks, and precarious, as far as limited management of cyber resilience within the organisations.

USE OF DIGITAL TECHNOLOGIES

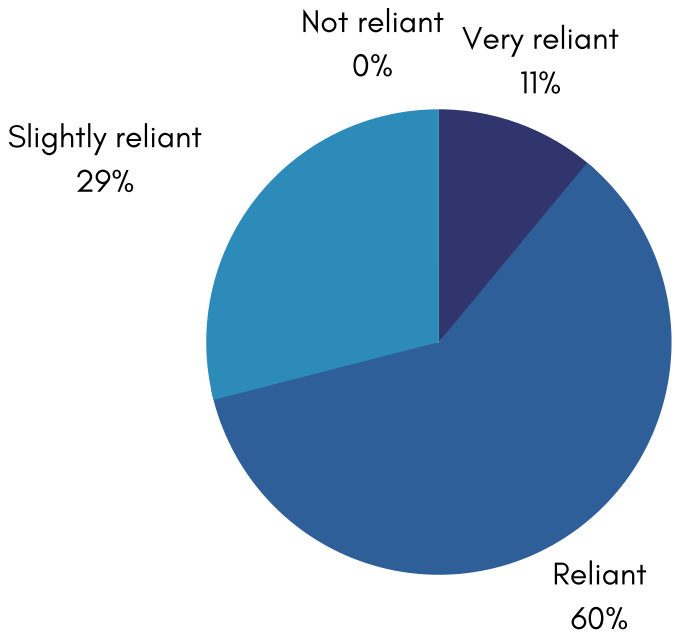
Congruent with the global situation, most local CSOs increasingly rely on ICT for their operations (see Figure 1). Some organisations have integrated digital technologies in both their operations and information security – one organisation not only has recently launched an application for service users to receive updated information and make appointments, but they also possess a network monitoring system to protect their network from malicious software.

At the other end of the spectrum, some organisations could operate with limited reliance on digital technologies, but still employing basic IT resources, such as social media platforms and websites, to communicate with colleagues and service users.

It is worth noting that the organisations' reliance on digital technologies has surged rapidly since the COVID-19 pandemic began, most notably with the increased use of virtual meetings with organisational stakeholders.

This increased reliance of local CSOs on digital technologies alludes to the associated importance of cyber resilience to ensure continuity of organisations' operations and existence, despite adverse cyber incidents.

Figure 1. *Organizations' reliance on ICT*



MANAGEMENT OF ORGANISATIONAL CYBER RESILIENCE

Most of the organisations engaged considered cyber resilience as important; this alludes to the importance ascribed to having cybersecurity plans and policies in place. The organisations articulate the goal of cyber resilience in terms of business continuity, especially the provision of daily services to clients as well as minimising the impact of adverse incidents.

A significant majority (i.e., 84%) of the organisations recognise the importance of having a cybersecurity plan in place and a further majority (i.e., 66%) also find it important to invest heavily in solutions and mitigation strategies against potential organisational risks. However, these perceptions do not translate into practice and are not reflected in the perceived cybersecurity posture of the organisations – there are mixed levels of effectiveness in their existing cybersecurity policies (see Figure 2) and an overwhelming majority (73%) of the organisations do not have measures in place to identify cybersecurity risk (see Figure 3).

Less than 10% of the organisations undertake risk assessment that covers cybersecurity risks (Figure 3). More strikingly, only a small fraction of the organisations (14%) have processes to understand the risks they face, to identify critical organisational resources and impact of incidents, and to put in place mitigation strategies (see Figure 4).

Figure 2. *Effectiveness of cybersecurity policies and processes*

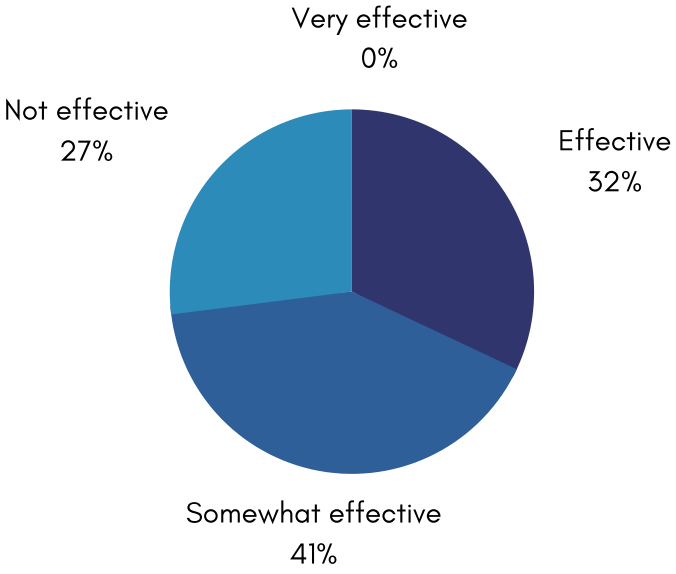


Figure 4. *Risk identification and assessment procedures*

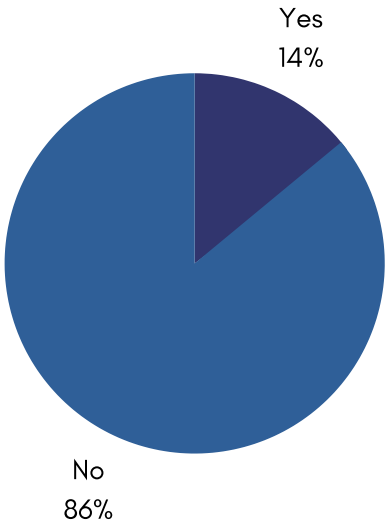
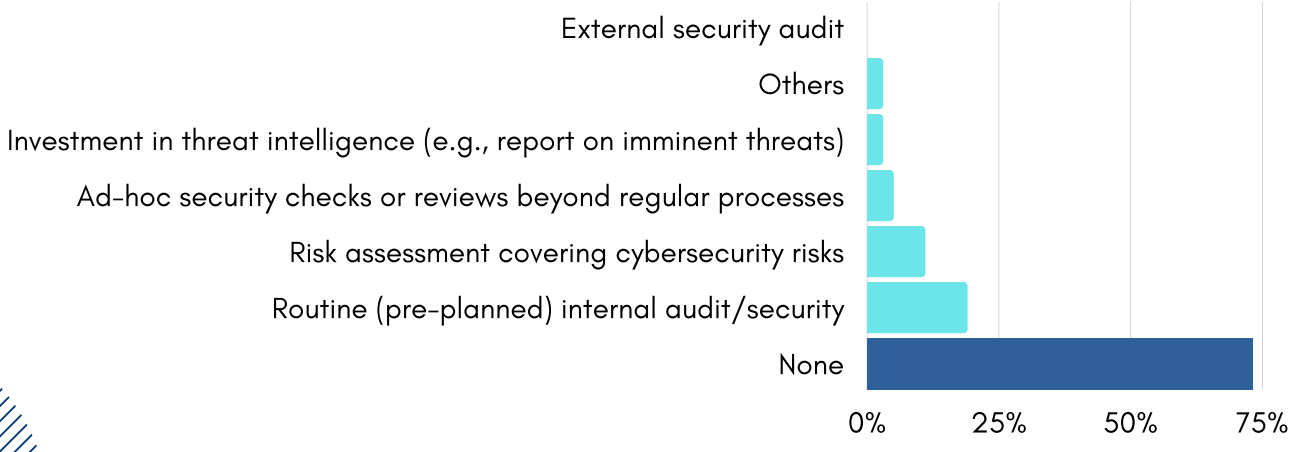


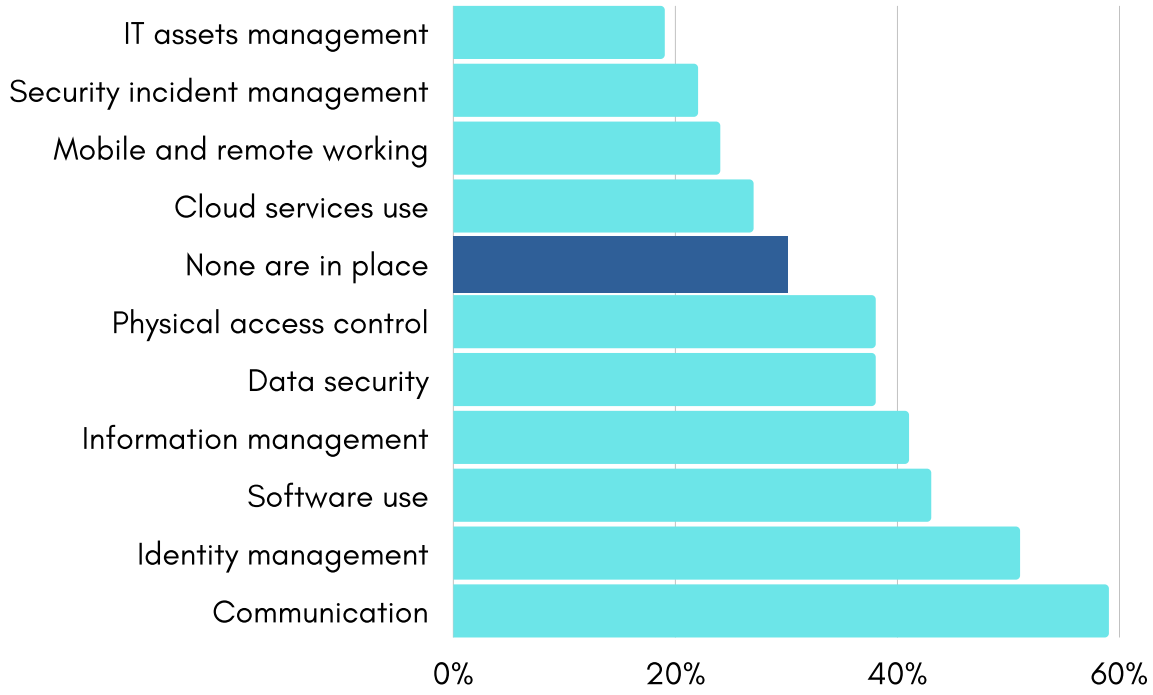
Figure 3. *Cybersecurity risk identification measures undertaken by the organisations*



In general, most of the organisations do not have formal or written guidelines in place for the various dimensions of information security, with 30% of the organisations indicating that they have no relevant cybersecurity-related policies and guidelines at all. The organisations have policies and guidelines mostly on communication (incl. social media use, email use, information exchange) and identity management (incl. password management), and least on management of IT assets and security incidents (see Figure 5).

Therefore, there is a disparity between the organisations' perception of the importance of cyber resilience and their capacity of attaining organizational cyber resilience. They recognise the significance of cyber resilience, but they are not able, due to their limited capability and constrained resources, to put effective measures towards achieving organisational cyber resilience.

Figure 5. *Cybersecurity policies and guidelines*

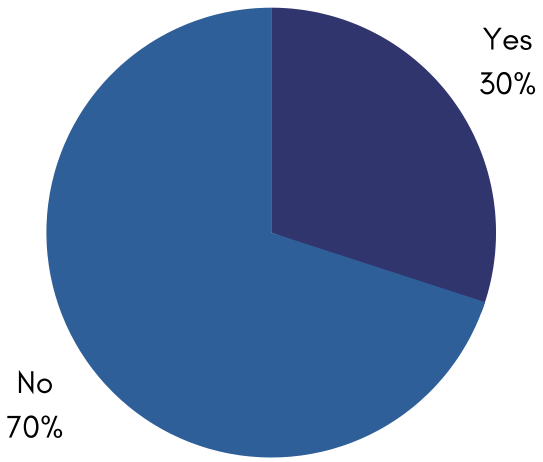


CYBERSECURITY MANAGEMENT MATURITY

Cyber resilience management within organisations is operationalised through policies, guidelines, processes, and procedures that are implemented throughout the organisation. Within the cybersecurity domain, several maturity models have been developed to assist organisations to assess their cybersecurity maturity and to implement relevant controls towards increased maturity. These controls are typically articulated across a common set of domains within organisations' operational context.

This research explored the level to which the organisations were implementing relevant controls across common domains such as asset management, human resources management, access control, physical security, communications and operations management, incident management, and risk management and continuity planning.

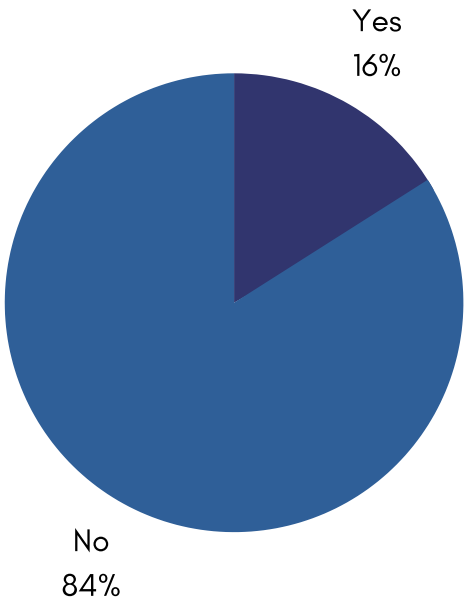
Figure 6. *Organisational asset inventory*



Our findings show that most of the organisations were implementing cybersecurity management at the basic level of maturity through ad-hoc practices and approaches. Illustratively most of the organisations are not managing their ICT resources effectively and securely, in terms of asset inventory, asset classification, and acceptable use procedures (see Figure 6, Figure 7, and Figure 8). Further, some of the organisations are also using systems that are old and outdated. One of the interview respondents noted this phenomenon across the organisation as follows:

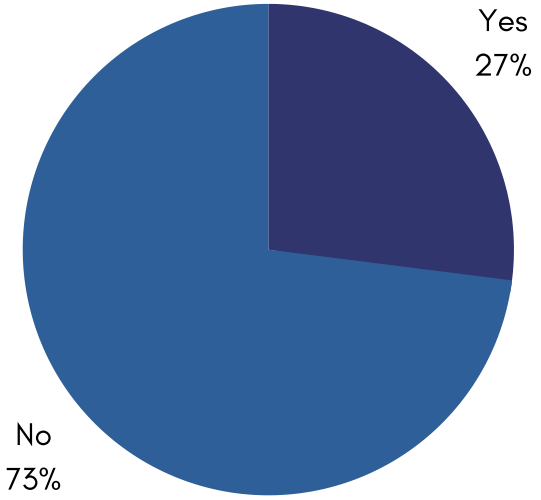
> **So we have to apply to replace some hardware facilities because we have been using the same system for a very long time, that is, the same hardware. Those hardware may have been products from eight years ago, or it was eight years ago when we bought it. Production is not an issue of how many years ago. So, you know that these technological matters vary on a monthly and yearly basis, right? We all know that our hardware equipment may have a huge gap with the new equipment nowadays. right? So, these are also the feedback we received from the IT companies. If we change that system, it should actually fasten some of our speed and be relatively stable.**

Figure 7. *Organisational asset classification*



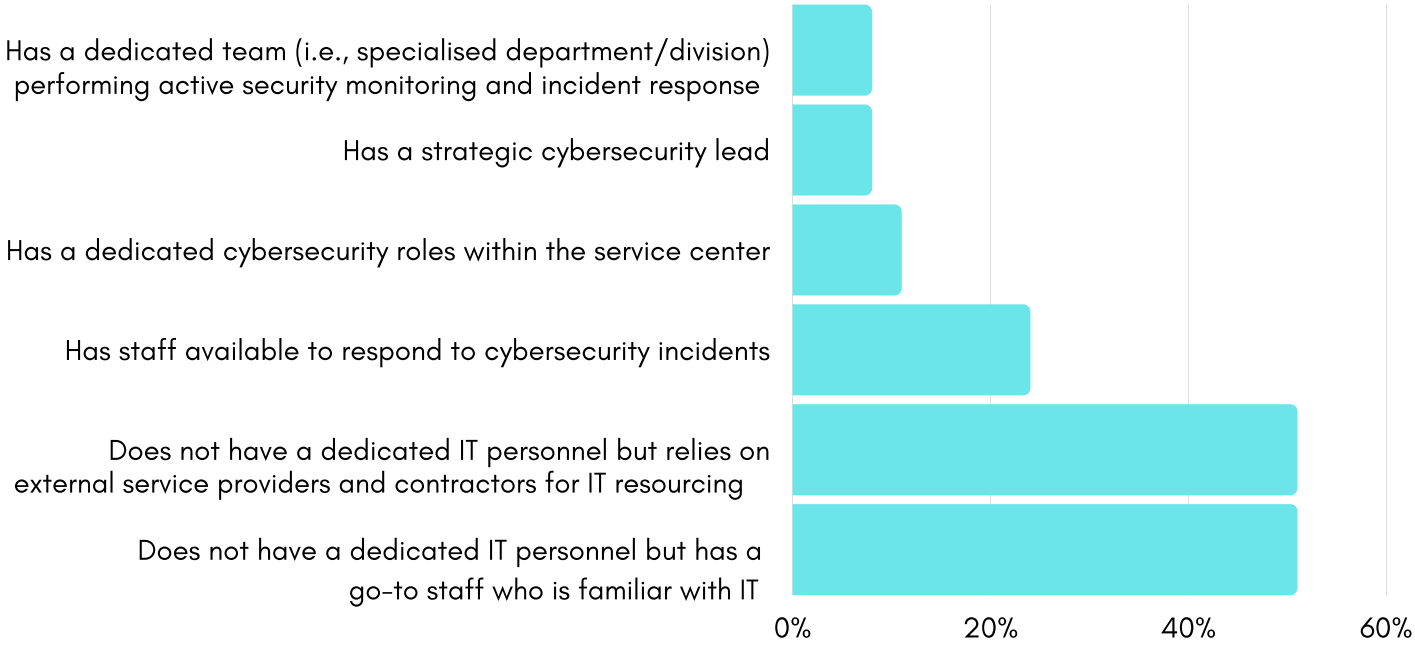
As CSOs are under-resourced, some of them rely on free software and security applications, such as those available to non-profits for free, which can expose them to potential cyber threats due to limited support and obsolescence.

Figure 8. *Acceptable use policy for IT resources*



Despite the ad-hoc measures towards cybersecurity management, some of the organisations have been able to effectively implement information security measures, such as having established processes and policies for regular data and system backup, as well as installing basic antivirus applications.

Figure 9. *Organisational cybersecurity capacity*



ORGANISATIONAL CYBERSECURITY CAPACITY

One of the biggest obstacles for CSOs to effectively implement cybersecurity measures is the lack of internal capacity and expertise. Notably, most organisations do not have dedicated IT personnel to actively perform security monitoring and incident response. Instead, the majority of the organisations depend on staff familiar with IT within their organisations and affiliate organisations or on outsourced IT support from service providers and contractors (see Figure 9).

In general, the staff who are assigned with IT-related responsibilities within the organisations mostly handle basic procurement, maintenance, and disposal of IT resources, as well as basic response to IT-related incidents.

The lack of cybersecurity capacity within the organisations further manifests through the limited cybersecurity capacity-building and training that the organisations' stakeholders undergo.

In most (over 80%) of the organisations, none of the key stakeholders (such as contractors, volunteers, general staff, directors, and managers) have undergone any cybersecurity training (see Figure 10). In very few organisations cybersecurity training has been undertaken for directors, general staff, IT-related staff, and contractors. Only one of the organisations undertakes regular cybersecurity training for the IT-related staff. For the organisations that provide cybersecurity training, the focus of the training is broad and spans across the different topics in cybersecurity, with most emphasis placed on data and information handling, password management, web security, email security, and software and application security.

These observations point to the need for internal IT capacity-building within the organisations, which is accentuated by the fact that most organisations resort to internal processes and resources for handling adverse cyber incidents (see Figure 11).

Figure 10. *Organisational cybersecurity capacity-building*

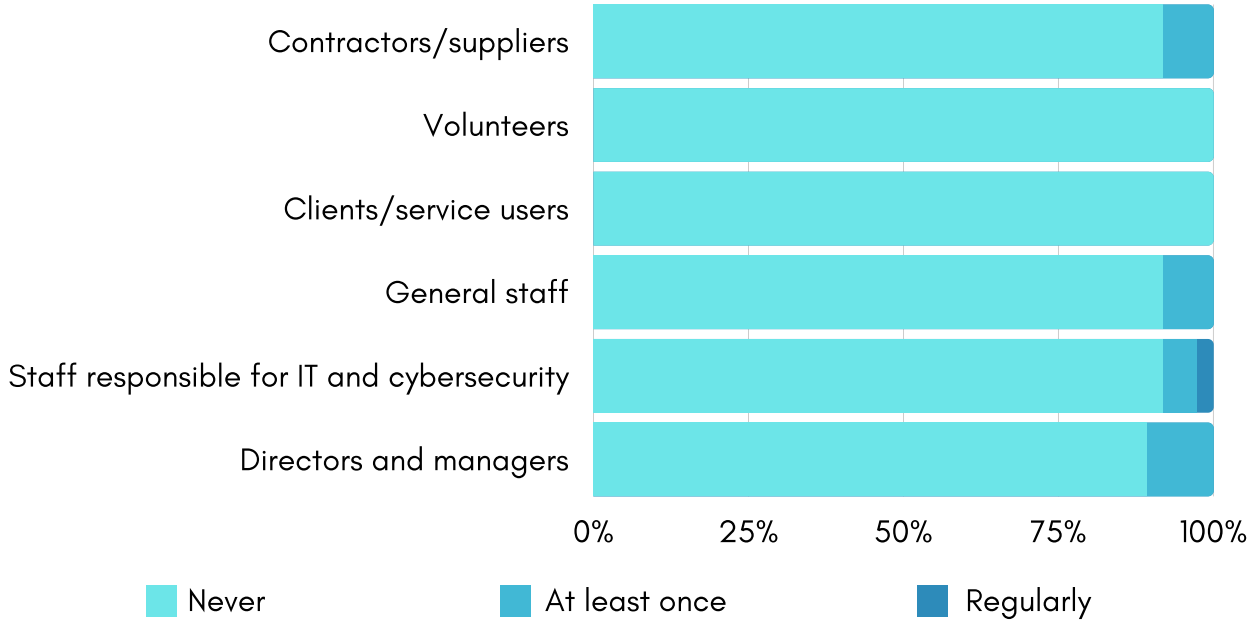
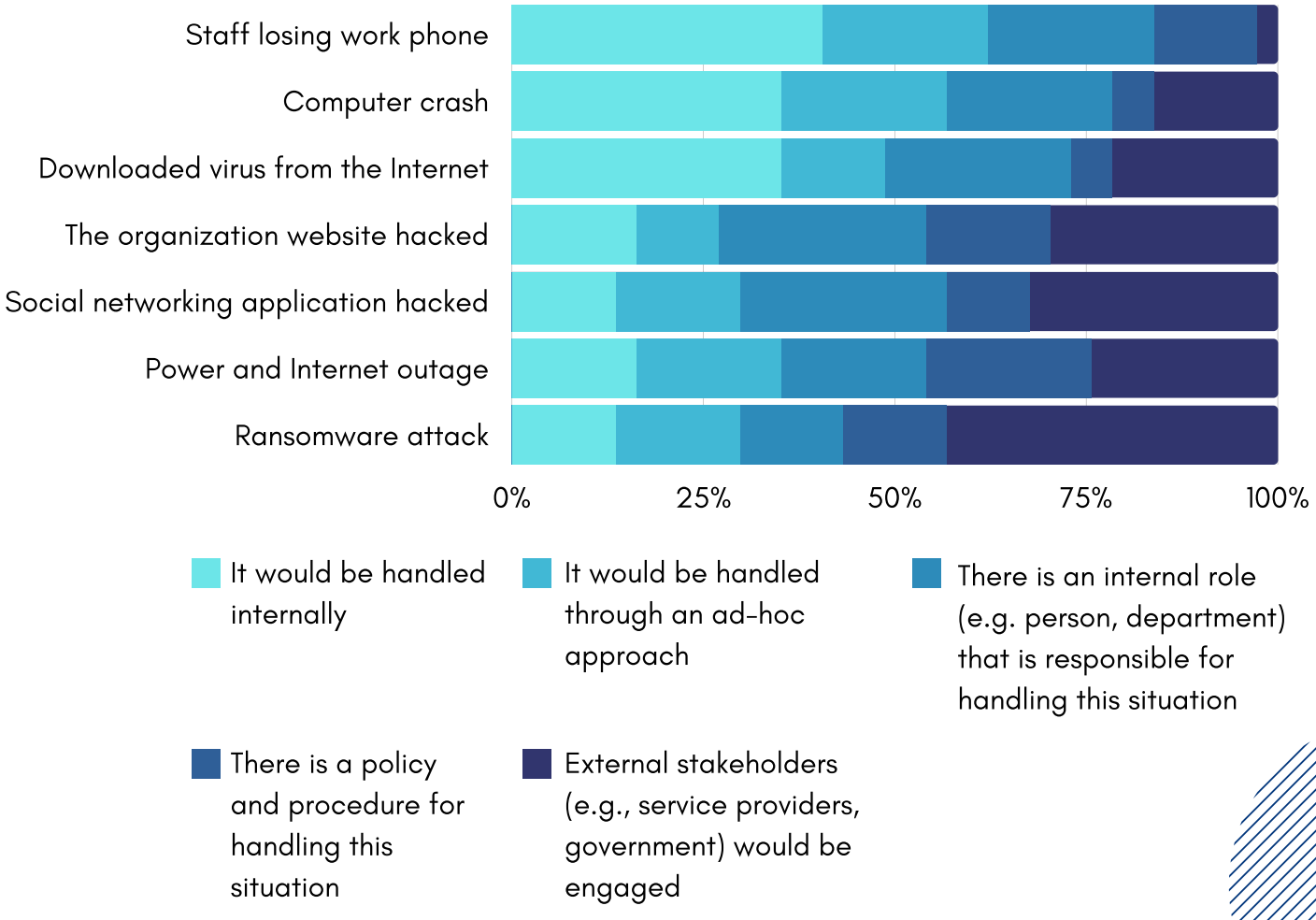


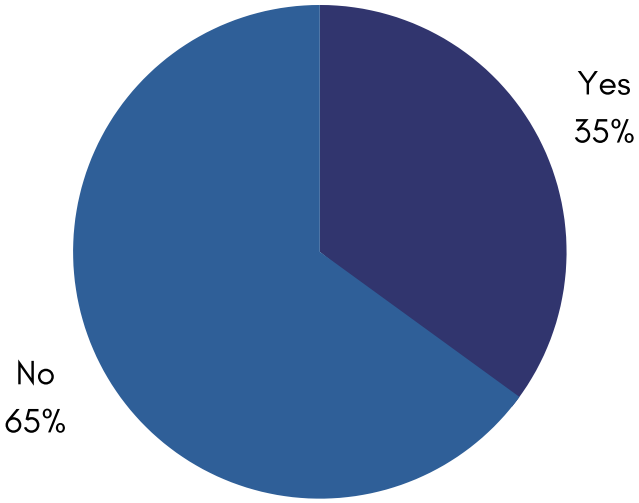
Figure 11. *Cyber incident scenario handling*



CYBERSECURITY INCIDENT HANDLING

As noted above, most organisations resort to internal mechanisms for handling and resolving adverse cyber incidents. This can be attributed to several factors including lack of resources to engage external commercial services providers, lack of awareness of available support within the ecosystem (see Figure 12), and lack of awareness of compliance requirements associated with certain types of cybersecurity incidents – for example, disclosure requirements associated with data leakages and breaches. While there is limited cybersecurity incident handling support within the local context, there are, however, existing regulations and public entities, such as the Office for Personal Data Protection (GPDP), Macau Computer Emergency Response Team (MOCERT), and Cybersecurity Incidents Alert and Response Centre (CARIC), which are designated to provide some level of support to local stakeholders experiencing adverse cyber incidents. There is also some limited support available from the private sector, in terms of dedicated cybersecurity companies, as well as general IT service providers.

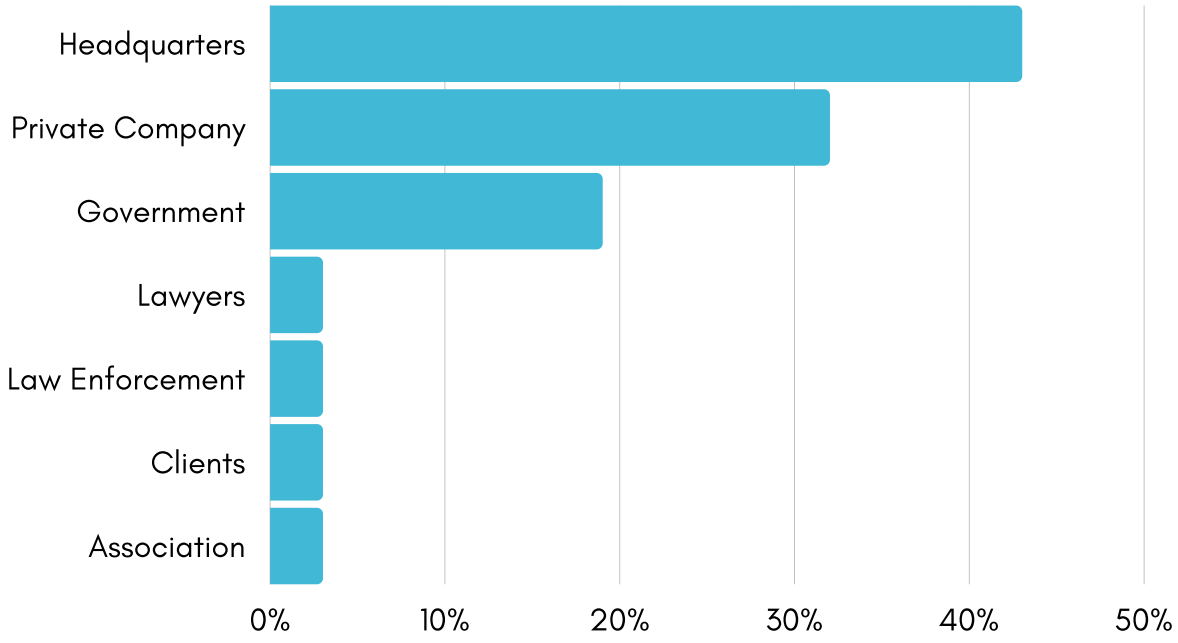
Figure 12. *Awareness of external support service providers*



The level of organisational engagement with external stakeholders for incident handling and resolution is generally limited, with the largest cohort (i.e., 43%) of organisations resorting to engaging their association's headquarters for incident handling (Figure 13). Private sector service providers are the second common stakeholders that organisations would consider engaging for incident handling, followed by the government stakeholders. Since most of the organisations engaged in this research

provide services related to social work, the key government department that the organisations would engage with is the Social Welfare Bureau. Few other organisations would engage law enforcement and legal practitioners as part of their incident handling.

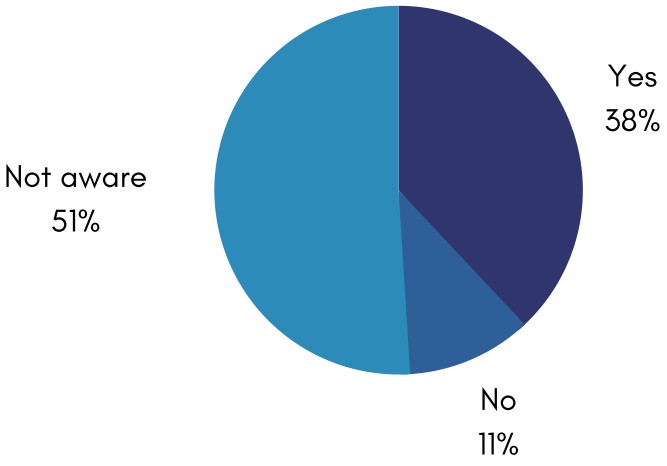
Figure 13. *External stakeholders engaged in incident handling*



POLICIES AND PROCEDURES FOR LEGAL COMPLIANCE

Findings from this research reveal that over half (i.e., 51%) of the organisation are not aware of any cybersecurity-related regulatory and legal requirements that they need to comply with. 11% of the organisations believe that they are not subject to any compliance requirements.

Figure 14. *Awareness of compliance requirements*



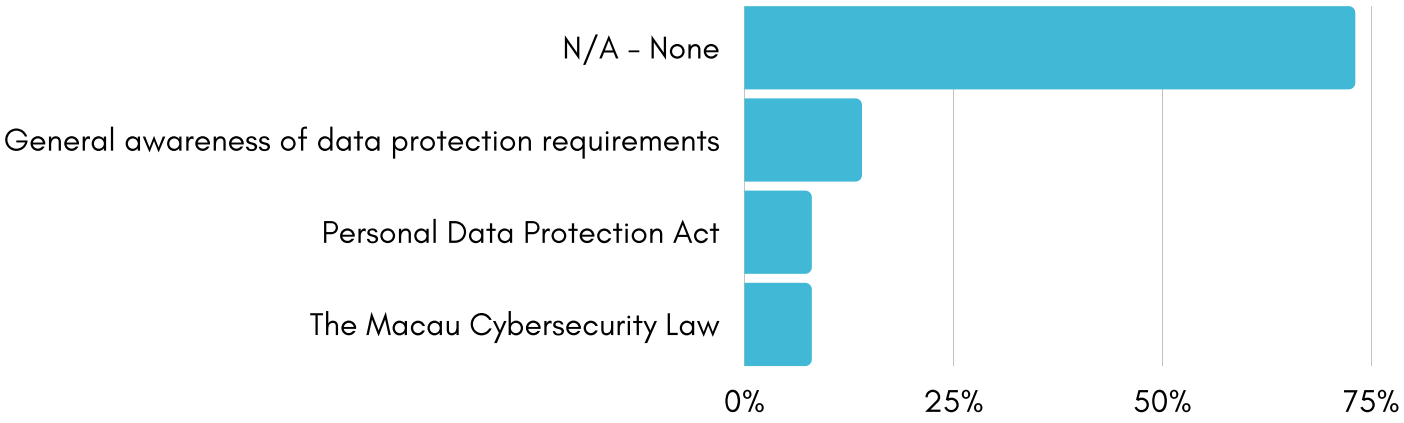
In Macau, the Personal Data Protection Act (PDPA) is the main legal instrument that is relevant for the local civil society organisations to ensure the protection of the personal data of their service clients. Organisations are made aware of the significance of the PDPA through guidelines and educational sessions prepared by the Office for Personal Data Protection (GPDP).

While most (73%) of the organisations were not able to name the specific compliance regulations, a few (i.e., 8%) were able to identify the Personal Data Protection Act and the Macau Cybersecurity Law. A further small fraction (i.e., 14%) of the organisations had a general awareness of compliance regulations related to personal data protection (see Figure 15).

Most of the organisations engaged in this research process sensitive personal data of their social service clients, who are sometimes also vulnerable members of society. Most organisations are also aware of the importance of protecting this data and of the serious risks associated with data breaches and leakage.

Our findings show that while there is a very strong sentiment of the importance of personal data protection within the organisations, measures (including, policies, procedures, processes, and tools) to ensure user data privacy and confidentiality are not effectively managed nor implemented. For example, only 38% of the organisations had written policies related to data security (see Figure 5).

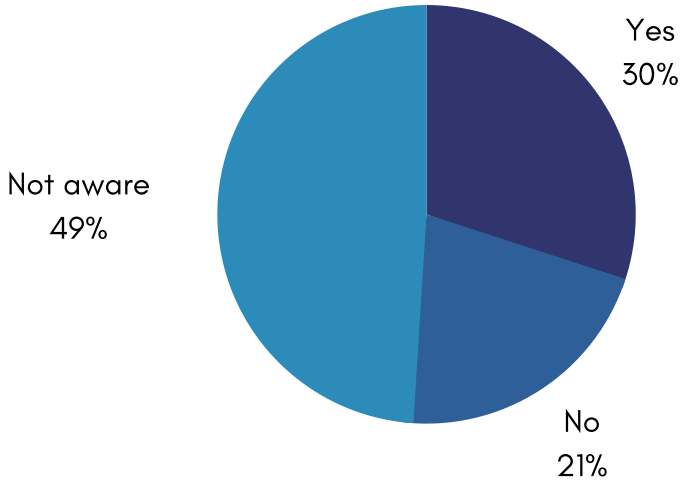
Figure 15. *Awareness of specific compliance regulations*



Indeed, concerns over data breaches and leakages as well as over the lack of awareness amongst personnel to protect service clients' personal data are widespread across the organisations interviewed. For example, respondents from some organisations have voiced out instances where some of the young and inexperienced personnel were not careful with the placement of documents with sensitive personal information in the organisations' public space. Further, organisations have also perceived risks arising from the use of certain digital technologies. For example, one organisation noted that the use of personal phones for work communication, instead of duty phones, may lead to the retention of personal information longer than needed.

As far as measures to improve compliance with the personal data protection requirements, some organisations include relevant content and guidelines in the organisations' staff handbooks and notify service users about the relevant PDPA clauses during the collection and processing of their personal data. At the operational level, some organisations are deterred from adopting cloud-based technologies, such as document processing and cloud-based storage services, to comply with the data localisation requirements as well as due to fear of potential data leakages and breaches. For some organisations, the operational measures extend to disposal of IT assets, where the organisations follow the requirements from donor organisations, such as the Social Welfare Bureau, the Macau Foundation, and the Environment Protection Bureau (DSPA) 's Electronic and Electrical Equipment Recycling Program, to ensure that the data is securely removed when the IT equipment is disposed of.

Figure 16. *Awareness of government support for compliance*



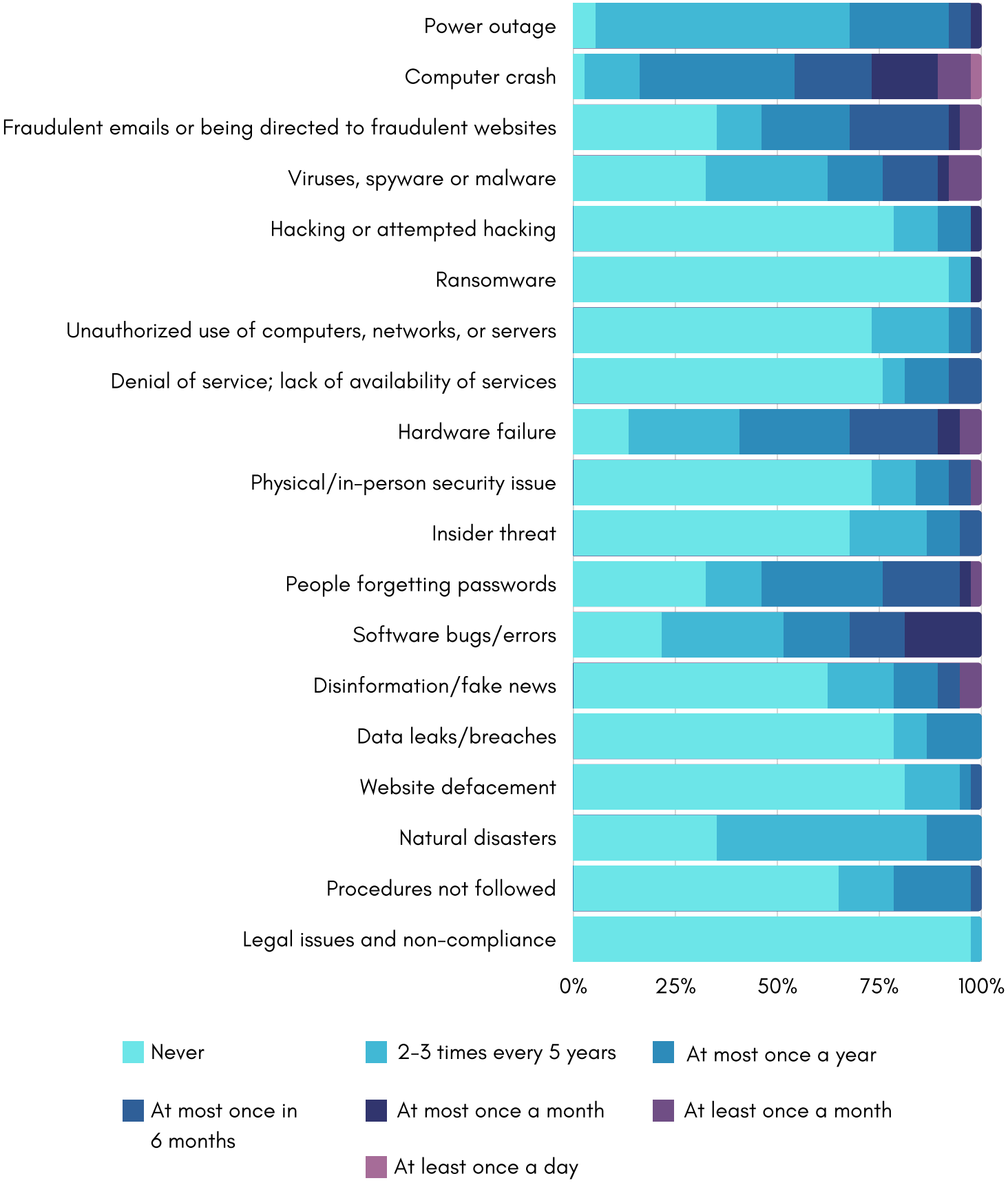
Invariably, to ensure better legal compliance, greater capacity-building and external support for the organisations are needed. In this research, only 30% of the organisations indicated that they received support from the government for compliance with cybersecurity-related regulations and legal requirements (see Figure 16). Almost half of the organisations were not aware of having received support from the government.

EXPERIENCES OF CYBER INCIDENTS

Organisations are exposed to many different types of cyber-related threats including technical, natural, socio-technical, and institutional threats. This research investigated the frequency at which the organisations experienced some of the common cyber threats (see Figure 17). It is worth noting that while the organisations would be able to accurately perceive the occurrence of some of the threats, it is also possible for the organisations to not be aware of some of the attacks that have affected them, for example, data leakages and data breaches through sophisticated data exfiltration techniques.

Out of the various cyber incidents the organisations have encountered, disinformation, password mismanagement (i.e., "people forgetting passwords"), physical security violations, hardware failure, malicious software (i.e., "viruses, spyware or malware"), software engineering attacks (i.e., "fraudulent emails or being redirected to fraudulent websites") and computer crashes are the regularly (i.e., at least once a month) experienced threats by some of the organisations. One of the organisations indicated experiencing computer crashes at least every day, while over 95% of the organisation have experienced computer crashes at some point in the life of the organisation. This is associated with the observation that hardware failures and software errors are the other commonly experienced threats (see Figure 17) and that some of the organisation use old, outdated, and obsolete systems which are less reliable (see Section 4.3).

Figure 17. *Organisations' experience of adverse cyber incidents*



While social engineering attacks are one of the regularly experienced threats by some of the organisations, there are also organisations (i.e., 35%) that have never experienced fraudulent emails or being directed to fraudulent websites. In reflecting on their experiences of some of these adverse cyber incidents, one of the respondents interviewed claimed,

> **To give an example, maybe it was because they look for short videos by themselves... Maybe they set up a group (service) for themselves, "I want to do this thing, find some short videos to see how to do it". Perhaps, they wanted to find some interesting video clips for service users to watch... or maybe to use them when performing group (services). But maybe they did not know the websites of these short films which cause problems. Yes. But like what I just said, each device has its own antivirus software, and so maybe it just happened that it could not block that (website). Yet, the data was not hacked by others, so there was no need to pay to open the file... we have not had this kind (of incident).**

The least common threats, which have never been experienced by most organisations, are the legal and non-compliance threats, ransomware, and website defacement. As far as legal compliance risks are concerned, as previously noted, since many organisations have limited awareness of the compliance requirements (see Section 4.6), organisations may overestimate their ability to comply with legal regulations, or conversely understate the requirements that they need to comply with in the operations. Further, the minimal enforcement and policing of data protection compliance might also explain the limited experience of this threat. However, as noted previously (section 4.6), most organisations also have a strong sense and a culture of prioritising personal data protection in their operations, which invariably minimises the associated risks of non-compliance.

Most of the cybersecurity threats investigated in this research (see Figure 17) are framed from the internal context of the organisations. However, cybersecurity risk exposure could emanate and cascade from the external context through partners and suppliers. One of the interview respondents noted these potential risks and the threat of inadvertent data leakage from the interaction with their suppliers, as follows:

> **Recently, in my own experience, I have seen some suppliers combined the data packets of our contract with the contracts of other departments from the company (association) when they provide their services, and they just shared the email for all of our departments to see.'**

In general, small organisations tend to have limited influence on third party stakeholders to enforce control measures that reduce the associated risks; they could, however, leverage the power of associations to attain some level of influence and to collectively enhance their cybersecurity posture (e.g., through economies of scale in cybersecurity investments) [53].

ENHANCING ORGANISATIONAL CYBER RESILIENCE

Achieving cyber resilience within organisations needs a multi-dimensional approach that engages the different functions and entities within the organisations as well as the stakeholders in the organisations' ecosystem. The literature identifies the following four factors that affect organisations' success in securing their cyberspace: budget, expertise, capability, and influence [53]. These factors have been observed to be relevant and significant towards enhancing the cyber resilience of the local organisations.

BUDGET / FINANCES

As far as the budget and availability of financial resources are concerned, our research found that, notwithstanding the current national COVID-19 pandemic expenditure control measures, most local organisations are financially stable and obtain long-term financial support from the government. However, most organisations reported not having sufficient financial resources to invest in IT-related resources and programs. This is because any further investment in cybersecurity hinges on the approval of the senior management and the government.

It was remarked and found out in this research that the senior management in CSOs are not fully aware of the importance of cybersecurity and, therefore, that support for cybersecurity investments is limited. Further, organizations are required to use their budgets in conformance with the government's funding criteria, which does not prioritise nor provide specifications on cybersecurity expenditure. For example, one of the guiding principles from the Social Welfare Bureau regarding the procurement of IT assets, in the words of the CSO staffs interviewed, is that 'the bid belongs to items with the lower price（價低者得）' - this foregrounds cost-effectiveness as opposed to security of the IT asset as the most important criterion.

EXPERTISE

It is important for organisations to have relevant expertise to enable them to improve their cyber resilience. At a basic level, there is a need for personnel to have a functional level of awareness of cybersecurity risks and the measures that they can implement to improve their cybersecurity; at a mature level, organisations need to have trained and professional cybersecurity expertise within their organisations to provide the needed support.

From the interviews, one of the key obstacles to cybersecurity that the organisations identified is this lack of awareness and expertise. The organisations have reported the need to have a team of IT experts, especially at the headquarter level, to handle requests for IT and cybersecurity support. In the absence of this support, organisations rely on their personal networks and colleagues from affiliate organisations to provide the support.

The organisations also identified the need to increase the technical awareness and training not just for IT-related personnel, but also general staff and the senior management. One of the interview respondents stated:

> **I believe that in fact, the best way is to continue to provide training to us... Not only our centre, but our entire association also needs some training to let more employees or service unit directors realise how important this matter is, and the profound impact it has.**

CAPABILITY

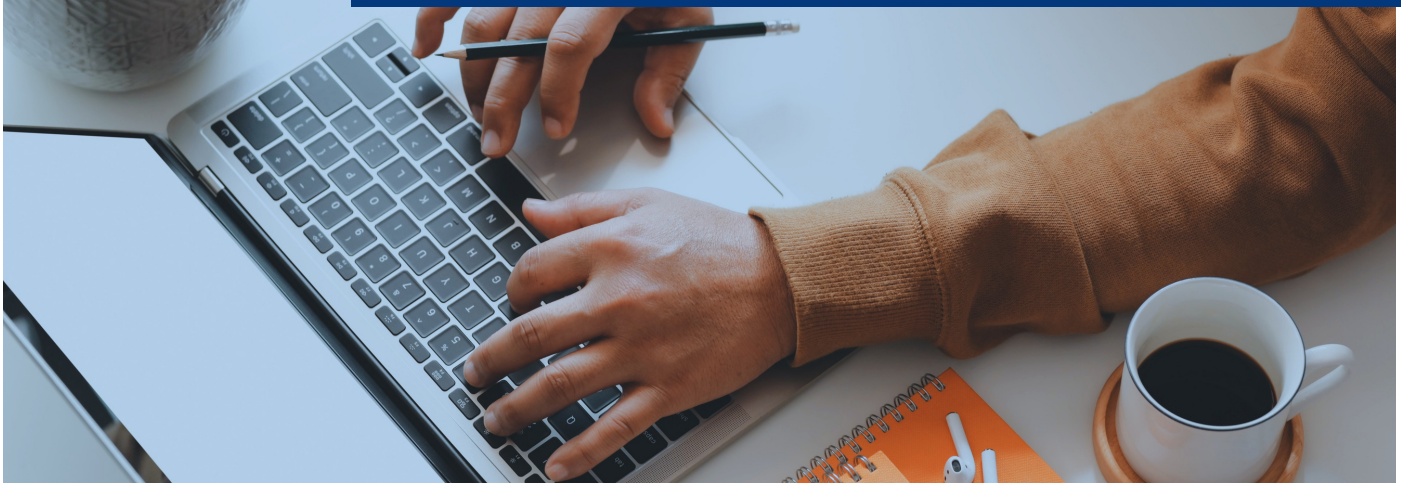
Beyond having the required finances and technical expertise, organisations need to have the capability to implement planned cyber resilience measures and controls. This is expressed in terms of factors such as organisational awareness, understanding of risks, control over changes and effective use of technology [53]. As organisations grow in the cyber resilience maturity, their understanding of their cybersecurity landscape and the associated risk exposure as well as their ability to effectively use technology also increases. Enhancing organisational cybersecurity is therefore an organisation-wide, systemic, and multi-dimensional undertaking that consequently increases the overall cybersecurity capability of organisations.

INFLUENCE

The cybersecurity posture of organisations is influenced by their interaction with external stakeholders. This is both in terms of the cascading effect of risks that emanate from the third-party stakeholders, and in terms of the support from external stakeholders to mitigate and respond to cybersecurity risks. This dynamic is prevalent for all organisations and only differs in terms of the strength and impact of the influences. In this research, the interaction of the organisations with IT service providers, service uses and clients, government stakeholders, and with affiliate organisations has been noted.

The ability for organisations to exert influence and bargaining power with third parties, such as vendors and partners is, therefore, important as it enables organisations to shape both their risk exposure and their risk mitigation strategies.

RECOMMENDATIONS



The recommendations for enhancing the cyber resilience of the local CSOs are framed for the following three key actors – CSOs, private service providers, and the government, of which the latter is typically also the main funder. In order to deliver the most appropriate support to CSOs, these three key actors are well-positioned to leverage their respective expertise and resources to contribute towards CSOs' cyber resilience.

RECOMMENDATIONS FOR CIVIL SOCIETY ORGANISATIONS

1 Undertake capacity-building for senior management

The majority of CSOs do not have sufficient and effective cybersecurity management policies, procedures, and processes in place (see Section 4.2). This reflects the CSOs' overall lack of cybersecurity capacity and their basic level of cybersecurity maturity; however, more importantly, this alludes to the senior management's limited capacity to manage organisational cyber resilience.

We recommend that CSOs undertake cyber resilience capacity-building for their senior management to enhance their understanding of organisational risk management, information technology management, and cybersecurity management; their awareness of the local cybersecurity landscape, their ability to develop and operationalise cybersecurity plans and strategies, as well as their understanding of the compliance requirements.

2 Adopt an appropriate cyber resilience management model

We recommend that CSOs roll out rigorous cybersecurity management strategies within their organisations, and make use of relevant cyber resilience management frameworks and models. Cybersecurity management, including the relevant frameworks, models, and tools, should be contextually informed – it should take into consideration CSOs' value-focused objectives, mission orientation, limited resources, and commitment to responsibly

provide services to their clients.

Part of cyber resilience management should entail formulating and identifying controls across the prepare, absorb, recover, and adapt phases of cyber resilience and across the various cybersecurity domains. For example, CSOs should ensure that data protection is mainstreamed into all data processing operations, implementing standardised documentation of digital threats, coordinating with relevant stakeholders, including other CSOs, funders, and Cybersecurity Incident Response Teams, for information sharing and dissemination, and incident handling.

3 Allocate and prioritise funding for cybersecurity

We recommend that CSOs prioritise cybersecurity investments and allocate a dedicated budget line for cybersecurity expenditure. Budgeting for cybersecurity should be in line with the organisation's overall cybersecurity management strategy, which should be informed by the risk exposure, risk tolerance, and cybersecurity objectives of the organisation.

Cybersecurity investments should be prioritised across the various organisational units, domains, and processes – for example, in capacity-building and training, human resources, and communications [54]. CSOs should prioritise cybersecurity investments that are essential to protect critical organisational assets which are most susceptible to cyber threats.

Grant-receiving CSOs should also include cybersecurity budgeting in their funding proposals.

4 Undertake targeted organisation-wide capacity-building

Organisational cybersecurity and cyber resilience are not only the responsibility of the management nor the cybersecurity personnel, although they do play a critical role. They are also the responsibility of all personnel that is engaged and interacts with the organisations. Therefore, enhancing organisational cyber resilience needs to be systemic and organisation-wide.

We recommend that CSOs undertake targeted cybersecurity capacity-building for different stakeholders, such as professional training for IT and cybersecurity personnel, basic cyber hygiene training for general personnel, and IT and cybersecurity management training for senior management. Depending on their capacity, we also recommend that CSOs undertake some level of cybersecurity awareness-raising for their critical partners (such as service clients and volunteers) who might otherwise be conduits of cybersecurity risks.

It is important for CSOs to build internal cybersecurity capacity, not only as part of organisational cybersecurity culture, but also to provide incident handling and response capability within the organisation. For core security processes and functions, internal personnel, with their understanding of the organisations' operations, mission, and context, may be best positioned to manage and respond to cybersecurity threats.

5 Leverage external support and partnerships for cybersecurity

In general, CSOs have limited human and financial resources to allocate to non-mission-core investments, such as IT and cybersecurity operations. As such, CSOs outsource non-core functions and resource-intensive operations to third-party service providers and partners, when it is cost-effective to do so. Notably, some research suggests that cybersecurity investments generate effective returns when resource-constrained organisations migrate from old and complex legacy systems to outsourced cloud applications and systems [53]. Similarly, security products requiring more dedicated resources and professional expertise to maintain could be outsourced to a managed security service provider (MSSP).

We recommend that CSOs leverage the cybersecurity support available within their ecosystem, in terms of private sector service providers and public sector cybersecurity agencies, towards enhancing their cybersecurity operations. We also recommend CSOs to leverage partnerships with affiliate and peer organisations, in terms of information and knowledge sharing, and cybersecurity incident handling support. For example, CSOs could establish a dedicated IT team at the headquarter level to offer subsidiary organisational units cybersecurity support.

RECOMMENDATIONS FOR PRIVATE SECTOR

1 Define clear service level agreements for CSOs with cybersecurity commitments

Private-sector technology providers, such as telecom services and app providers, constitute one of the key cybersecurity support for incident handling for CSOs (see Figure 13). In view of this critical role, we, therefore, recommend that the private sector stakeholders should define clear Service Level Agreements (SLAs) with commitments to specific cybersecurity targets, and to include cybersecurity support in negotiated service and support contracts for CSOs.

Moreover, SLAs are important to elevate the bargaining power of CSOs and guarantee private sector compliance with CSOs' cybersecurity goals – for example, compliance with data protection requirements when dealing with CSOs' data.

2 Provide context-sensitive and informed solutions to CSOs

Ideally, private service providers should forge long-term partnerships with the CSOs to ensure contextually informed support that is both reliable and consistent. In this manner, private companies could help CSOs prioritise investment productively, and reduce the time and cost required for seeking external technical assistance [14]. Currently, only some CSOs interviewed seek contracted support, especially for maintenance of IT equipment, whereas other organisations reach out to private service providers for ad hoc IT support.

Technical assistance from private companies needs to consider CSOs' specific context. This requires private companies to understand CSOs' goals and profile, operating context, cybersecurity threat landscape and risk exposure, and IT capabilities. We also recommend that private sector service providers should track and mitigate threats specific to their client CSOs, notify CSOs about vulnerabilities and risks, and perform regular updates and patch management [26].

RECOMMENDATIONS FOR GOVERNMENT

1 Prioritise cybersecurity in CSOs' funding instruments

As the key funder for local CSOs, the government is well-positioned to shape the cyber resilience posture and environment for CSOs.

We recommend that the government prioritises cybersecurity in funding instruments for CSOs as the key strategy for enhancing their cyber resilience. Currently, cybersecurity allocations are missing in the government's guidelines (e.g., the Social Service Facilities' Regular Funding Budget Guidelines - see Section 3.2.3) and in organisations' internal policies and guidelines. Given the limited budget available to CSOs, the government should provide funding for a list of main security items, such as operations security, personnel security, and compliance, to guide CSOs into taking appropriate cybersecurity measures.

2 Strengthen the local cybersecurity ecosystem to provide specific support for CSOs

We recommend that the government should create a more holistic cybersecurity support infrastructure for CSOs by strengthening the existing support ecosystem as well as creating new entities specific to CSOs' needs. In the context of Macau, the government could establish a civil society dedicated CERT, such as CiviCERT, or bolster the operation of existing agencies, such as CARIC and MOCERT, to include technical assistance to CSOs.

Either of the solutions points to the need for a new model for direct technical assistance to local CSOs - the support should be accessible, affordable and leverage existing assistance networks [14].

Accessibility ensures contextually informed support from practitioners with regional and subject-matter expertise, while affordable solutions lower the cost barrier for CSOs, for example, by subsidising private companies to provide discounted or free security programs to financially constrained CSOs. Also, this new model calls for maximising effective distribution of work among existing technical assistance providers available to CSOs. For example, MOCERT could enhance cooperation with CiviCERT and APCERT to support local CSOs by developing useful guidelines for CSOs.

In recognition of cybersecurity as a public good and as advancing the national development and security interests – the government should employ its power of influence to promote systemic cyber resilience and the mainstreaming of societal stakeholders' interests [55].

3 Provide capacity-building for CSOs

Due to the limited internal IT and cybersecurity expertise amongst CSOs, the government should support CSOs to promote such awareness and coordinate meaningful capacity-building. We recommend the government, especially the CSO-relevant cybersecurity entities (e.g., MOCERT and GPDP) to leverage their respective expertise and collaborate on regular awareness-raising, cybersecurity training, and capacity-building.

Invariably, capacity-building should be framed towards cyber resilience in terms of preparing for, absorbing, recovering from, and adapting to adverse cyber incidents.

Such capacity-building efforts should take into account CSOs' risk exposure as well as the local cybersecurity landscape, in terms of the availability of relevant actors and support mechanisms [13]. CSOs should also be trained on the compliance requirements that affect their organisations – for example, compliance with the data protection stipulations in the PDPA legislation.

4 Develop locally relevant cybersecurity resources for CSOs

While there are many cybersecurity resources publicly available online that CSOs can use to improve their cyber resilience, there remains a need for resources that are locally relevant and sensitive to the context and situation of local CSOs. For example, there is a need for resources that take into consideration the local cybersecurity threat landscape as well as the CSOs' situation of limited resources to guide the management and implementation of cybersecurity measures.

We recommend the government to develop actionable general guidelines that capture the needs, practices, and context of the organisations. By incorporating existing mature cyber resilience approaches and frameworks, such as the NIST Cybersecurity Framework or the CIS controls, the security guidelines should empower the CSOs to make informed decisions towards better management of cyber resilience. For example, our interview findings show that the organisations' policies on procurement and development of IT assets do not take into consideration digital security needs, and that their policies on the disposal of IT assets follow different guidelines from various donor entities (see Section 4.3). We recommend the government to develop standardised cybersecurity guidelines for CSOs and the external stakeholders they engage with. Further, the government, especially the GPDP, could refer to existing civil society cybersecurity toolkits available globally, such as Security in-a-Box toolkit, when developing accessible and actionable guidelines for the general CSOs' personnel.

Beyond guidelines and toolkits, there is an opportunity for the government to support the development of local technology solutions that improve the cyber resilience of CSOs. For example, with data localisation stipulations within the PDPA and the effectiveness of cloud storage solutions for data backup, local CSOs would benefit from local cloud storage services towards enhanced cyber resilience.

5 Strengthen cybersecurity threat intelligence research and communication

Given the limited availability of data and reports on CSOs' cybersecurity posture in Macau, we recommend the government to support research and analysis focused on the local cybersecurity threat landscape. This should involve developing the profiles of threat actors and the cyber-attack methods they employ, the technical and operational cybersecurity practices of CSOs, as well as barriers to CSOs' adoption of digital security tools and practices. Subsequently, this information could be shared with CSOs and relevant support networks, such as their technical assistance providers, to develop better, coordinated preparation and mitigation strategies against any future cyber threats.

CONCLUSION

As digital technologies have become integral to the effective functioning of societies worldwide, the risks associated with the various adverse cyber incidents have also become inevitable. Civil Society Organisations (CSOs) increasingly employ digital technologies to provide critical services to citizens, including vulnerable population groups. However, the adoption of these technology has the potential to cause harm and have negative impacts on the organisations. Compared to the public and private stakeholders, CSOs remain in a precarious and vulnerable cyber resilience position. They are ill-prepared to deal with adverse cyber incidents mainly because they have limited resources and lack the technical capability for managing their cyber resilience.

This report recommends that governments, CSOs, and private service providers coordinate capacity-building, knowledge-sharing, and cybersecurity resourcing, and undertake meaningful partnerships towards enhancing not only CSOs' cyber resilience but overall societal cyber resilience.

The report echoes the core "leave no one behind" principle of the United Nations Sustainable Development Goals to ensure that no civil society organisation is left behind in cybersecurity and cyber resilience.

REFERENCES

[1] The Global Risks Report 2021, 16th ed. World Economic Forum, 2021. [Online]. Available: http://wef.ch/risks2021

[2] D. M. Cook, "Mitigating Cyber-Threats Through Public-Private Partnerships: Low Cost Governance with High-Impact Returns," Aug. 2010. [Online]. Available: https://ro.ecu.edu.au/icr/3

[3] "Global NGO Technology Report 2019," Sep. 2019. Accessed: Mar. 22, 2021. [Online]. Available: https://funraise.org/techreport

[4] Y. Hasenfeld and B. Gidron, "Understanding multi-purpose hybrid voluntary organizations: The contributions of theories on civil society, social movements and non-profit organizations," Journal of Civil Society, vol. 1, no. 2, pp. 97-112, Sep. 2005, doi: 10.1080/17448680500337350.

[5] "Overview," The World Bank. https://www.worldbank.org/en/about/partners/civil-society/overview (accessed Mar. 22, 2021).

[6] J. E. Montalvan Castilla and C. Pursiainen, "Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not?," Journal of Civil Society, vol. 15, no. 4, pp. 392-411, Oct. 2019, doi: 10.1080/17448689.2019.1672288.

[7] R. Hulshof-Schmidt, "The 10th Annual Nonprofit Technology Staffing and Investments Report," May 2017.

[8] D. V. Gioe, M. S. Goodman, and A. Wanless, "Rebalancing cybersecurity imperatives: patching the social layer," Journal of Cyber Policy, vol. 4, no. 1, pp. 117-137, Jan. 2019, doi: 10.1080/23738871.2019.1604780.

[9] S. Brooks, "Defending Politically Vulnerable Organizations Online," Jul. 2018. Accessed: Mar. 22, 2021. [Online]. Available: https://cltc.berkeley.edu/defendingpvos/

[10] H. Whitehead, "Over a quarter of charities experienced cyber attacks last year," Civil Society Media Limited, Mar. 26, 2020. https://www.civilsociety.co.uk/news/over-a-quarter-of-charities-experienced-cyber-attacks-last-year.html (accessed Mar. 22, 2021).

[11] R. Root, "COVID-19 brings wave of cyberattacks against NGOs," Devex, Apr. 13, 2020. https://www.devex.com/news/covid-19-brings-wave-of-cyberattacks-against-ngos-96934 (accessed Mar. 22, 2021).

[12] "2021 Nonprofit Cybersecurity Incident Report," Feb. 2021. Accessed: Mar. 22, 2021. [Online]. Available: https://communityit.com/2021-nonprofit-cybersecurity-incident-download/

[13] P. K. Jagalur, P. L. Levin, K. Brittain, M. Dubinsky, K. Landau-Jagalur, and C. Lathrop, Cybersecurity for Civil Society. IEEE International Symposium on Technology and Society (ISTAS) , 2018. doi: 10.1109/ISTAS.2018.8638270.

[14] S. Brooks, "Digital Safety Technical Assistance at Scale," Jun. 2020. Accessed: Mar. 22, 2021. [Online]. Available: https://cltc.berkeley.edu/security-at-scale/

[15] "About DDP," Digital Defenders Partnership. https://www.digitaldefenders.org/ (accessed Mar. 26, 2021).

[16] R. Hulshof-Schmidt, "The 10th Annual Nonprofit Technology Staffing and Investments Report," May 2017. Accessed: Mar. 22, 2021. [Online]. Available: https://www.nten.org/wp-content/uploads/2019/11/2017-Nonprofit-Technology-Staffing-and-Investments-Report_updated-2019.pdf

[17] "2017 Not-for-Profit Governance and Financial Management Survey," New York, Dec. 2017. Accessed: Mar. 22, 2021. [Online]. Available: https://www.cohnreznick.com/insights/2017-not-for-profit-governance-financial-management-survey

[18] V. Franz, B. Hayes, and L. Hannah, "Civil Society Organizations and General Data Protection Regulation Compliance," 2020.

[19] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," Decision Sciences Journal, vol. 43, no. 4, pp. 615-660, 2012.

[20] K. Huang and K. Pearlson, "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture," in 52nd Hawaii International Conference on System Sciences, 2019, pp. 6398-6407. [Online]. Available: https://hdl.handle.net/10125/60074

[21] M. Daud, R. Rasiah, M. George, D. Asirvatham, and G. Thangiah, "BRIDGING THE GAP BETWEEN ORGANISATIONAL PRACTICES AND CYBER SECURITY COMPLIANCE: CAN COOPERATION PROMOTE COMPLIANCE IN ORGANISATIONS?," International Journal of Business and Society, vol. 19, no. 1, pp. 161-180, 2018.

[22] S. Mierzwa and J. Scott, "Cybersecurity in Non-Profit and Non-Governmental Organizations," Feb. 2017. [Online]. Available: www.icitech.org

[23] N. Samarin, A. Frik, S. Brooks, C. Cheshire, and S. Egelman, "Surveying Vulnerable Populations: A Case Study of Civil Society Organizations," CHI 2020 Networked Privacy Workshop Position Papers, Mar. 2020, [Online]. Available: http://arxiv.org/abs/2003.08580

[24] A. Jezard, "Who and what is 'civil society?,'" World Economic Forum, Apr. 23, 2018. https://www.weforum.org/agenda/2018/04/what-is-civil-society/ (accessed Mar. 22, 2021).

[25] S. Brechenmacher, T. Carothers, and R. Youngs, "Civil Society and the Coronavirus: Dynamism Despite Disruption," Carnegie Endowment For International Peace, Apr. 21, 2020. https://carnegieendowment.org/2020/04/21/civil-society-and-coronavirus-dynamism-despite-disruption-pub-81592 (accessed Mar. 22, 2021).

[26] R. J. Deibert, "Communities @ Risk: Targeted Digital Threats Against Civil Society," Citizen Lab, no. 48, Nov. 2014, Accessed: Mar. 22, 2021. [Online]. Available: https://targetedthreats.net/

[27] "Microsoft Digital Defense Report," Sep. 2020. Accessed: Mar. 22, 2021. [Online]. Available: https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf

REFERENCES

[28] M. Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," Science and Engineering Ethics, vol. 20, no. 3, pp. 701–715, 2014, doi: 10.1007/s11948-014-9551-y.

[29] L. Maschmeyer, R. J. Deibert, and J. R. Lindsay, "A tale of two cybers – how threat reporting by cybersecurity firms systematically underrepresents threats to civil society," Journal of Information Technology and Politics, vol. 18, no. 1, pp. 1–20, 2021, doi: 10.1080/19331681.2020.1776658.

[30] "SolarWinds Breach: Considerations for Cyberpeace," The CyberPeace Institute, Dec. 17, 2020. https://cyberpeaceinstitute.org/news/solarwinds-breach-considerations-for-cyberpeace/ (accessed Mar. 22, 2021).

[31] "About CiviCERT." https://www.civicert.org/about/ (accessed Apr. 26, 2021).

[32] "DFAK / About." https://digitalfirstaid.org/en/index.html (accessed Apr. 26, 2021).

[33] "APCERT_Annual_Report_2019_reading," 2019.

[34] A. Seng et al., 2020 Internet Usage Trends in Macao. Macao Association for Internet Research, 2020. [Online]. Available: www.macaointernetproject.net

[35] N. Moura, "Cybersecurity risks for local organisations have increased considerably during pandemic – Company," Macau Business, Apr. 21, 2021. https://www.macaubusiness.com/cybersecurity-risks-for-local-organisations-have-increased-considerably-during-pandemic-company/ (accessed Apr. 26, 2021).

[36] N. Moura, "Health Bureau claims to have beent he target of a cyber-attack," Macau Business, Jan. 29, 2020. https://www.macaubusiness.com/health-bureau-claims-to-have-been-the-target-of-a-cyber-attack/ (accessed Mar. 22, 2021).

[37] R. M. MDT, "Portuguese School IT System Hacked For Ransom," Macau Daily Times, Aug. 21, 2020. https://macaudailytimes.com.mo/portuguese-school-it-system-hacked-for-ransom.html (accessed Mar. 22, 2021).

[38] "印務局-第8/2005號法律," Aug. 22, 2005. https://bo.io.gov.mo/bo/i/2005/34/lei08_cn.asp (accessed Apr. 26, 2021).

[39] "第11/2009號法律 - 印務局," 澳門特別行政區政府印務局, Jul. 06, 2009. https://bo.io.gov.mo/bo/i/2009/27/lei11_cn.asp (accessed Apr. 26, 2021).

[40] "第13/2019號法律 - 印務局," Jun. 24, 2019. https://bo.io.gov.mo/bo/i/2019/25/lei13_cn.asp (accessed Apr. 26, 2021).

[41] "General Data Protection Regulation GDPR." https://gdpr-info.eu/ (accessed Apr. 26, 2021).

[42] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Nov. 23, 1995. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed Apr. 26, 2021).

[43] "社會服務設施定期資助撥款指引," Mar. 2019. Accessed: Mar. 22, 2021. [Online]. Available: https://www.ias.gov.mo/wp-content/uploads/2017/11/2019-03-26_124618_97.pdf

[44] P. Cortés and L. Machado, "Amendments to Macau's law combating cyber crime," International Bar Association, Jul. 20, 2020. https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=66791638-131e-4bac-8077-4301eb0d6fcf (accessed Mar. 22, 2021).

[45] "What is GDPR, the EU's new data protection law?," GDPR.eu. https://gdpr.eu/what-is-gdpr/ (accessed Mar. 22, 2021).

[46] "認識歐盟《資料保護總規章》." 個人資料保護辦公室, May 25, 2018. Accessed: Mar. 22, 2021. [Online]. Available: https://www.gpdp.gov.mo/uploadfile/2018/0511/20180511052147496.pdf

[47] "Welcome to MOCERT," Macau Computer Emergency Response Team Coordination Centre (MOCERT).

[48] "全部," 澳門特別行政區印務局. https://www.io.gov.mo/cn/entities/priv/cat/allassoc (accessed Mar. 22, 2021).

[49] "Macao's Certification Training Session on Certified Information Security Professionals (CISP) Kicked Off ," The Science and Technology Development Fund (FDCT), Oct. 15, 2019. https://www.fdct.gov.mo/en/fund_information/article/k1so8out.html (accessed Mar. 22, 2021).

[50] "2019 Cybersecurity Technology Exchange Tour," The Science and Technology Development Fund (FDCT), Nov. 19, 2019. https://www.fdct.gov.mo/en/fund_information/article/k359fez4.html (accessed Mar. 22, 2021).

[51] N. Moura, "Local security authorities carry out first-ever large scale cybersecurity attack drill," Macau Business, Dec. 11, 2020. https://www.macaubusiness.com/local-security-authorities-carry-out-first-ever-large-scale-cybersecurity-attack-drill/ (accessed Mar. 22, 2021).

[52] N. Moura, "Challenges remain for local companies when improving cybersecurity protection – Deloitte," Macau Business, Aug. 08, 2020. https://www.macaubusiness.com/challenges-remain-for-local-companies-when-improving-cybersecurity-protection-deloitte/ (accessed Mar. 22, 2021).

[53] "The Security Bottom Line: How much security is enough?," Oct. 2019. Accessed: Mar. 22, 2021. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/se/2019/10/Collateral/security-bottom-line-cybersecurity.pdf

[54] E. Christian and S. Anthony, "Enhancing Digital Security Awareness for CSOs in Africa," WACSeries Op-Ed No.8 – October 2019 , Oct. 2019.

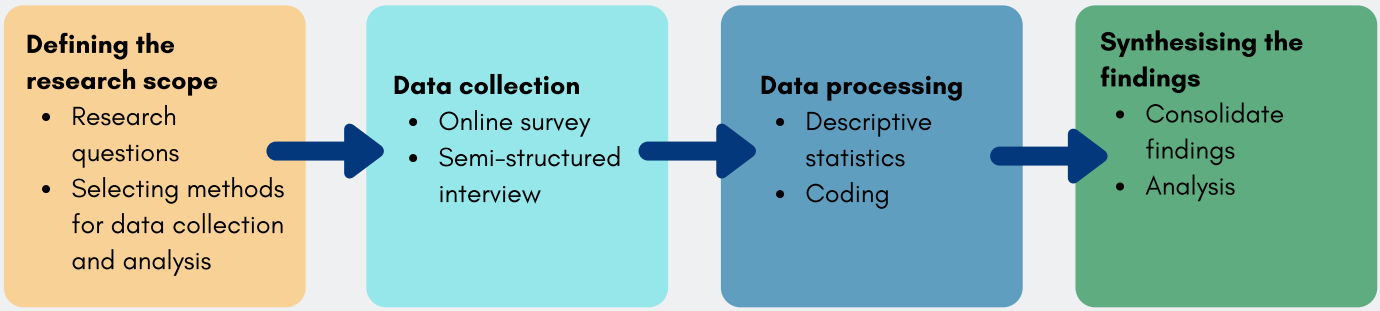
[55] S. Weber, "Coercion in cybersecurity: What public health models reveal," Journal of Cybersecurity, vol. 3, no. 3, pp. 173–183, May 2017, doi: 10.1093/cybsec/tyx005.

APPENDIX

METHODOLOGY

In this research, we use the grounded theory approach to capture the essential themes arising from the data collection activities and address the research subjects' ecology. In doing so, we apply a four-step research protocol (see Figure 1).

Figure 1. *Research protocol*



DEFINING THE SCOPE OF RESEARCH

In our data collection quest, we are interested in understanding the current state, desired outcomes, and requirements of Civil Society Organizations (CSOs) in Macau SAR in terms of their organisational resilience that is supported by information and communication technologies (ICTs). As a guide to achieving this study's goal, we define three research questions:

- RQ1: How do CSOs define resilience and what role do ICTs play in supporting their resilient functioning?
- RQ2: What are the risks that shape CSOs resilient functioning and what controls are in place to mitigate the risks?
- RQ3: What are the internal and external factors contributing to CSOs cyber resilience and how can they be optimised and improved?

RQ1 is intended to capture attitudes and perceptions around cybersecurity and cyber resilience, current use of ICTs in supporting organisation's functioning, and desired state of organisational resilience. RQ2 is intended to identify known and unknown risks that could affect organisation's ability to achieve its objectives, organisational risk perception, and risk management practices at their disposal. Finally, in RQ3, we seek to understand the organisation's assessment towards the likelihood and impact of different kinds of cyber incidents, incident management practices that have been

implemented, and cyber resilience interdependence within the organisation's ecosystem.

DATA COLLECTION

To answer these questions, we employ surveys and interviews as data collection methods.

Survey

The survey is intended to obtain quantitative data to inform an understanding of the organisation's profile, perceptions on cybersecurity and cyber resilience, experiences of cybersecurity incidents, and opinions on hypothetical cybersecurity scenarios. Additionally, as the survey is intended to obtain preliminary information about the organisation's cyber resilience posture, several organisational resilience management frameworks are used to inform the design of the questions.

The survey questionnaire consists of close-ended (i.e., demographic questions, dichotomous questions, multiple choice questions, rating scale questions, semantic differential questions, staple scale questions, and matrix table questions) and open-ended questions. It is accessible online to the managers/directors of organisations involved in this study.

Interview

Interviews are conducted to better understand findings from the survey and explore in depth perceptions, knowledge, and experiences of the respondent' organisation with regard to the research questions. We employ semi-structured interview to allow opportunities for more detailed inquiry into topics that arise during researcher-respondent interactions and discovery of new information. The questions are open-ended. The interviews are conducted with the managers/directors of organisations involved in this study.

DATA PROCESSING

Descriptive statistics

A total of 37 responses is obtained through the online survey. Survey data is processed to obtain descriptive statistics which are then used to derive a conclusion regarding the current cyber resilience posture of respondents, their risk landscape, and organisational situational awareness.

Coding

The interviews are conducted to a total of 22 respondents. A combination of inductive / deductive approach is employed in the development of the codebook used to code the interview data. An initial codebook is developed based on a sample of interview transcripts and existing organisational cyber resilience management frameworks. The codebook undergoes several iterations through inductive process before the final version is used to code all the interview data.

UNITED NATIONS UNIVERSITY
Institute in Macau

ISBN: 978-92-808-9131-7