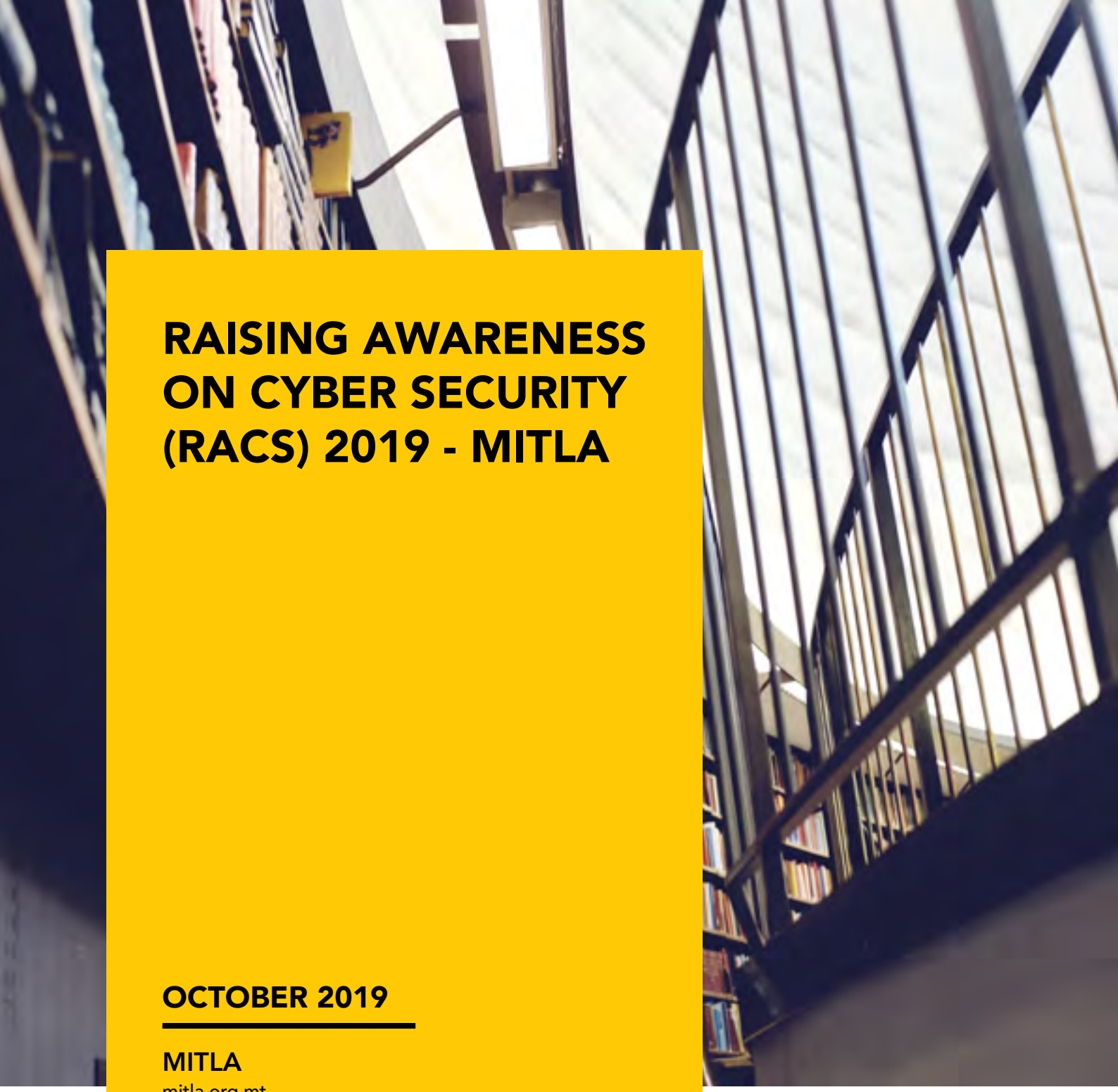


RAISING AWARENESS ON CYBER SECURITY (RACS) 2019 - MITLA

OCTOBER 2019

MITLA
mitla.org.mt

This project is funded through the Voluntary Organisations Project Scheme managed by the Malta Council for the Voluntary Sector on behalf of the Ministry for Education and Employment.

VOPS

Malta Council for the VOLUNTARY SECTOR

PARLIAMENTARY SECRETARY FOR YOUTH, SPORT AND VOLUNTARY ORGANISATIONS

MALTA IT LAW ASSOCIATION

1 | HIGH LEVEL INTRODUCTION

HIGH LEVEL INTRODUCTION

The Raising Awareness on Cyber Security **(RACS)** project spearheaded by the Malta Information Technology Law Association **(MITLA)** seeks to provide a benchmark on comparative legal studies in Cyber Security and additionally provides a realistic snapshot of Maltese Small to Medium Enterprises (SMEs) and Voluntary Organisations' (VOs) practical responses to risks and gauge the actual Cyber Security threats they face.

This project was funded through the Voluntary Organisations Project Scheme managed by the Malta Council for the Voluntary Sector on behalf of the Ministry for Education and Employment.

The **RACS** project was split into three parts, namely:

1. Work Package 1 (WP1) - *Building a Path through the Patchwork of Cybercrime Laws* delivered by the Department of Information Policy & Governance at the University of Malta, studied the Maltese cyber security legal framework, to determine laws regulating cyber security and any legal developments in the field which apply to VOs and local businesses to protect them against cyber threats. The involvement of other VOs interested in cyber security, cyber security experts, ICT lawyers and law student organisations, was sought for the identification of such laws. The review has considered local, EU and international legal instruments which regulate online security, including privacy and data protection laws, criminal laws, intellectual property laws, electronic communications laws, laws on electronic commerce, and other instruments regulating confidentiality. This analysis identified and researched technical permutations of local VOs and SMEs which are directly dependent on legal obligations related to cybersecurity.

2. Work Package 2 (WP2) - *Accessing Cyber-Security Readiness with SMEs and VOs* delivered by EMCS Limited, investigated the level of awareness on cybercrime amongst VOs and SMEs in Malta and gauges measures implemented by said entities to mitigate security breaches. The current understanding amongst local entities remained unclear up till now and warranted an investigation, in line with the local and EU laws, towards effective cyber security. A situational analysis was

conducted through the involvement and interviewing of local stakeholders, particularly, other voluntary organisations and SMEs to make collaboration and the involvement of VOs and various sectors of the economy a key initiative for the RACS project. When completed, all respondents' replies, and the survey were extrapolated and consolidated in a report.

3. Work Package 3 (WP 3) of the RACS project consolidates the conclusions derived from both WP 1 and WP 2 and is publishing a report taking into consideration the previous two deliverables. It also disseminates and markets the individual reports derived from WP 1 and WP 2 to relevant audiences. WP 3 ensures that the highly specialised material made possible through VOPS funding is made available to interested parties.

The RACS project is in line with the Government Cyber Security Initiative, which aims to foster cooperation and collaboration amongst various stakeholders at national level. The RACS project, along with the published data, intends to: raise awareness and educate local micro-businesses and VOs on the existence of cyber-threats and the current state of play in this field, including the extent of the problem at the domestic front. This shall in turn raise awareness amongst the local communities and encourage them to adopt adequate measures to protect themselves against said threats. VOs and micro businesses shall have the tools to identify common threats and security measures that specifically target them (thanks to the survey conducted through this project.

Besides businesses and VOs, the information in the RACS report will also be easily consumable by anyone interested in ICT, including security experts and non-experts, regulators and the Government, in line with local and EU proposals for a safer digital Malta.

In addition to knowledge sharing and availability of data to the public, the RACS project is designed to be self-sustainable and periodic re-runs can be conducted.

Dr Antonio Ghio
MITLA President

Dr Sharon Xuereb
Dr Deo Falzon
MITLA RACS Project Managers

"The RACS project, along with the published data, intends to: raise awareness and educate local micro-businesses and VOs on the existence of cyber-threats and the current state of play in this field, including the extent of the problem at the domestic front."

The objects and purposes for which the Malta IT Law Association has been constituted are:

To promote the advancement and development of information technology law, including but not solely limited to computer law, internet law, electronic communications law, information law, electronic commerce law, remote gaming law and cybercrime, (hereinafter referred to as "ICT Law") in Malta and the advancement of Malta as an international centre of excellence in ICT Law;

To actively research, discuss and circulate information on legal developments taking place on the international plane and within the European Union with respect to ICT Law and the knowledge economy;

To promote with international and regional organisations or associations and other national government and non-government bodies legislative and regulatory changes related to ICT Law and to consider together with these entities proposals for legislative interventions having the same aim;

To afford opportunities for the discussion and consideration of matters of interest to members of the Association and to undertake or assist in the preparation of legal instruments and papers in respect of such matters; and

To collect and circulate statistical and other information of interest to the members of the Association and to form a collection of publications and documents accessible to the members of the Association.

MALTA IT LAW ASSOCIATION

2 | BUILDING A PATH THROUGH THE PATCHWORK OF CYBERCRIME LAWS

BUILDING A PATH THROUGH THE PATCHWORK OF CYBERCRIME LAWS

WORK PACKAGE 1

Access the entire research document compiled by the Department of Information Policy & Governance at the University of Malta or at https://www.mitla.org.mt/publications/cybersecurity

Introduction

In its simplest definition, cybercrime refers to those activities conducted online that lead to the commission of an act that the law classifies as a crime. These can range from those acts that compromise the confidentiality or integrity of electronic data, to copyright and intellectual property breaches of a criminal nature, to content-related offences such as child pornography. Its effects can be devastating on communities, businesses and governments and comes at a significant cost to both national and global economies each year.

MITLA has over the past year funded research into gauging the current level of awareness on cyber security in Malta, and the extent to which businesses and other entities in Malta prioritise this issue when going about their daily business. The project has not only looked at the legal frameworks that exist in Malta, but also at those that exist in other EU states. This research has in turn been coupled with market research conducted amongst SMEs and NGOs and the end result is one that paints a fairly accurate picture on where things currently stand in Malta.

Key Findings

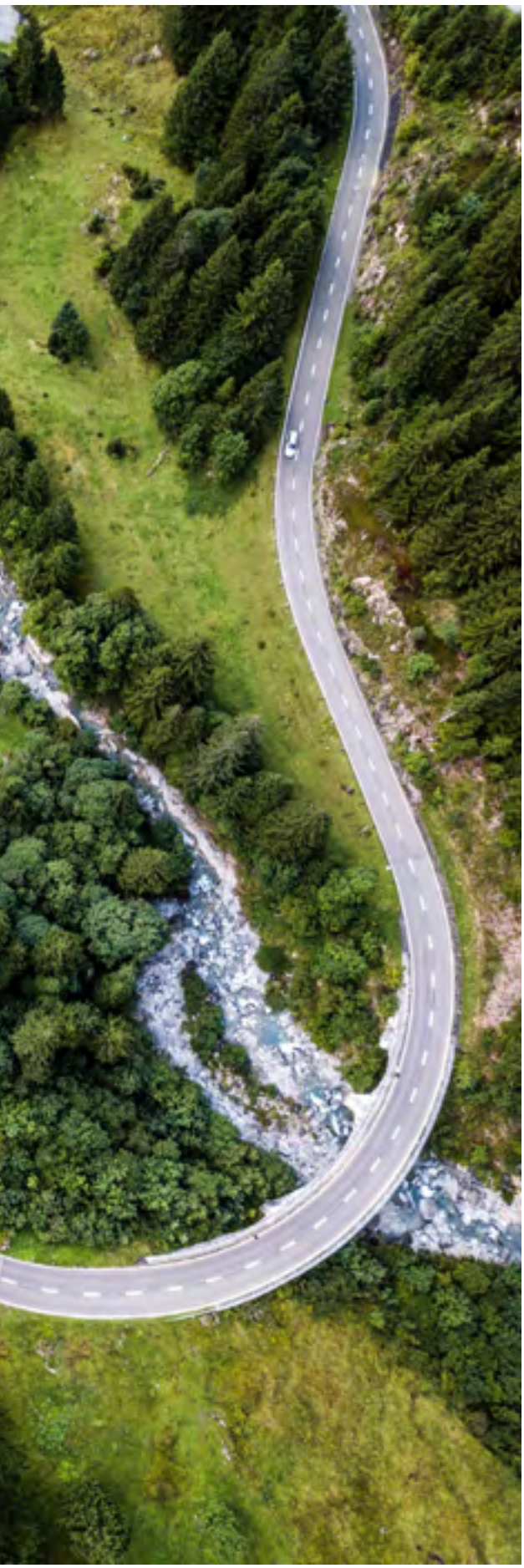
The key findings that the project has yielded can be summed up as follows:

- According to the EU's cybersecurity strategy, it is predominantly up to the member states to deal with security challenges in cyberspace. This has inevitably led to a somewhat fragmented legislative structure at European level, with the various member states often trailblazing in different directions with varying levels of success.

- The Council of Europe adopted Convention 185 in 2001, which includes most European states, and includes the USA, Japan and Australia. The aim of the Convention is to address crimes committed on the internet and that affect issues of copyright, computer-related fraud, child pornography, hate crimes and violations of network security. In these areas, the Convention attempts to create base levels of harmonisation, which in turn allow for a fast and effective regime of cooperation amongst states in investigating and prosecuting these cross-border crimes such as these.

- Convention 185 has been transposed into the national laws of most EU member states, and the project has looked at the various ways in which this transposition has taken place. Although in some areas there is a high level of harmonisation amongst the EU states in question, in other areas this appears to be lacking. Crucially, several EU member states have not adopted specific provisions that address the specific needs of SMEs and NGOs, which are therefore covered in exactly the same way as any other legal person for the purposes of the law. This includes Malta.

- At an EU level, cybercrime is a borderless problem that still depends heavily on the member states having strong and effective legislation in place at national level in order to combat that problem.



The EU rests strongly on Convention 185 of the Council of Europe and has adopted it as its own legal benchmark for tackling cybercrime, and has built on it, rather than create completely different directives and regulations. This is perhaps a practical approach that avoids having its member states fly too far, so to speak, from a base level of regulation. The EU has consequently issued a vast number of strategies and policy papers that go a long way towards creating harmonisation across the bloc, albeit in a patchwork manner. One of the key ways in which harmonisation has been attained is through the General Data Protection Regulation, which came into force in May 2018 and which has attempted, amongst other things, to standardise security measures and organisational safeguards that affect the processing of personal data.

- Apart from other EU states, Malta has adopted the vast majority of the available EU legal instruments into its own legislation. This includes a robust set of laws that have been included in its Criminal Code, and which deal specifically with cybercrime and other crimes that involve the misuse of computer and telecommunications equipment.

Recommendations

The research project has gone beyond merely providing a roundup of the legal situation in Malta and elsewhere in the EU, but has also considered practical ways in which Maltese entities, and specifically SMEs and NGOs can best be supported in equipping their businesses against the effects of cybercrime. The principal recommendations that have been issued include:

- Supporting SMEs and NGOs in better understanding and implementing appropriate security measures within their businesses, either by making reference to specific ISO standards, or by developing certification programmes for basic technical controls.

- Setting up a one-stop-shop style of entity that provides information and support on cyber-security issues. This can be achieved either by building a public information platform (or extending the purpose of existing platforms), and by grouping the currently fragmented laws and regulations into a single legal Code that deals specifically with cybercrime.

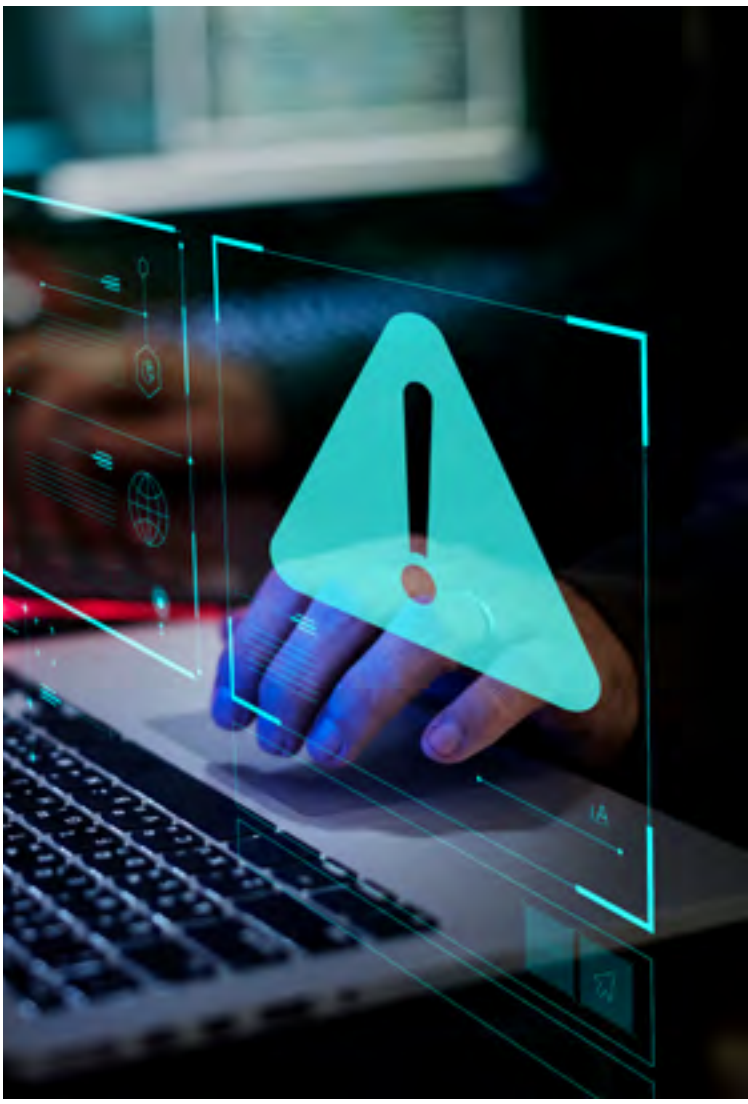
Conclusions

- The project has recognised that SMEs and NGOs require special focus and additional support when battling cybercrime issues – due to the fact that their financial, technical and human resources cannot be funded to the same level of large enterprises. A one-size-fits-all approach is therefore often difficult to apply to them. It follows that providing funding for fostering know-how in meeting cybersecurity standards needs to become a higher priority in Malta and elsewhere. Similarly, information and resources on cybersecurity issues need to become more easily accessible to those same SMEs and NGOs.

- On a parallel level, there is an increased importance of knowledge transfer between government, academia and private entities, as this is conducive towards the protection of the country's economy and well-being as a whole. Measures that foster the exchange of information between the various players, and which create platforms where different actors can collaborate on issues of cybersecurity need to take centre-stage position. This includes the creation of programmes that develop the skills of SME and NGO personnel in the area of cybersecurity, through ongoing training.

- Lastly, the project has underscored the severe need for raised awareness in all matters relating to cybercrime and cybersecurity. This is ultimately the starting point in ensuring that all players are aware of the risks that befall them and places them in a position to decide how best to safeguard themselves against those risks.

Access the entire research document compiled by the Department of Information Policy & Governance at the University of Malta or at https://www.mitla.org.mt/publications/cybersecurity



"The project has recognised that SMEs and NGOs require special focus and additional support when battling cybercrime issues – due to the fact that their financial, technical and human resources cannot be funded to the same level of large enterprises."

3 | ASSESSING CYBER-SECURITY READINESS WITH SMEs AND VOs

ACCESSING CYBER-SECURITY READINESS WITH SMEs AND VOs

WORK PACKAGE 2

Access the entire research document compiled by EMCS Limited:
https://www.mitla.org.mt/publications/cybersecurity

Introduction

Conducting an actual qualitative and quantitative study into cyber-security readiness in the general scheme of things 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 Committee 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 risks. The level of investment in cyber security overall is insufficient. Most businesses do not realise its importance until after experiencing a security breach . 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."

Key Findings

DEPENDABILITY ON IT SYSTEMS

Percentages are expressed out of the total of entities surveyed.

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 organisations place higher levels of trust in data collected and stored by third parties than other Europeans (65% of local businesses trust as opposed to 30% of Europeans).

VOs in particular tend to have higher levels of dependability on social media platforms than businesses (87% as opposed to 77% for businesses). Another marked difference between businesses and NGOs is the used of personal devices, which reaches an 86% level among NGOs, as opposed to 43% in businesses.

Both SMEs and NGOs recorded high levels of use of cloud computing (Businesses 67% / NGOs 87%), principally due to the economical cost of doing so. Roughly one-third of Medium and Large businesses expressed a preference to host their data on their own servers, citing security as the main reason for doing so.

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 with 73% considering cybersecurity to be of importance to their organisation.

From a sectorial perspective, it was professional business that rated cybersecurity as important with a 95% score, whilst lower down the list, media, IT, wholesale & retail, and repair or personal services registering scores of 50% or less.

Medium and large enterprises consider cybersecurity to be far more of a priority than micro enterprises, with 71% of medium and large businesses giving cybersecurity a top rating priority score, contrasted against only 19% of micro enterprises that rated it at the same priority level.

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

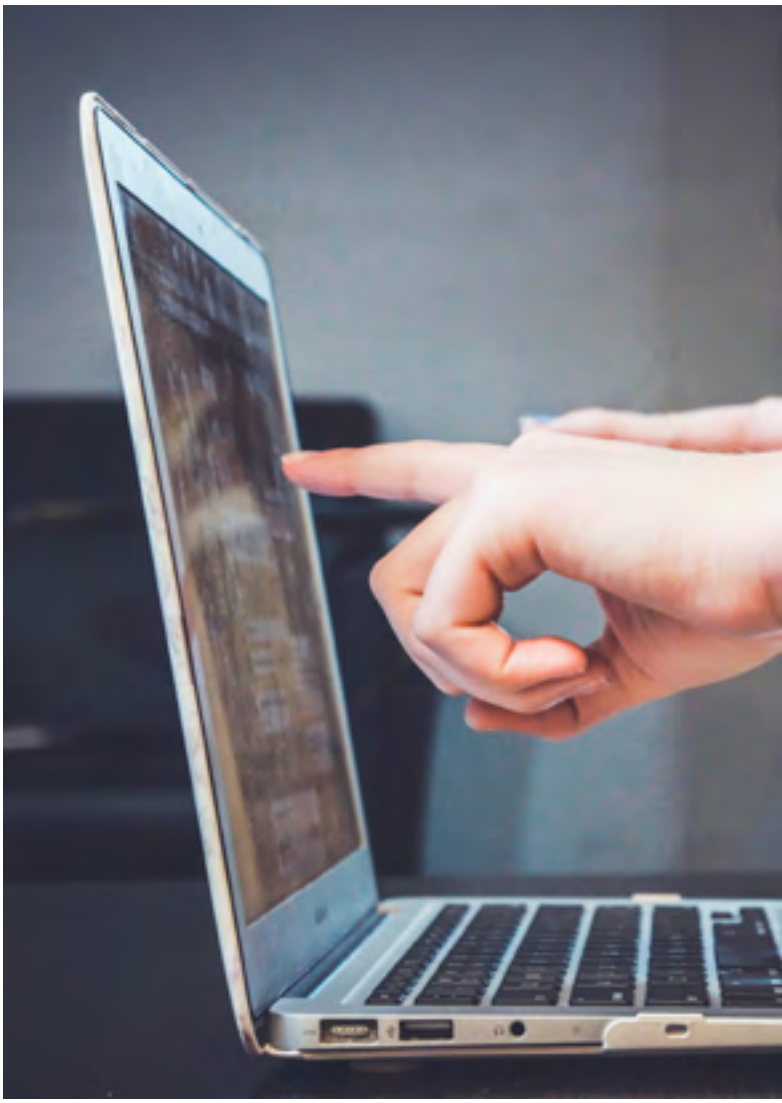
The main drivers to cyber security relate to:

Having sensitive data. The financial and healthcare businesses appeared to be acutely aware of the risk they faced in holding large volumes of sensitive data and the devastating effect on their business a breach to their systems could cause.

Exposure to cyber security attacks. Behavioural change was often noted to be reactive rather than pre-emptive in this regard, with businesses bolstering their systems only after they had come into close contact with a cyber-attack.

Legal requirements that impose action. The bringing into force of the GDPR in May 2018 was a prime motivating factor for businesses to review their systems and approaches to cybersecurity. Micro businesses were far less inclined to do so.

While the relative majority of businesses and NGOs sought information or the assistance of external security or IT consultants, the next most popular means of seeking this information was by means of general internet searches. Only 17% of businesses and NGOs sought out the government as a source of information. A worrying percentage of those who did not seek any advice felt that there was no need to (Businesses: 54% / VO's 57%).



TRAINING

A total of 54% of businesses and 31% of NGOs highlighted that they currently have security policies in place, with professional and courier service businesses scoring highest on this element (89% and 85% respectively).

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.

RECOMMENDATIONS

The study shed light on awareness levels on the actual extent of cyber security threats and following the responses collated, taking into consideration the issues faced the following potential recommendations are proposed.

A general lack of awareness of cyber-security at board level – Create awareness and adoption of a proactive approach as well as engaging top-level management which will instigate a strategic organisational approach rather than a sporadic effort by individual departments.

Lack of skills and training – Promote cyber-security training to expand the skill set of Maltese IT professionals and further training and awareness activities for non-IT staff, apart from formal face-to-face training, other methods such as webinars are advised to increase availability reach and consequently uptake.

Technology vulnerability – Lobby with IT service providers to provide a common platform assisting vulnerable organisation and serve as an opportunity to promote services which can assist with the subject matter.

A lack of trust to share information leads to underreporting – Greater information sharing and coordination amongst stakeholders, this will in turn enable them to understand that joint efforts to address the risks and threats can be better coordinated if the true extent of threats are accurately reported and analysed. (this can be possibly achieved through the common platform highlighted above).

Lack of incident response plans – Maltese companies need to evaluate the level of cyber risks they face and build appropriate resilience against attacks. Naturally such incident response plans need to take into consideration and achieve a balance between cost of defence and likelihood of attacks.

Organisational design – Cyber Security should become a top-level management issue and information and knowledge should be disseminated and trickle down to all members within the organisation.

Access the entire research document compiled by the Department of Information Policy & Governance at the University of Malta or at https://www.mitla.org.mt/publications/cybersecurity

ADDRESSING THREATS

The research clearly shows that the top three major defences used by businesses and VOs are:

1. Email Spam Protection software,
2. Software updates and
3. Appropriately configured firewalls

This should be directly compared with the incidence of breaches experienced on the local front which has been reported in this study as:

1. Phishing attacks (through fraudulent emails or fraudulent websites),
2. People impersonation and lastly
3. Viruses and other forms of spyware).

Through this direct comparison it is evident that the major threats out there are not being effectively or appropriately addressed by the existing measures. The top 3 defences deployed by the surveyed entities do not effectively address the major breaches and attacks reported by such entities, whereas spam protection and updatesmay mitigate the usual phishing spam bots for instance they will do very little to protect from fraudulent websites and social engineering attacks which require effective employee or subject person training to be appropriately addressed.

MALTA IT LAW ASSOCIATION

MITLA
P.O. Box 49
San Gwann

info@mitla.org.mt
www.**mitla**.org.mt