

Raising Awareness for Cyber-Security (RACS)

Assessing cyber-
security readiness with
SME's and VO's

OCTOBER 2019
Malta IT Law Association

Malta Information Technology Law Association (MITLA)

www.mitla.org.mt

info@mitla.org.mt

© Malta Information Technology Law Association (MITLA), 2019 Reuse is authorised provided the source is acknowledged. For any use of quoted or referenced material, permission must be sought directly from the copyright holder

TABLE OF CONTENTS

Table of Contents

1. ACRONYMS	8
2. EXECUTIVE SUMMARY	10
Section A	13
Overview	13
3. INTRODUCTION.....	14
4. METHODOLOGY.....	17
4.1. Overview	18
4.2. Approach	19
4.3. Phase 1 – Preparatory Stage	19
4.4. Phase 2 – Fieldwork phase	27
4.5. Phase 3 – Analysis and reporting	27
Section B	28
Research Results.....	28
5. PROFILING MALTESE BUSINESSES AND VO_s	29
5.1. Brief	30
5.2. Online Exposure	30
5.3. Use of personal devices.....	31
5.4. Use of externally hosted web services (Cloud Computing)	32
6. AWARENESS AND ATTITUDES	34
6.1. Brief	35
6.2. Perceived importance of cyber security.....	35
6.3. Main drivers of cyber security.....	38
6.3.1. Organisations which held sensitive personal information	38
6.3.2. Being exposed to a cyber security attack.....	39
6.3.3. Changes in legislations and compliance	39

6.4.	Sources of Information	39
6.4.1.	Where organisations and VOs get their information or guidance	40
6.4.2.	Entities that did not seek further advice	41
6.5.	The General Data Protection Regulation.....	42
6.6.	Attitudes and behaviours	43
7.	<i>APPROACHES TO CYBER SECURITY.....</i>	45
7.1.	Brief	46
7.2.	Cyber security policies and its management within businesses.....	46
7.2.1.	Policies	46
7.2.2.	Cyber security Management.....	47
7.3.	Actions taken to prevent or minimise cyber security attacks	48
7.4.	Staff Training on Cyber security.....	49
7.4.1.	Training attended	50
7.4.2.	Inclination to attend training	50
7.4.3.	Best way to receive training	51
7.4.4.	Participation in training	51
7.5.	Use of external providers.....	52
8.	<i>The impact and incidence of breaches or attacks</i>	54
8.1.	Brief	55
8.2.	Experience of breaches or attacks	55
8.3.	Types of breaches or attacks experienced by businesses and NGO's.....	55
8.4.	Number of breaches or attacks experienced amongst businesses and NGO	57
8.5.	Who would be contacted if a breach was experienced	58
9.	<i>COMPARISONS TO EU STUDIES.....</i>	60
9.1.	Brief	61
9.2.	Comparison of Maltese businesses and VOs with the EU population	61
9.2.1.	Overview	61
9.2.2.	Awareness of the risks of cybercrime	62
9.2.3.	Attitudes to cyber security	62
9.3.	Comparison of Maltese businesses and VOs with the EU businesses.....	64
9.3.1.	ICT security policies	65

9.3.2.	Cyber security changes with the implementation of GDPR in 2018.....	68
9.3.3.	Comparison of Current cyber threats and vulnerability landscape	70
9.4.	Factor/s inhibiting cyber security.....	74
9.4.1.	Awareness at a board level	75
9.4.2.	Skills and training on cyber security	77
9.4.3.	Cyber security spending	78
9.4.4.	Technologies vulnerabilities.....	78
9.4.5.	Trust in sharing information.....	79
9.4.6.	Incident response plans	80
9.4.7.	Organisational designs	81
10.	<i>READINESS INDEX FOR MICROENTERPRISES AND VOs.....</i>	83
10.1.	Brief.....	84
10.2.	Methodology	84
10.3.	Microenterprises readiness Index	88
10.3.1.	Overall	88
10.3.2.	A review of responses by the various criteria.....	89
10.4.	Voluntary Organisations readiness Index.....	92
10.4.1.	Overall	92
10.4.2.	A review of responses by the various criteria.....	92
10.5.	Benchmarking results	95
11.	<i>Conclusions & Recommendations</i>	96
11.1.	Conclusions.....	97
11.1.1.	IT Dependability.....	97
11.1.2.	Awareness	97
11.1.3.	Main drivers of cyber security	98
11.1.4.	Seek information.....	98
11.1.5.	Have policies in place.....	98
11.1.6.	Training.....	99
11.1.7.	Breaches or attacks.....	99
11.1.8.	Trustworthiness	99
11.1.9.	Main threats.....	99
11.1.10.	GDPR	100
11.1.11.	Readiness Index	100
11.2.	Recommendations	100
Annex 1 - Profiling Malta's businesses and VOs		105

1.ACRONYMS

BYOD	Bring Your Own Device
CEO	Chief Executive Officer
DDoS	Distributed Denial of Service
DoS	Denial of Service
EESC	European Economic and Social Committee
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IRP	Incident response plan
IT	Information Technology
MITLA	Malta IT Law Association
NGO	Non-Governmental Organisation
RACS	Raising Awareness on Cyber Security
SME	Small and Medium sized Enterprise
UK	United Kingdom
VO	Voluntary Organisation
WP	Work Package

2.EXECUTIVE SUMMARY

This report presents the findings for MITLA's call for proposals that sought to determine where small and medium sized enterprises (SMEs) and voluntary organisations stand on cyber security and cyber threats.

To successfully meet the pre-set requisites EMCS underwent a three-phased research approach that incorporated:

1. Desk research
2. Face-to-face in-depth interviews and
3. The distribution of questionnaires.

The main findings being:

IT Dependability Local businesses' dependability on digital communication or services relates primarily to email (88%), social media pages (77%) website/blog (73%) and online banking (72%), with social media and emails being the primary digital services utilised by local voluntary organisations (87% and 48% respectively). Furthermore, 67% of microenterprises and 87% of VOs tend to use externally hosted web services, with such high incidence possibly attributable to such organisations' limited financial resources and their overall positive perception and their trust in the security provision of such services. Also, the research has evidenced that local organisation have more trust in data collected and stored by third parties. This contrasts with the general perception among Europeans (65% of local businesses trust as opposed to 30% of Europeans)

Awareness Awareness levels among local businesses varied by sector, with the overall percentage standing at 66%. Such score is comparable to the EU population average that was 50%. Local VOs perceive themselves to be more aware (67%).

Inhibiting Factors Factors that are inhibiting organisations from prioritising cyber security are:

- The need for flexibility – in terms of people and operation processes
- Lack of awareness
- Time constraints and
- General lack of interest in the subject (this could be linked to the lack of awareness)

Main drivers The main drivers to cyber security relate to:

- Having sensitive data
- Exposure to cyber security attacks
- Legal requirements that impose action

Training

On average, one in five businesses indicated to have gone some form of training on cyber security. Furthermore, 71% of VOs and 51% of businesses indicated to be willing to undergo training on the topic in question in the future. That said, the primary restricting factors – limited financial and human resources – coupled with time constraints ought to be kept in mind when devising appropriate course/s.

Readiness Index


Microenterprises have a readiness index of 49% (in line with the UK) fall within the developing stage. This implies that overall local microenterprises have achieved a good level of readiness across several areas, but still have gaps and threats to address if they are to become a truly Cyber Ready business.

Voluntary organisations, with an overall readiness index of 54% also fall within the developing stage.

Section A

Overview

3. INTRODUCTION



The Malta IT Law Association (MITLA) embarked on a project - Raising Awareness on Cyber Security (RACS) - funded through the Voluntary Organisations Project Scheme managed by the Malta Council for the Voluntary Sector on behalf of Parliamentary Secretary for Youth, Sports and Voluntary Organisations within the Ministry for Education and Employment”.

Malta is increasingly dependent upon the use of Information and Communications Technology (ICT), to the extent that its disruption may affect service, business and potentially, everyday life.

Malta Cyber security Strategy 2016.

The Raising Awareness on Cyber Security (RACS) project seeks to determine where SMEs and Voluntary Organisations (VOs) in Malta stand on cyber security and cyber threats.

More specifically, the study comprises three (3) phases, that may be broadly segmented as follows:

- Phase 1 - Discovery Phase;
- Phase 2 - Research Phase; and
- Phase 3 - Dissemination

Such study was deemed of essence in view of the growing risk of cyberattacks, with European studies evidencing that most European companies are still unprepared and unaware of the risk. Furthermore, a recent study commissioned by the European Economic and Social Committee¹ highlighted how small and medium-sized companies (SMEs) are the most exposed, often in view of their budget constraints that limited their investment in cyber security. Furthermore, almost 70% of European companies do not understand the extent of their exposure to cyber risks².

The level of investment in cyber security overall is insufficient. Most businesses do not realise its importance until after experiencing a security breach³.

The above further highlights how imperative it is to attain “a better understanding of cyber-security practices and regulations, also amongst local businesses and VOs in the light of the Maltese context, where, due to local geographic proportions, the vast majority of local businesses are micro-enterprises or SMEs, with small or non-existent internal IT departments.”

¹ Cyber security – Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. European Economic and Social Committee (2018)

² <https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study>

In line with the above, this report presents the findings of the 2nd phase (referred to as WP2 in the call for proposals) that sought to investigate the level of awareness on cybercrime amongst VOs and businesses in Malta and gauge measures implemented by said businesses to mitigate security breaches. Furthermore, in line with the call, a situational analysis was conducted "*through the involvement and interviewing of local stakeholders*" among other endeavours.

4.METHODOLOGY

4.1. Overview

The methodology adopted for this study sought to address the expected deliverables relating to WP2

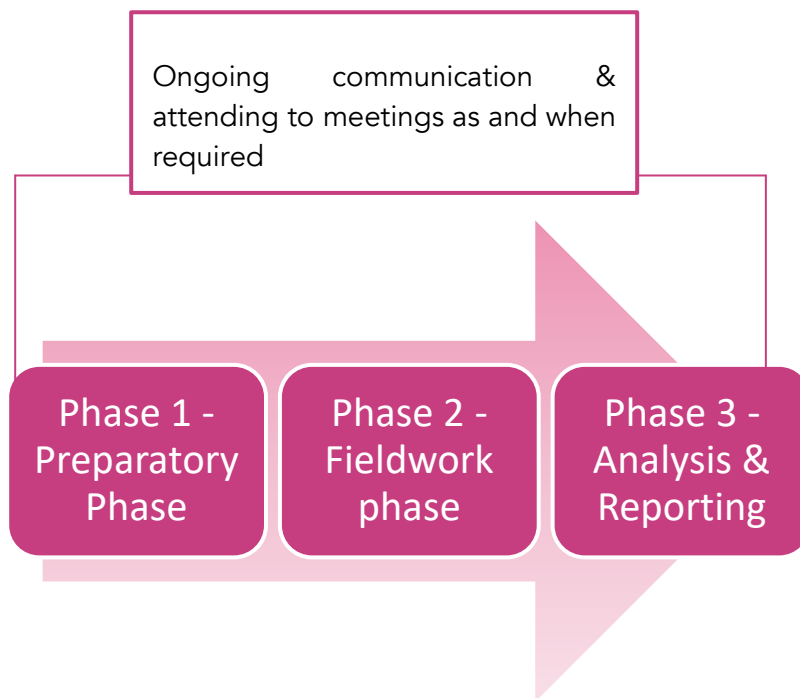


as identified in the call for quotations, that related to:

In line with the above, EMCS kept an ongoing communication with the client and participated in all meetings and project management sessions as necessary with MITLA.

4.2. Approach

In order to meet the above indicated activities and attain meaningful data to MITLA in its attainment of both the specific and overall objectives, of which WP2 is a component of, EMCS undertook a three-phased approach:



4.3. Phase 1 – Preparatory Stage

This phase included the following efforts:

- Kick-off meeting

In line with normal procedures a kick-off meeting was set up to kick start the project. All material of relevance to the successful conduct of this study was passed on to EMCS. During such meeting EMCS went through the various deliverables and time frames presented in its proposal so as to ensure that all is clear. The sampling methodology was also explained, discussed and agreed to. Furthermore, communication flow and contact persons were determined and agreed to.

- Data review & desk research

During the first 4 weeks of the project EMCS experts devoted their energies to identifying the salient points from WP1 and other aspects that were deemed of relevance to form an integral part of the questionnaires that was eventually distributed to the target audience.

Furthermore, through desk research EMCS experts collated data relating to similar researches conducted internationally. Such efforts aided in:

- I. The drawing up of the questionnaire;
- II. Drawing comparisons from the data collated pertaining to the readiness index for micro-enterprises and VOs in Malta to EU studies and readiness-indices presently available.

- Involvement with MITLA team involved in the preparation of WP1

In view of the importance of ensuring that the questionnaire truly encapsulates the information required, and notwithstanding the stringent time frames presented, EMCS communicated with MITLA prior to the finalisation of the questionnaire. Furthermore, EMCS consulted with its IT experts.

- Draw up the questionnaire

Following the above indicated activities EMCS draw up 2 distinct questionnaires – one for the face to face interviews, and another questionnaire to collate quantitative information through the utilisation of telephone interviews and online questionnaires.

- Testing of the questionnaires

In line with our normal procedures that aid in the provision of quality and meaningful data, the drafted questionnaires were tested prior to launch. This phase enabled us to ensure that the questions being proposed were being understood by the target audience, and equally important, that the data collated from such questions were meaningful in terms of enabling us to determine: the target audiences' awareness levels, current procedures undertaken in relation to cyber security, and also enabled us to draw up a readiness index.

- Draw up the sample to be targeted (for both quantitative and qualitative research)

Quantitative data collection

The target audience was segmented into 2:

- I. Micro enterprises, and
- II. Voluntary organisations.

Micro Enterprises

The importance of micro enterprises at both local and EU level cannot be undermined. The desk research (Eurostat 2017) evidenced that micro entities represent the vast majority of enterprises in the EU, as highlighted in the table below.

	Micro	Small	Medium	SME	Large	Total
NUMBER OF ENTERPRISES						
In Thousands	22,232	1,392	225	23,849	45	23,894
In % Total of enterprise population	93.0%	5.8%	0.9%	99.8%	0.2%	100.0%
NUMBER OF PERSONS EMPLOYED						
In Thousands	41,669	27,982	23,398	93,049	46,665	139,7141
In % of Total Employment	29.8%	20.0%	16.7%	66.6%	33.4%	100.0%
VALUE ADDED						
In EUR Trillion	1,482	1,260	1,288	4,030	3,065	7,095
In % of Total Value Added	20.9%	17.8%	18.2%	56.8%	43.2%	100.0%
Source: Eurostat, National Statistical Offices, and DIW Econ Note: Date as of 30 June 2017. Totals may differ from sum of components due to rounding.						

The situation is also reflected locally with micro enterprises accounting for 93.4% of all enterprises in Malta and employing just under 42,500 individuals (Eurostat – table below refers).

The above information is of relevance as it enabled us to compare results collated with similar international studies on cyber-crime

Class size	Number of enterprises			Number of persons employed			Value added		
	Malta		EU-28	Malta		EU-28	Malta		EU-28
	Number	Share	Share	Number	Share	Share	Billion €	Share	Share
Micro	26 808	93.4 %	93.0 %	42 497	31.5 %	29.8 %	1.7	35.9 %	20.9 %
Small	1 497	5.2 %	5.8 %	31 384	23.3 %	20.0 %	1.2	25.5 %	17.8 %
Medium-sized	331	1.2 %	0.9 %	33 152	24.6 %	16.7 %	1.0	20.7 %	18.2 %
SMEs	28 636	99.8 %	99.8 %	107 033	79.3 %	66.6 %	3.9	82.0 %	56.8 %
Large	60	0.2 %	0.2 %	27 866	20.7 %	33.4 %	0.8	18.0 %	43.2 %
Total	28 696	100.0 %	100.0 %	134 899	100.0 %	100.0 %	4.7	100.0 %	100.0 %

These are estimates for 2016 produced by DIW Econ, based on 2008-2014 figures from the Structural Business Statistics Database (Eurostat). The data cover the 'non-financial business economy,' which includes industry, construction, trade, and services (NACE Rev. 2 sections B to J, L, M and N), but not enterprises in agriculture, forestry and fisheries and the largely non-market service sectors such as education and health. The following size-class definitions are applied: micro firms (0-9 persons employed), small firms (10-49 persons employed), medium-sized firms (50-249 persons employed), and large firms (250+ persons employed). The advantage of using Eurostat data is that the statistics are harmonised and comparable across countries. The disadvantage is that for some countries the data may be different from those published by national authorities.

In order to collect a representative sample of the micro enterprises locally we sought to conduct 400 telephone interviews, with such sample providing a 95% confidence level and a confidence interval (margin of error) of 5%.

Furthermore, in view of the distinct realities pertaining to the various subsectors that constitute this population, the above sample was further segregated by sector of activity. In this respect we sought to follow, in so far as reasonably possible, the classification utilised by the National Statistics Office when collating data on the business community that segregates the business population into numerous categories.

For the purpose of this research we sought to target the top 13 clusters that together represented 94% of all businesses. Furthermore, the sample was initially split to represent the percentage of entities within each category (as evidenced in the table below):

Nace Code	Nace Description	% of SME on Business Registry ⁴
G	Wholesale and retail	23.20
M	Professional	11.05
F	Construction	9.60
A	Agri/ fisheries	7.03
S	Memberships, repairs, personal services	6.08
C	Manufacture	5.74
N	Admin & support	5.46
I	Accommodation, food & beverages	5.38
H	Courier services	4.50
P	Education	4.40
R	Creative arts, entertainment	4.30
L	Real estate	4.10
J	Media, IT	3.40

As commenced with the conduct of the research we were faced with the issue that certain categories comprised a higher percentage of medium sized entities rather than micro enterprises (such as the

⁴ As per 2010 –no major shift variances have been observed over the years.

construction, and education sectors). For this reason, we then amended the sample size to ensure that we collate primarily micro enterprises in line with the brief.

Voluntary Organisations

The latest available data (https://education.gov.mt/en/vo_home/Pages/vo_list.aspx) indicates that there are circa 1,100 voluntary organisations across Malta and Gozo. We sought to target a sample of 285 voluntary organisations to attain a 95% confidence level and a confidence interval (margin of error) of 5%.

Qualitative Research

A total of 30 face-to-face interviews as follows:

- 22 interviews with micro-businesses, of which 5 operate from Gozo
- 8 interviews with voluntary organisations of which 2 operate from Gozo

These interviews enabled us to substantiate data collated from the quantitative research and to probe further where necessary to attain a clearer picture of the current scenario.

The sample of entities to be interviewed was drawn up bearing in mind the variances between the different clusters and in so doing ensured that meaningful information was collated of relevance to the project deliverables.

- Prepare the necessary paperwork/ etc (comprising uploading of the questionnaire online)

The EMCS team subsequently drew up the necessary paperwork/ groundwork and uploaded the questionnaire onto our online system such that interviewers could input the data directly online.

The online system offered the added advantage that, when an entity wished to participate but had difficulty in allocating a time for the interview to be carried out, then EMCS forwarded the link to the online survey such that the individual could complete such survey independently.

In line with its normal operating practices, EMCS ensured that it abides to all the data protection regulations.

Standard procedure when contacting potential participants whereby they are notified beforehand and are given the option to opt out from the study making reference to the privacy policy of both EMCS and that of the respective client. The rights of the participants are made clear, these being:

Interviewee/respondent's rights

Under the GDPR, you have the following rights:

- to access your personal data;
- to be provided with information about how your personal data is processed;
- to have your personal data corrected;
- to have your personal data erased whenever you opt for;
- to object to or restrict how your personal data is processed;
- to have your personal data transferred to yourself or to another third-party business in certain special circumstances;
- to complain to a supervisory authority.

Furthermore, all individuals who are subject to personal data collected by MITLA and EMCS are entitled to:

- ask what information is being stored and why;
- ask how to gain access to the information;
- ask how the information is being kept up to date;
- be informed on how MITLA and EMCS is taking all the necessary steps to meet the data protection obligations.

4.4. Phase 2 – Fieldwork phase

This phase included the actual conduct of the research. This fieldwork phase included the conduct of:

- Telephone interviews;
- Face-to-face interviews; as well as
- Online data collection
- Details provided in the above section (preparatory phase)

4.5. Phase 3 – Analysis and reporting

The final phase of this study incorporated 3 interlinked phases that ultimately formed an integral part of this report, namely:

- I. Data analysis
- II. Drawing comparisons to EU studies and readiness-indices presently available; and
- III. Drawing-up a readiness index for micro-enterprises and VOs;

Section B

Research Results

5. PROFILING MALTESE BUSINESSES AND VO_s

5.1. Brief

In this section we briefly set out the businesses' and VOs exposure to cyber security risks, as well as their use of cloud computing. This was tackled by taking a look at entities' online exposure, use of personal devices for their business endeavours and the extent to which cloud computing is used.

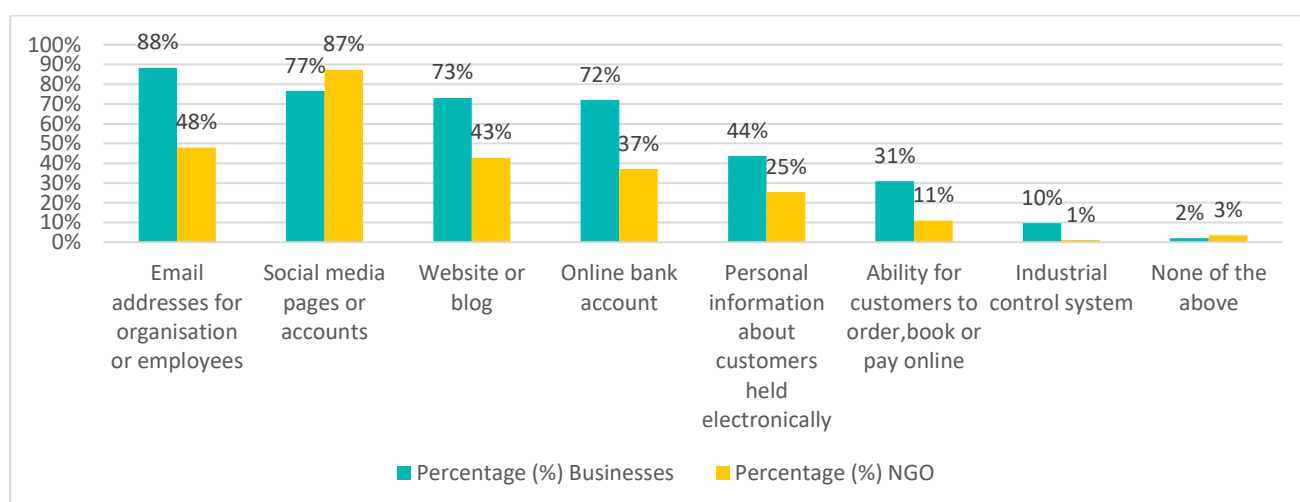
5.2. Online Exposure

The quantitative research sought to determine to what extent Maltese businesses and VOs depended on digital communication and/or services. The digital communication or services under review related to:

- Email addresses for organisation or employees,
- Social media pages or accounts,
- Website or blog, online back account,
- Personal information about customers held,
- Ability for customers to order online, book or pay online, and
- Industrial control system/s.

The findings illustrate that, by and large, all entities mentioned at least one of the above digital communication or services (98% of businesses and 97% of VOs – figure 1 overleaf). 'Email addresses for organisation or employees' and 'Social media pages or accounts' are the most common communication or services mentioned by both sectors, though varying in percentages.

Figure 1: Organisations reliance on online Services

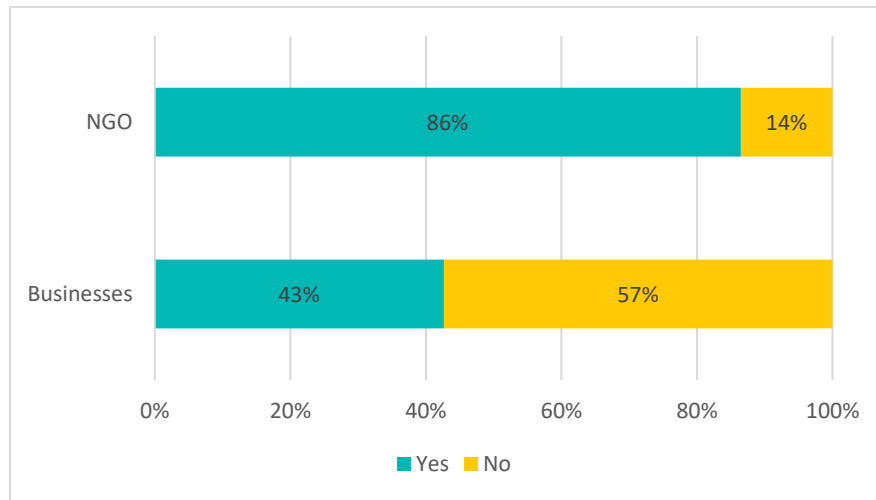


The above figure also evidences that, of the digital communication and services under review, 'social media pages or accounts' was the only one to rank higher among non-governmental organisations (VOs) than businesses.

5.3. Use of personal devices

The study highlighted that VOs were more inclined to use their own personal devices for business use than businesses did. In this respect, 86% of VOs indicated to use their own personal devices for business. Among businesses this factor stood at 43%.

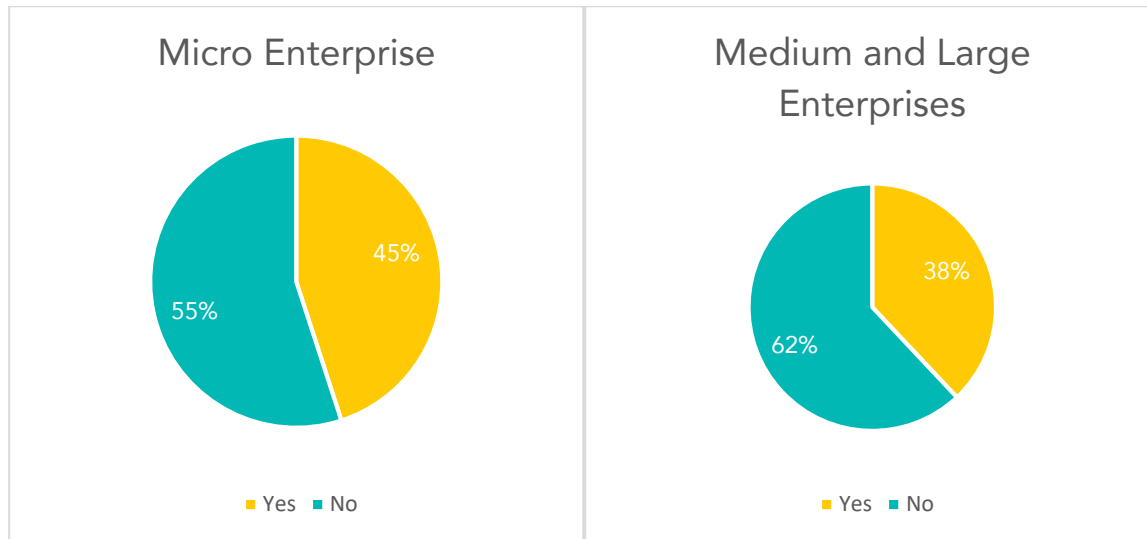
Figure 2: Bring your own device/s (BYOD) NGO vs Businesses



From the in-depth interviews carried out with VOs, the lack of financial resources was highlighted as the major reason why employees within this sector utilised their own devices, particularly their personal mobile phones. In certain instances, individuals (employees/ volunteers) within this sector indicated that they had provided financial contributions (from their personal funds) to assist their respective NGO in its operations.

A review of results by enterprise size does not evidence any significant variances (Figure 3 below) with 55% of individuals in micro enterprises indicating using their personal devices for work purposes whilst for medium and large enterprises the percentage stood at 62%.

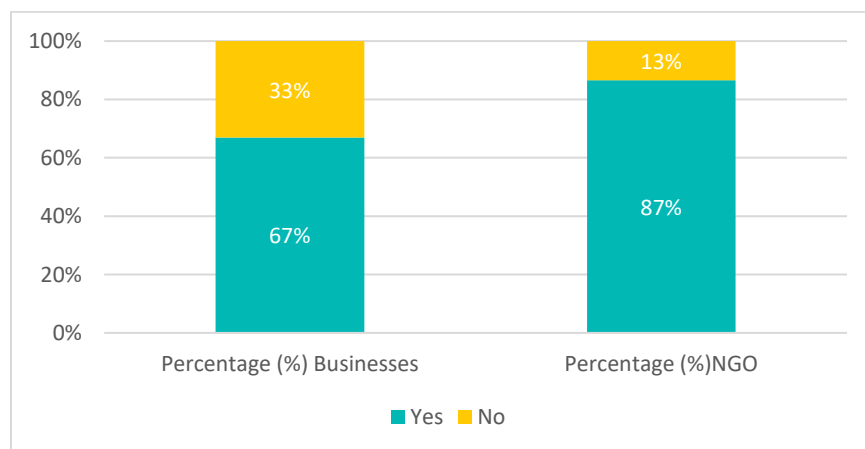
Figure 3: BYOD Micro enterprises vs Medium and Large enterprises.



5.4. Use of externally hosted web services (Cloud Computing)

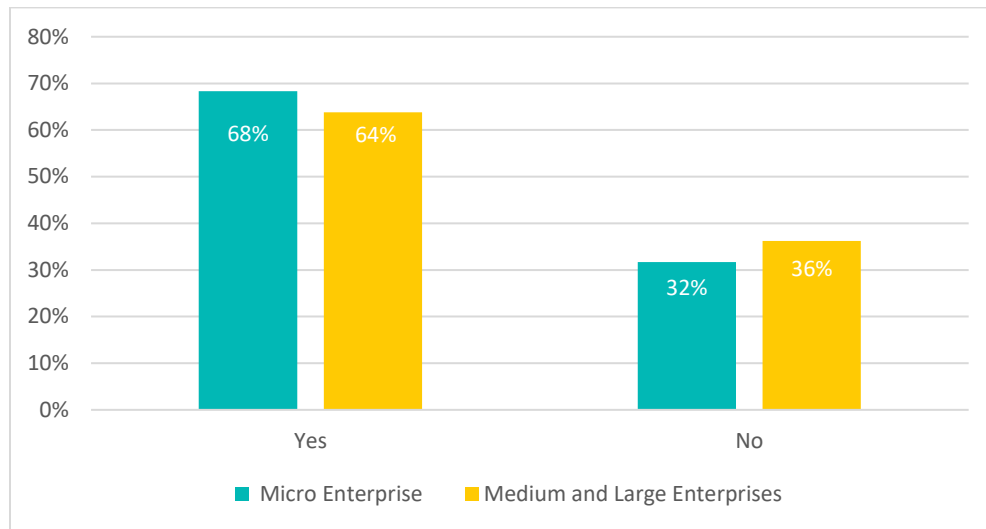
The use of externally- hosted web services is be widespread across both businesses and VOs.

Figure 4: Use of cloud computing in businesses vs VOs.



A review of responses by business size (Figure 5 below) evidences no significant difference between micro enterprises and medium and large enterprises in the use of cloud computing.

Figure 5: Use of cloud computing in micro enterprises and medium & large enterprises



The in-depth interviews shed light on the following:

VOs

The two main reasons instigating this sector to make use of the free cloud services provided by Microsoft (OneDrive) and Google (Google Drive) are:

- Their limited financial resources, and
- The minimal data storage requirements they generally require.

Businesses

A number of entities expressed their preference to keep the data stored internally (on their server) with such data being accessible only by company owned devices. Such entities indicated security as the main reason for them to prefer storing data locally than relying on third parties to store data.

The interviews carried out among the different business clusters further confirmed information collated from desk research - with the professional sector (which includes finance and insurance businesses) and the healthcare sector being particularly prone to holding sensitive customer data, these two clusters were also the most likely business clusters to store their information on internal servers whilst also making use of externally-hosted web services to transfer data to other parties.

6. AWARENESS AND ATTITUDES

6.

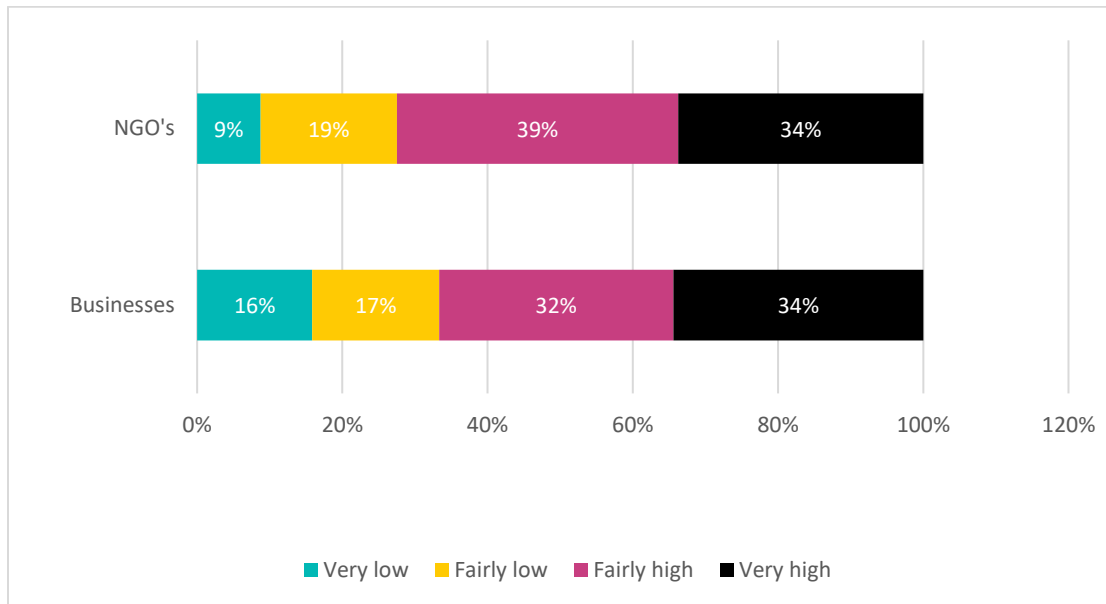
6.1. Brief

This section highlights entities' perception of cyber security and the main cyber security drivers. Furthermore, this chapter identifies where organisations generally seek information, advice or guidance's about cyber security from. Whilst cyber security covers not only the protection of personal data, it is an important aspect of it. Consequently, the final part of this section tackles organisations' levels of awareness of General Data Protection Regulation (GDPR) and its implications on such organisations following its introduction in 2018.

6.2. Perceived importance of cyber security

Two-thirds of businesses (66%) and around three-quarters of VO's (73%) consider cyber security to be of importance to their organisation (Figure 6 below).

Figure 6: Perceived importance of cyber security in VO's and Businesses



Furthermore, a further analysis of responses by business sector (Table 1 below), evidences that the professional sector are more likely to consider cyber security as a priority whilst sectors such as 'wholesale and retail' do not consider cyber security to be as important.

Table 1: Perceived importance of cyber security by sector

Sector	Percentage (%)
Professional	95%
Courier services	91%
Other Sectors	89%
Administration & Support	73%
Creative Arts, Entertainment	67%
Accommodation, food & beverages	61%
Agri/fisheries	60%
Construction	60%
Real estate	57%
Education	56%
Manufacturing	52%
Media, IT	50%
Wholesale and retail	46%
Memberships, repairs, personal services	15%

A further in-depth analysis of these results as collated through the in-depth interviews evidenced that in the majority of instances the smaller enterprises (particularly sole traders and individuals involved in the wholesale and retail segments such as hair dressers, grocery stores, small clothes shop and the like), were still predominantly paper based and/or backed up soft copies of all the data which could inhibit the operations of their business should it get stolen.

Furthermore, similar responses were observed for other sectors too, with entities involved in the memberships, repairs and personal services sector highlighting that they did not depend on IT systems to carry out their day to day business operations since they only required a cash register and a mobile phone to store any data which they required (along with paper based tools such as a diary to keep appointments and jot down information).

Among other segments, the main inhibiting factors from enabling entities to prioritize cyber security related to:



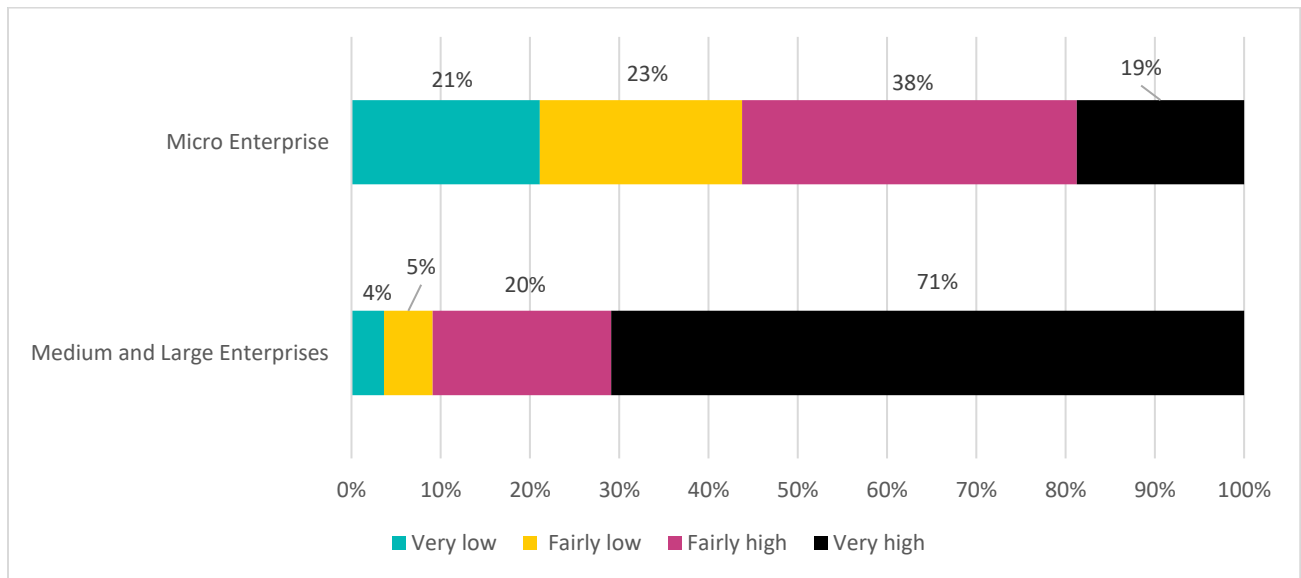
Interviews with a number of micro businesses and VOs highlighted that such entities felt that they were taking a reasonable approach towards cyber security, notwithstanding their limited human and financial resources, with the human resource issue being particularly pronounced among VOs. Some entities indicated time constraints, while others discussed the importance of finding a balance between user controls and the flexibility of allowing their employees to carry out their day-to-day tasks.

The interviews also highlighted entities that felt that they could be doing more to strengthen cyber security within their organisation, though they were unclear on the steps to take. Others indicated not being interested in the topic at hand.

A number of respondents involved in the varying sectors (wholesale and retail, agriculture, fisheries, memberships, repairs and personal services and construction) indicated to be minimally concerned with cyber security and highlighted that should they experience a cyber security attack, they would be able to recover the data (contracts and invoices) from their paper-based system.

A review of responses by enterprise size (Figure 7 below) evidences that medium to large enterprises give more priority to cyber security than micro enterprises do (Micro Enterprises: 57% vs Medium and Large Enterprises:91%).

Figure 7: Perceived importance of cyber security



6.3. Main drivers of cyber security

The main drivers of cyber security within businesses are:

- The type of data they held,
- Their experience with breaches,
- Changes in regulation and compliance.

6.3.1. Organisations which held sensitive personal information

Organisations which typically held sensitive, personal information tended to invest in measures to ensure that their data was safe.

The in-depth interviews evidenced that the financial and healthcare businesses typically fell within this category and held large amounts of sensitive personal information. These businesses highlighted the devastating effects a breach in their systems could have on their business in terms of: reputation, loss of trust in the enterprise and subsequently the potential loss of customers.

It must also be noted that on this issue, the in-depth interviews evidenced that such-businesses tended to place more weight on the business-to-consumer relationship, rather than the business-to business relationship, highlighting how negative word of mouth could be devastating to their business and difficult to reverse. In relation to business-to-business relationships, respondents in this sector tended to agree that, whilst such relationships were important, should issues arise with a business (relating to cyber security), it was more feasible to seek to build relationships with other businesses who offer the same or similar products without jeopardising their customer base.

6.3.2. Being exposed to a cyber security attack

The research evidenced that a primary driver to cyber security and behavioural change related to an entity's exposure to a cyber security attack.

The face-to-face interviews evidenced that in those instances where businesses had experienced some form of cyber-attack, such experiences instigated such entities to attain advice from cyber security specialists to bolster their cyber security systems.

Case Studies of attacks

A large enterprise within the wholesale and retail sector experienced a ransomware attack by a hacker who impersonated itself as an individual from Microsoft to get access to their system.

A medium sized entity within the courier services sector that operates predominantly in Gozo experienced a Spear Phishing attack.

6.3.3. Changes in legislations and compliance

The research evidenced that the introduction of GDPR in 2018 had compelled a number of organisations to review their systems and approaches to cyber security. The majority of medium sized entities indicated how systems were reviewed in view of GDPR. Micro enterprises were less conversant on the topic.

A review of VOs evidenced that the more established entities had reviewed their operations to be in line with GDPR. Conversely, the smaller and often voluntary run entities were less aware and up-to-date on the topic and its potential implications in terms of breaches.

In terms of compliance, entities within certain industries (such as healthcare) highlighted that it was obligatory for entities within their sector of activity to update their cyber security measures to be in line with legal requirements since audits were regularly carried by the authorities to ensure that the data held was secure and in line with pre-set requisites.

6.4. Sources of Information

Around three-in-ten businesses (27%) sought information or guidance on the cyber security threats faced by their organisation in the last twelve months. Though minimal, VOs were slightly more likely than businesses to seek further information or guidance on cyber security.

Seek information or guidance on cyber security

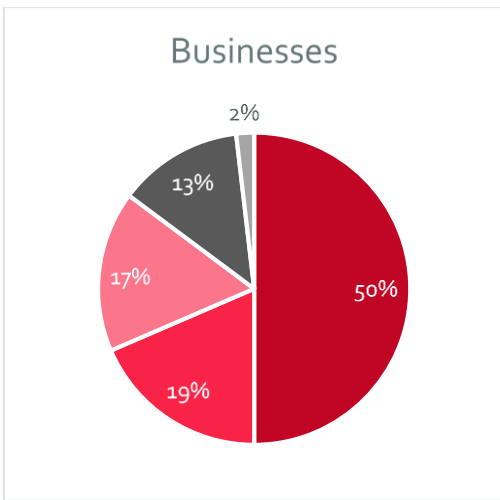


An analysis of the businesses that sought information on cyber security in the last twelve months evidences minimal variances between companies with 54% of microenterprises and 46% of medium and large enterprises indicating to have sought information.

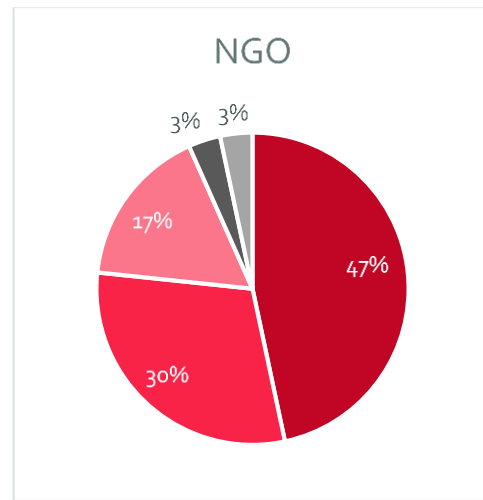
6.4.1. Where organisations and VOs get their information or guidance

Both businesses and VOs refer primarily to 'external security or IT consultants' (Figure 8 below). 'General internet searching' ranked 2nd across the board, though a higher percentage of VOs indicated to seek information from this medium than did businesses (Businesses: 19% vs NGO: 30%).

Figure 8: Where did entities get their information/ guidance in the last twelve months



- External security or IT consultants
- General internet searching
- Government sources of information on cyber security
- No Answer
- Other

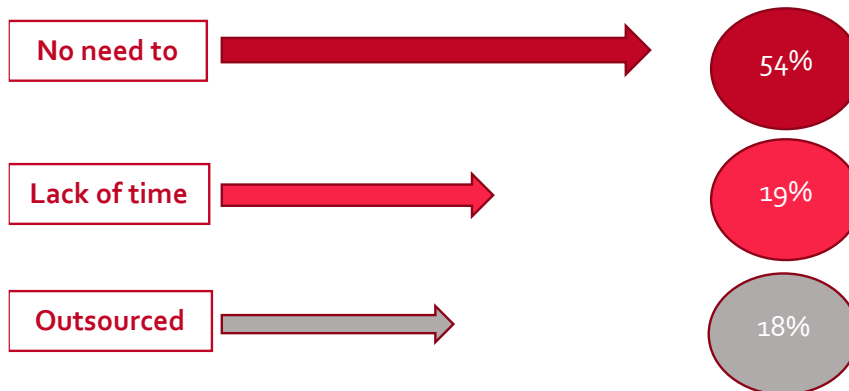


- External security or IT consultants
- General internet searching
- Government sources of information on cyber security
- No Answer
- Other

6.4.2. Entities that did not seek further advice

Businesses

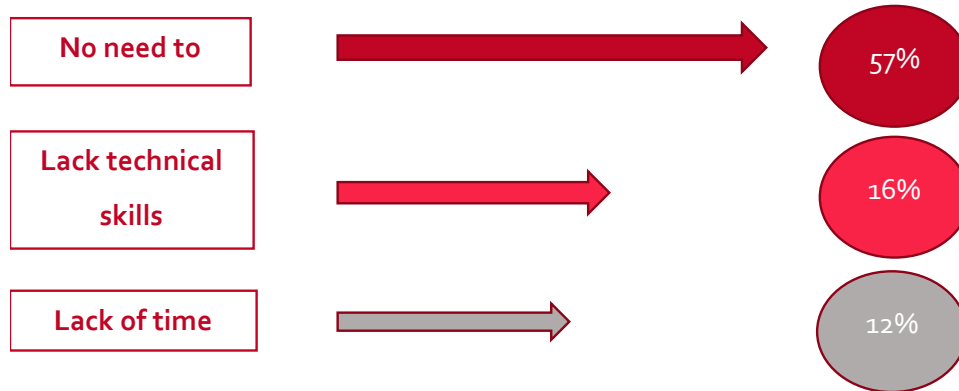
Amongst businesses, the most common reason for not seeking further advice was because they did not feel the need to seek further advice (54%).



It was common for small businesses to outsource their IT function and have a representative from within the company to act as the contact point. Such individual was generally also responsible to contact such outsourced entity should/when they experience a cyber-attack. This representative was usually a member of the accounting or HR department.

VOs

Likewise, among VOs the most common reason for not seeking further advice was because they did not feel the need to do so (57%).



6.5. The General Data Protection Regulation

Both businesses and VOs felt that they were aware of GDPR. In total, three quarters of businesses (75%) and 87% of VOs answered in the positive (to be aware).

A review of responses by sector of activity highlighted variances in replies, with the 'memberships, repairs, personal services sector' being the least aware (62% indicated not to be aware of the new GDPR rules which came into place in 2018), followed by wholesale and retail sector (50%).

Table 2: GDPR awareness by sector.

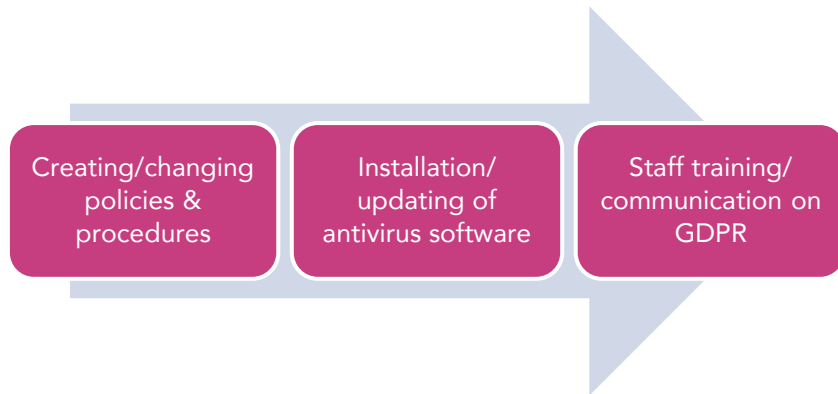
Memberships, repairs, personal services	62%
Wholesale and retail	50%
Manufacturing	36%
Education	31%
Real estate	29%

Accommodation, food & beverages	22%
Agri/fisheries	20%
Construction	20%
Other Sectors	<11%

While the majority of organisations indicated to be aware of GDPR, 45% of businesses and 16% of organisations highlighted that no changes were made once GDPR came into force.

6.6. Attitudes and behaviours

GDPR impact on attitudes and behaviours was further explored during the in-depth interviews, highlighting that the most common changes that were implemented were similar for both businesses and VOs. The most common additions/alterations relating to:



Furthermore, the in-depth interviews further strengthened the findings highlighted earlier with entities indicating not to need to be more/informed about GDPR. On this topic, respondents, particularly those operating within the memberships, repairs, personal services and wholesale retail sectors highlighted that they did not hold any confidential information and usually stored all the required information in a diary and/or mobile phone and their primary/ main device used related to a cash register. Individuals within these sectors tended to agree that since they do not usually store any sensitive information about clients, they did not need to seek further/ information about GDPR.

When discussing training, time constraint was a factor voiced throughout the interviews that acted as a deterrent for to them attending training.

"Attending training to get more information (on GDPR) would result in a loss of time which could be used towards servicing new clients".

Entity involved in the retail sector

7. APPROACHES TO CYBER SECURITY

7.

7.1. Brief

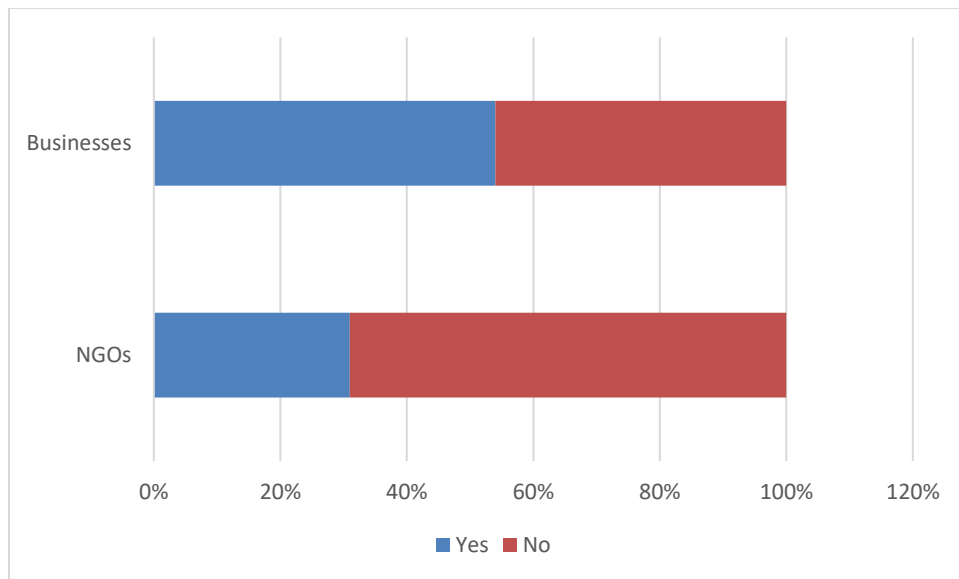
In this section we assess to what extent policies and procedure are in place to identify and reduce cyber security risk, and also shed light on how organisations approach cyber security with their staff.

7.2. Cyber security policies and its management within businesses

7.2.1. Policies

A total of 54% of businesses and 31% of VOs highlighted that they currently have cyber security policies in place.

Figure 8: Entities that have cyber security policies in place



A review of responses among the business community evidences that some sectors are more likely to have cyber security policies in place than others.

Top sectors with cyber security policies in place

- Courier services (89%)

- Professional (85%)
- Media, IT (75%)
- Administration & Support (64%)
- Education (63%)
- Real estate (60%)

From the in-depth carried out, it transpires that entities that have cyber security policies in place are generally more inclined to have provided training and/or information to staff on how to keep data safe and how to avoid being exposed to cyber security attacks. With respect to the latter, this generally revolved around sending out emails to employees on the topic in question.

Interviews with individuals within the IT sector highlighted that cyber security training was generally carried out on an ongoing basis and employees were usually trained on how to use the multiple layers of security which they had in place.

7.2.2. Cyber security Management

The quantitative research evidenced that a higher percentage of VOs typically manage cyber security internally than do businesses. As can be seen in Table 3 overleaf, 73% of VOs typically manage cyber security internally whilst for businesses this figure stood at 59%.

The research evidenced that in most instances, within the NGO sector, cyber security was managed by the individual (employee or volunteer) deemed to be most knowledgeable on IT related matters.

Table 3: The management of cyber security amongst businesses and VOs

How is your organisation's cyber security managed	Businesses (%)	NGO (%)
In-house by someone who is in charge of (security) policies on behalf of the organisation	39%	23%
Outsourced to an independent specialist or organisation	29%	15%
I manage my own cyber security	20%	50%
Other	9%	0%

By the Internet Service Provider	3%	12%
Grand Total	100%	100%

From the in-depth interviews it transpired that, at board level, awareness of the risks of cyber security was still lacking in all sectors. Furthermore, cyber security was generally not a topic that was discussed at a board level and was usually handled by the Chief Technology Officer (in the case of larger companies) or by the CEO (in the case of smaller companies).

The same in-depth interviews highlighted that in most instances, the lack of board member/s or trustees with cyber security responsibilities related to:

- I. **The perceived small size of the entity**
- II. **GDPR not given due importance**

Small size

Entities perceived themselves to be too small or insignificant to warrant thought to cyber security consideration. Furthermore, they did not give due importance to the implementation of GDPR policies and procedures.

Lack of importance given

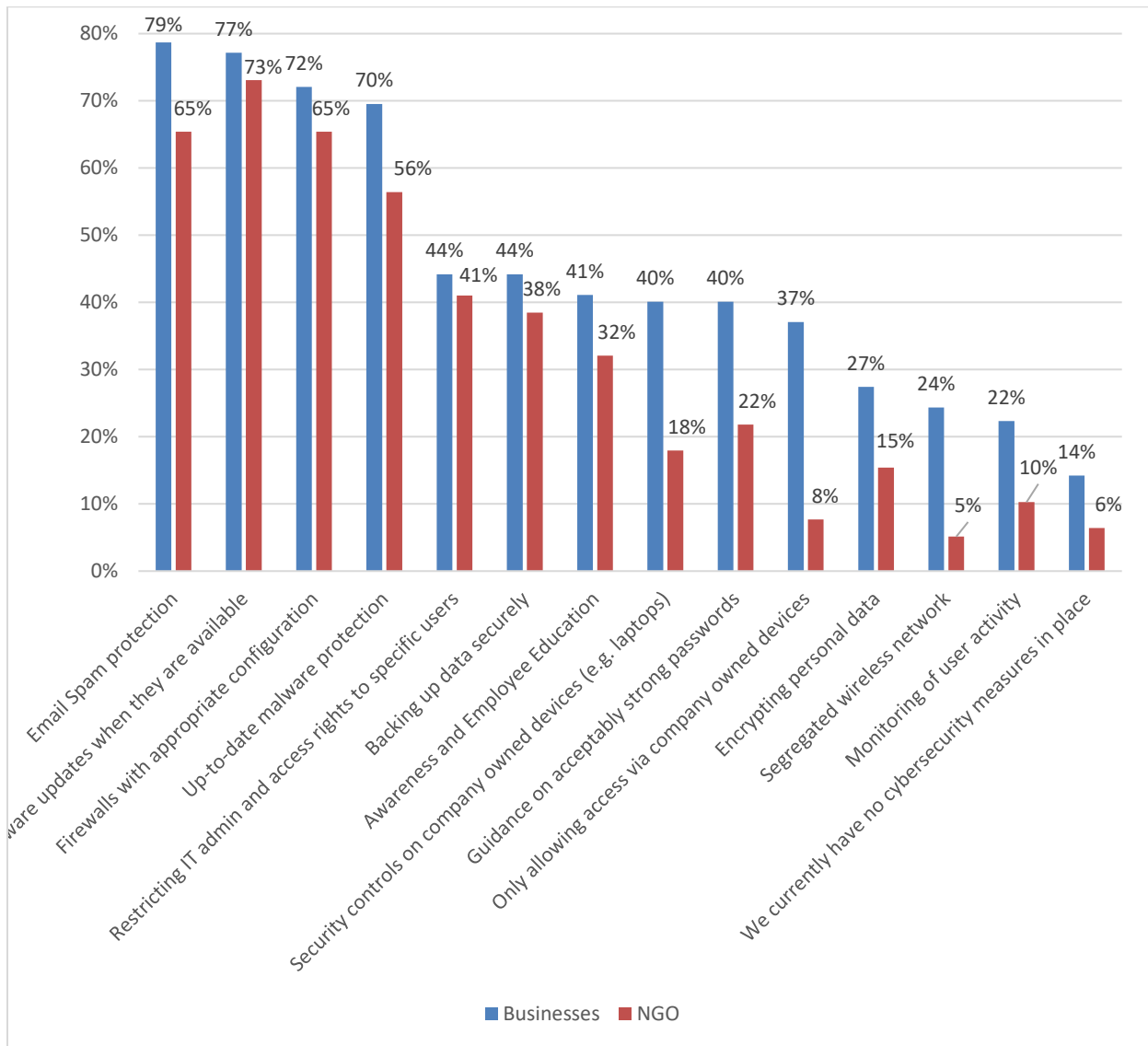
Another factor mentioned by interviewees was that they usually have more pressing topics to discuss (rather than GDPR).

7.3. Actions taken to prevent or minimise cyber security attacks

A review of the rules and controls in place (Figure 10 below), evidences that both businesses and VOs have a number of cyber security rules or controls in place. In this respect, the most common controls (among both businesses and VOs) relate to:

- Email spam protection,
- The application of software updates when available,
- Having configured firewalls, and
- Having an up to date malware protection.

Figure 9: Cyber security rules and controls implemented by VOs and Businesses.



The above figure evidences that, overall, VOs lag behind businesses. This is particularly so in certain areas such as: security controls on company owned devices and only allowing access via company owned devices.

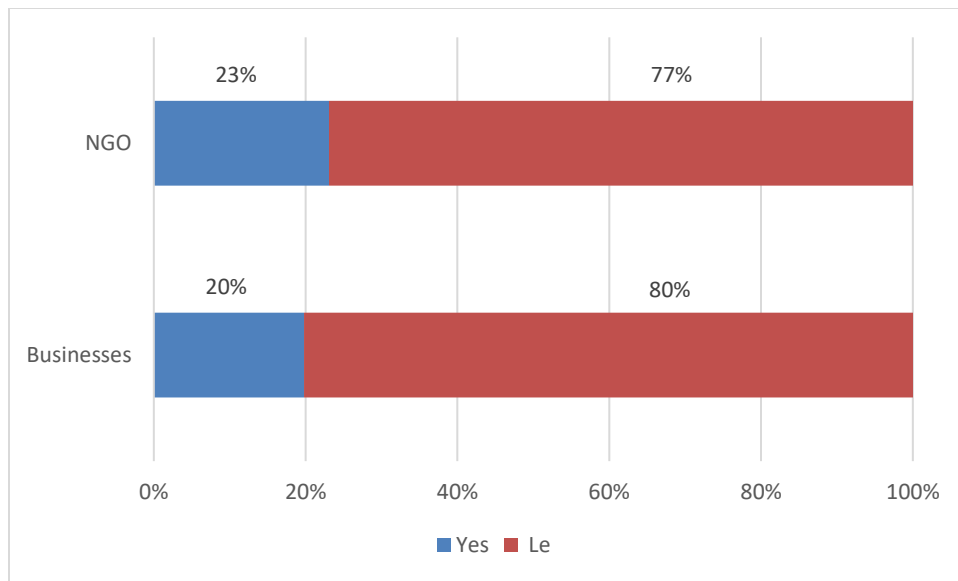
7.4. Staff Training on Cyber security

Part of the quantitative research sought to determine entities' propensity to the provision of training on cyber security. As cyber security is constantly changing and evolving, continuous training is highly recommended to keep abreast with the various cyber security attacks that an organisation could be exposed to.

7.4.1. Training attended

The research has evidenced (Figure 10 below), that cyber security training is quite low across both businesses and VOs with 20% of businesses and 23% of VOs indicating that they attended cyber security training in the past 12 months.

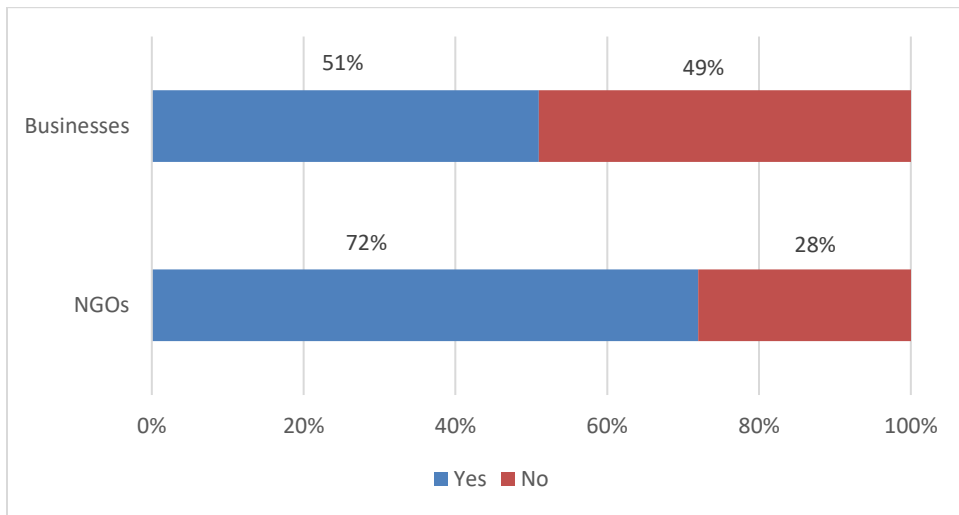
Figure 10: Staff training on cyber security in the last 12 months.



7.4.2. Inclination to attend training

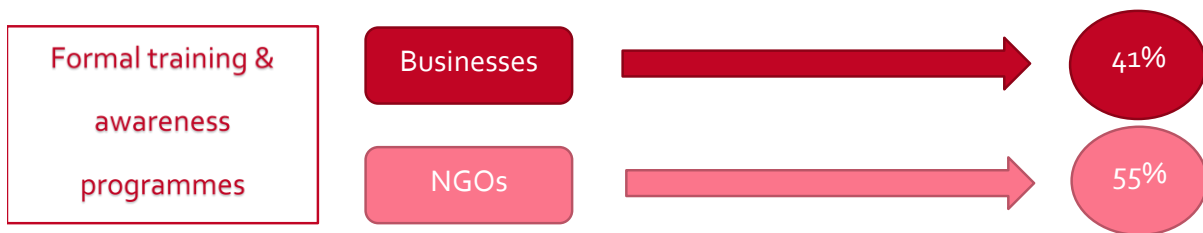
Whilst a low percentage of respondents have attended cyber security training in the past 12 months, both businesses and VOs highlighted that they would be willing to attend cyber security training. In this respect almost three-fourths of VOs and half the businesses answered in the positive.

Figure 11: Willingness to attend cyber security training



7.4.3. Best way to receive training

The quantitative research also sought to determine entities perceived most apt method of effective training on cyber security. Both Businesses and VOs indicated 'formal training and awareness programmes' as the best way to educate individuals on cyber security.



The second most popular choice for training related to the provision of written policies and clear instructions to end users, with this option proving to be particularly positively viewed among VOs (43% of VOs and 24% of businesses).

7.4.4. Participation in training

The topic of training was discussed extensively during the in-depth interviews.

While the qualitative research once again highlighted that the target audience was keen and perceived training as a positive initiative, the discussions also evidenced a major constraint that had prohibited (and thus could continue to act as a stumbling block) such entities from participating in training courses – time restrictions.

Such a limitation is indeed a primary inhibiting factor voiced by respondents throughout the research study – both through the qualitative and quantitative study.

A number of respondents indicated that it could be an issue/ inconvenience for them to attend training especially if it was classroom based. The need to travel (traffic and parking considerations highlighted) was identified as a time-consuming factor that hindered their participation.

The provision of online videos / podcasts could be a solution to this limitation.

7.5. Use of external providers

Around one third of all businesses (29%) highlighted that their cyber security functions were outsourced to an independent specialist or organisation (Table 3, page 39), this figure being double the number of VOs that indicated to also outsource (15%).

A review of responses by business size evidences that a higher percentage of micro enterprises outsourced than did medium to large enterprises.

Number of businesses that outsource their cyber security functions



While outsourcing is common among business, the in-depth interviews did highlight variances in the way this was carried out.

Broadly, outsourcing fell within one of two categories:

- I. **Businesses that chose to outsource all of their cyber security and IT functions;**
- II. **Business that maintained some control over their business's function and chose to partially outsource certain IT functions.**

A more in-depth analysis among micro enterprises highlighted various factors that instigated such entities to outsource:

- Lack of know how** Some micro businesses indicated that an outsourced IT consultancy firm that focused on security was generally more knowledgeable on the subject, both in terms of technical skills as well as experience gained through dealing with a multitude of clients and consequently being more inclined to have faced multiple cyber-attacks and hence have identified the most apt means for protecting its clients, dependent on the type of cyber threat.
- An evolving topic** The role of managing cyber security is continuously evolving as new types of cyber security attacks are always being invented. Such a stance requires continuous training on new cyber security developments. This is deemed too costly especially for micro enterprises with limited financial resources.
- Lack of skilled labour** As a result of the highly demanding nature of cyber security, skilled labour within this sector was/is scarce. Consequently, such individuals are generally hard to find, and costly to recruit. As a result, only larger companies with bigger budgets tend to afford to employ such individuals.

8.The impact and incidence of breaches or attacks

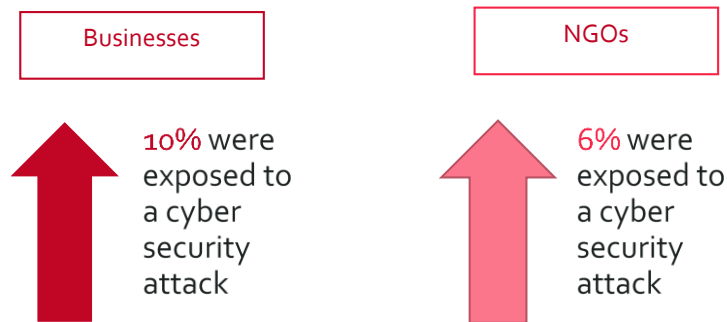
8.1. Brief

In this section we cover the level and impact of cyber attacks and breaches on businesses and VOs.

It must also be noted that this study could only measure the breaches or attacks that were identified by the organisations. It is likely that businesses and VOs are exposed to attacks which go unidentified. As a result the findings here may underestimate the full extent of cyber-attacks on the target audience (businesses and VOs).

8.2. Experience of breaches or attacks

The quantitative research evidences that, by and large, businesses and VOs were not aware of being exposed to a cyber security attack in the past 12 months.



A review of responses among entities that indicated to have experienced a breach evidences that microenterprises were less likely to experience a cyber security attack than larger businesses. (Microenterprise: 7% vs Medium and Large businesses:17%).

8.3. Types of breaches or attacks experienced by businesses and NGO's

A review of the most common types of cyber security attacks identified by Maltese businesses in the last 12 months were:

- Phishing attacks – through fraudulent emails or being directed to fraudulent websites (33%).
- People impersonating the organisation in emails or online (33%).
- Viruses, spyware or malware (28%)

A further in-depth analysis of such findings evidences that the most common cyber security attacks reported were:

For micro enterprises:

- Fraudulent emails or being directed to fraudulent websites (38%),
- Viruses Spyware, Malware (38%) and
- Denial of service attacks⁵ (38%).

For VOs:

- Phishing attacks (50%)
- Denial-of service attacks (50%)
- Cyber-attacks which involved others impersonating the organisation in emails or online (25%) and
- Viruses, spyware and Malware (25%).

The in-depth interviews evidenced that the professional and IT sectors were particularly prone to cyber-attack attempts. Furthermore, it transpires that over the last 2 years, there has been a surge in the number of cyber hacking attempts.

The desk research too evidenced that cyber hacking attempts were on the rise.

Cyber Crime Unit - "We noted a 24 per cent increase in fraud cases between 2017 and 2018. Scams are becoming a lot more sophisticated nowadays. Instead of sending out an email telling 10,000 people that they have won the lottery, the perpetrators are doing more homework, and targeting more specific groups of people".

Inspector Zammit

⁵ DoS attacks attack both network and web-based applications. This is done by flooding the target with traffic or sending it information that triggers a crash. The DoS attack generally deprives legitimate users (i.e. employees, members, or account holders) temporarily of the service or resource they expect/ed

Furthermore, the interviews once again confirmed that common types of cyber security attacks experienced were Phishing attacks by email and viruses and malware being attached to email attachments.

Case Study

A professional entity indicated:

- Phishing attacks as the most common type of cyber-attacks received - 20 times in the last 28 days - followed by
- Malware attacks - 3 times a month and
- Brute force attacks on passwords - around 1 time every month.

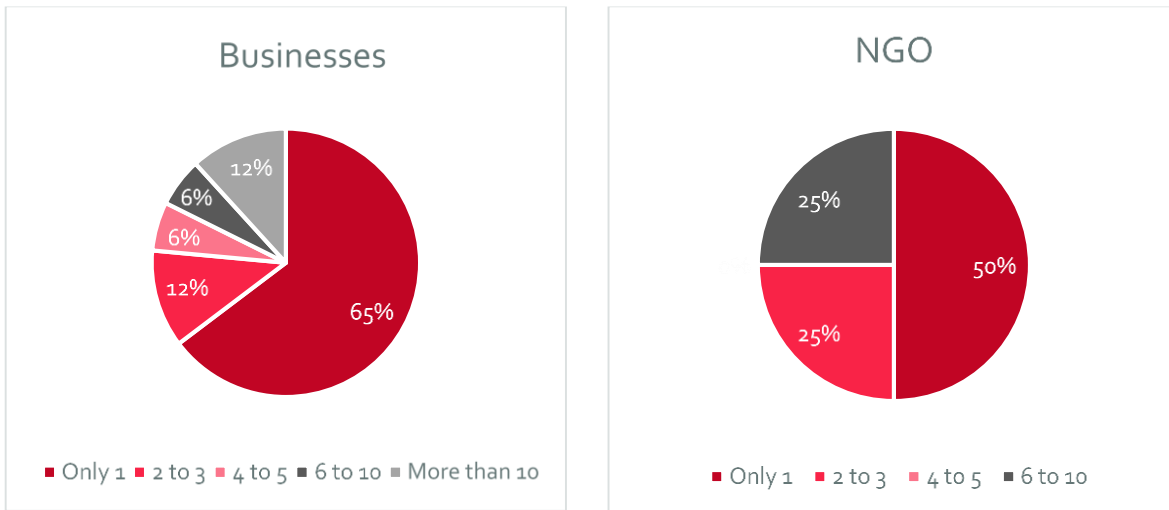
The same business highlighted that throughout its lifetime the business also experienced 3 ransomware attacks where their B2B data was encrypted by hackers and financial compensation was required to release the stolen data.

8.4. Number of breaches or attacks experienced amongst businesses and NGO

As evidenced in Figure 11 below, among businesses that were exposed to cyber security attack/s, the majority (65%) received one cyber security attack in the past 12 months, with the rest indicating to have experienced more.

A review of responses among VOs evidences that half those that had experienced cyber security attack/s, indicated to have experienced one cyber security attack.

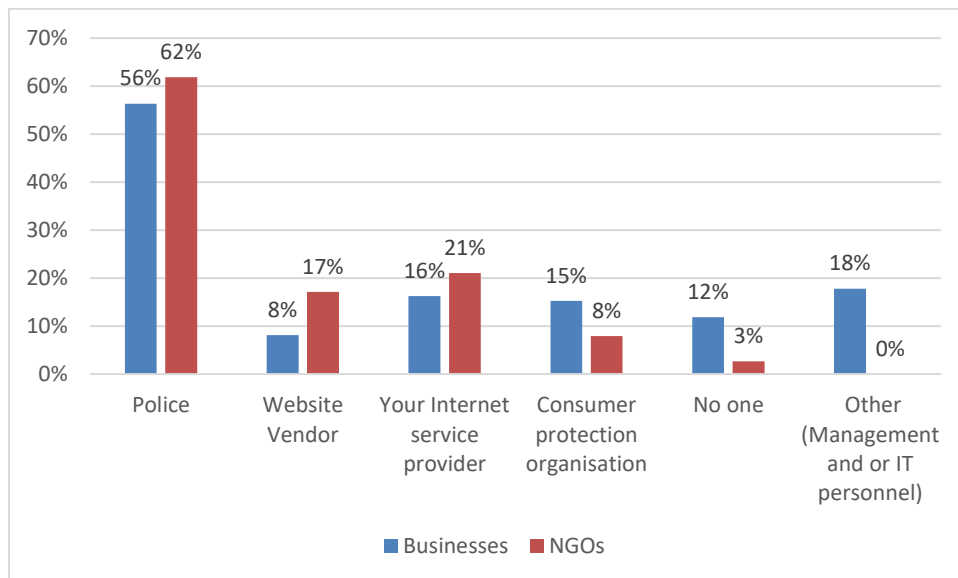
Figure 11: Number of breaches experienced by businesses.



8.5. Who would be contacted if a breach was experienced

The research sought to determine who was the first point of call for entities, if a breach was experienced, with results indicating that most businesses and VOs would contact the police first if they were to experience a cyber security attack.

Figure 12: Who would be contacted if the business/ NGO was to experience a cyber security attack.



That said, the in-depth interviews evidenced that, whether the police were likely to be contacted or not was dependent on the gravity of the cyber security attack. It was not uncommon for businesses to receive monthly reports from webhosting providers that they had received multiple hacking attempts. In such instances the norm was that businesses did not contact anyone. When delving further on such point, the main reasons given related to:

- Nothing happened
- Entities were not too worried as they did not store any sensitive information on their website and/or
- Backups were made regularly.

We do not contact the police in cases where a cyber-attack was not successful or if the damage was considered to be immaterial to the company.”

Entity within the professional sector

9. COMPARISONS TO EU STUDIES

9.1. Brief

The risk of cyber-attacks is a persistent threat to both businesses and VOs. The research has evidenced that organisations are increasingly faced with multifaceted cyber risks coming from both external and internal sources.

In this section we analyse studies carried out by the European Commission⁶, Ponemon Institute⁷ and the UK Government Department for Digital, Culture, Media and Sports⁸ on the topic in question. These studies allowed us to assess the current cyber threat and vulnerability landscape across Europe – both in relation to the population at large as well as with respect to European businesses and assess how Maltese businesses and NGOs fared in comparison.

In the final part of this section we analysed the key cyber security challenges across different sectors (in so far as possible).

9.2. Comparison of Maltese businesses and VOs with the EU population

9.2.1. Overview

A number of studies⁹ that analyse the current state of play among businesses compare their findings with the EU population at large. The same research studies evidence that such data is comparable and give an indication of the general trend/ state of play, since such individuals form an integral part of such businesses.

⁶ <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/85495>

⁷ https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf?utm_campaign=2018%20Ponemon%20Nurture%20Workflow&utm_source=hs_automation&utm_medium=email&utm_content=72316430&_hsenc=p2ANqtz-_10UfCD2c0_6JkEYoNgU0ZiART0bGulGqEEPIRNF_XXC4MAH8fUuRj6q-nD8gimvA8apWkdPp0GhLIV8QMTk1y7S9wjA&_hsmi=72316430

⁸ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791940/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF

⁹ Cyber security. The station of the Union 2017. European Commission, 2018.
Attitudes towards the impact of digitisation and automation on daily life, Eurobarometer, 2017.
Eurobarometer on Cyber security (EBS 464)

PWC, Global State of Information Security Survey, 2016 and <http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/>

How to protect your networks from ransomware, CCIPS, 2016 <https://www.justice.gov/criminal-ccips/file/872771/download>
Continental European Cyber Risk Survey 2016 Report.

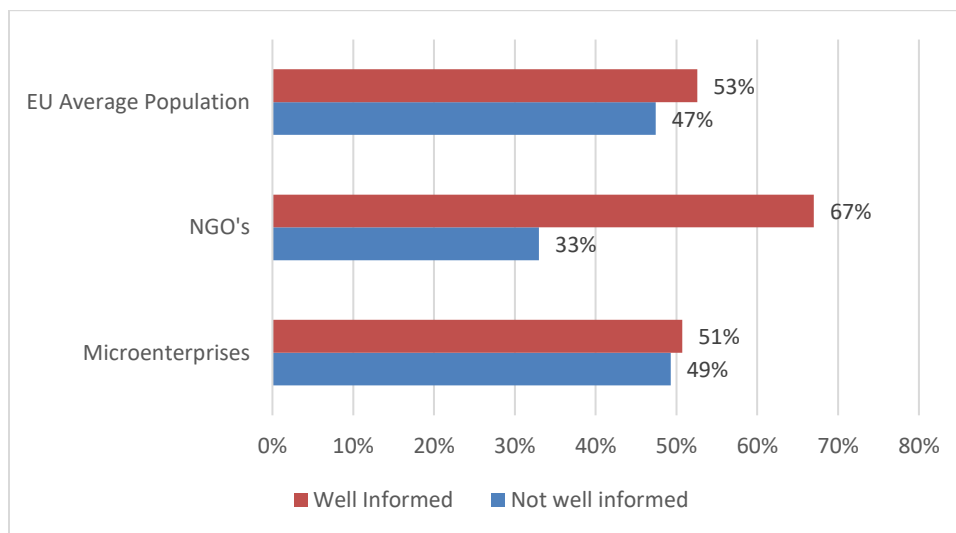
In line with the above, in the first part of this section we compare the results of our study with reports issued by the European Commission on cyber security.

9.2.2. Awareness of the risks of cybercrime

In terms of awareness levels, we benchmarked our findings to a study published by the European Commission in March 2019 on cyber security awareness across the EU¹⁰.

Our research evidences that half the microenterprises (51%) felt that they are 'well informed' about the risks of cybercrime, with VOs (67%) being more optimistic about their awareness levels.

Figure 13: Awareness of the risks of cybercrime¹¹



Benchmarking these results with the EU average population illustrates that local microenterprises awareness levels are in line with the EU average population. Local VOs on the other hand perceive themselves to be more aware than the average EU population.

9.2.3. Attitudes to cyber security

¹⁰ <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/85495>

¹¹ Don't/ No Answers were eliminated from these results to ensure consistency in comparisons

The quantitative research sought to determine local businesses and local VOs attitudes to cyber security. In this respect, perceptions in relation to the following factors were analysed:

- Whether online information and data were kept secure by websites;
- Whether online information and data is kept secure by public authorities;
- Whether disclosing of any personal information online is avoided or not;
- Protection capability against cybercrime;
- Whether the risk of being a victim of cybercrime was increasing.

The results were then compared to a European Commission Report¹² that targeted the topic in question.

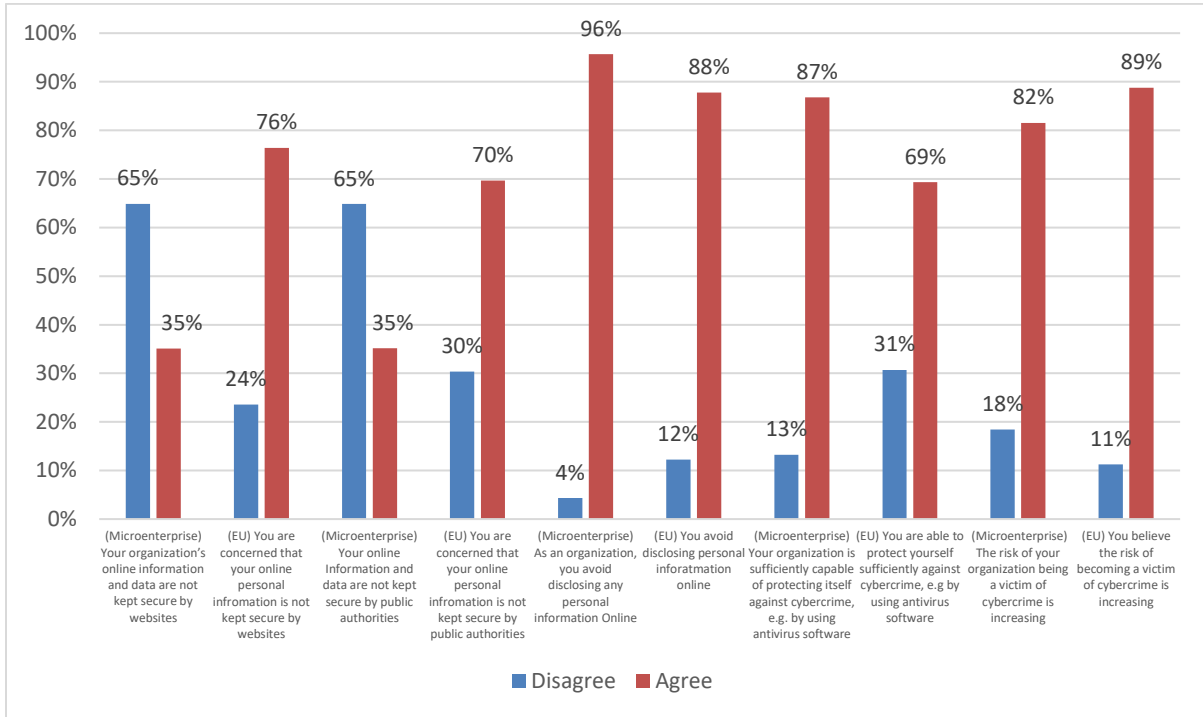
As can be seen in Figure 14 below, EU respondents were more concerned that their online information and data was not kept secure by websites than Maltese microenterprises (Microenterprises: 35% vs EU Average: 76%). Likewise, local microenterprises were much less concerned about data and information that is held by public authorities than the EU population at large (Microenterprises: 35% vs EU Average Population: 70%).

That said, both local businesses and the EU population had similar views with respect to:

- Where possible, they avoided disclosing personal information online (Microenterprises: 96% vs EU Average: 88%);
- Overall entities/ individuals are sufficiently capable against cybercrime (Microenterprises: 87% vs EU Average Population:69%); and
- That the risk of being a victim of cybercrime was increasing (Microenterprises: 82% vs EU Average Population:89%).

¹² Special Eurobarometer 480 - Europeans' attitudes towards Internet security, Fieldwork October-November 2018, Publication March 2019 <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/85495>

Figure 14: Attitudes to cyber security – Local microenterprises vs EU



A comparison of responses among the EU population and local VOs evidences similar trends to those observed by local microenterprises (Figure 15 below).

EU respondents were more concerned than local VOs about

- The security of data and information that is held by websites (VOs:46% vs EU Average Population:76%) and
- Data held by public authorities (VOs:47% vs EU Average Population: 70%).

Conversely, local VOs are in line with the EU average in relation to

- Disclosing personal information online (VOs:87.5% vs EU Average Population:88%) and

Protection against cybercrime, (75% of VOs and 69% of EU population).

9.3. Comparison of Maltese businesses and VOs with the EU businesses

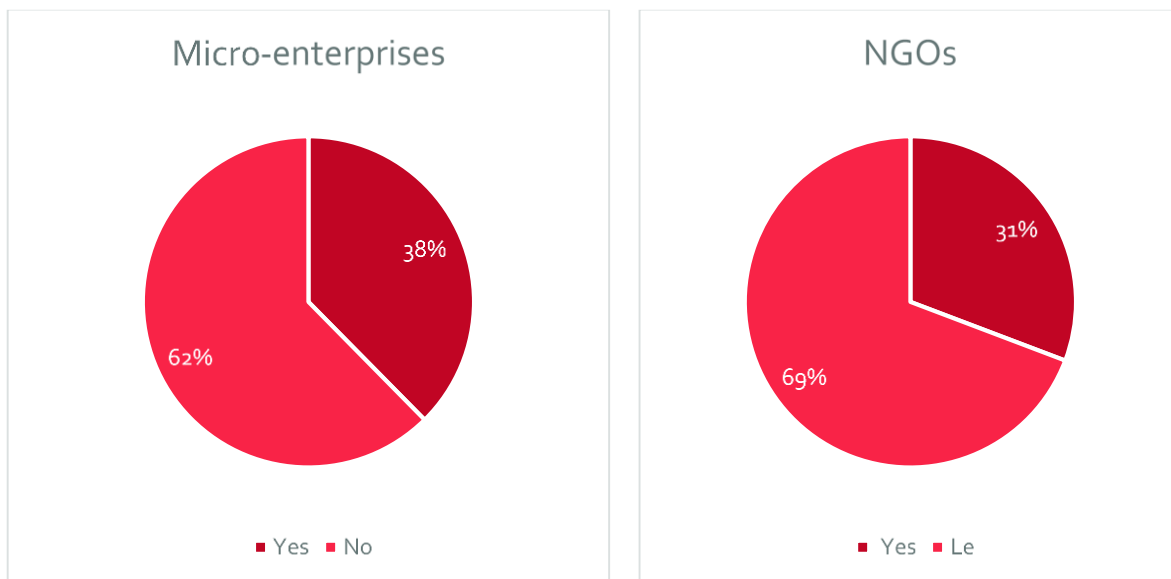
9.3.1. ICT security policies

The desk research evidenced the increasing need for organisations (both locally and internationally) to protect themselves from cybercrimes and design strategies towards capacity building and awareness.

In line with the above, the quantitative research sought to determine the extent to which local entities understood the importance of protecting their organisations from the relevant cyber security risks. This was carried out by determining the existence (or otherwise) of ICT security policies in place within enterprises. Such information also provided useful information in relation to an enterprise's strategy to safeguard data and ICT security systems.

The research results (Figures 17 below) evidenced that circa one third of entities had a formally defined ICT security policy in place (38% of micro-enterprises and 31% of VOs).

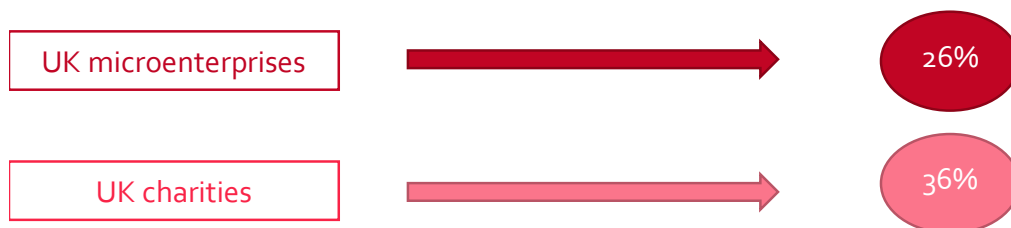
Figure 17: Implementation of formal cyber security policies



a. Comparison with the UK

A report issued in 2019 by the Department for Digital, Culture Media & Sports¹³ on the topic in question illustrates that the results collated locally are comparable to the scenario in the UK.

Have a formal policy covering cyber security risks



b. Comparison with the EU

Data published by Eurostat in relation to ICT security policies¹⁴ (2015) among enterprises in the EU evidence similar results, with the report indicating that one out of every three enterprises in the EU had a formally defined ICT security policy.

Have a formally defined ICT security policy



The same report¹⁴ illustrates similar results for small enterprises¹⁵, though the percentage is marginally lower.

¹³https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791940/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF

¹⁴https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_policies_by_enterprise_size.2C_sector_and_country

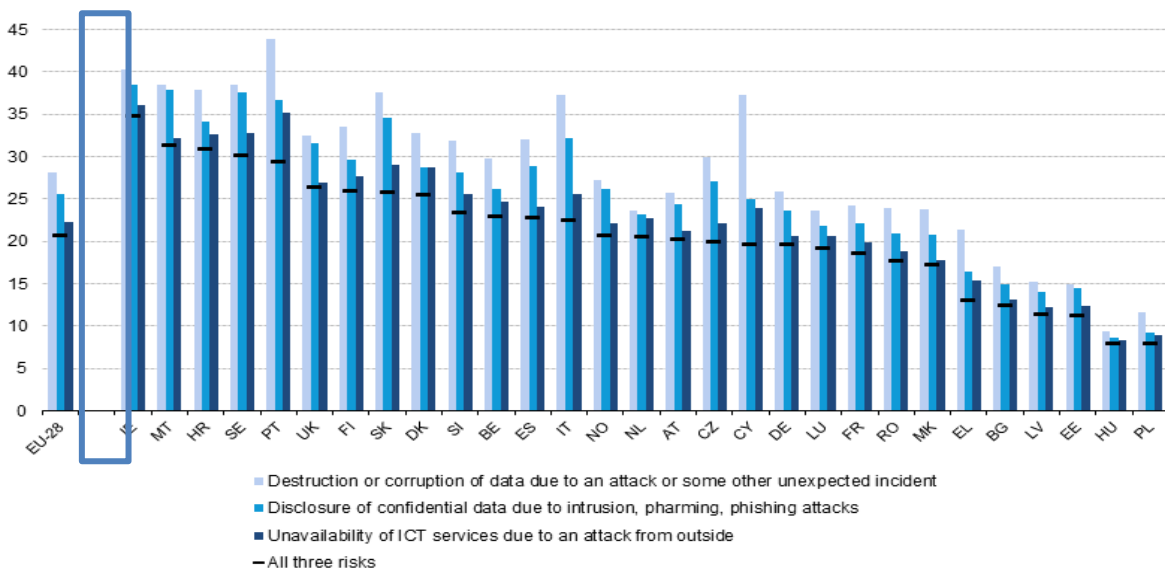
¹⁵ The report indicates that data relating to small enterprises incorporates entities comprising 10-49 employees and excludes the financial sector

Have a formally defined ICT security policy



In line with the above, Figure 18 overleaf illustrates data provided by a Eurostat report - Enterprises having a formally defined ICT security policy, by size class, EU-28, 2015¹⁶ that compares data for each European Union country, with such report placing Maltese companies quite highly amongst other European countries.

Figure 18: Enterprises addressing specific ICT security risks, by country, 2015



LT, TR : data unreliable

¹⁶ [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Enterprises_having_a_formally_defined_ICT_security_policy,_by_size_class,_EU-28,_2015_\(%25_enterprises\)_new.png](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Enterprises_having_a_formally_defined_ICT_security_policy,_by_size_class,_EU-28,_2015_(%25_enterprises)_new.png)

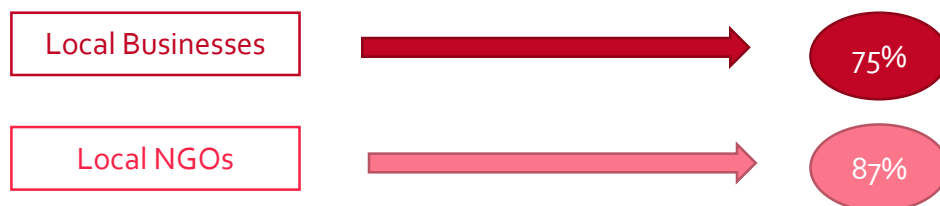
9.3.2. Cyber security changes with the implementation of GDPR in 2018

With the introduction of General Data Protection Regulation (GDPR) in 2018, businesses had to ensure that data maintained was compliant with GDPR. The desk research evidenced that, more often than not, such a stance required businesses to make changes. Consequently, our research sought to determine to what extent (if any) entities:

- Were aware of GDPR; and
- Underwent changes in preparation of the new Data Protection Act.

c. Awareness

The majority of entities under review indicated being aware of GDPR.



d. Changes in preparation for the introduction of GDPR

The research evidenced that close to half the businesses (45%) did not make any changes.

Table 4 below highlights that, among those that carried out some change/s, the creation/ amendment/s to policies and procedures were the most common changes made (35% of businesses and 41% of VOs). 'Installed, changed or updated antivirus or anti-malware software' ranked 2nd (24% of businesses and 22% of VOs).

Table 4: Cyber security changes made

Types of cyber security changes made in preparation of the new Data Protection Act (2018) (Multiple choice)	Businesses (%)	NGO (%)
No changes were made	45%	32%
Created or changed policies and procedures	35%	41%
Installed, changed or updated antivirus or anti-malware software	24%	22%
Additional staff training or communications	23%	19%
Other	9%	7%
Don't know as outsourced	8%	6%

The lack of changes made, could imply that:

- Entities were unaware/uninterested in compliance
- Entities felt that they were already compliant prior to the new Act

A review of the situation across European businesses (research conducted by RSM Global¹⁷ towards the end of 2017 - prior to the introduction of GDPR) evidenced a similar scenario with one in four business leaders (28%) indicating to be completely unaware of the regulation they would have had to

¹⁷ <https://www.rsm.global/news/92-european-businesses-are-unprepared-gdpr>

adhere to within a few months. Furthermore, 26% of business leaders familiar with their GDPR strategy, admitted that their organisation would not have been compliant by the May 2018 deadline. With such data relating to business leaders, it is assumed that overall, the percentage of the whole sector would be higher, and thus in line with the current trend across the Maltese islands.

Both the quantitative research findings (as evidenced throughout this report), and the in-depth interviews evidenced that the limited financial and human resources faced by micro-enterprises and VOs made compliance an arduous endeavour. Such feedback is congruent with international studies¹⁸ that evidenced that one third of organisations did not have the proper technology to address the regulations.

9.3.3. Comparison of Current cyber threats and vulnerability landscape¹⁹

Organisations are increasingly faced with the difficulty of dealing with multifaceted cyber risks which may affect businesses' continuity, intellectual property and professional integrity.

As highlighted earlier on in the report, the most common cyber security attacks experienced were:

For micro enterprises:

- Fraudulent emails or being directed to fraudulent websites (38%),
- Viruses Spyware, Malware (38%) and
- Denial of service attacks (38%).

For VOs:

- Phishing attacks (50%)
- Denial-of service attacks (50%)
- Cyber-attacks which involved others impersonating the organisation in emails or online (25%) and

¹⁸ Veritas GDPR Report, 2017.

RSM Global Report on GDPR, 2017 - <https://www.rsm.global/news/92-european-businesses-are-unprepared-gdpr>

¹⁹ Reference is being made to businesses (incorporating small, medium and large enterprises) across Europe

- Viruses, spyware and Malware (25%).

These results are congruent with cyber threats faced by EU businesses.

An EY Global Information Security Survey 2018 – 2019 report entitled ‘Is cyber security about more than security?’²⁰ which looked at the current practices reported by 1,400 participants from global business across 20 sectors evidenced that the biggest threats amongst organisations were Phishing (22%) and Malware (20%).

Furthermore, another study issued by the European Economic and Social Committee – Cyber security: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks - published in March 2018²¹; evidenced similar results to those attained locally with the most common threats²² amongst enterprises being:

a) Malware and Phishing and

b) Distributed Denial of Service (DDoS)²³

The same report evidences that the main European sectors exposed to cyber security attacks were finance, healthcare, retail, business services and information technology sectors. This falls in line with the local scenario with our findings with the exception of retail.

Our in-depth interviews with the wholesale and retail sector highlighted that a large proportion of micro-enterprises did not really depend on IT services since they generally only needed a cash register and a mobile phone (to store contacts) to carry out their day to day operations. As a result, their exposure to online web services and cyber-attacks was limited.

e. Malware and Phishing attacks

Malware and Phishing constitute one of the most common cyber threats encountered by businesses and VOs both in Malta and across Europe. These types of attacks work hand in hand and often are grouped together since malware generally enters a targeted server or computer as an attachment to a phishing email. This type of attack seeks to steal or corrupt data and as a result can have multiple

²⁰ [https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/\\$FILE/ey-global-information-security-survey-2018-19.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf)

²¹ https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf

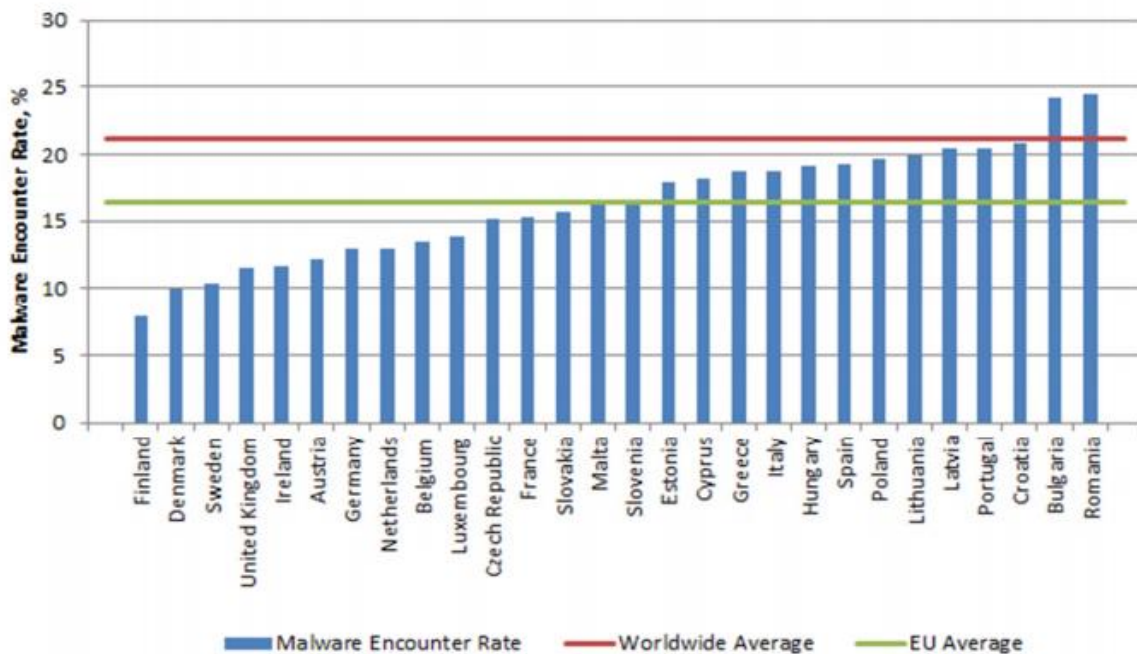
²² This report also gave reference to data breaches that was not covered in our analysis

²³ A Denial-of-Service (DDoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DDoS may be viewed as a subset of DOS

repercussions on the business's operations. Such repercussions include financial damages, reputational damage and/or a reduction in the firm's competitiveness.

According to the Microsoft Security Intelligence Report²⁴ which analysed the 2016 yearly data of country specific Malware encounter rate in the EU, Malta's encounter rate stood at around 16% which is line with the EU-28 average. A comparison of such findings with data collated relating specifically to micro enterprises (page 63), it transpires that micro-enterprises are generally more at risk of being exposed to these types of attacks than the country at large.

Figure 19: Malware encounter rate in the EU-28



²⁴ Anthe et al., "Microsoft Security Intelligence Report - Volume 21 | January through June, 2016."

a. Denial of Service attacks

With the rise of Internet of Things (IoT)²⁵ devices, businesses have become increasingly exposed to distributed denial-of-service (DDoS) attacks.²⁶ These attacks maliciously attempt to disrupt the normal traffic to websites.

A notable DDoS attack on large internet companies was an attack on DNS-services in October of 2016 which left companies such as Facebook, Twitter and Amazon with temporarily shut down web access in the EU and in the US.²⁷

The quantitative research among microenterprises (as highlighted earlier in this report) evidenced DDoS attacks to be one of the most common forms of cyber-attacks experienced by microenterprises (38%).

The desk research evidenced that these attacks are more often targeted towards more digitized economies and larger companies. Nonetheless, a report issued by the Economic European Economic and Social Committee in March 2018 – Cyber security: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks²⁸, highlighted that 51% of all companies regardless of their size have experienced a DDoS attack.

A major consideration with respect to the above is that, larger companies usually have better mitigation structures and policies in place to combat such attacks than do micro enterprises. Indeed, in the absence of adequate response capabilities, a DDoS attack may have profound effects on microenterprises that depend heavily on web services.

Our research has evidenced that denial of service attacks is also prevalent among local VOs. That said, the feedback collated from the in-depth interviews showed that VOs are usually less concerned about denial of service attacks than Malware or Phishing attacks. The reasons given for such considerations being:

²⁵ Internet of Things (IoT) – definition: The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

²⁶ Nexusguard, "Distributed Denial of Service (DDoS) Threat Report Q1 2017," Threat Report (San Francisco, CA, USA: Nexusguard, 2017), 12

²⁷ Nicky Woolf, "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say," The Guardian, October 26, 2016, sec. Technology, <http://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.

²⁸ https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf

- In those instances where web services were not a crucial part of VOs operations, having limited access to their website for one week or two was not considered as bad as having their subscribers list stolen or corrupted by Malware or Phishing attacks.
- Denial of service attacks did not require financial or human resources to repair data since the attack generally only focused on temporarily limiting access to web services.

9.4. Factor/s inhibiting cyber security

There are several factors that inhibit organisations from undertaking the necessary cyber security measures. The European Economic and Social Committee report – Cyber security: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks²⁹ (page 70) identifies a number of factors, and broadly segmented such factors into two main categories:

- External perspectives; and
- Internal perspectives

While a snapshot of the various factors that fall under both categories are presented overleaf, this section will focus primarily on the internal perspectives that relate specifically to issues relating to businesses and discuss their relevance also within the local perspective.

²⁹ https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf (pg70)

External

- A lack of adequate legal and regulatory framework to support cyber security practices
- A lack of financial and facilitating instruments to help businesses deal with cyber security threats
- A lack of educational cyber security programs
- A lack of appropriate intelligence sharing

Internal

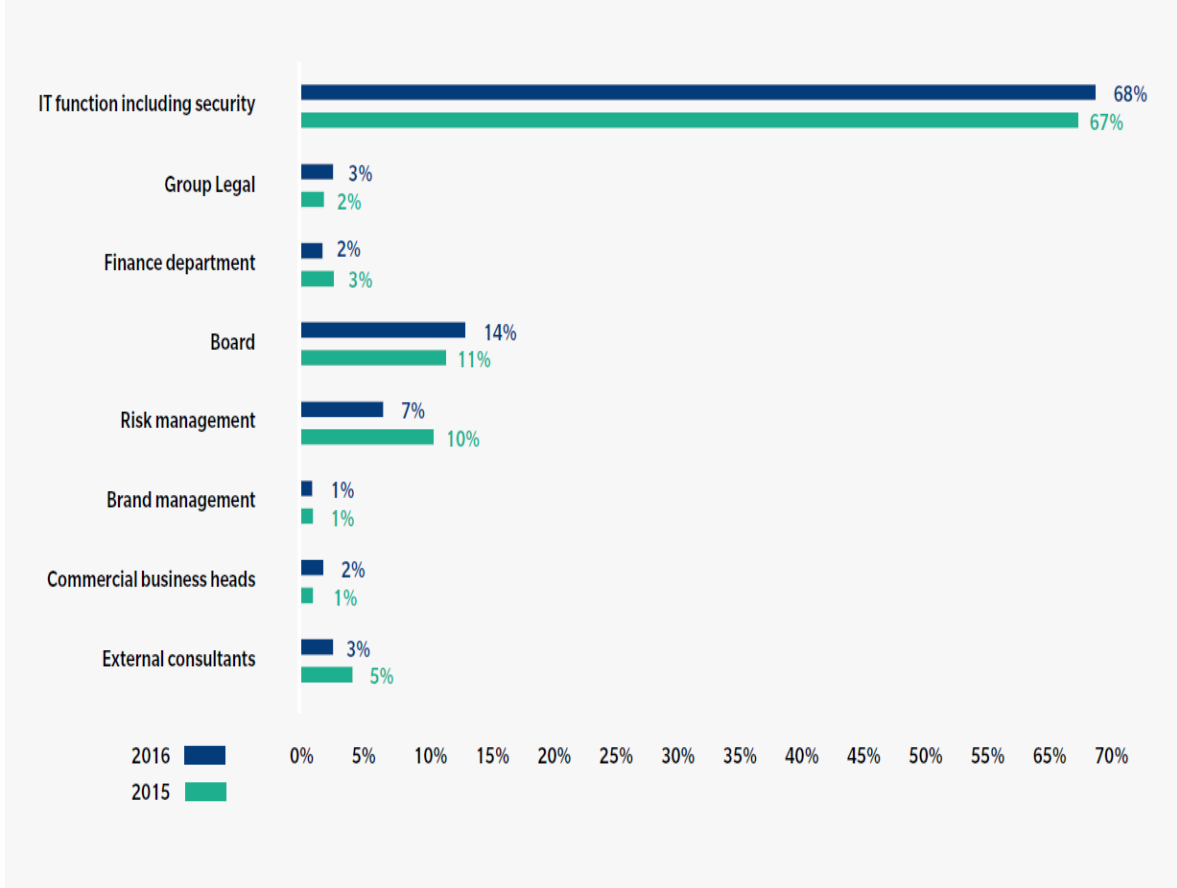
- A general lack of awareness of cyber security at a company board level
- Lack of appropriate training and availability of skilled IT cyber security personnel
- Inadequate cyber security spending
- Technologies vulnerabilities
- A lack of trust to share information can lead to corporate entities under-reporting the cyber security treats that they encountered
- A lack of incident response plans
- Organizational designs

9.4.1. Awareness at a board level

The in-depth interviews on the topic (as highlighted in section 7.2.2 of this report) evidenced that there is still a lack of cyber security discussions at a board level. Such a situation is in line with businesses at European level.

In this respect, a survey conducted by Marsh - Continental European Cyber Risk Survey: 2016 Report³⁰ revealed that “While cyber risk continues to rise up the boardroom agendas of European organisations, they still hold a limited understanding of the risk and their degree of exposure.” The same report evidences that “The board retains primary responsibility in just 14% of cases, suggesting that even while the risks posed by cyber threats are now being taken far more seriously across organisations, their boards are still not taking ownership of the risk.”

FIGURE 3 Please indicate which of the following potential stakeholders takes primary responsibility for the review and management of cyber risks in your organisation.
 Source: Marsh Continental European Cyber Risk Survey



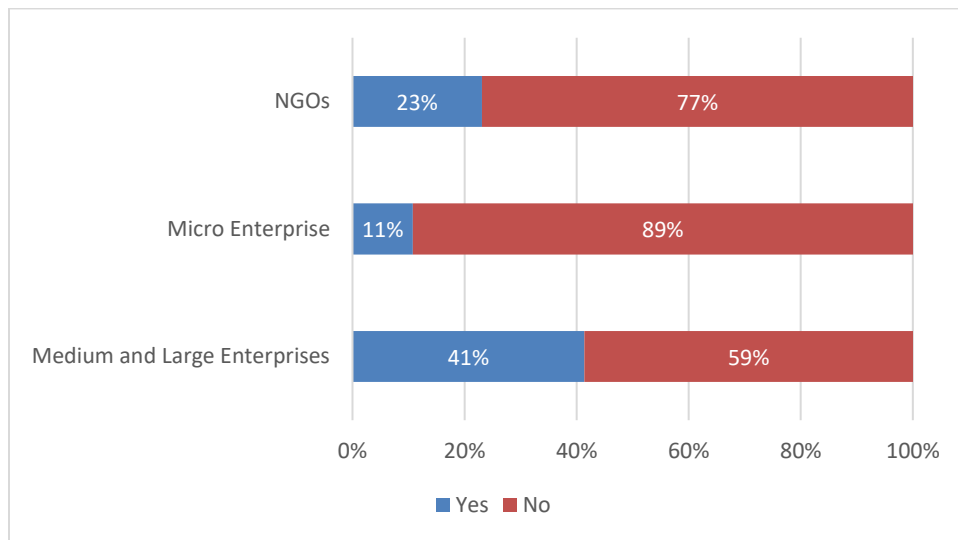
Continental European Cyber risk management 2016 Report (page 5)

³⁰ Marsh, “Continental European Cyber Risk Survey: 2016 Report,” October 2016, 7.

9.4.2. Skills and training on cyber security

Cyber education is another important aspect which has been overlooked by both businesses and VOs at a local level. As can be seen in Figure 20 below, the research conducted locally evidenced that training on cyber security was still lacking and was more likely to be carried out among medium sized enterprises as opposed to micro enterprises (NGO:23%, Microenterprises:11%, Medium and Large Enterprises: 41%).

Figure 20: Cyber security training in the last 12 months in businesses and VOs



The importance of ongoing/regular training on the topic cannot be undermined. The lack of expertise on the latest developments of cyber security, inhibits companies and users from adequately protecting themselves against cyber threats.

The lack of adequate skills was also highlighted in the Global EY survey titled 'EY's Global Information Security Survey'³¹ that indicated that 56% of organisations found that a lack of skilled resources was

³¹ [https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/\\$FILE/ey-global-information-security-survey-2018-19.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf)

one of the main obstacles faced by organisations. Furthermore, at an EU level, a report on the same topic - Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015- 2020) evidenced that the European private sector faces a shortage of digital skills with the availability of highly-skilled ICT personnel declining and the gap in vacancies required expected to reach 755,000 potential vacancies by 2020³².

9.4.3. Cyber security spending

The resources limitations (particularly financial constraints) amongst local micro-enterprises and VOs poses significant challenges in the implementation of appropriate cyber security practices. The quantitative research highlighted how budget constraints were considered to be one of the major obstacles that inhibited the implementation of appropriate cyber security functions.

The same EY report³³ referenced to earlier evidenced that over 87% of businesses needed up to 50% more to their existent cyber security budget and 89% of business indicated that their cyber security function did not fully meet their organisation's needs.³⁴

Furthermore, a study carried out by the European Economic and Social Committee³⁵, identified the lack of investment and availability of funding to be a reason for concern amongst SMEs. The same study highlighted that this target audience (European SME's) generally lacked awareness on the availability of public funds (targeting cyber security) and those entities that were aware, often took no action with the complex bureaucratic procedures being identified as the primary factor that discouraged them from seeking available cyber security funding.

9.4.4. Technologies vulnerabilities

The local scenario with respect to technologies is analogous to organisations across Europe that are reliant on externally-developed technologies for software and hardware (and certain services).

In line with European practices, the in-depth interviews confirmed that local microenterprises and VOs increasingly made use of technologies that were imported, with the cost being the primary reason for this practice. Entities highlighted it made more sense to purchase software from large companies such as Microsoft that had the resources and capital at their disposal to continually invest in research and

³² Husing, Korte, and Dashja, "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)," 23.

³³ The Global Information Security Survey

³⁴ [https://www.ey.com/Publication/vwLUAssets/ey-giss-2018-executive-summary-en/\\$FILE/ey-giss-2018-executive-summary-en.pdf](https://www.ey.com/Publication/vwLUAssets/ey-giss-2018-executive-summary-en/$FILE/ey-giss-2018-executive-summary-en.pdf)

³⁵ https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf

development and upgrade as necessary thereby ensuring that they remained in the forefront in their field of competence.

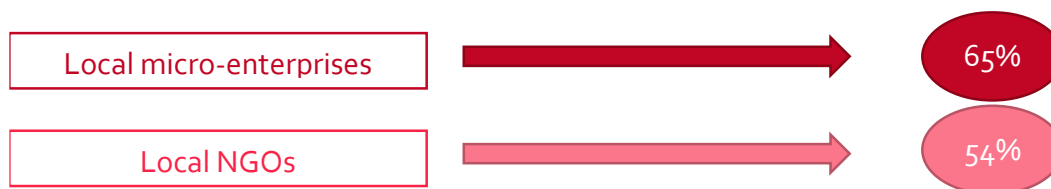
A study carried out by the European Economic and Social Committee³⁶ (study referenced earlier) evidenced that EU companies experienced similar trends. The same study further established that SMEs across Europe typically relied on outdated legacy systems³⁷. This increased the risk of further exposing businesses to cyber security attacks.

9.4.5. Trust in sharing information

Gauging the level of trust is a factor that is used to determine to what extent cyber security may be developed further.

As evidenced in Section 9.2.3 above, local business and VOs both felt that they could trust the public authorities to keep their online information and data secure.

Trust the public authorities to keep their online information and data secure

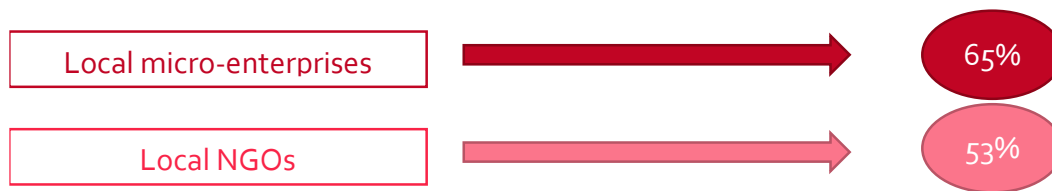


Furthermore, local businesses and VOs indicated that they trust that websites store their information and data in a secure manner.

Trust that websites store their information and data in a secure manner

³⁶ https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf

³⁷ Legacy system – definition - In the context of computing, a legacy system refers to outdated computer systems, programming languages or application software that are used instead of available upgraded versions.



The above figures highlight that overall, local business and VOs had trust in both government and private entities' websites for the storage of information and data. This is in contrast to the general situation among European businesses.

A review of the situation across the EU, as per study carried out by the European Economic and Social Committee, identifies lack of trust to share information as the primary issue (particularly in preparing for and responding to cyber threats and incidents), both from an external, public policy perspective, and from the internal, company perspective³⁸. On this topic – trust - the same report indicates that concerns of information sharing relate to the sharing of information at various levels:

- Between individual member States,
- Between governments and private enterprises,
- Between Computer Security Incident Response Team (CSIRTs), and
- Between individual enterprises across industries and borders

The above clearly illustrates a major variance between local organisations and their European counterparts with respect to trust issues.

9.4.6. Incident response plans

The ability of microenterprises and VOs to respond to a cyber security attack is dependent on the existence of a formulated incident response plan (IRP) and regular updating and testing of such a plan.

Whilst our study did not analyse whether micro-enterprises and VOs have implemented an incident response plan, we will be using the level of implementation of cyber security policies as a proxy since businesses and VOs that do not have cyber security policies in place are highly unlikely to have an IRP plan too. Furthermore, the likelihood is that not all entities that have some form of cyber security policy in place also have a formulated incident report plan in place.

³⁸ https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf (page 89)

The research evidenced that circa one third of local entities had a formally defined ICT security policy in place (38% of micro-enterprises and 31% of VOs).

A review of the situation across the EU (study carried out by the European Economic and Social Committee) evidenced that circa 60% of EU companies had some form of IRP in place.

There were however variances between countries. With reference to the UK the same report quoted another study³⁹ that highlighted that *“All in all, only 18% (of businesses) reported having a well-defined plan that is applied consistently throughout their entire enterprise”*.

Having a dedicated incident response/crisis management plan has proven to have a positive effect when mitigating the operational, financial and reputational impact of a cyberattack.

Cyber security: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks

9.4.7. Organisational designs

Our in-depth interviews (and secondary research) evidenced that locally, a good number of microenterprises tend to have an informal organisational structure in place.

Such informal setting is also the result of such entities' limited financial and human resources at their disposal. As a result, within such organisations a jack of all trades master of none mindset prevailed with individuals lacking specialisation. This approach was particularly predominant in the retail and wholesale sector (though not only) that comprised a good number of sole traders and family businesses. With each individual being tasked to look after multiple functions, cyber-preparedness levels within the organisation/ business entity were generally lacking as less time was allocated toward improving IT systems and security within the business/NGO.

At European level (study carried out by the European Economic and Social Committee), businesses, particularly small enterprises tended to have similar informal structures that was predominant among

³⁹PonemonInstitute, “TheCyberResilientOrganisationintheUnitedKingdom: LearningtoThriveagainstThreats,” January2016,8.

local entities. Furthermore, the same report established that cyber security strategies remained confined to IT departments with little involvement of senior management. Such a stance was highlighted as a possible restriction to the effectiveness of the cyber security measures and low preparedness levels.

The average age of directors is also of relevance, as older board members generally find new technologies intimidating and may prefer to channel ICT-related issues towards IT departments.

Interview with Mr. Arie van Bellen (ECP), 24 October 2017

10. READINESS INDEX FOR MICROENTERPRISES AND VOs

10.1.Brief

The cyber security landscape is never static and continually evolving. This situation necessitates businesses to have a proactive approach and be cyber ready.

Being cyber ready revolves around being aware and prepared for the threats present today and tomorrow and being able and capable of reacting, responding and recovering when the worst happens, not just trying to prevent it. This involves embracing digital change, and the possible opportunities and disruptions that this could bring with confidence and composure. In line with this, the final part of this analysis sought to determine micro-enterprises and VOs cyber security readiness.

To draw up a comparable readiness index we have used a report published by Vodafone International - The Vodafone Cyber Ready Barometer 2018⁴⁰ - that specifically investigated the levels of Cyber Security and Readiness in businesses around the world, with reference to 5 European countries, these being: Ireland, the United Kingdom, Spain, Italy and Germany.

We define a Cyber Ready business as one that is effectively prepared for the challenges and opportunities of cyber security - able to not just survive but thrive. As the cyber landscape evolves at pace, businesses and decision makers must too – adopting a more proactive, attacking approach to securing their information, people, places and things.

Vodafone Cyber Ready Barometer 2018

The objective of this section, in line with the baseline report, is thus to assess the levels of security readiness and resilience across businesses and VOs locally, compare such findings to those collated internationally and gain a better understanding of the factors that contribute towards being cyber ready and how it affects business success.

10.2.Methodology

In line with the baseline report, our readiness index sought to assess local businesses and VOs across six criteria contributing to readiness levels and assigned an overall readiness score out of 100. This score was then used to categorise the level of Cyber Readiness that fell under one of the following classifications:

⁴⁰ https://img.en25.com/Web/VodafoneGroupPLC/%7b1dd2abd4-17b9-4e81-9b23-347f2b41f338%7d_Vodafone-Cyber-Ready-Barometer-research-report-2018.pdf

Advanced – score of 75+

The leading subset of Cyber Ready companies - this group of businesses are leading the way in their approach to cyber security, readiness and resilience - and reaping the rewards.

Proactive – score of 61 to 74

This group of businesses are Cyber Ready today, gaining a competitive advantage on their less ready competitors, but there is still potential for further improvement.

Developing – score of 46 to 60

This group of businesses have shown they have achieved a good level of readiness across several areas, but still have gaps and threats to address if they are to become a truly Cyber Ready business.

Reactive – score of 26 to 45

This group of businesses have taken some action to secure their business, but are generally on the back foot when it comes to cyber security. They have significant scope for improvement across the board.

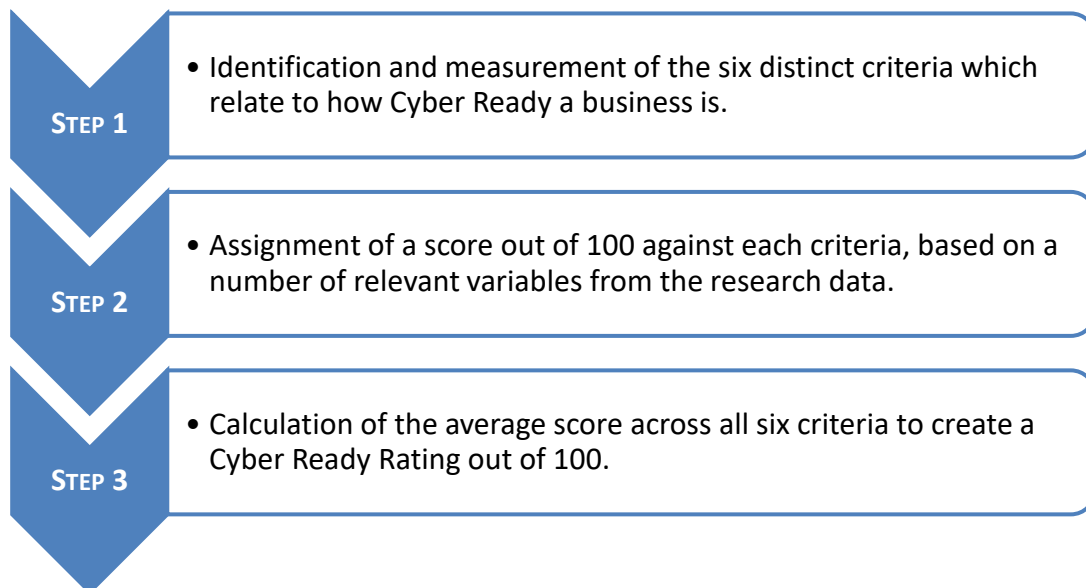
Basic – Score of 25 or less

This group is lagging behind the rest, whether due to a lack of budget, skills or awareness, and it is leaving them at significant risk and at a distinct competitive disadvantage.

Cyber ready

Businesses that fell within the Proactive or advanced classification are classed as Cyber Ready.

Method adopted:



In line with the Vodafone study, the following 6 criteria were utilised to determine organisations' cyber security readiness:

Digital Footprint

Relates to the trail of data entities create while using the Internet, and includes such factors as emails sent, and information submitted to online services. This factor also included the extent of employees' use of bring your own device (BYOD) within organisations. In this respect our survey incorporated three questions that tackled this criterium:

- If organisations make use of more than one online service
- If staff in organisations use their own personal devices (such as mobile phones, laptops, tablets) for regular work
- The extent to which businesses consider online services (services provided via the internet) as a core part of the goods and services they provide as an organisation

Cyber Operations

This focusses on an organisation's confidence in its ability to secure their sensitive and personal data, whether in the cloud or on mobiles. It also looks at the level of investment in information security. In this

respect our survey incorporated two questions that tackled this criterium:

- The extent to which organisations are sufficiently capable of protecting itself against cybercrime, e.g. by using antivirus software
- The extent to which organisations make use of external web based services such as Gmail, One Drive etc to send emails with data, transfer or storage of data.

Cyber Resilience

This assesses whether businesses have in place and test relevant security policies and look at their company's ability to identify, contain and recover/ learn from an attack. In this respect our survey incorporated two questions that tackled this criterium:

- The extent to which an organisations currently have cyber security policies in place
- Determining the steps taken by organisations to ensure that they do not get exposed to cyber attacks

Cyber Strategy

This factor assesses whether there is support and buy-in from senior management for improved security measures. It also digs into the extent to which the business understands that a strategic approach to security can differentiate in the eyes of customers. In this respect our survey incorporated three questions that tackled this criterium:

- Determine how high or low a priority cyber security is to organisations directors, trustees or senior management
- The extent to which organisations sought information assistance or consultation over the past 12 months, in relation to the threat of cyber security it faced
- The extent to which organisations are interested in attending training on cyber security.

Employee Awareness

Looking into whether businesses have plans and policies that specifically address the security behaviour and actions of employees and whether there is dedicated security training for staff. In this respect our survey incorporated two questions that tackled this criterium:

- Assess how well-informed organisations felt they were with respect to the cyber security threats they faced
- Determine whether employees attended training – internally or externally – relating to cyber security over the past 12 months.

Understanding Risk

Determining the level of awareness and consideration of security issues in organisations, especially when implementing new initiatives. In this respect our survey incorporated three questions that tackled this criterium:

- Assess the percentage of outsourced services by organisations
- Determine organisations' perceived risk of being a victim of cybercrime
- Determine what efforts were undertaken to reduce the risk of hacking attempts.

While the research followed the 6 criteria utilised by the baseline report, there were some minor alterations with respect to the distinct questions that categorised each criterium; This being dependent on the data collated from the primary research whilst ensuring congruency with data extrapolated from the secondary research.

10.3. Microenterprises readiness Index

10.3.1. Overall

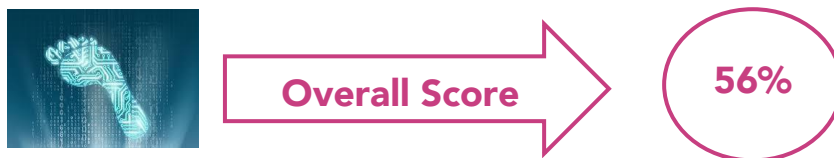
With an overall score of 49%, local microenterprises fall within the developing stage of readiness. This implies that overall, microenterprises have achieved a good level of readiness across certain areas, but still have gaps and threats to address if they are to become a truly Cyber Ready businesses.



10.3.2. A review of responses by the various criteria

f. Digital Footprint

With an overall score of 58%, the digital footprint of microenterprises is overall positive, with this criterium ranking 2nd among the 6 criteria under review.



A further in-depth analysis evidences that local entities rank high with respect to the utilisation of multiple online services – attaining an overall score of 76%. Entities had contrasting opinions with respect to the perceived importance of online services (services provided via the internet) for the conduct of their business provision, with this factor attaining an overall score of 56%. The other factor considered in relation to digital footprint related to the propensity of employees to use personal devices for work purposes, with this factor attaining an overall score of 44%.

g. Cyber Operations

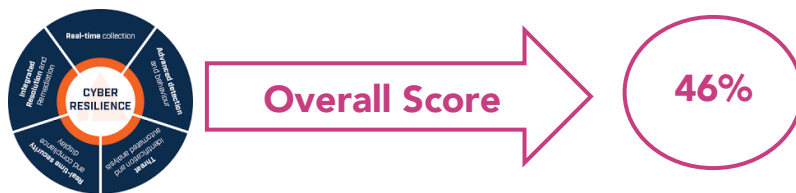
Overall, local microenterprises have considerable confidence in the security of cyber operations, with this criterium ranking highest among the various factors under review.



Two factors were analysed here. The first related to organisation’s perceptions as to how sufficiently capable they were at protecting themselves against cybercrime, with the majority of the opinion that they were capable – with an overall score of 87%. The second element assessed to what extent entities had trust in web-based services and subsequently utilised them to transfer or store data (such as Gmail, One Drive and similar). The assumption being that lack of confidence would result in lack of utilisation of such services. Overall, this factor attained a score of 68%.

h. Cyber resilience

Cyber resilience refers to how well an enterprise can manage a cyberattack or data breach while continuing to operate its business effectively.



The two factors that were analysed under this criterium related to assessing:

- I. To what extent microenterprises had cyber security policies in place **With an overall score of 38% microenterprises generally did not have cyber security policies in place.**
- II. The step/s organisations took to ensure that their organisation would not get exposed to cyber attacks **In our study organisations were asked to indicate the various layers of protections undertaken. It was subsequently assumed that entities that adopted 3 or more steps were deemed to be rather cyber resilient. Overall, microenterprises scored 55%.**

i. Cyber Strategy

This factor relates to businesses’ belief in and support towards a cyber security strategy, with results evidencing that microenterprises are not particularly geared towards a cyber strategy.



An assessment of board-level support for a cyber security strategy provided mixed views, with this factor attaining an overall score of 56%.

To determine to what extent stakeholders believed that information security was of high strategic importance for the organisation, this exercise determined to what extent organisations sought information, assistance or consultation over the past 12 months, in relation to the threat of cyber security it faced. The assumption done here being that the two factors – importance given to information security and actual information sought were interlinked. Overall, this factor attained a low score of 18%.

Another element considered related to determining to what extent organisations were interested in attending training on cyber security. Views varied with the overall score for interest in attending such sessions standing at 40%.

j. Employee awareness

Among the various factors under review, employee awareness rated lowest.

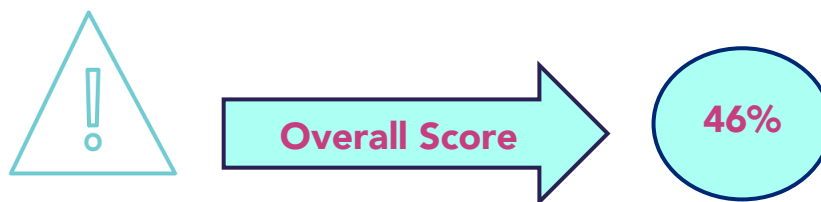


Two factors contributed to this criterium. One factor focused on how well-informed employees felt they were on cyber security, with views varying among this target audience. Overall this factor attained a score of 49%.

The other factor sought to determine, whether employees had attended, internally or externally to training, seminars or conferences on cyber security. With an overall score of 9% the vast majority of microenterprises answered in the negative.

k. Understanding risk

This criterium relates to microenterprises aptitude to invest in the necessary skills to minimise its cyber security risk and their perceptions on their propensity to a cyber security breach and actions taken to minimise such occurrence.



With a score of 79% microenterprises understood the risks they faced and the likely increase in threat over the coming months. Nonetheless, notwithstanding the limited specific skills available internally,

microbusinesses were not inclined to outsource to acquire such skill sets (overall score of 26%). Furthermore, with a score of 35%, overall such target audience did not undertake any specific measures to reduce the risk of hacking attempts.

10.4. Voluntary Organisations readiness Index

10.4.1. Overall

With an overall score of 54% local VOs too fall within the developing stage of readiness. This implies that overall, they have achieved a good level of readiness across certain areas, but still have gaps and threats to address if they are to become a truly Cyber Ready businesses.



10.4.2. A review of responses by the various criteria

a. Digital Footprint

With an overall score of 72%, the digital footprint of VOs is overall very positive.



A further in-depth analysis evidences that local VOs rank high across the various factors that related to this criterium, these being:

- VO makes use of more than one online services
- Staff in the organisation use their own personal devices for regular work
- Online services (services provided via the internet) considered to represent a core part of their VO endeavours

Such a stance is in line with feedback collated from the in-depth interviews with the sector whereby such entities tend to lack of resources and consequently utilise readily available, free online services at their disposal. Furthermore, the financial limitations resulted in individuals, particularly those operating on a voluntary basis, to use their own personal devices for regular work.

b. Cyber Operations

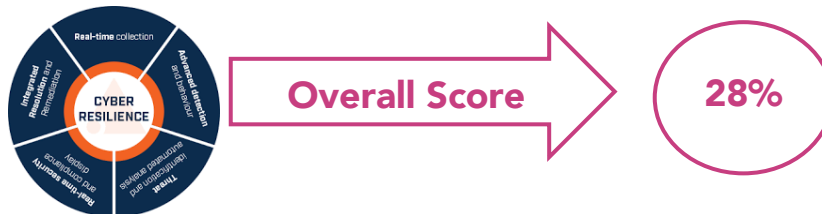
Overall, local VOs have considerable confidence in the security of cyber operations, with this criterium ranking highest among the various factors under review.



Two factors were analysed here. The first related to organisation's perceptions as to how sufficiently capable they were at protecting themselves against cybercrime, with the majority of the opinion that they were capable – with an overall score of 75%. With a score of 87%, the vast majority of individuals working with VOs indicated having trust in web-based services and subsequently utilised them to transfer or store data (such as Gmail, One Drive and similar).

c. Cyber resilience

Cyber resilience refers to how well an enterprise can manage a cyberattack or data breach while continuing to operate its business effectively, with local VOs rating very low.



VOs indicated that they generally did not have a cyber security policy in place (overall score of 31%). Furthermore, with an overall score of 26% such entities generally did not take the necessary step/s to ensure that their organisation would not get exposed to cyberattacks.

d. Cyber Strategy

This factor relates to entities' belief in and support towards a cyber security strategy, with results evidencing that VOs perceive themselves to be geared towards a cyber strategy.



The two factors that rated high under this criterium relate to the importance given to cyber security risk (an overall score of 73%) and such target audience's interest in attending training on the topic in question (an overall score of 72%).

That said, with an overall score of 35% generally, VOs had not sought information, assistance or consultation over the past 12 months, in relation to the threat of cyber security it faced.

e. Employee awareness

Employees felt that they were fairly aware of the topic in question.



Two factors contributed to this criterium. One factor focused on how well-informed employees felt they were on cyber security, with this factor attaining a score of 67%.

The other factor assessed whether employees had attended, internally or externally to training, seminars or conferences on cyber security. This factor attained an overall score of 23%.

f. Understanding risk

This criterium relates to VOs aptitude to invest in the necessary skills to minimise its cyber security risk and their perceptions on their propensity to a cyber security breach and actions taken to minimise such occurrence.



VOs awareness of the risks they faced and the likely increase in threat over the coming months attained a score of 58%. With an overall score of 15% VOs were not inclined to outsource to acquire such skill sets. A review of VOs measures undertaken to reduce the risk of hacking attempts resulted in a score of 46%

10.5. Benchmarking results

With an overall score of 49% microbusinesses are in line with the UK (with this country also attaining a score of 49%). This readiness index implies that, overall, such organisations are in the developing stage.

Ireland (40%), Germany (42%), Spain and Italy (both on 44%) fall within the reactive stage; implying that businesses within this segment have taken some action to secure their business but are generally on the back foot when it comes to cyber security. Such entities have significant scope for improvement across the board.

A primary factor that has enabled Maltese entities attain a high score relates to the positive perception, and trustworthiness organisations have of data stored by public entities and other private organisations. Linked to this is organisations' general willingness to utilise web-based services to send data via email, and to utilise other web-based services for the transfer or storage of data.

Further to this, on a national level, it can be seen that Malta was ranked in the 46th place out of 131 countries (50.65%) in the NCSI National Cyber Readiness Index.⁴¹ This highlights that at a National level, Malta is ranked fairly high amongst other countries worldwide.

Another noteworthy consideration which has an impact on the development of cyber security is the ICT Development Index and the Networked Readiness Index where Malta was ranked in the 24th place and 34th place respectively in each Index.⁴² These two indexes indicate that Malta is well positioned to develop its IT systems which in turn would help to combat the cyber security threats faced by microenterprises and VOs.

Another separate study conducted by ITU, revealed that when it comes to National Cyber security commitments, Malta was considered to be in the maturing stage which means that that Malta had developed complex commitments, and engaged in cyber security programmes and initiatives.⁴³

⁴¹ <https://ncsi.ega.ee/country/mt/?pdfReport=1>

⁴² <https://ncsi.ega.ee/country/mt/>

⁴³ https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

11. Conclusions & Recommendations

11.1. Conclusions

This report has identified a number of factors pertaining to cyber security and cyber threats among local businesses and voluntary organisations.

11.1.1. IT Dependability

The research has evidenced that overall entities – both microenterprises and VOs depend on some form of digital communication or services. Businesses primarily rely on:

- Email (88%),
- Social media pages (77%);
- Website or blog (73%) and
- Online bank account (72%)

Among VOs, social media attained the highest score (87%) followed by emails (48%).

Furthermore, in line with the above, the research evidenced that both microenterprises and VOs tended to use externally-hosted web services (VOs 87%; businesses 67%). The high incidence may be attributed to entities limited financial resources and their positive perception of such external service providers. That said, a number of businesses indicated to prefer keeping the data stored internally on their server. Such views were primarily voiced by the professional (which include finance and insurance businesses) and healthcare sectors.

One of the factors to determine organisations' cyber security readiness index related to individuals' inclination to utilise personal devices for work purposes. The study highlighted that the vast majority of individuals working with VOs did so (86%), with the number of individuals employed in the private sector that utilised their personal devices being much lower (43%).

11.1.2. Awareness

In terms of awareness, overall, businesses and VOs perceived cyber security to be important to their organisation (66% and 73% respectively). A review of responses among businesses evidences variances by sector of activity with the professional and courier services sectors ranking cyber security to be extremely important (with overall scores of 95% and 91% respectively), while at the other end of the scale: members, repairs and personal services did not perceive cyber security to be of importance (with an overall score of 15%).

A comparison of local organisations with EU counterparts evidenced that local microenterprises' awareness levels were in line with the EU average population at around 50%, with local VOs perceiving themselves to be more aware (67%).

The in-depth interviews evidenced that sole traders and individuals that were involved in retail, services such as hair salons, grocery stores and the like (particularly village outlets), were still predominantly paper based and/or backed up soft copies of data. Relying predominantly on a cash register and a paper-based notebook minimised their reliance on web-based services/ activities.

A review of the main inhibiting factors from enabling entities to prioritise cyber security related to financial constraints. Lack of human resources also ranked high. Other factors mentioned being:

- The need for flexibility;
- Lack of awareness
- Time constraints and
- Lack of interest in the subject.

11.1.3. Main drivers of cyber security

The study has highlighted the main drivers of cyber security to relate to:

- I. The type of data stored by the organisation, with entities that collated and stored sensitive data more prone to give importance to cyber security
- II. Exposure to cyber security attacks, with organisations that had experienced an attack more prone to take measures to minimise a reoccurrence;
- III. Changes in regulation and compliance, with the GDPR being a case in point that instigated organisations to review their systems.

11.1.4. Seek information

The majority of organisations (both businesses and VOs) did not seek information or guidance on cyber security. The main reasons for this being similar to the inhibiting factors highlighted above.

11.1.5. Have policies in place

In terms of policies, half the businesses indicated to have some form of cyber security policy in place. Amongst VOs this stood at 31%. The study further highlighted that cyber security is generally handled internally among VOs and businesses (73% and 59% respectively). This position possibly relates once again to entities limited financial resources.

That said, both businesses and VOs indicated having one or more cyber security rules and controls in place, with the most common being:

- Email spam protection;

- The application of software updates when available;
- Having configured firewalls and having an up-to-date malware protection.

11.1.6. Training

Circa one fifth of those interviewed indicated to have undergone some form of training on cyber security. An assessment of organisations' future inclination/willingness to undergo similar training has shown that VOs (71%) look to such training more positively than do businesses (51%), with formal training and awareness programmes being identified as the most apt method.

That said time constraints and limited resources – both financial and human – are limitations that cannot be undermined when determining/ drawing up courses for such target audiences.

11.1.7. Breaches or attacks

The number of breaches or attacks recorded were minimal (10% for businesses and 6% for VOs), with medium to large sized entities more inclined to have experienced a breach than microenterprises (17% vs 7%). That said, reports⁴⁴ indicate that, on average it takes a organisation around 200 days for it to realise it has been attacked, hence there could be an element of under reporting among respondents (apart from instances where entities were not aware that they had been breached or attacked).

The research identified the police as the most likely entity organisations are to contact should they experience a cyberattack by both businesses and VOs (56% and 62%)

11.1.8. Trustworthiness

Overall local organisations have trust in data collated and stored by third parties. 65% of businesses indicated to trust such institutions as opposed to 30% of EU population.

11.1.9. Main threats

Maltese microenterprises and VOs have to deal with a number of cyber security risks (both external and internal), and while all sectors are exposed (though to varying degrees) to cyber security attacks,

⁴⁴ <https://safeatlast.co/blog/cyber-security-statistics/>
<https://smallbiztrends.com/2018/09/data-breach-statistics.html>
<https://www.itgovernance.co.uk/blog/detecting-cyber-attackers-how-long-does-it-take>

the professional sector is deemed to be the most likely to be exposed to a cyber security attack due to the valuable sensitive nature of data which they held.

Conversely, the 'wholesale and retail' sector was deemed to be the least exposed due to the limited online exposure found in their business processes.

In terms of company size, both microenterprises and VOs are particularly vulnerable in view of their limited resources – both financial and human.

At a local level, the main threats identified related to fraudulent emails; spyware and malware, viruses and denial of service attacks. These results being congruent with the primary threats identified among EU businesses.

11.1.10. GDPR

The research has indicated that businesses (75%) and VOs (87%) are (or perceive themselves to be) aware of GDPR. Nonetheless, almost half the businesses interviewed (45%) indicated that no changes were made once GDPR came into force. Such a stance is comparable to the EU.

11.1.11. Readiness Index

Microbusinesses readiness index was 49%, indicating that such organisations fall within the developing stage – implying that they have achieved a good level of readiness across several areas, though gaps remain.

Malta's readiness index is comparable to the UK (also 49%), with other countries included in the study, namely: Ireland, Italy, Spain and Germany having a score of around 42% that placed such countries in the reactive stage – implying that such businesses took some action to secure their business but were generally on the back foot when it came to cyber security.

The scoring revolved around 6 categories, these being: digital footprint, cyber operations, cyber resilience, cyber strategy, employee awareness and understanding risk. Local microenterprises rated highest with respect to cyber operations, and low on employee awareness and cyber strategy.

VOs cyber readiness index stood at 54% - thereby also falling within the developing stage. A review of responses for the 6 categories that constituted this readiness index evidences that VOs attained a high percentage score for digital footprint and cyber operations and a low scoring for cyber resilience.

11.2.Recommendations

The various research tools utilised have evidenced that cyber threats comprise a major risk for (European) businesses and as a rule, their vulnerability increases as their size falls⁴⁵.

Furthermore, this study has shed light on businesses awareness levels on the actual extent of cyber security threats to their businesses, with feedback collated, particularly during the in-depth interviews evidencing that in line with their European counterparts, microenterprises remain unaware or seem to underestimate and even neglect the potential impact a cyberattack could have on their businesses.

A survey conducted by Marsh revealed that as much as 69% of European companies have either no or only basic understanding of their exposure to cyber risks.

Marsh, "Continental European Cyber Risk Survey: 2016 Report ,"October 2016, <http://www.hkbb.ch/uploads/6869>

Data clearly indicates that cyberattacks are continually increasing and continuously evolving in terms of sophistication and novelty. **This situation highlights the importance for effective protection and response** and further evidences the vulnerability of VOs and microenterprises that have highlighted their human resource compliment and financial restraints as inhibiting factors for successfully adopting and maintaining effective cyber security measures.

The study has highlighted several issues faced by microenterprises and VOs that are non-technical in nature. The table below lists a number of these issues and provides potential recommendations to help deal with them.

45 <https://fortika-project.eu/>

Issues

Possible Recommendations

A general lack of awareness of cyber security at a company board level

- Ongoing efforts to create awareness and instigate top management/ board to adopt a proactive approach rather than a reactive approach.
- Engaging top level management will in turn facilitate the promotion of an attitude change towards how cyber security is managed
- This will result in a strategic organisational approach that involves all rather than being handled by an individual/ IT management/ department that revolves around sporadic efforts.

Lack of skills and training

- Promote cyber security training and certifications to expand the skill set of Maltese IT professionals.
- Set up training and awareness-raising activities amongst non-IT staff members so that they are able to improve their cyber security knowledge
- Create multiple tools and techniques to reach out to the individuals. Apart from formal face-to-face training consideration ought to be given to online tools such as webinars and podcasts to increase reach and consequent uptake.

Technological vulnerability

A lack of trust to share information which leads to corporate entities under-reporting

Lack of incident response plans

- Lobby with IT service providers to have a common platform that assists vulnerable organisations. This could be an opportunity for IT service providers to promote their products/service offerings
- In line with the above, the creation of local systems where security updates can be easily applied without much IT knowledge ought to be considered.
- Microenterprises ought to be encouraged to improve their backup and data recovery systems and procedures to significantly reduce the downtime and harm inflicted by any cyber security attacks.
- Technological deterrents need to be balanced with people centric efforts.
- Greater information sharing and coordination amongst stakeholders is required (possibly through the common platform highlighted above).
- Maltese companies need to evaluate the level of cyber risks that they face and build up their IT systems to be resilience against possible cyber security attacks. The implementation of an incident response plan should also be considered (this might not be relevant to all entities – the cost to carry this out need to be balanced against the likelihood of being attacked and the cost of such attack). Furthermore, once such a plan is adopted, organisations need to regularly

review it and see that it is applied throughout.

Organisational design

- Cyber security should become a top-level management issue and all the management should be involved. Furthermore information/ knowledge should be passed on to other members within the organisation (linked to the issue of awareness highlighted above).

Annex 1 - Profiling Malta's businesses and VOs

Online exposure

This section sets out businesses' and VOs exposure to cyber security risks. These risks can come about via their reliance on digital services and ecommerce, use of personal devices in the workplace (also known as bringing your own device, or BYOD).

- 1) How well informed do you feel about the risks of cybercrime? (single choice)
 - Very well informed
 - Fairly well informed
 - Not very well informed
 - Not at all informed
 - DK/NA

- 2) Do you consider online services (services provided via the internet) as a core part of the goods and services you provide as an organisation? (Single Choice)
 - Yes
 - No

- 3) What percent of your organisation's user devices contain current anti-virus/antimalware protections? Please select the percentage range for each computing device listed below.

	None	< 20%	21 to 40%	41 to 60%	61 to 80%	> 80%	All	Don't know
Laptop								
Desktop								
Other Devices								

4) Which of the following, if any, does your organisation currently have or use? (Multiple Choice)

- Email addresses for organisation or employees
- Website or blog
- Online bank account
- Social media pages or accounts
- Industrial control system
- Ability for customers to order, book or pay online
- Personal information about customers held electronically
- Other: ____

5) Do the staff in your organisation use their own personal devices (such as mobile phones, laptops, tablets) for regular work? (Single Choice)

- Yes
- No

6) Do you use externally hosted web services such as hotmail, Gmail or One drive to email, transfer or store data? (Single Choice)

- Yes
- No

Data

7) With regards to Cyber security, do you consider IT systems such as laptops, desktops, smartphones and other mobile devices as an important matter for your organisation's business operations?

- 0 - Not that important

- 1 - Somewhat important
- 2 - Neutral
- 3 - Very important
- 4 - Extremely important
- Don't know

7a) (If Q7 0,1 are selected) Why? (Multiple Choice)

- Insufficient people resources
- Complexity of compliance & regulatory requirements
- Lack of in-house skilled or expert personnel
- Lack of central accountability
- Lack of monitoring and enforcement of end users
- Insufficient budget
- Insufficient technology resources
- Security is not taken seriously as our organisation is not perceived as vulnerable to attack
- Other (Please Specify): _____

8) What are the top 3 types of data that are needed in your daily business to support your operations of the organisation?

- Consumer Data (e.g. ID number/ credit card number/ contact details)
- Business Client Data (e.g. contact details/ credits/ etc.)
- Transaction Data (e.g. payment information/ purchased items/ etc.)
- Business Proprietary Information (e.g. intellectual property, contracts, business confidential documents/ etc.)
- Other Sensitive Data (e.g. patient data/ membership data, etc.): _____ (Q8a)

8a) Which?

Answer: _____

Awareness and attitudes

This section looks at how big a priority cyber security is to businesses and VOs. It also covers where these organisations get information, advice or guidance about cyber security.

Importance of cyber security

- 9) How high or low a priority is cyber security to your organisation's directors, trustees or senior management? (Single Choice)
- Very high

- Fairly high
- Fairly low
- Very low
- Don't know

10) What are the reasons for prioritising or deprioritising cyber security? (Multiple choice)

- Organisational culture
- The seniority and time-commitment of staff overseeing cyber security
- Other priorities are given more priority
- It is a burden to implement cyber security
- Time
- Other: _____

Sources of information

11) Have you sought any information, advice or guidance in the last 12 months on the cyber security threats faced by your organisation? (Single Choice)

- Yes
- No

11a) If yes, from who?

- General internet searching
- Government sources of information on cyber security
- External security or IT consultants
- Other: _____
- No Answer

11b) If No, what are the reasons for not seeking advice? (Single Choice)

- Time
- Don't have the technical skills
- IT or cyber security functions are outsourced
- Did not feel a need to seek further advice
- Other _____

The General Data Protection Regulation (GDPR)

12) Are you aware of new GDPR rules that have come into force?

- Not at all aware
- Slightly aware
- Somewhat aware
- Moderately aware
- Extremely aware

13) What type of Cyber changes did your organisation make in preparation for the new Data Protection Act 2018 (GDPR)?

- Created or changed policies and procedures
- Additional staff training or communications
- Installed, changed or updated anti-virus or anti-malware software.
- Other _____
- Don't know as outsourced
- No changes were made

Approaches to cyber security

This section of questions looks at how much businesses and VOs approach the subject of cyber security with their staff, and the policies and procedures they have in place to identify and reduce risks.

Impact of outsourcing cyber security

14) How is your own/your organisation's cyber security managed?

- In-house by someone who is in charge of (security) policies on behalf of the organisation
- I manage my own cyber security
- Outsourced to an independent specialist or organisation
- By the Internet Service Provider
- Don't know
- Other _____

Staff training

15) Have you attended internal or external training, or seminars or conferences on cyber security in the last 12 months?

- Yes
- No

16) Would you be interested in attending training on the topic of cyber security?

- Yes

- No

17) What is the best way to educate employees (end users) within your organisation about safe data protection and security practises? (Multiple Choice).

- Conduct formal training and awareness programs
- Provide written policies and clear instruction to end users
- Automate policies that automatically enforce requirements behind the scenes
- Hold supervisors and managers accountable for educating subordinates on safe data protection
- Other (please specify): _____
- Don't know

Governance and planning

18) Does your organisation currently have cyber security policies in place?

- Yes
- No

19) What are the top factors that are hindering your organisation's ability to advance its cyber security efforts?

- Insufficient awareness within executive management
- Insufficient knowledge to prepare the documents
- Insufficient resources to prepare the documents
- Lack of time
- Lack of training
- Not relevant

20) What steps does your organisation take to ensure that your organisation does not get exposed to cyber attacks? Please select all that apply. (Unaided)

- Use of a firewall
- Email Spam protection
- Up-to-date malware and virus protection
- Enforce strict cyber security policies
- Security controls on company owned devices (e.g. laptops)
- Other: _____
- Don't know

20a) Which of the following cyber security measures do you have in place to safeguard your organisation against cyber security attacks? (Aided)

- Applying software updates when they are available
- Firewalls with appropriate configuration
- Email Spam protection
- Awareness and Employee Education
- Up-to-date malware protection
- Restricting IT admin and access rights to specific users
- Only allowing access via company owned devices
- Security controls on company owned devices (e.g. laptops)
- Segregated wireless network
- Monitoring of user activity
- Encrypting personal data
- Guidance on acceptably strong passwords
- Backing up data securely
- We currently have no cyber security measures in place
- Other (Please Specify) _____

Incidence and impact of breaches

Experience of breaches or attacks

21) Did your organisation experience a data breach involving the loss or theft of confidential or sensitive business information in the past 12-month period?

- Yes (Go to Q22)
- No (Go to Q26)
- Don't know (Go to Q26)

22) If yes, what type of records were lost or stolen?

- Mostly data involving consumers (individuals or B2C)
- Mostly data involving business customers (other organisations or B2B)
- Other business confidential information
- Don't know

23) If yes, how many separate incidents did your organisation experience in the past 12 months?

- Only 1
- 2 to 3
- 4 to 5
- 6 to 10
- More than 10
- Don't know

Types of breaches or attacks experienced

24) If yes, what type of breaches or attacks did you encounter in the last 12 months?

- Fraudulent emails or being directed to fraudulent websites
- Viruses, spyware or malware
- Others impersonating organisation in emails or online
- Ransomware
- Unauthorised use of computers, networks or servers by outsiders
- Hacking or attempted hacking of online bank accounts
- Denial-of-service attacks
- Unauthorised use of computers, networks or servers by staff
- Any other breaches or attacks: _____
- None of the above

25) If yes, how often has your organisation experienced or been a victim of the following situations?

	Often	Occasionally	Never	Don't know/ NA
Identity theft (somebody stealing your personal data and impersonating you)				
Receiving fraudulent emails or phone calls asking for your personal details (including access to your computer, logins, banking or payment information)				
Online fraud where goods purchased are not delivered, are counterfeit or are not as advertised				

Your organisation social network account or email being hacked				
Being a victim of bank card or online banking fraud				
Being asked for a payment in return for getting back control of your device				
Discovering malicious software (viruses, etc.) on your device				

26) If your organisation experienced or was a victim of a cyber-attack, who would be contacted?

- Police
- Website\Vendor
- Your Internet service provider
- Consumer protection organisation
- Other
- No one
- Don't know/ No Answer

27) To what extent do you agree or disagree with each of the following statements?

	Totally Agree	Tend to agree	Tend to disagree	Totally disagree	DK
Your organisation's online Information and data are not kept secure by websites					
Your online Information and data are not kept secure by public authorities					
As an organisation, you avoid disclosing any personal information Online					
The risk of your organisation being a victim of cybercrime is increasing					

<p>Your organisation is sufficiently capable of protecting itself against cybercrime, e.g. by using antivirus software</p>					
--	--	--	--	--	--

Demographics

28) How would you describe your entity?

- An NGO
- Medium and Large Enterprise
- Micro Enterprise
- Other_____

29) Where do you generally operate from?

- Malta
- Gozo
- Both
- None
- Other _____

30) Which category most closely fits your organisation type?

- Wholesale and retail
- Professional
- Construction
- Agri/fisheries
- Memberships, repairs, personal services
- Manufacturing
- Administration & Support
- Accommodation, food & beverages

- Courier services
- Education
- Creative Arts, Entertainment
- Real estate
- Media, IT

31) How many employees work for your organisation? –

- 1-9 people
- 10-49 people
- 50-249 people
- 250+