Journal of Information Systems Engineering and Management
2023, 8(2), 20713
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Concerns about Cybersecurity: The Implications of the use of ICT for Citizens and Companies

Sandro Carvalho[1,3,4], João Vidal Carvalho[2], João Carlos Silva[1,3], Gilberto Santos[1], Gonçalo S. de Melo Bandeira[1]

[1] Polytechnic Institute of Cávado and Ave - IPCA, Barcelos, Portugal
[2] CEOS.PP, ISCAP, Polytechnic University of Porto, Rua Jaime Lopes Amorim, 4465-004 S. Mamede de Infesta, Portugal
[3] 2Ai – Applied Artificial Intelligence Laboratory
[4] LIACC - Laboratory of Artificial Intelligence and Computer Science

*** Corresponding Author:** scarvalho@ipca.pt

Citation: Carvalho, S., Carvalho, J. V., Silva, J. C., Santos, G., and Bandeira, G. S. D. M. (2023). Concerns about Cybersecurity: The Implications of the use of ICT for Citizens and Companies. *Journal of Information Systems Engineering and Management*, 8(2), 20713. https://doi.org/10.55267/iadt.07.13226

ARTICLE INFO

Received: 17 Mar 2023
Accepted: 27 Apr 2023

ABSTRACT

The widespread use of Information and Communication Technologies - ICT substantially increases the risks related to information security. In fact, due to the increase in the number and type of cyber attacks, Cybersecurity has become a growing concern in today's society. This phenomenon affects not only individual citizens, but also companies and even State entities. Despite the numerous advantages of this "digitalisation" of society, there are several risks, ranging from identity theft, scam emails or phone calls, online fraud, offensive material and child pornography, material promoting racial hatred or religious extremism, access to online services, email account hacking, online banking fraud, cyber extortion or malicious software. In order to determine the impact that cyber attacks have on society it is necessary to understand how people and companies use ICTs, such as social networks, the information they share, their privacy concerns, or the use of electronic services such as online payments or the cloud. This study becomes central not only to try to prevent/minimise risks, showing what has been done in this area, but more importantly, the way forward to try to prevent or minimise possible risks in the future.

Keywords: Cybersecurity; Cybercrime; Cyber-attacks, Cyber-threats; Information Security; Online fraud; Cyber extortion, ICT.

INTRODUCTION

Information Cybersecurity is increasingly becoming an aspect to be taken into account in today's society. The risk of cyber attacks increases exponentially due to the increasingly widespread use of Information and Communication Technologies - ICT. This evolution in the use of ICT happened in important in areas such as health (Carvalho et al., 2012; Carvalho et al., 2015), wellbeing (Queirós et al., 2010; Carvalho et al., 2022a) or tourism (Carvalho et al., 2020a; Figueiredo et al., 2022). This way, nobody is immune, being a phenomenon that affects from individual citizens to companies, including even government entities, in all sectors of our society (Carvalho et al., 2022b).

The way to determine the impact that cyber-attacks may have and the possible preventive measures that should be taken is to understand the way people and companies use ICTs.

Initially, society should become aware of the potential risks involved in the use of ICT, which can include, but are not limited to: identity theft; scam emails or phone calls; online fraud; offensive material and child pornography; material promoting racial hatred or religious extremism; access to online services; email account hacking; online banking fraud; cyber extortion; or malicious software (Carvalho et al., 2020b; Ferreira et al., 2019; Commission, 2017).

Knowing the possible threats, it is also essential to identify the various targets, in order to recognise at various levels (from the ordinary citizen to companies and government institutions) the most vulnerable points and on which the most urgent measures need to be taken.

Recognising the threats and possible targets should be studied, namely regarding the use of secure servers, security software or the cloud.

The way citizens and companies view the problems derived from cybercrime is also fundamental to find out if good practices are being used, what are the main risks that are happening, wich are the fields in which protection is being taken into account the most. Regarding citizens, determining the percentage of the population that uses the internet, the provision and consent in the access to their personal data, economic losses, the use of online services (such as cloud services), or the characteristics of the verified attacks and the people affected, is crucial in order to prevent attacks. As far as companies are concerned, analysing the occurrences, the use of online services (cloud services, for example), or the rate of implementation of security policies, is the way to mitigate what has been done and, even more so, to determine improvements in terms of the security measures implemented.

Given the risks exposed, finding out the number and percentage of secure servers is extremely important to determine the care that a country is taking with regard to the security of its information. The incidence rate of malware is also significant, as well as the percentage of machines with security software activated. In addition, and in view of the ever-increasing use of the cloud, cloud threat intelligence are very real threats, and can involve illegitimate access to a huge amount of information, which can be highly confidential, such as health information.

This article presents a study on the aspects mentioned so far in the Portuguese scenario, namely cyber-threats, targets of cyber-threats, Portugal's concern regarding cyber-security, cyber-security for citizens and cyber-security for companies.

CYBER-THREATS

Online security problems are real and affect a growing number of users. In fact, these attacks are one of the main threats to the privacy of citizens or the proper functioning of companies, which are increasingly a target of attackers.

Among the main concerns are (Commission, 2017):

- Identity theft - Somebody stealing your personal data and impersonating you;
- Scam emails or phone calls - Receiving fraudulent emails or phone calls asking for your personal details;
- Online fraud - Online fraud where goods purchased are not delivered, are counterfeit or are not as advertised;
- Offensive material and child pornography - Child pornography online;
- Material promoting racial hatred or religious extremism
- Access to online services - Not being able to access online services like banking or public services because of cyber-attacks;
- Email account hacking - Social network account or email being hacked;
- Online banking fraud - Being a victim of bank card or online banking fraud;
- Cyber extortion - Being asked for a payment in return for getting back control of your device;
- Malicious software - Discovering malicious software (viruses, etc) on your device.

The most common dangers are: violence, abuse of personal data, unauthorized and harmful content on the Internet, persecution, harassment and fraud, both to individuals and organizations. Furthermore, these threats not only affect the users and information systems that are the target of the attack, but also affect the confidence of users and business entities (Carvalho et al., 2020b).

TARGETS OF CYBER-THREATS

Cyber-attacks affect all of today's society. In fact, no one is immune from becoming a target of criminals. From ordinary citizens to companies or even public institutions, all of them are potential targets, depending on the type of attack and the information the attackers want to obtain. Indeed, hostile actors conducting cyber-attacks can target the government (and/or military), business and individuals (CPNI, 2019).

Another aspect to take into account is that often an attack on an entity ends up, directly or indirectly, affecting other entities.

The main targets of cyber-attacks are:

- Citizens - the risks for citizens are essentially related to privacy issues and undue access to personal information. Bank fraud or identity theft are also serious risks for citizens;
- Companies - the goal of the attackers is to take control of the data processing systems, which are the "heart" of the company's operation;
- Government institutions - attacks on government institutions are generally focused on their information systems, given the quantity, typology and scope of the data they contain.

The dangers for citizens are exacerbated by the use of social networks, individuals establish a variety of communications, regardless of where they are in the world. Citizens are often unaware of their consequences. For Corporations, many have weak or inadequate security protection measures, which can be catastrophic, as not only does it expose their information and that of their clients, but it can also prevent the company from functioning at all. As for Government Institutions, if we look at the institutions involved, such as hospitals, schools, and even nuclear power plants, we can see that the consequences can be catastrophic.

CYBERSECURITY CONCERN IN PORTUGAL

Given the growing number and type of cyber attacks, there has been an increasing awareness on the part of companies and citizens about the risks involved. The fight against these practices depends on everyone involved, from ordinary citizens to

companies and even government institutions (Barros, 2018). Given the possible implications of cyber attacks, the effort must be a concerted task among the various stakeholders of the system, both at public and private level.

At this level, one of the ways to prevent attacks on user accounts is through the use of secure servers, so the percentage of these servers in each country represents an indicator of their concern regarding cybersecurity. Portugal hosts 85,095 secure servers, which corresponds to 2.3% of all servers hosted. This is below the EU28 average, which is 3.8%. According to the OECD, 83% of the total number of secure servers hosted worldwide are in OECD member countries. It also states that of the 16 million servers in the world, only 10% have a known location (OCDE, 2017a). Albeit we must not forget that since 2021/1/31-2021/5/1 it happened the Brexit. Now EU only has 27 member countries. United Kingdom is out until now.

According to a Microsoft study (Microsoft, 2017), Portugal is the 8th country in the EU with the highest risk of Cybercrime. Regarding threats, we can consider the impact of malware, trojans and cloud threat intelligence for society.

Regarding malware, according to the same study, the Malware incidence rate, i.e. the percentage of computers using Microsoft security software that detected Malware, potentially unwanted software or a specific threat during the first quarter of 2017, was 9.1%. Among the 109 countries in the study Portugal is only in 74th position. However, if we consider the 28 EU28 countries, it ranks 9th, being one of the countries with a higher malware incidence rate. In March 2017 malware was found on 8.3% of computers in Portugal, above the global incidence rate (7.8%).

Other threats include Trojans, which were found, in the same period, in more than 7.0% of computers, viruses, identified in 0.8% of computers, and Downloaders & Droppers, in 0.7% of computers.

In addition, and in view of the significant increase of services available in the cloud, attacks on the cloud have also become a growing concern. In fact, more and more organisations rely on cloud services to support their business, so threats to this type of technology gain importance. According to Microsoft (2017), attacks on cloud user accounts increased 300% in the first quarter of 2017 compared to the first quarter of 2016. This type of attack is achieved by stealing the access credentials of system users, mostly due to the use of weak passwords, phishing attacks or breaches of third-party services, with the attackers being able to access the company's services using them. This access leads to huge losses for the organisation, not only in terms of direct monetary impact, but also in terms of intellectual property.

Despite the not very encouraging figures regarding the incidence of threats/attacks, Portugal registers a high rate regarding the use of security software, with a rate of 90.3% of computers in March 2017, only being surpassed by Finland (92.2%) (Microsoft, 2017).

According to the ITU, Portugal is in the 22nd position (EU28) in terms of degree of commitment to Cybersecurity, and in place 62 among the 193 countries worldwide considered in the study. This study highlights that the critical areas in which Portugal is in the worst position in terms of Cybersecurity are: (i) training; (ii) standards for professionals; (iii) strategy at organisation level; (iv) definition of metrics; (v) standard-setting bodies; (vi) good practices; (vii) R&D programmes in the area; (viii) bilateral agreements; (ix) multilateral agreements; and (x) public-private partnerships (ITU, 2017).

Portugal has follow very close the cybercriminal laws from UE. *Rectius* with Cybercrime Law n. 109/2009, 9/15 until the changes of Law n. 79/2021, 9/24, transposing Framework Decision n. 2005/222/JHA, of the Council, of 24 February, on attacks against information systems, and adapts domestic law to the Council of Europe Convention on Cybercrime. Here we can find the follow crimes: computer fraud, counterfeiting of cards or other payment devices, use of counterfeit cards or other payment devices, acquisition of counterfeit cards or other payment devices, preparatory acts for counterfeiting, acquisition of cards or other payment devices obtained through computer crime, damage relating to programs or other computer data, computer sabotage, illegitimate access, illegitimate interception, illegitimate reproduction of protected program.

The Portuguese Cybercrime Law also has rules about the follow points: criminal liability of legal persons and equivalent entities (Bandeira, 2013), loss of goods, scope of application of procedural provisions, expedited data preservation, expedited disclosure of traffic data, injunction to present or grant access to data, computer data search, seizure of computer data, seizure of electronic mail and communications records of a similar nature, interception of communications, covert actions, scope of international cooperation, permanent point of contact for international cooperation, expedited preservation and disclosure of computer data in international cooperation, reasons for refusal, access to computer data in international cooperation, cross-border access to stored computer data when publicly available or with consent, interception of communications in international cooperation, application in space of Portuguese criminal law and jurisdiction of Portuguese courts, applicable general regime, competence of the Judiciary Police for international cooperation, protection of personal data. Without forget the article 221 from the Portuguese Criminal Code: computer and communications fraud. And the Portuguese law of law: the Constitution. With the article 35: use of informatics. And if we speak about also informatic crime in Portugal and in the world we must not avoid two basic instruments: 1) Portuguese Charter of Human Rights in the Digital Age (Law n. 27/21, 5/17 and Law n. 15/22, 8/11; Bandeira, 2023a); and 2) Lisbon Declaration-Digital Democracy with a Purpose (2021/6/1; Bandeira, 2023b).

CYBERSECURITY FOR CITIZENS

In Portugal, in 2016, only 51.3% of men and 45.9% of women using the internet provided some kind of personal information online in the last 12 months, the worst result in the EU28 (average of 72.9% for men and 71.6% for women) (OCDE, 2017b). This result, while may denote some caution regarding the risks inherent to the use of the Internet, also shows a lack of trust regarding the services that are increasingly made available online, namely governmental services. In fact, the main reason

given for not sending official forms online is the concern with the protection and security of personal data, a reason given by 33.7% of users (OCDE, 2017c).

However, if Portugal is the country where citizens provide the least their personal data (48.6%) and contact information (15.2%) over the Internet (71.4% and 61.1% in the EU28), the percentage of people who provided other personal information, such as photographs, location data and information on their health and income, reaches 33.5%, well above the 22.4% of the EU28 (OCDE, 2017d).

Despite this, 72.3% of people who use the internet control access to their personal information (59.5% in the EU28). This control includes limiting access to profiles and content on social networks (57.2%), preventing use for advertising purposes (52.2%) and/or restricting access to geographic location information (48.0%) - respectively 39.5%, 46.0% and 31.1% in the EU28 average (OCDE, 2017e).

In 2016, considering people who had used the internet in the 12 months prior to the survey, Portugal was the second EU28 country where most people refused to provide personal information over the internet (51%), well above the 28% of the EU28 average (Eurostat, 2016).

One of the services that causes reticence to users in Portugal are online payments. In this aspect, in 2015 it was found that 0.49% of Portuguese people suffered losses due to fraudulent online payments, a relatively low figure (only 20th in the EU28) (OCDE, 2017f). Another recurring problem is phising/pharming attacks. At this level, the percentage of people affected in Portugal increased from 0.97% in 2010 to 1.58% in 2015 (OCDE, 2017g). These low figures are due to the lower number of users of this type of online services compared to other countries.

In 2015, in Portugal, about 2.8% of people reported having suffered a privacy breach in the last three months, an increase of 49% compared to 2010. 24.6% of people aged between 16 and 74 reported having suffered digital security incidents (5th worst record among the 23 EU28 countries considered) (OCDE, 2017h). Regarding the population affected, it appears that more incidents occur to people with higher levels of education (36.9% - people with higher education; 34.6% - people with medium education; 16.9% - people with low education). These figures are due to the fact that people with higher education levels use technologies more, namely online services, being therefore more exposed to the inherent risks (OCDE, 2017i).

In 2016, 55.7% of people in Portugal were concerned about their online activities being recorded for the purpose of targeted advertising (61.1% in the average of the EU28 countries), and of these 24.9% even report being "very concerned" (24.9%, the 3rd highest among the 19 EU28 countries considered) (OECD, 2017j). The risk of misuse of personal data and economic losses, namely through identity theft, are among the greatest fears of Internet users (OCDE, 2017i).

Due to these misgivings, many internet users have been avoiding performing online activities, citing security concerns as the main reasons (48.4%), with providing personal information in online communities for social and professional networking (28.9%), with ordering or buying goods or services for private use (18.9%) and with downloading software, music, video files, games or other data files (18.7%) (OCDE, 2017k).

Note that in Portugal, in 2014, 16.9% of people did not use cloud computing services due to privacy or security concerns, a figure above the 12.7% average for 28 EU countries (OCDE, 2017l).

CIBERSECURITY FOR COMPANIES

Portugal is the EU28 country that registers the highest level of incidents in terms of Cybersecurity. Analysing the distribution of these incidents, we see that companies with between 50 and 249 workers were the most affected, with 47.1%. The largest companies (those with more than 250 workers) had a slightly lower figure (42.6%). Finally, the least affected were the small companies (with between 10 and 49 workers), with 39.3%. (OCDE, 2017m).

In view of these high figures, there is concern among enterprises in the use of digital services. Thus, and although cloud services have had a significant increase, providing more and more features, in 2014 44.9% of companies reported not using cloud computing due to the risk of security breach (28.5% average in the EU28), and 39.9% also identified uncertainty about the location of data as one of the reasons for not using it (25.6% average in the EU28) (OCDE, 2017n).

Thus, and in view of the existing concern, very much cemented by the incidence rate of occurrences, companies were led to implement and strengthen their security policies. In this field, Portugal is the second country of the EU28 with the highest percentage of enterprises that have formally implemented security policies in ICTs (48.8%), well above the 31.6% of the EU28 average. Large enterprises are those with the highest value, 80.7%, while SMEs, the majority of the Portuguese business fabric, have a value of 48.1% (OCDE, 2017o).

In turn, 36.7% of companies have implemented a formal policy to manage digital privacy risks, something implemented more frequently in companies with more employees: 33.5% in companies with between 10 and 49 employees; 52.0% in companies with between 50 and 249 employees; 64.8% in companies with more than 250 employees (OCDE, 2017p).

METHODOLOGY

The Special Eurobarometer series on cybersecurity is an essential resource for learning about cybercrime in Europe (Commission, 2017). It is an important resource because it does the treatment and analysis of representative data of different types of cybercrimes collected in the last seven years in the 28 member states of the European Union.

The most recent report covers a wide range of threats and aims to understand European citizens' experiences and perceptions of cybersecurity issues. The survey adopted in this report was carried out between the 8th and the 22nd October

2019, by TNS opinion & social, carried out the wave 87.4 of the Eurobarometer survey, on request of the European Commission. The wave 87.4 covers the population of the European Union Member States' respective nationalities, residents in each of the 28 Member States, and aged 15 years and over. In total, 27607 respondents (1007 from Portugal) from different social and demographic groups were interviewed face-to-face at home in their mother tongue on behalf of the Directorate-General for Home Affairs.

The findings from this survey, update previous surveys that were carried out in 2013 (Commission, 2013), 2015 (Commission, 2015) and 2017 (Commission, 2017). These surveys provide insight into the evolution of knowledge, behaviour and attitudes towards cybersecurity in the European Union.

The documents published by the Portuguese Ministry of the Economy are also extremely important, as they provide an overview of the Portuguese position in relation to the other EU members. The document considered, Economic Themes - Cybersecurity in Portugal (Barros, 2018), from 2018, provides a set of relevant information regarding the use of ICT by the Portuguese citizens.

The study presented in this article aims to understand the potential risks in terms of cybercrime, as well as the potential targets of these crimes. Portugal's concern regarding cyber security, cyber security for citizens and cyber security for companies are also fundamental topics addressed in this paper, as they show how Portuguese society is facing this very serious problem.

RESULTS

From the study carried out in this article it was possible to detect a significant increase in the number and type of threats, which affect the whole society, from the common citizen to companies and government institutions.

Figure 1 shows the comparison between Portugal and the EU28 regarding some parameters such as percentage of secure servers, malware detection rate and cybercrime risk.

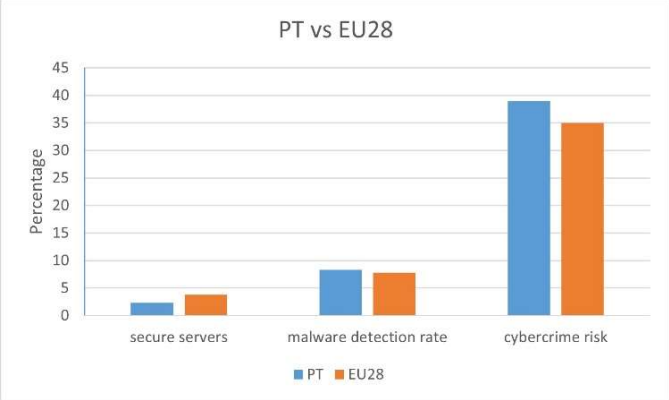

Figure 1. Concerns about Cibersecurity (PT vs EU28)

As can be seen in **Figure 1**, Portugal is below the EU28 average regarding the percentage of secure servers (2.3% vs 3.8%), something alarming since its risk of cybercrime is higher than the average of the EU28 countries (39% vs 35%). Actually, according to a Microsoft study (Microsoft, 2017), Portugal is the 8th country in the EU with the highest risk of Cybercrime.

Despite this, the malware detection rate is higher (8.3% vs 7.8%), which shows concern regarding cyber-dangers. Indeed, despite the not very encouraging figures regarding the incidence of threats/attacks, Portugal registers a high rate regarding the use of security software, with a rate of 90.3% of computers in March 2017, only being surpassed by Finland (92.2%) in the EU (Microsoft, 2017).

According to the ITU, Portugal is in the 22nd position (EU28) in terms of degree of commitment to Cybersecurity, and in place 62 among the 193 countries worldwide considered in the study. This study highlights that the critical areas in which Portugal is in the worst position in terms of Cybersecurity are: (i) training; (ii) standards for professionals; (iii) strategy at organisation level; (iv) definition of metrics; (v) standard-setting bodies; (vi) good practices; (vii) R&D programmes in the area; (viii) bilateral agreements; (ix) multilateral agreements; and (x) public-private partnerships (ITU, 2017).

Figure 2 shows the citizens' online behaviour, namely the percentage of population sharing some type of personal information online, contact information, photographs, location or health information, as well as the control of access to personal information and the refusal to provide personal information over the internet, in a comparison between Portugal and the EU28.

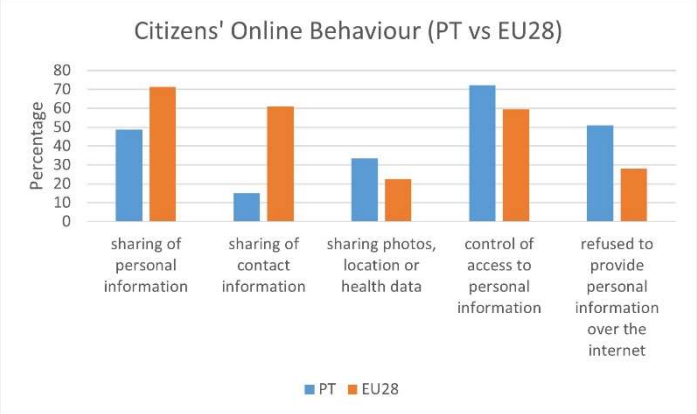

Figure 2. Citizens' Online Behaviour (PT vs EU28)

The result presented in Figure 2 show that, while there is some caution regarding the risks inherent to the use of the Internet (Portugal is the country where citizens provide the least their personal data (48.6%) and contact information (15.2%) over the Internet (71.4% and 61.1% in the EU28)), the percentage of people who provided other personal information, such as photographs, location data and information on their health and income reaches 33.5%, well above the 22.4% of the EU28 (OCDE, 2017d).

Despite this, 72.3% of people who use the internet control access to their personal information (59.5% in the EU28). This control includes limiting access to profiles and content on social networks (57.2%), preventing use for advertising purposes

(52.2%) and/or restricting access to geographic location information (48.0%) - respectively 39.5%, 46.0% and 31.1% in the EU28 average (OCDE, 2017e). The level of users who refused to provide personal information over the internet was 51%, well above the 28% EU28 average.

It can therefore be seen that although some care is taken with online activities, the sharing of photographs and location is still a problem that the Portuguese need to be aware of, which stems a lot from the massive use of social networks in Portugal.

Figure 3 shows the percentage of incidents in Portugal in 2015.

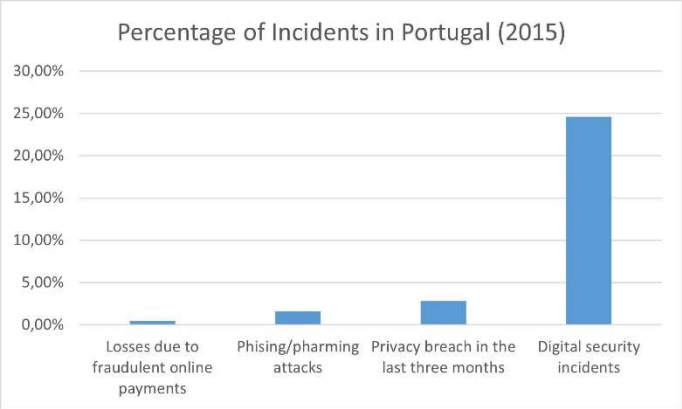

Figure 3. Percentage of Incidents in Portugal (2015)

As can be seen in Figure 3, one of the services that causes reticence to users in Portugal are online payments. In 2015, 0.49% of Portuguese people suffered losses due to fraudulent online payments, a relatively low figure (only 20th in the EU28) (OCDE, 2017f). Another recurring problem is phising/pharming attacks. At this level, the percentage of people affected in Portugal increased from 0.97% in 2010 to 1.58% in 2015 (OCDE, 2017g). These low figures are due to the lower number of users of this type of online services compared to other countries. In the same year, about 2.8% of people reported having suffered a privacy breach in the last three months, an increase of 49% compared to 2010. 24.6% of people aged between 16 and 74 reported having suffered digital security incidents (5th worst record among the 23 EU28 countries considered) (OCDE, 2017h). Regarding the population affected, it appears that more incidents occur to people with higher levels of education (36.9% - people with higher education; 34.6% - people with medium education; 16.9% - people with low education). These figures are due to the fact that people with higher education levels use technologies more, namely online services, being therefore more exposed to the inherent risks (OCDE, 2017i).

In 2016, 55.7% of people in Portugal were concerned about their online activities being recorded for the purpose of targeted advertising (61.1% in the average of the EU28 countries) (OCDE, 2017i). Many internet users have been avoiding performing online activities, citing security concerns as the main reasons (48.4%).

Figure 4 shows the main reasons cited (OCDE, 2017k).

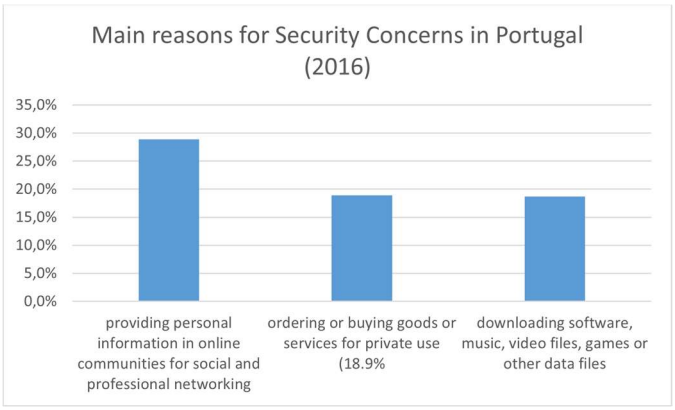

Figure 4. Main reasons for Security Concerns in Portugal (2016)

With regard to companies, **Figure 5** shows the distribution of attacks according to company size.

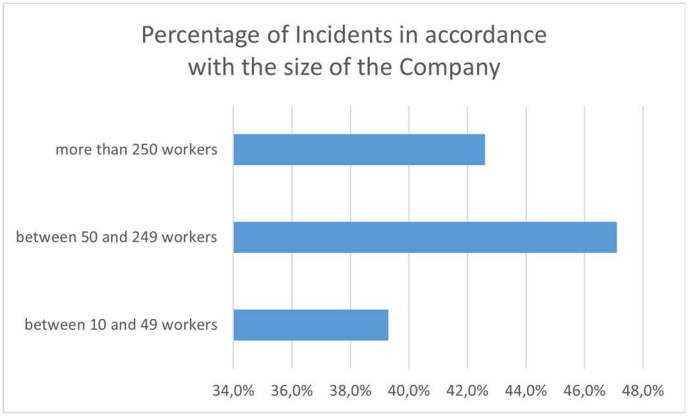

Figure 5. Percentage of Incidents in accordance with the size of the Company

As seen in **Figure 5**, companies with between 50 and 249 workers were the most affected, with 47.1%. The largest companies (those with more than 250 workers) had a slightly lower figure (42.6%). Finally, the least affected were the small companies (with between 10 and 49 workers), with 39.3%. (OCDE, 2017m). Given these high values, there is concern among enterprises in the use of digital services and in 2014 44.9% of companies reported not using cloud computing due to the risk of security breach (28.5% average in the EU28), and 39.9% also identified uncertainty about the location of data as one of the reasons for not using it (25.6% average in the EU28) (OCDE, 2017n).

To address the high rate of attacks and existing concerns, Portugal is the second country of the EU28 with the highest percentage of enterprises that have formally implemented security policies in ICTs (48.8%), well above the 31.6% of the EU28 average. Large enterprises are those with the highest value, 80.7%, while SMEs, the majority of the Portuguese business fabric, have a value of 48.1% (OCDE, 2017o). In fact, 36.7% of companies have implemented a formal policy to manage digital privacy risks, something implemented more frequently in companies with more employees. **Figure 6** shows the difference in the implementation of these measures according to the size of the companies (OCDE, 2017p).

As **Figure 6** shows larger companies are more likely to implement these measures.

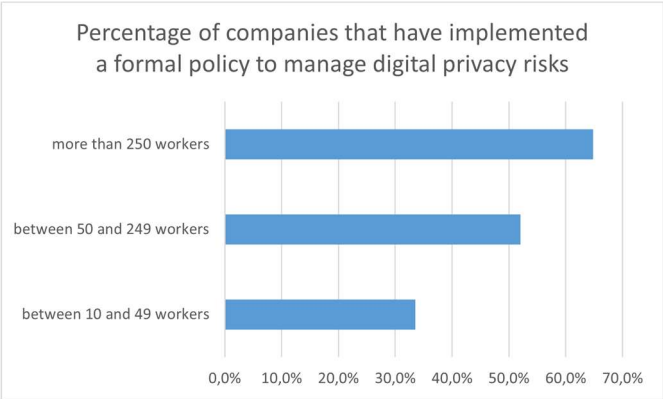

Figure 6. Percentage of companies that have implemented a formal policy to manage digital privacy risks

DISCUSSION

Cybersecurity in Portugal is an increasingly important issue due to Portugal's growing dependence on digital technology for communication, commerce, and government services. As a NATO member and part of the European Union, Portugal must also comply with EU cybersecurity directives (Markopoulou et al. 2019; Fuster & Jasmontaite, 2020; Kovács, 2018; Georgieva, 2016; Alexandre, 2020).

Portugal has taken a number of steps to improve its security infrastructure and protect itself from cyber threats. The government has implemented the Portuguese National Cybersecurity Strategy, which includes initiatives to improve cyber resilience, develop national capabilities and capacities, and establish a secure environment for the use of information and communication technologies (ICT) (Strategy, 2019). The Portuguese National Cybersecurity Strategy provide a comprehensive framework for securing government information systems, companies and citizens. The strategy is intended to protect Portugal's digital resources, including its critical infrastructure, while promoting innovation, economic growth, and trust in the digital environment. The strategy is guided by four main principles: ensuring a secure and resilient digital environment; protecting citizens and their data; developing a cyber-security culture; and promoting international cooperation. To ensure a secure and resilient digital environment, the strategy recommends measures such as strengthening technical capabilities for network defense, developing a national incident response plan, and creating a national cyber range for testing and certifying products and services. To protect citizens and their data, the strategy calls for measures such as raising public awareness about cyber threats, introducing measures to combat cybercrime, and providing incentives for companies to adopt cyber security best practices. The strategy also seeks to create a cyber-security culture by encouraging public-private partnerships to promote research and development, and by providing training opportunities for public and private sector employees. Finally, the strategy calls for increased international cooperation on cyber security through the exchange of information, best practices, and standards. Overall, the Portuguese National Cybersecurity Strategy is an important step forward in ensuring the security of the country's digital resources. It will be important to monitor the implementation of the strategy to ensure that the goals are achieved.

The Government has also taken measures to strengthen its cyber defense capabilities by increasing investments in cyber education and training (Gasiba et al. 2020). Cyber education and training has become increasingly important in today's technological landscape, especially in Portugal due to the country's reliance on digital infrastructure. With cyber threats becoming more sophisticated and pervasive, it is essential for Portugal to invest in the development of its citizens' cyber security skills. To this end, the Portuguese government should establish a national framework for cyber security education and training. This would include creating standards for cyber security curricula, providing resources for universities and educational institutions, and establishing partnerships between educational providers and industry experts. In addition, the government should incentivize employers to invest in cyber security education and training for their employees. This could involve offering tax breaks or other incentives for companies to promote cyber security awareness and education amongst their staff. Finally, Portugal should invest in public awareness campaigns to increase the understanding of cyber security risks and best practices among the general population. This could include providing educational materials, hosting seminars and workshops, and encouraging companies to look into cyber security solutions. By investing in cyber security education and training, Portugal can ensure that its citizens are equipped with the necessary skills to protect themselves and their data, and to create a secure digital infrastructure (Silva et al. 2022).

The launch of a national cybersecurity center in Portugal is also a great investment for the country (Silva, 2019). With the increasing threats to companies and government institutions from cyber-attacks, it is important for countries to invest in their cyber security infrastructure. A national cybersecurity center would provide a centralized hub for the detection, prevention, and mitigation of digital threats. It could also serve as a resource for government and private sector stakeholders to exchange information and best practices on cyber security. The center could provide a variety of services including threat intelligence, risk assessment, incident response, and other technical support. Additionally, the center could host educational and awareness programs to educate the public on cyber security practices. This would help the overall population become better prepared to protect themselves against digital threats. In terms of investments, Portugal should consider both public and private funding sources. Private sector companies should be encouraged to invest in the project, as they will benefit from its services as well. Government funding can be used to cover the cost of developing the center and its services. A combination of public and private funding could also be used to promote research and development into emerging cyber security technologies. Overall, launching a national cybersecurity center in Portugal could be an important step towards improving the country's cyber security posture. It could provide essential services to both the public and

private sectors and increase public awareness of cyber security threats.

The implementation of these measures has had positive effects on cyber security in the country; however, citizens and companies are still vulnerable to cyber attacks. Citizens may be the target of ransomware, phishing scams, identity theft, and other cyber-crime activities. Similarly, companies may be the target of data breaches, malware, cyber espionage, or other malicious activities (Cardoso, 2017; Antunes, 2021). In order to better protect citizens and companies from cyber threats (Kohn, 2020; Tonge at al. 2013), Portugal should continue to invest in strengthening its cyber security infrastructure, developing national capabilities and capacities, and establishing a secure environment for the use of ICT (Tasevski, 2016). Additionally, the government should encourage citizens and companies to adopt best practices for online safety through public awareness campaigns. Finally, it is important for Portugal to collaborate with other countries and organizations around the world in order to ensure effective global cyber security.

CONCLUSIONS

The spread of ICT in recent years has improved the quality of life of citizens and provided opportunities for companies. The advantages range from access to an endless amount of information from anywhere to e-commerce, improved communications or even a new way of working remotely. For companies, they allow not only better access to information but also new perspectives for communicating and promoting their products. The same applies to governmental organisations, which are increasingly able to make their services available online, facilitating interaction with citizens.

However, despite the many advantages, this "digital life" carries a number of risks, ranging from identity theft, scam emails or phone calls, online fraud, offensive material and child pornography, material promoting racial hatred or religious extremism, access to online services, email account hacking, online banking fraud, cyber extortion or malicious software. This phenomenon affects individual citizens as well as companies and state entities themselves.

The way to mitigate the risks involved and to promote preventive measures is to study the behaviour of individuals and companies, namely how they view the problems derived from cybercrime and the practices that are being used to combat this scourge.

This article presents a study on the behaviour of Portuguese citizens and companies regarding the risk of cybercrime. In the case of citizens, statistics are shown on, for example, the percentage of the population that uses the Internet, the provision and consent in the access to their personal data, the use of online services (such as cloud services), or the characteristics of the verified attacks and the people affected. Regarding companies, statistics are shown on the use of online services (such as cloud services), or the rate of implementation of security policies.

Faced with the increasing number and type of cyber attacks, there has been an awareness on the part of companies and citizens about the risks involved. Combating these practices depends on everyone and should be a concerted task among the various stakeholders.

ACKNOWLEDGMENTS

This work is financed by Portuguese national funds through FCT – Fundação para a Ciência e Tecnologia, under the project UIDB/05422/2020.

REFERENCES

Alexandre, P. M. (2020). Europeanization processes regarding matters of cybersecurity: The case of Portugal (Master's thesis).

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219-238.

Bandeira, G.S. de M. (2013). «*Criminal Liability of Organizations, Corporations, Legal Persons, and Similar Entities on Law of Portuguese Cybercrime: A Brief Discussion on the Issue of Crimes of "False Information," the "Damage on Other Programs or Computer Data," the "Computer-Software Sabotage," the "Illegitimate Access," the "Unlawful Interception," and "Illegitimate Reproduction of the Protected Program"*», *Organizational, Legal, and Technological Dimensions of Information System Administration*, Irene Maria Portela (*Polytechnic Institute of Cávado and Ave*, Portugal) and Fernando Almeida (*Polytechnic Institute of Gaya*, Portugal), 321 pages, DOI: 10.4018/978-1-4666-4526-4, ISBN13: 9781466645264, ISBN10: 1466645261, EISBN13: 9781466645271, DOI: 10.4018/978-1-4666-4526-4.ch006, IGI Global, USA, September, pp. 96-108;

Bandeira, G.S. de M. (2023a). Carta Portuguesa de Direitos Humanos na Era Digital-CPDHED, Diário do Minho, Braga;

Bandeira, G.S. de M. (2023b). Declaração de Lisboa-A Democracia Digital com um Propósito, Diário do Minho, Braga;

Barros, G.O. (2018). A Cibersegurança em Portugal. Temas Económicos, Gabinete de Estratégia e Estudos - Ministério da Economia, N. 56.

Cardoso, M. G., Laureano, R. D., & Serrão, C. (2017). Cybersecurity culture in Portuguese organizations: an exploratory analysis. In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). IEEE.

Carvalho, S., Pavão, J., Queirós, A., Dias, A. (2012) A platform for the gathering, agregation and integration of social information. In: 7th Iberian Conference on Information Sys-tems and Technologies, CISTI 2012; Madrid; Spain.

Carvalho, S., Pavão, J., Queirós, A., Rocha, N. (2015) Platform of

Services to the Support and Development of Applications for Care Activities. Procedia Computer Science, 2015, 64, pp. 659–665.

Carvalho, S., Carvalho, J.V. (2020a) The implications of digital marketing and e-commerce in the tourism sector growth. In: Smart Innovation, Systems and Technologies, 171, pp. 161–170.

Carvalho, J.V., Carvalho, S., Rocha, Á. (2020b). European strategy and legislation for cybersecurity: implications for Portugal. Cluster Computing - The Journal of Networks, Software Tools and Applications. Springer US. 2020. DOI: https://doi.org/10.1007/s10586-020-03052-y

Carvalho, S., Pereira, D., Santos, J., Carvalho, J.V. (2022a) Vital Signs Monitoring Platform to promote Sports and Wellness Tourism. International Conference on Tourism, Technology & Systems - ICOTTS2022. Santiago do Chile, Chile. Proceedings ICOTTS2022. Homepage: https://www.icotts.org/

Carvalho, S., Carvalho, J.V., Silva, J.C., Casquilho, M., & Santos, G. (2022b) The Use of ICT in Today's Society from the Perspective of Citizens and Businesses: Security risks and their influence on the quality of life of the Portuguese population. International Journal for Quality Research.

Commission, E. (2013). Cybersecurity. Special Eurobarometer 404.

Commission, E. (2015). Cybersecurity. Special Eurobarometer 423.

Commission, E. (2017). Europeans' attitudes towards cyber security. Special Eurobarometer 464a.

Commission, E. (2018). "Internet security". Special Eurobarometer EB480.

Commission, E. (2020). Europeans' attitudes towards cyber security. Special Eurobarometer 499.

CPNI - Center for the Protection of National Infrastructure: Cyber (2019). https://www.cpni.gov.uk/cyber. Accessed 20 Oct 2019

Eurostat (online data codes: isoc_ci_ifp_iu and isoc_ci_ifp_fu) (2016).

Ferreira, N., Santos, G., Silva, R. (2019). Risk level reduction in construction sites: Towards a computer aided methodology – A case study. Applied Computing and Informatics 15 (2),136-143

Figueiredo, B., Carvalho, S., Silva, J.C., Carvalho, J.V. (2022) Freecycle Applied to Communi-ty Tourism: An Approach. In: International Conference on Tourism, Technology & Systems - ICOTTS2021. Cartagena de Indias, Colombia. Proceedings ICOTTS2021. Homepage: https://www.icotts.org/

Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European union: the digital, the critical and fundamental rights. The ethics of cybersecurity, 97-115.

Gasiba, T., Lechner, U., Pinto-Albuquerque, M., & Zouitni, A. (2020). Design of secure coding challenges for cybersecurity education in the industry. In Quality of Information and Communications Technology: 13th International Conference, QUATIC 2020, Faro, Portugal, September 9–11, 2020, Proceedings 13 (pp. 223-237). Springer International Publishing.

Georgieva, L. (2016). The first EU-wide legislation on cybersecurity: The Directive on Security of Network and Information Systems as a game-changer for stronger European cybersecurity. European Energy & Climate Journal, 6(3), 62-76.

International Telecommunication Union - ITU (2017). "Global Cybersecurity Index (GCI) 2017". Telecommunication Development Bureau.

Kohn, V. (2020). How Employees' Digital Resilience Makes Organizations More Secure.

Kovács, L. (2018). Cyber security policy and strategy in the European Union and NATO. Land Forces Academy Review, 23(1), 16-24.

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336.

Microsoft (2017). Microsoft Security Intelligence Report – Portugal. Volume 22, January through March, 2017. https://www.microsoft.com/en-us/security/intelligence-report

OECD Digital Economy Outlook (2017a) http://dx.doi.org/10.1787/888933586616

OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (2017b). http://dx.doi.org/10.1787/888933620284

OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (2017c) http://dx.doi.org/10.1787/888933620227

OECD Digital Economy Outlook 2017 (2017d) http://dx.doi.org/10.1787/888933586502

OECD Digital Economy Outlook 2017 (2017e) http://dx.doi.org/10.1787/888933586578

OECD Digital Economy Outlook 2017 (2017f) http://dx.doi.org/10.1787/888933586540

OECD Digital Economy Outlook 2017 (2017g) http://dx.doi.org/10.1787/888933586559

OECD Digital Economy Outlook 2017 (2017h) http://dx.doi.org/10.1787/888933586483

OECD Digital Economy Outlook 2017 (2017i) http://dx.doi.org/10.1787/888933586445

OECD Digital Economy Outlook 2017 (2017j) http://dx.doi.org/10.1787/888933586331

OECD Digital Economy Outlook 2017 (2017k) http://dx.doi.org/10.1787/888933586350

OECD Digital Economy Outlook 2017 (2017l) http://dx.doi.org/10.1787/888933586369

OECD Digital Economy Outlook 2017 (2017m) http://dx.doi.org/10.1787/888933586426

OECD Digital Economy Outlook 2017 (2017n) http://dx.doi.org/10.1787/888933586388

OECD Science, Technology and Industry Scoreboard 2017 - The Digital Transformation (2017o) http://dx.doi.org/10.1787/888933620265

OECD Digital Economy Outlook 2017 (2017p) http://dx.doi.org/10.1787/888933586730

Queirós, A.; Da Rocha, N.P.; Carvalho, S.; Pavão, J. (2010) Integrated care of the elderly and the continuous development and adaptation of information systems. In: 12th IEEE In-ternational Conference on e-Health Networking, Application and Services, Healthcom 2010.

Strategy, National Strategy for Cyberspace Security (2019). Resolution of the Council of Ministers No. 92/2019. Portuguese Official Journal, Series 1 — No. 108 — 5 June, 2019.

Silva, C., Serra, A., Folgado, D., Santos, H., Oliveira, Â., & Lopes, A. (2022). It'sa Fraud: Learning about Cybersecurity. In 2022 17th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.

Silva, J. Cybersecurity and Cybercrimes in Portugal. In Digital Privacy and Security Conference 2019 (p. 39).

Tasevski, P. (2016). IT and cyber security awareness-raising campaigns. Information & Security, 34(1), 7-22.

Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. IOSR Journal of computer Engineering, 2(12), 67-75.