SOSİAL TƏDQİQATLAR MƏRKƏZİ
SOCIAL RESEARCH CENTER

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EUROPEAN UNION

CYBERCRIME AND CYBERSECURITY BAROMETER IN AZERBAIJAN

ANALYTICAL REPORT

REGIONAL QUANTITATIVE AND
QUALITATIVE ANALYSIS OF THE ATTITUDE
TOWARDS CYBERCRIME AND ONLINE SECURITY

SOSİAL TƏDQİQATLAR MƏRKƏZİ

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

A JOINT PROJECT OF THE EUROPEAN UNION, THE COUNCIL OF EUROPE AND THE SOCIAL RESEARCH CENTER

CYBERCRIME AND CYBERSECURITY BAROMETER IN AZERBAIJAN

REGIONAL QUANTITATIVE and QUALITATIVE ANALYSIS of the ATTITUDE TOWARDS CYBERCRIME and ONLINE SECURITY
(October 2021 - January 2022)

Developed within the framework of the "CyberEast" project funded by the European Union and the Council of Europe, as well as the "Cybersecurity East" projects implemented by the European Union.

Baku – 2022

Contacts

Giorgi JOKHADZE
Project Manager
Giorgi.Jokhadze@coe.int
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania

Besnik LIMAJ
Team Leader
Tel:+383 44 506 403
Besnik.Limaj@gfa-group.de
GFA Consulting Group

Disclaimer

This report has been produced as part of a project co-funded by the European Union and the Council of Europe. The research report was drafted by the Social Research Center (Azerbaijan) with inputs from experts Donika Emini (Kosovo), Dan Petre and Vlad Tureanu from D&D Research (Romania), and Roeland van Zeijst (Netherlands). The views expressed herein can in no way be taken to reflect the official opinion of either party.

Team of project researchers and experts:

• European Union Expert Group:
Roeland van Zeijst (Netherlands), Dan Petre and Vlad Tureanu ("D&D Research", Romania) and Donika Emini (Kosovo)

• Azerbaijan Research Group (Social Research Center):
Zahid Oruj (Head of Research team), Tahira Allahyarova, A. Balayeva, I. Shahbazov, Z. Efendiyev and B.Aliyev.

Information about the organization

Social Research Centre was founded in 2019. The purpose of the center is to analyze the dynamics of social relations, identify current trends in this area and conduct research on various sociological, political, economic and cultural issues.
The Center provide with analytics, monitoring and consequential reporting to consideration of state and public institutions. To date, the Center has conducted more than 70 surveys and research projects involving more than 60,000 respondents.

TABLE OF CONTENTS

1. LIST OF ACRONYMS

CC - Criminal Code
CERC - Computer Emergency Response Center
CI - Critical Infrastructure
CIS - Commonwealth of Independent States
CoE - Council of Europe
CP - Core population
CSOC - Cybersecurity Operations Center
EU - European Union
GCSI - Global Cyber Index
GCVI - Global Cyber Vulnerability Index
GDP - Gross Domestic Product
GDPR - General Data Protection Regulation
ICT - Information and Communication Technologies
IoT - Internet of Things
ISP - Internet Service Providers
IT - Information Technology
ITU - International Telecommunication Union
KOS - Small and medium business
KPG - Capacity Building for Cybersecurity
LE - Law Enforcement
MDDT - Ministry of Digital Development and Transport
MIA - Ministry of Internal Affairs
OSCE - Organization for Security and Cooperation in Europe
PPP - Public private partnership
SCISA - Special Communication and Information Security Agency
SSPS - Special State Protection Service
SSS - State Security Service
UN - United Nations

Aim of the project

1. Quantitative and qualitative analysis of the attitude of public opinion towards this area in order to assess the real situation with cybercrime and online security in Azerbaijan;

2. Assessment of the compliance of the current situation in Azerbaijan with the Budapest Convention on Cybercrime approved by the member states of the Council of Europe;[1]

3. In order to strengthen the overall security of Azerbaijan, increase resilience to cyberattacks, strengthen the work of relevant institutions and the capacity of law enforcement agencies in the direction of ensuring cybersecurity;

4. Contribute to the development and implementation of an effective national concept and strategy for combating cybercrime, as well as a state program towards the development of mechanisms for mutual technical cooperation and cooperation with European institutions by submitting proposals and recommendations that further strengthen and improve the fight against cybersecurity and cyberattacks.

2. EXECUTIVE SUMMARY

As a country that has made significant progress in the development of the information and communication technology (ICT) sector, Azerbaijan is an interesting example of cybersecurity. Azerbaijan has implemented a number of policies and initiatives aimed at promoting innovation, expanding access to technology and stimulating economic growth. Because of historical and geopolitical considerations, Azerbaijan's foreign and domestic policy has always included both physical and cybersecurity elements. With the emergence of pandemic circumstances, cybersecurity became even more important, as internet activity expanded, presenting the new potential for cyberattacks. In 2021, botnets[2] and phishing[3] were the most prevalent offenses. Since the beginning of 2021, CERT has expanded public knowledge of cyber fraud cases and methods to defend against such acts by 40%.

According to the results of our survey, the smartphone was the most often used gadget for personal requirements. When using their devices, 73.3% are cautious in their actions. A larger proportion of the sample (62.8%) was unfamiliar with the term cybercrime. The term "phishing" is unknown to 93.6% of respondents. The majority of respondents (86.7%) believe they have not been targeted by an effort at computer/online criminal conduct. After being given the definition, 74.3% of respondents claimed they have heard of this kind of crime occurring. The majority of phishing victims were either unaffected or saw it as a nuisance (69.6%). While more than half (56.9%) feel that if someone in their neighbourhood would receive a phishing message, 52.7% know enough about phishing to protect themselves and their family. The term "ransomware"[4] is unfamiliar to 97.7% of people. According to 60.7% of respondents, if someone in their area was the victim of a ransomware attack and lost access to their computer, smartphone, or the data or pictures they held, they would report it to the authorities/police. Almost two-thirds of those asked declined to answer questions concerning intimidation/abuse. Among the people who agreed to answer questions concerning this topic, 91% had never experienced internet online abuse.

The majority have not become aware that login credentials to a personal account of them had been exposed online in the past 12 months. When it comes to preventing online identity theft, 61.6% of people believe they are knowledgeable enough. Data breaches and online identity theft are the most concerning offenses for 40.6% of respondents, despite the fact that only a tiny number of respondents have experienced them.

A significant number of enterprises do not have a dedicated role or department in charge of cybersecurity.

---

[1] Azerbaijan signed the Budapest Convention in 2008, which is considered a historical achievement in the fight against cybercrime, and ratified it in 2009.

[2] Botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.

[3] Phishing is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

[4] Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.

The weight of expenditure on cybersecurity within the IT budget is generally low, and the most enterprises do not have insurance. ISO 27001 is the most prevalent safety framework followed in the sample. More companies rank cybersecurity within their company either low or non-existing. Among cybersecurity technologies currently in place, anti-malware software to protect against viruses, spyware and others was noted by the majority, while spam/phishing filtering and data protection and control came next. The responses to several questions on cybercrime victimization indicate a very low rate of victimization among enterprises. Greater budgets and the use of advanced security technologies, according to 45,3% and 46,9% of respondents, respectively, will assist raise security standards inside their organization. On laptops, file encryption is used by 65.6% of businesses. The opinions on whether the COVID-19 epidemic has increased cybercrime against businesses are about equally divided.

Focus groups provided very useful insights into the views of people regarding cybercrime. Through mainly two channels, 57 participants were attracted (using the snowball method): students of universities where the research group teaches and b) personal and professional connections established during the cooperation with other agencies. Victims were identified through the survey. Their mobile numbers were written down during the survey and contacted by the Centre's survey team afterwards. An official invitation letter was sent to multiple law enforcement agencies. Professionals in the IT sector and NGO representatives were recruited through both official invitation letter and personal connections of the IT/media department of the Social Research Centre.

Among GPGs (general population group), only three offences came up at varying frequencies - online abuse, identity theft, and phishing. All other cybercrimes (i.e., ransomware, exposure of personal details) were extremely limited or even unheard of. Regarding the victimization of cybercriminals, identity theft stood out both in terms of frequency and magnitude of impact. Among GPGs although online abuse was slightly more prevalent (9 cases) than identity theft (4 bank card and 3 social media account theft), the former had no impact on victims. The fact that all participants received phishing calls and emails but only two victims were identified, suggests a high level of awareness of and protection from this cybercrime.

The majority of people felt insecure when online and using smartphones. "Nothing and nowhere is safe" statement was dominant. Concerning safety, one of the most crucial insights gathered from focus groups came from ISP officials. Despite all the strict measures taken, even they did not feel fully secure because the devices and software used are all imported or produced abroad.

In terms of perceptions of cybercrime, the phrases "internet crime" and "data crime" were often flagged as all-encompassing phrases among GPGs, while markedly different responses were recorded among IT professionals and ISP representatives.

In comparison to other crimes, cybercrime is viewed as potentially more dangerous. It was determined that cybercrime can have a social impact, whereas violent and property crimes frequently occur on an individual or communal level. Further, IT professionals, ISP representatives, and certain law enforcement officials highlighted the idea of easily hacking another person's vehicle or smart home system to cause harm.

While phishing was mentioned as the most concerning cybercrime among most of the GPG and victims, different responses (DDoS, attack on critical infrastructure areas) were recorded in other groups.

For law enforcement respondents a particularly concerning feature of cybercrime is its ability to damage critical infrastructure and thus, cause mayhem. Across some groups, there was also a widespread agreement that cybercrime can result in suicides in certain cases, such as intimidation.

Most of the crime types cited, as well as the term "cybercrime," were familiar to all respondents, although phishing and ransomware were almost unheard of. Respondents mostly recognized them once explanation was given.

While one group (18-21) would report future cybercrime victimization to the police, other GPGs in general, as well as NGO representatives, would go to an IT specialist, though they did not exclude the possibility of reporting to the police. That is, while they had

little trust in the police`s ability to handle their report, they would report to them as the last resort. This and the relevant findings previously mentioned above point to a need for more cooperation between IT sector and the police in clearing up and recording cybercrimes.

It is worth noting the risks facing school children. One focus group's suggestion was nationwide and schoolwide awareness programs, and all those suggestions came from three women and one man who were either parents or working in the education sector. This may indicate the severity of the problem across schools, hence, a need for parent-only focus groups in the future. In fact, as noted by a female, teachers can unintentionally play a role in spreading phishing mails. Given high use of smartphones and tablets among pupils, it is possible that there is a significant "dark figure" (unknown) of cybercrime among this subgroup.

All groups agreed, without exception, that cybercrime will deteriorate in the future as a result of greater usage of electronic services (e-gov and e-commerce), as well as the digitalization of formerly paper-based data. Nevertheless, the most significant difference between the survey responses and those of the focus groups is related to cybercrime expectations. While almost every focus group respondent anticipates an intensification of cybercrime in the future, nearly half of the survey population thinks the opposite as they anticipate a decrease. This significant difference can be explained, perhaps, by the selection criteria. When selecting participants for focus groups, certain criteria (e.g., active use of the internet, working in the IT or ISP sector, etc.) were applied, and thus, bias played a role. For the survey, though, selection was random.

To summarize, not all forms of cybercrime have gained traction in Azerbaijan. The victimization rate across many cybercrimes is quite low – both on individual and organizational levels. Despite its relative prevalence, most respondents are unaware of the term phishing. Overall, there were serious complaints about banks' reluctance to deal with phishing or bank card theft related matters, and police's inability and lack of expertise in pursuing criminals. While CERT, SSS, and MIA all make significant efforts to raise awareness, more has to be done, particularly in terms of personnel development and more successful investigations. When it comes to cybercrime's seriousness, it was almost unequivocally seen as potentially more dangerous than other crime types among focus groups, while a significant number of survey participants rated cybercrime more serious than other crimes.

3. BACKGROUND

What is cybercrime and cybersecurity? Cybercrime is a crime comprehending the use of computer devices and the Internet. It can be committed against an individual, a group of people, government, and private organizations. This is ordinarily done with the intent to ruin someone's reputation, cause them physical or emotional pain, or profit from it in some way, such as financial gain, inciting fear and hatred, etc.

Cybersecurity is the practice of protecting systems, computers, networks, programs, personal data, etc. from unauthorized access, digital attacks, and threats. This is a measure to protect information and other communication systems from unauthorized use, modification or manipulation of the device. Cybersecurity is also called information technology security. It includes how to protect computers, networks, programs and data from unauthorized access or attacks that could damage or exploit them in any way. In fact, cybersecurity is a technical approach to protecting systems from such attacks.

Since cybersecurity is inextricably linked to the Internet, it is worth studying the usage statistics in Azerbaijan. The population of Azerbaijan became 10,26 million people by January 2022.[5] There were 8.26 million Internet users in Azerbaijan in January 2021. The number of Internet users in Azerbaijan increased by 202 thousand (+2.5%) in the period from 2020 to 2021. The rate of Internet penetration in Azerbaijan was reported as 81.1% in January 2021. As of January 2021, there were 4.30 million social media users in Azerbaijan. Between 2020 and 2021, the number of social media users in Azerbaijan increased by 600 thousand (+16%). As of January 2021, the num-

[5] Azerbaijan Population (LIVE). - https://datareportal.com/reports/digital-2022-azerbaijan

ber of social media users in Azerbaijan was equivalent to 42.2% of the total population. There were 11.30 million mobile connections in Azerbaijan in January 2021. The number of mobile connections in Azerbaijan grew by 92 thousand (+0.8%) in the period from January 2020 to January 2021. In Azerbaijan, mobile connections were equivalent to 111.0% of the entire population in January 2021. (Note: Many people have more than one mobile connection, so the figures for mobile connections may exceed 100% of the total population)[6]. Lastly, 42.8% of Azerbaijan's population resides in rural regions, compared to 57.2% who live in urban areas.

4. INTRODUCTION

4.1. Cyberattacks and threat response

The analysis of the history of cyberattacks in Azerbaijan reveals that digital conflicts escalated in the Caucasus region in January 2000, when Armenian hackers attacked about twenty state websites of Azerbaijan, as well as the websites of the United States Embassy in Baku and several international organizations, inserting false and propagandistic information about Baku and its leading statesmen, especially the president Heydar Aliyev. Moreover, in January 2012, the websites of some state and news agencies were defaced to demonstrate anti-state sentiments.[7]

In accordance with another study, "Stuxnet, a computer worm assault, drew the focus of the country toward cybersecurity awareness, as it did in many other afflicted states throughout the world." Stuxnet has primarily targeted Iranian systems, although it has also been detected in other countries, including Azerbaijan. Undoubtedly, the timely response of effective countermeasures limited the damage from this "cyber missile", but the Stuxnet incident alarmed the existing cyberspace security systems in Azerbaijan. Furthermore, the country's authorities have initiated an investigation into the origin of 25 cyberattacks in 2012: 24 from Iran and one from the Netherlands.[8] Therefore, cybersecurity has become one of the most serious problems and challenges to Azerbaijan's national security".[9]

Allegedly Iranian-based attacks on Azerbaijani cyberspace further deteriorated already strained Baku-Tehran bilateral relations. Simultaneously, Azerbaijan's important national organizations and institutions are striving to strengthen cybersecurity against prospective cyber strikes from Armenia, Iran, and perhaps Russia.

At this instance, cyberattacks were first reported by the leading New Azerbaijan Party (NAP), and later, during the investigation, it turned out that the hackers' IP numbers were of Iranian origin. A month later it became known that the websites of Azerbaijani Airlines (AZAL) and the TV channel were attacked by Iranian hackers.[10]

The assessment of the processes related to Azerbaijan's countrywide electricity blackout at the substations of the Mingachevir Hydro Power Station on July 18, 2018 brought into question the national security of Azerbaijan, revealing major strategic deficiencies in this field.[11]

4.2 The Rise of Cyber threats

Currently, most of the services important to Azerbaijani society are digitized, and efforts in this direction are progressing rapidly. This process has begun on a global scale, and the future of all states is dependent on digital transformation and its state. In contrast, different actions have been made in our country to ensure cybersecurity during the last ten years. Work in this area has accelerated in the last three years.

The COVID-19 pandemic has prompted the public and private sectors to shift to digitalization in many areas, such as public health, education, commerce, and other public services.

---

[6] Digital 2021 Azerbaijan. - datareportal.com/reports

[7] Marcus Franda,Launching into Cyberspace: Internet Development and Politics in Five World Regions (London: Lynne Rienner Publishers, 2002), p. 121

[8] Government probe traces cyberattacks to Iran, Netherlands.- https://www.azernews.az/nation/40524.html

[9] Azerbaijan Cybersecurity Governance Assessment. Ms. Natalia Spînu. DCAF. Switzerland. November 2020, p.4

[10] https://www.azernews.az/nation/40524.html

[11] "Critical Infrastructure" and its protection: the world experience and the need for implementation in Azerbaijan. - newtimes.az/en/politics

The current situation impels the government and citizens to adapt to the changes with the help of technology. The epidemic helped Azerbaijan in its efforts to digitize the society.

In 2021, cybersecurity has practically become a daily headline in Azerbaijan's media. Discussion topics include "The rise of cyberbullying: who is to blame?" and others revealed an unprecedented level of cyber fraud in the world and in our country.

Experts also discussed the growth of cyberattacks in Azerbaijan. According to statistics provided by Special Communications and Information Security (CERT), the growth rate of cyberattacks in 2021 was 38%, while figure in 2020 was 28%. Head of the CERT Information Security Department Tural Mammadov at the conference "Cyber fraud in Azerbaijan during the pandemic" noted that "it turned out that many residents of the three largest cities in the country became the target of cybercriminals. The number of cyber threats using the Azerbaijani language has increased. At the same time, the volume of the activities aimed at informing the population about such threats has increased by 40%".[12]

People were cautious about disclosing personal information to third parties. One of the most frequently asked topics was whether the bank or the clients were the major culprits in this situation. Kapital Bank's customers were the most prevalent of those who complained about cyber fraud. Experts, media and relevant agencies have carried out educational work to draw public attention to how act in such a situation.

4.3 New" Smart Village/City" Concept: implementation and the importance of cybersecurity

Azerbaijan has begun implementing the concept of "smart cities and villages" in the liberated lands of Karabakh, employing the latest technology like as digital communications, automation, and renewable energy sources to maximize economic development. Azerbaijan has already taken the initial steps in implementing the smart cities process in these locations as part of the Smart City initiative. Because smart cities rely entirely on technical methods, they might become a target for cyber assaults. Smart city cybersecurity requirements are increasingly dependent on operational security.

Researchers have comprehensively discussed the implementation of Smart Cities, as well as its threats and weaknesses. One of them claims that:

"Azerbaijan has a digital divide between the capital and other urban/rural areas. There is a 20-percentage point gap between rural and urban households in fixed internet penetration. This digital divide is mainly due to shortages of fixed infrastructure and lower levels of digital literacy in rural areas. The country will also need to make broadband internet faster, cheaper, and more accessible. Although overall mobile broadband coverage and adoption is high, there is a significant digital divide between urban and rural areas in the quality/speed, use, and affordability of the internet" (World Bank, 2019).[13]

4.4 External cyber threats and sources of cyberattacks

In terms of the source of cyberattacks, the activity of Armenian hackers has been recorded in recent years. During the Second Karabakh war in the fall of 2020, Armenian hackers tried to attempt to assault Azerbaijani banks, including the country's Central Bank. Cyber threats from Armenian hackers have been eliminated, and there were no reported breakdowns in the Central Bank of Azerbaijan (CBA) and Azerbaijani banks' systems. The Central Bank of Azerbaijan was the primary target of external cyberattacks during the 44-day second Karabakh war (from late September to early November 2020). Azerbaijan has requested that international cybercrime fighting organizations investigate this crime after gathering appropriate evidence.[14] Also, phishing assaults may have been carried out by Armenian cybercriminals. Furthermore, DDoS attacks (distributed denial of service) were carried out against users, although these at-

[12] The number of cyberthreats in Azerbaijan is increasing... - az.sputniknews.ru
[13] Building Smart Cities and Villages in Azerbaijan: Challenges and Opportunities. - bakuresearchinstitute.org
[14] During the Patriotic War, Armenian hackers tried to attack the Central Bank. - az.sputniknews.ru

tempts were blocked by a system designed to prevent these type of cyberattacks.

Admittedly, these statistics are just the tip of the iceberg when it comes to threats faced by both individuals and organizations. However, they will provide an overview of the evolution and growing scale of cyber threats.

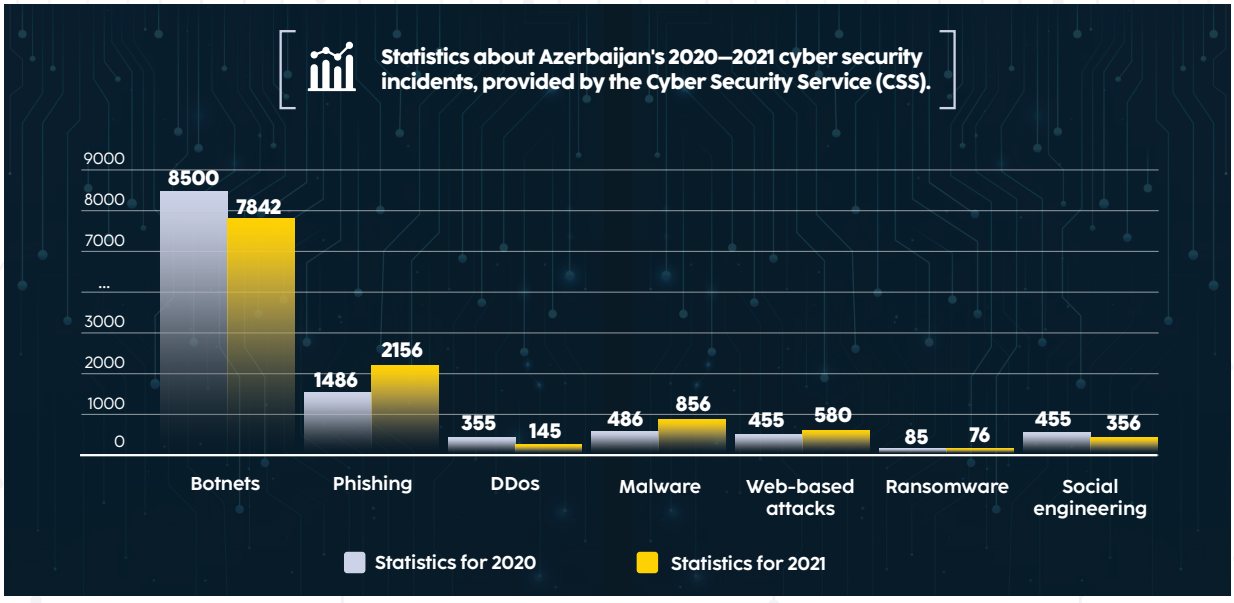
4.5. Increasing internal cybercrime, domestic threats

The members of the cybercriminals who defrauded roughly 10,000 people were exposed on November 20, 2021. During the investigation, it was found that the group had established a company in the country called "Insurance". The international pyramid known as "OCOS" (Ponzi scheme) was brought to Azerbaijan by them. They created a non-existent cryptocurrency through special local programs on the Internet, allegedly organizing its sale on the international currency market and fraudulently seizing citizens' money, promising exaggeratedly high incomes. Thus, the aforementioned persons attracted a large number of citizens in the form of a pyramid to the network business they created and sold them a fictitious cryptocurrency that did not exist. The investigation revealed that the cybercriminal members deceived a total of about 10,000 citizens and seized a large amount of money.[15] It should be highlighted that while the exact losses are not reported, the criminals admitted that they took from $ 3,000 to $ 10,000 from different victims. A large number of participants (10,000) of the first major cyber fraud indicates an increase in domestic cyber threats. On the other hand, it underlines how urgently the public needs to be educated about emerging crimes.

4.6. Statistics about Azerbaijan's 2020–2021 cybersecurity incidents, provided by the Cybersecurity Service (CSS).

Note: Incident-based statistics include those reported by citizens, private organizations, independent cybersecurity firms, and data collected by CSS:

- ❖ Phishing events surpassed botnet-related occurrences in frequency, increasing by 30% from the previous year.
- ❖ The Emotet trojan was the most used (once such viruses infiltrate a system, they gradually take over).
- ❖ The most common phishing scenarios involved obtaining payment card numbers, Internet banking login details (entering to system), social media, and email account credentials. Cybercriminals used fake SMS messages, messages on WhatsApp, and vishing



Source: Statistics about Azerbaijan's 2020–2021 cybersecurity incidents, provided by the Cybersecurity Service (CSS).

[15] Members of the gang who committed fraud against about 10,000 citizens were exposed. - www.txtreport.com/news

(caller ID spoofing) for this purpose. There is a sharp increase in vishing attacks.

❖ In 2021, the Electronic Security Centre (ESC) under the Ministry of Communications and High Technologies (MCHT) obtained data about 7842 IP addresses that indicate zombie activity. This figure is pretty similar to the value that was observed in 2020. These were the actions taken most often by the Andromeda, Emotet, and Avalanche botnets. There was observed an increase in infections with “FluBot” malware in recent months.

In terms of countermeasures, since the beginning of 2021, CERT has increased public awareness of cyber fraud cases and how to protect against such offenses by 40%.

Strengthening education efforts is related to an increase in the country's demand for non-cash payments and, as a result, a rise in the number of cyberattacks on individuals who make them. To support the country's population, an internet platform https://blacklist.gov.az/ was developed with information on sites that replicate the resources of numerous Azerbaijani organizations, enterprises, and governmental departments.

4.7. Legal and regulatory frameworks

Developing a national cybersecurity policy is essential for Azerbaijan, as it is for many other countries. Cyberattacks and cyber espionage are becoming increasingly common on government information and communication networks, as well as military and commercial operations. From this perspective, managing a country's cyberspace at the state level becomes crucial. The Azerbaijani government is actively promoting cybersecurity in its policy.

Cybersecurity legal and regulatory frameworks (laws, doctrines, and improvements to existing legislation) establish the legal and organizational framework for ensuring the cybersecurity of the state, directions, and principles of state policy in the field of cybersecurity. It also includes the powers of state bodies, enterprises, institutions, organizations, citizens and citizens in this area, as well as the basic principles for coordinating their activities. The development of legal and regulatory frameworks of cybersecurity policy of Azerbaijan mainly started in the 1999-2000s.[16]

Apart from legal documents that are related to cybersecurity, some policies directly concern cybersecurity. It is important to mention that there is no separate strategy for cybersecurity or cooperation with the private sector on the issue, but there are some provisions in various policies that are related to developing cybersecurity capabilities. These strategies are "National Strategy on the Development of Information Society for 2014-2020" and "2016-2020 State Program on the Implementation of the National Strategy for the Development of Information Society", "Azerbaijan 2020: Concept of Development," and "Strategic Road Map for the Development of Communication and Information Technologies in the Republic of Azerbaijan ".

"The National Strategy for Development of Information Society in Azerbaijan during 2014-2020" considers all experiences and recommendations which have been made by International Telecommunication Union (ITU) and the EU. The strategy's main goal is to "build an information society and make efficient use of its capabilities by citizens, communities, and the state for the country's sustainable socioeconomic, cultural, and economic development, including the development of ICT". The Ministry of Digital Development and Transport has been assigned the coordinating role for implementation. The article, which was published in the “CyberCrime@EAP” journal, mentioned that the strategy encompasses most aspects of cybersecurity. Among the major priorities is achieving information security. This priority aims to strengthen digital security, increase trust in the use of ICT, upgrade the legal framework and raise awareness. Objectives for achieving these goals include creating state policy on information security, decreasing dependence on foreign countries in terms of information security, protecting "e-government" networks, announcing cyber threats on a nationwide level, developing technical expertise in cybersecurity, strengthening "safe Internet" for children, raising awareness in society and among companies, and promoting an information security culture.

The above-mentioned strategy is imple-

[16] UNIDIR-The United Nations Institute for Disarmament Research. Cyber Policy Portal. https://unidir.org/cpp/en/states/azerbaijan

mented in two stages, each stage is accompanied by state programs. 2016-2020 State Program on the Implementation of the National Strategy consists of concrete steps on seven priorities for the implementation of the National Strategy. According to the action plan for information security, the Ministry of Digital Development and Transport (MDDT), State Security Service (SSS), State Agency and Ministry of Defence (MoD) are responsible for updating normative legal acts on cybersecurity. Due to the Strategic Road Map for the development of communication and information technologies and SWOT analysis of the ICT sector increasing challenges to network and information security are among the leading threats. One of the strategic goals is to enhance national cybersecurity preparedness and awareness.

- Some of the documents related to the legislative framework are as follows:
- Law of the Republic of Azerbaijan "On State Secrets", 2004
- National Security Concept, 2007
- Law of the Republic of Azerbaijan on ratification of the Convention "On Cybercrime", 2009
- Military doctrine of the Republic of Azerbaijan, 2010
- Law of the Republic of Azerbaijan "On Personal Data", 2010
- "On measures to improve activity in the field of information security" Decree of the President of the Republic of Azerbaijan, 2012
- The Law of the Republic of Azerbaijan on amending the Law of the Republic of Azerbaijan "On National Security", 2012
- Criminal Code of the Republic of Azerbaijan / Cybercrimes
- Decree of the President of the Republic of Azerbaijan on the approval of the Regulation on the Special Communication and Information Security State Service of the Special State Protection Service of the Republic of Azerbaijan and the Agency's structure, 2012
- Decree of the President of the Republic of Azerbaijan "On ensuring the operation of the Electronic Security Service under the Ministry of Digital Development and Transport of the Republic of Azerbaijan", 2012
- Law of the Republic of Azerbaijan on Amendments to the Law of the Republic of Azerbaijan "On Information, Informatization and Information Protection", 2017
- Decree of the President of the Republic of Azerbaijan "On improving management in the field of digital transformation", 2021
- Information Security Management in Banks Regulation, 2021
- Decree of the President of the Republic of Azerbaijan on approval of the Regulation on the Special Communication and Information Security State Service of the Republic of Azerbaijan, 2021
- Decree of the President of the Republic of Azerbaijan "On some measures in the field of ensuring the security of critical information infrastructure", 2021.

4.8. State of National Cybersecurity Strategy

As previously noted, Azerbaijan's cybersecurity policy for 2014-2020 created the foundation for an information society by addressing the broad use of ICT by its citizens, society, the private sector, and government agencies, laying the groundwork for future actions.

Over the past 3–4 years, the Department of Innovative Development of Information Society and Electronic Governance has informed that a new strategy for the future is being developed. Recently, the media has published headlines such as "Azerbaijan develops strategy for cybersecurity". The Head of the Department of Innovative Development of Information Society and Electronic Governance said that Azerbaijan in 2019 has developed a strategy for cybersecurity that will cover the years 2019–2022.[17]

Azerbaijan has also developed and is expected to approve a National Strategy for Information and Cybersecurity spanning the years 2021-2025, according to the Ministry of Digital Development and Transport (MDDT). Due to the Ministry, the action plan for the implementation of this strategy includes provisions to improve the legislation in this area. Once the strategy is approved, it will be presented to the public. The strategic document will serve to further organize and improve the activities in the field of cybersecurity in the

[17] Azerbaijan develops strategy for cybersecurity | eufordigital.eu

country. So, a cybersecurity strategy is under preparation, and the MDDT intends to implement a cyber operation centre for real-time monitoring of cyber threats.[18]

Explaining the delay with some additions to the strategy, the Ministry official noted the emergence of new points-information security issues are not reflected in the Strategy. Therefore, these two issues are now to be combined in the "Information Security and Cybersecurity Strategy". Work is underway to prepare an important document.

According to the Head of the Azerbaijan Internet Forum NGO, "based on the degree of improvement in governance in the field of digitalization, structural changes were made in the former Ministry and several new government agencies were established. The only structure that has not changed is the Electronic Security Service. Observations show that the organization has failed to fulfil many of its tasks. The "Information Security and Cybersecurity Strategy", which has been under development for a long time, has not been discussed yet. Recently, the work has even reached the point where other government agencies have begun to exercise the powers of this body. The e-Security Service has not yet been able to coordinate the Computer Incident. There are serious problems in increasing the digital literacy of the population. In addition, the organization of methodological and information support in the field of cybersecurity in the private sector is not effectively established and is not sufficiently accessible".

4.9. Main Actors of Cybersecurity in Azerbaijan

Some major government institutions are involved in the protection of Azerbaijan's cyber borders: The Ministry of Digital Development and Transport (MDDT), the Ministry of National Security (MNS), and the Azerbaijan National Academy of Sciences (ANAS) through its Information Technologies Institute (ITI), and the National Bank of the Republic of Azerbaijan (CBA).

A computer emergency response team, Computer Emergency Response Center / cert.gov.az, has been established to defend computer networks throughout Azerbaijan's Government Ministries. There is also an Electronic Security Service under MDDT that acts as a certification body. The Ministry made progress in facilitating public access to government services through The State Agency for Public Services to Citizens of Azerbaijan "ASAN". Currently, 450 e-services are being provided through this e-government portal.

The Cyberattacks Simulation Laboratory was established under the Information Computing Center of the MDDT in 2021. The laboratory will study cybersecurity processes, train specialists in this field, and carry out responses against possible cyberattacks.[19]

The Coordination Council was established in 2020 to conduct a national risk assessment (NRA) of the anti-money laundering and cyberterrorist financing (AML/CFT) system and "National Action Plan for the Promotion of Open Government for 2020-2022" was approved. However, there is no similar institution for the assessment of cyber threats and risks.

A number of private actors have emerged recently. For example, "an Azerbaijani company "DEFSCOPE", has been conducting cybersecurity activities in the global arena since 2018. In such a short period, the company has operated many projects around the globe and worked with some of the world's leading companies. It is currently serving its customers in Canada, the USA and Europe with up-to-date products and services. (https://www.defscope.com/about-us) Furthermore, Association of Cybersecurity Organizations of Azerbaijan was established on February 22, 2022.

4.10. Regional and International Cooperation

Safe and secure cyberspace could not be achieved without involving other states in bilateral and multilateral cyberspace cooperation. Beside the unilateral efforts, the state authorities of Azerbaijan are very active in establishing bilateral relations with other states for the enhancement of global cybersecurity mechanisms.

[18] Azərbaycanda kibertəhlükəsizlik üzrə beşillik strategiya hazırlanıb | xəbərlər.az
[19] Deloitte – Kiber və Texnologiya Xəbərləri İcmalı

Azerbaijan is interested in studying and applying best practices in the field of cybersecurity and is making constant efforts in the field of international cooperation. Azerbaijan closely cooperates with Estonia in the field of digital solutions since 2009 which ranks third among European countries. One of the great examples is the deployment of "Asan İmza" in Azerbaijan in cooperation with Estonia. The mobile identity service and the digital signature of "Asan İmza," provides ubiquitous and secure access to the public and private electronic services. Digital mobile signature is equated to a national identity at the legislative level.

Protection of cyberspace is one of the major dimensions of Azerbaijan-Romania bilateral cooperative relations.[20]

Azerbaijan started international cooperation with computer emergency response teams of more than 20 countries, such as Georgia, the Czech Republic.

Azerbaijan has been actively engaged within the framework of the NATO Science for Peace and Security (SPS) Program since 1995. The NATO SPS Program enables close collaboration on issues of common interest to enhance the security of NATO and partner nations by facilitating international efforts to meet emerging security challenges, support NATO-led operations and missions, and advance early warning and forecasting for the prevention of disasters and crises. The Program also helps to prepare interested eligible nations for NATO membership. Recent leading areas of cooperation included Cyber Defence, Counterterrorism, and Disaster Forecasting and Prevention. These activities, Advanced Researched Workshop (ARW) were led by experts from Turkey and Poland.

The foundations of NATO-Azerbaijan cooperation too are essential against the emerging threats of the world as well as cybersecurity is equally important with the issues of nuclear non-proliferation, energy security and terrorism. Within NATO, the Netherlands shared its vision with Azerbaijan for the protection of cyberspace.[21]

Accession to international conventions. Azerbaijan is one of the leading states which are strong proponents of international cyber laws. Azerbaijan signed and ratified Convention on Cybercrime (Signature: 30/06/2008 Ratification: 15/03/2010; Entry in force: 01/07/2010)[22]

On June 30, 2008, Azerbaijan's campaign for the promotion of cyber laws was appreciated by the Council of Europe when it joined the Convention on Cybercrime. After joining the European multilateral alliance to combat cybercrimes, Azerbaijan activated its computer specialists for the prevention of cybercrimes and other illegal activities in cyberspace. As a consequence, Azerbaijan became one of the most active members of the world's first treaty for the prohibition of illegal usages of the internet and cyberspace. The then-head of the Council of Europe in Baku (K.Yerokostopulos) praised Azerbaijan's unconditional support in the fight against cybercrime in the Budapest Convention on Cybercrime. The fundamental objective of the Budapest treaty is to contain internet crimes, which include misuse of computer networks, infringements of copyright, computer-related fraud, child pornography, violations of network security and others."[23]

Alongside the aforesaid multilateral initiatives, Azerbaijan is internally designing its digital laws for the prohibition of domestic cybercrimes. Recently, Azerbaijan signed a decree to take steps to improve the cybersecurity situation. The decree primarily focuses on the safety and security of computerized resources in Azerbaijan.

The cyber-legislation for the prohibition of computer abuses and the strengthening of cybersecurity is divided into two parts. One is the "Law on National Security" (June 2004), and the other is the Law on the Protection of Unsanctioned Information Collection" (September 2004).

Moreover, Azerbaijan Criminal Code defines in its Chapter 30 (titled: Crimes in the Sphere of Computer Information) the rules and regulations on the internet and computer networks, which cover many areas, such as "unauthorized access to, and breaches of the

[20] Azerbaijan Interested in Political Dialogue with NATO – Romanian Envoy, April 04, 2013 www.news.az
[21] Dutch Envoy Comments on Hacker Attacks on Azerbaijan Websites, www.news.az
[22] Chart of signatures and ratifications of Treaty www.coe.int
[23] Convention on Cybercrime, Budapest, 23.XI.2001. rm.coe.int

security of computer systems, including the development and use of computer viruses."

The partnership of Azerbaijan, Georgia, Moldova, and Ukraine within the organization "For democracy and economic development – GUAM"23 is an example of regional cooperation. Currently, Cybersecurity EAST24 (EU4Digital) is a joint project of the European Union and the Council of Europe. The fight against cybercrime through the Council of Europe is mainly focused on projects related to improving the capacity of relevant government agencies in Azerbaijan in the fight against cybercrime.

Azerbaijan started international cooperation with computer emergency response teams of more than 20 countries, such as Georgia, Czech Republic and others. In 2015, the Electronic Security Centre under the MDDT was elected a full member of the "First" International Organization in the field of cybersecurity.

Important efforts have been made to strengthen cybersecurity standards within Eastern Partnership (EaP) countries. As noted, back in 2008, Azerbaijan signed the Council of Europe Convention on Cybercrime and is also actively participating in the cooperation project in the field of combating cybercrime, implemented within the framework of the Eastern Partnership, a mechanism of the European Union. Numerous major treaties underpin the core Council of Europe cybersecurity standards over the last 13 years since the foundation of EaP (2009), providing the strategic framework for the implementation of these standards to bring states closer to de facto cybersecurity.

In this context, the European Union-Council of Europe-funded CyberEast project and the European Union-funded CyberSecurity EAST project aim to support Eastern Partnership countries in improving both cybersecurity and cybercrime-related capacities of the criminal justice and security community.

4.11. Research on Cyber Threats

There is a significant gap in cybersecurity research and extensive analysis of cybercrime in Azerbaijan. Therefore, the projects initiated by the European Union (EU4Digital, Cybersecurity, CyberEast, etc.) should be acknowledged. Existing studies describes various issues associated with cybersecurity policy.[24] As for academic research, cybersecurity is conducted at the Institute of Information Technology of the Azerbaijan National Academy of Sciences (ANAS). There has been no extensive research at the level of official institutions on evaluating Azerbaijan's cybersecurity policy and strategy.

In regards to private actors, two companies - Deloitte in Azerbaijan and Kaspersky in Azerbaijan - have been more active in recent months in terms of research and analysis of cyber threats in the country.

Deloitte's Research Centre's Baku Cyber Team presented first cybersecurity review on January 8, 2021.[25] It chose 26 banks in Azerbaijan as the review targets. Within the review was studied their publicly available web resources on the Internet. As set of criteria was used for cybersecurity assessment: Availability, Domain reputation, HTTP Headers security settings, TLS and SSL security, e-mail leaks, Open ports, Cybersquatting, and Private data security compliance based on the GDPR requirements.

The review results revealed that some banks in Azerbaijan do not apply all cybersecurity standards and practices. The study noted various findings, starting from weak security settings or usage of vulnerable encryption protocols on webservers through the lack of user awareness in cybersecurity matters. The report highlights all the identified issues and contains recommendations on the possible ways of addressing them. "In the review we did not assess criticality level of our findings. However, our global experience depicts that there is no minor risk in Cybersecurity. Not all cyber leaders at banks are aligned when it comes to steering the best course to protect infrastructure. Many banks do not follow standard security best practices when they set up their web servers. As a result, even without using specialized software, we have identified important deficiencies at a number of banks.

[24] Marcus Franda, Launching into Cyberspace: Internet Development and Politics in Five World Regions (London: Lynne Rienner Publishers,2002); Azerbaijan Cybersecurity Governance Assessment Author Ms. Natalia Spînu (2020). DCAF.Switzerland; K. Makili-Aliyev & Rehman. (2013). A.Cybersecurity Objective: Azerbaijan in the Digitalized World. SAM Review. - ict.az/en

[25] Azerbaijani banks cybersecurity review. Cyber Risk Advisory. 2020. Deloitte Research Centre.

What's more, a large number of these were not new problems or zero-day breaches, but rather fairly old and well-known cybersecurity issues. Although these deficiencies may seem insignificant, they can lead to leaks of confidential financial data or direct theft of funds from client accounts. At the same time there are cases when we see lack of banks employee's awareness of cybersecurity matters. It is an indication of weakness in existing cybersecurity policies and cyber education programs applied in banks. In fact, one ill-fated click from an unknowing employee could threaten the entire bank's data".

Kaspersky has recently conducted a number of surveys in Azerbaijan. At the end of 2021, there have been announced the results of a survey and noted that some 87% of users in the cities of Baku, Sumgait and Ganja have faced cyber threats over the past year. This indicator shows that in the mentioned cities every 9 out of 10 users faced the cyber threats. "Most of the threats (80%) came from instant messengers (WhatsApp, SMS, Viber), 32% - from social networks, and 28%-phone calls. Besides, 27 percent of the fraudsters said they represented banking structures, 27% companies, 17%- shopping facilities and 15%- sellers of online platforms. Additionally, there was mentioned that in 34% of cases, the fraudsters offered to allegedly transfer the winnings from a lottery, in 25% - profit from investments, while in 14% of cases – to take part in a simple and profitable transaction. The cyber fraudsters aim to obtain information about card data (36% of cases), transferring funds from card to card, personal and payment data of citizens (21%), and in 16 percent of cases, victims are asked to switch to "fraudulent link".[26]

Due to neighbouring nations' defeats in the war and certain revenge efforts, cyber threats and cyber war have been a continuous issue since 2020. As noted in previous research reports, for the majority of EaP states, the major sources of cyber threats are external, as almost all of these states are involved in rather complex and challenging relations with their immediate neighbours. The Azerbaijan authorities are aware of the necessity of raising cybersecurity both at state and general population level.

According to The National Cybersecurity Index-which measures the preparedness of countries to prevent cyber threats and manage cyber incidents, Azerbaijan's position is 82nd-National Cybersecurity Index; 40th-Global Cybersecurity Index; 65th-ICT Development Index; 76th-Networked Readiness Index.[27]

Azerbaijan improved its ranking in the 2020 report of The Global Cybersecurity Index 2020 (GCI), moving up 15 points to 40th place. With 89.31 points in total, Azerbaijan is 3rd in the CIS after Russia and Kazakhstan.

[26] Azerbaijan talks cyberthreats faced by local users in several large cities. - en.trend.az/business
[27] National Cybersecurity Index – Azerbaijan. 17 Mart 2020

5. QUANTITATIVE RESEARCH

5.1. Summary

The smartphone was the most regularly used device for personal needs. 73.3% take some careful measures with what they do when using their devices. A relatively larger proportion (62.8%) of the sample was not familiar with the word cybercrime, whereas remaining 37.2% did have knowledge of this term. 93.3% are not familiar with the word phishing. Most respondents (86.4%) believe that they have not been targeted by an attempt of what they felt, then, was computer/online criminal activity. Once they were provided the definition, 74.3% said that they have heard of this type of crime happening. Among phishing victims, most have not been affected or viewed it as a nuisance (69.6%). More than half (56.9%) feel that if someone in their neighbourhood would receive a phishing message, 52.7% know enough about phishing to protect themselves and their family. 97.6% are not familiar with the word ransomware. After the explanation, 60.7% feel that in case of a ransomware attack to someone in their neighbourhood and they lost access to their computer, their mobile phone, or to the data or photos that they contained, they would report it to the authorities/police. Almost two-third refused to participate in questions about intimidation/abuse. 91% (of the people who consented to answer questions about these sensitive topics) have not experienced online abuse. The majority have not become aware that login credentials to a personal account of them had been exposed online in the past 12 months. 61.6% feel they know enough to protect themselves and their family from online identity theft. Data breaches and online identity theft is the most concerning offence for 40.6%, even though a very small percentage has suffered it.

A significant number of enterprises do not have a dedicated role or department in charge of cybersecurity. The weight of expenditure on cybersecurity within the IT budget is generally low, and most of the enterprises do not have insurance. ISO 27001 is the most prevalent safety framework followed in the sample. More companies rank cybersecurity within their company either low or non-existing. Among cybersecurity technologies currently in place, anti-malware software to protect against viruses, spyware, and other software was noted by the majority, while spam/phishing filtering and data protection and control came next. The responses to a number of questions on cybercrime victimization indicate a very low rate of victimization among enterprises. 45,3% and 46,9% think the application of advanced security technology and larger budgets will help improve their organization's security levels respectively. 65,6% of enterprises use file encryption on laptops. The responses with regards to whether the COVID-19 pandemic has exacerbated cybercrime against enterprises are almost equally divided.

5.2. Technical Information – all in charts to provide an overview of the structure of the respondents

5.3. Research Methodology – as presented in the ToR and all country specifics to be included

Research design

The study adopted cross-sectional research design.

Sample and scope

In order to cover all administrative regions and create a nationally representative survey of the population, a cluster sampling method was applied nationwide for the face-to-face survey. Due to the latest Census (2020), the population size was 10,067,100. The target confidence interval and margin of error in the survey were 95% and 3% (or less). Across all administrative regions, three settlement types – city, county and village were covered, of which the distribution is presented in the respective table.[28]

[28] In the official classification of settlements, a city is a geographical unit of which the population is above 15,000 and most of its workforce is employed in industry and budget-funded organizations (State Statistics Committee, 2019). A district or county, on the other hand entails a settlement of which the maximum population is 15,000. Villages' population levels vary.

Following the criteria set by the Council of Europe, stratified sampling was used. We used a three-stage stratified sample with strata at the level of the electoral district, household, and individual. Respondents were questioned face-to-face by interviewers at their residences. Only one respondent per household was selected for participation in the survey, with quotas for gender-age and gender-education. The response rate of those who were contacted was 48%, for a final sample of 1,600 respondents.

Data collection

The study employed two methods of data collection, resulting in triangulation. In the first stage of data collection, a face-to-face survey was conducted among 1600 respondents. The average duration of the survey was approximately 13 minutes (median = 12.50 minutes, standard deviation = 3.36 minutes).

Regarding the survey with enterprises, a face-to-face survey was conducted among 64 respondents. The primary reason for not reaching 100 enterprises is related to a) lack of IT use in many companies contacted; b) no use of incentives; and c) lengthy period of sending letter and getting official response from the companies.

Twenty pollsters were employed to conduct the survey. The pollsters went to those houses that were selected in the sample and delivered the surveys by hand. If the household agreed to participate, at least one person over the age of 18 filled out the survey. The survey was conducted on diverse days of the week and at different times of the day in order to cover all segments of the population as much as possible.

Analysis

The data were analysed in SPSS (Statistical Package for the Social Sciences).

Ethical issues

Responses were anonymous and confidential. All participants who attended focus groups in person had to write their name, and surname and put down their signature, while those joining over Zoom did not sign. Implied informed consent was obtained before starting the discussions.

Training

To conduct the survey, 20 pollsters were hired. All pollsters had varying years of fieldwork experience, and most had degrees in sociology, psychology, and social work. Prior to fieldwork, all pollsters were given an intensive training by the coordinator and manager. They were then asked to conduct survey in between themselves, which was followed by a pilot study.

Fieldwork issues

While the fieldwork went largely smoothly, the greatest obstacle was the almost total absence of internet coverage in a number of villages (particularly mountainous ones). This prompted us to switch to different sampling points after the data collection started. The second issue we frequently encountered was that some people (particularly in remote villages) used the internet primarily for one purpose and on an intermittent basis, such as WhatsApp texting when needed or watching YouTube. Since they could be deemed mostly passive users, they were not eligible for the survey, but nonetheless, this issue extended the duration of fieldwork to some extent.

In terms of enterprises, the biggest hurdle was related to the very limited adoption of IT security measures by enterprises outside cities. Thus, when rural enterprises were interviewed and the initial data analysed at the beginning of the fieldwork, one pattern emerged that substantially delayed data collection. Particularly, those enterprises tended to rarely use any IT security measures since most of their business was conducted offline. Due to this particular issue, they did not respond to many questions in the survey. In order to make the data collection more meaningful a second round of sampling was conducted.

5.4. GENERAL PUBLIC

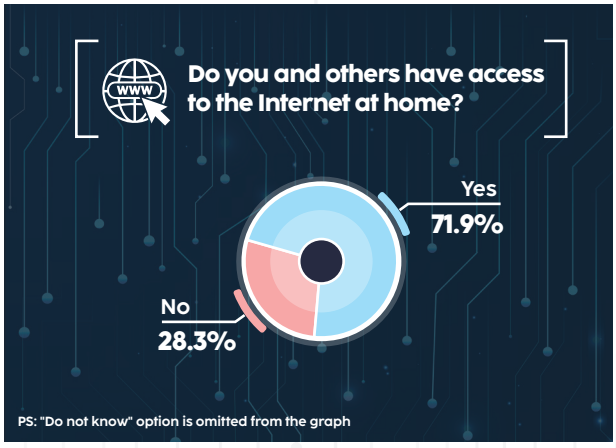
5.4.1. Use of Internet

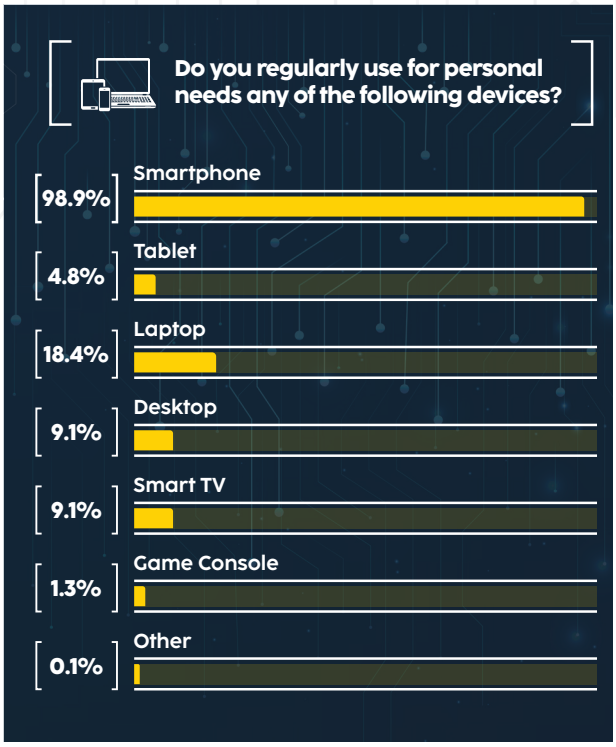
5.4.1.1. Online Activities

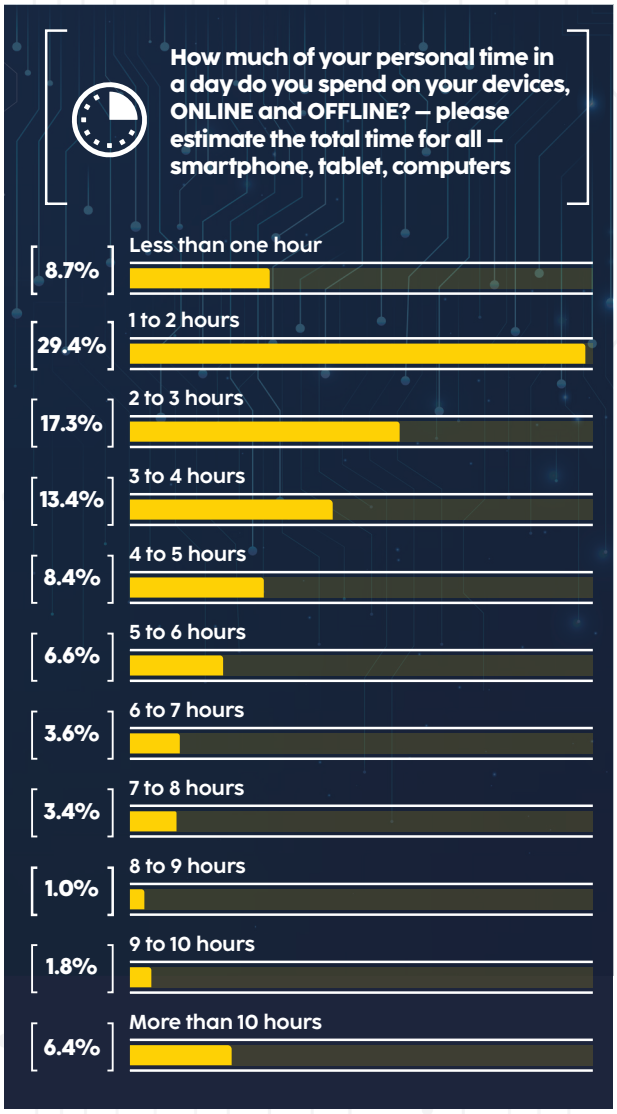
Among the contacted sample (2233), 71.7% (1600) of the households had access to the internet.

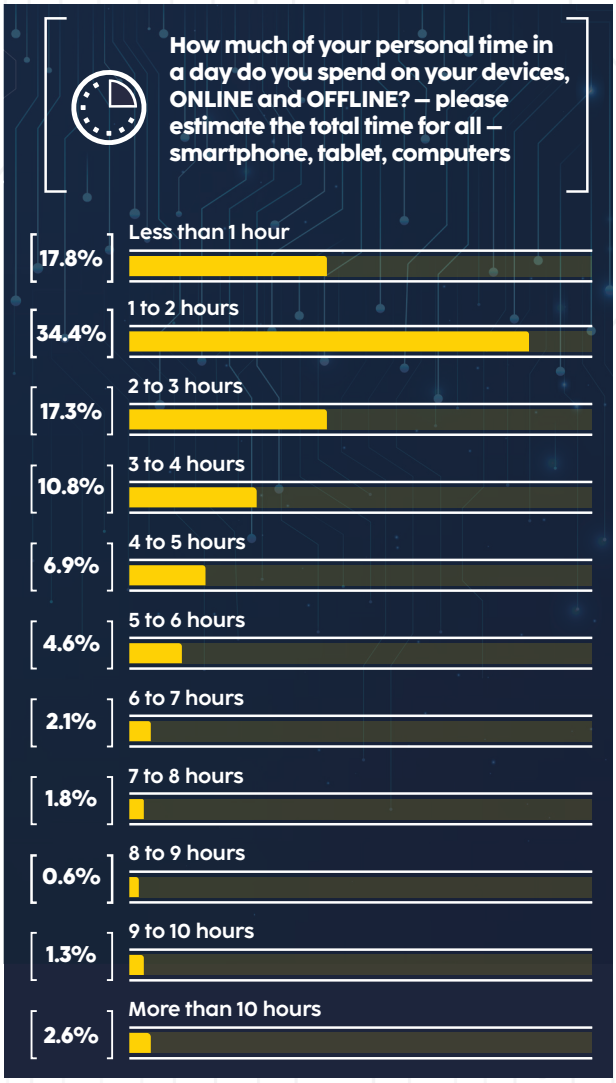
Smartphones were the most regularly used device for personal needs (98.9%). Geographical location and devices used for personal needs are correlated, with Baku and Aran regions (the most populated economic regions) having higher usage of smartphone and computer users. Overall, 81% of smartphone and computer users were from urban areas.

A relatively larger proportion (29.4%) of the sample spends 1-2 hours of their personal time each day on their devices. The figure is similar for the time spent online (34.4% using 1-2 hours).





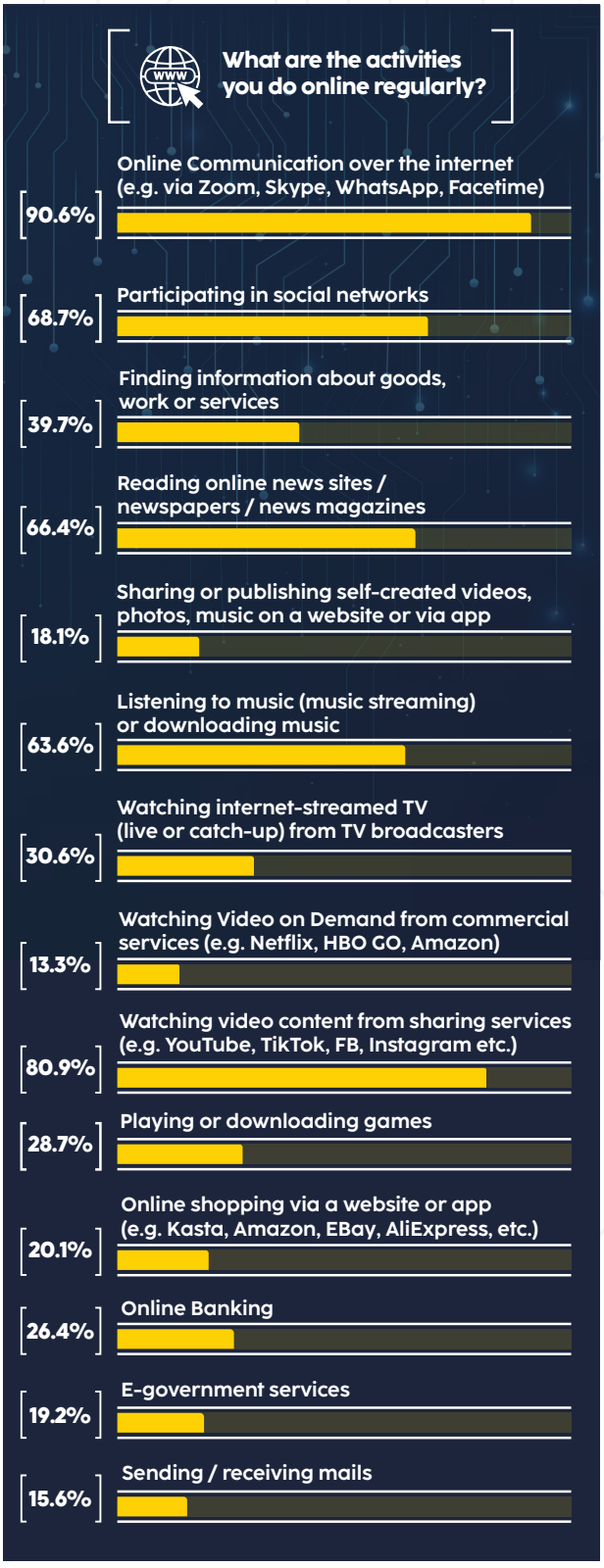




Online communication (including video calls) over the internet was the most widespread online activity (90.6%). The likelihood of spending more than 4 hours online was found to be higher for urban dwellers than rural dwellers. Thus, one may interpret it as urban dwellers being at a higher risk of victimization. On the other hand, one of the most fascinating discoveries in terms of the most widespread online activity is the figure for watching videos on demand (80.9%), an activity that is less likely to create a risk for cybercrime victimization.

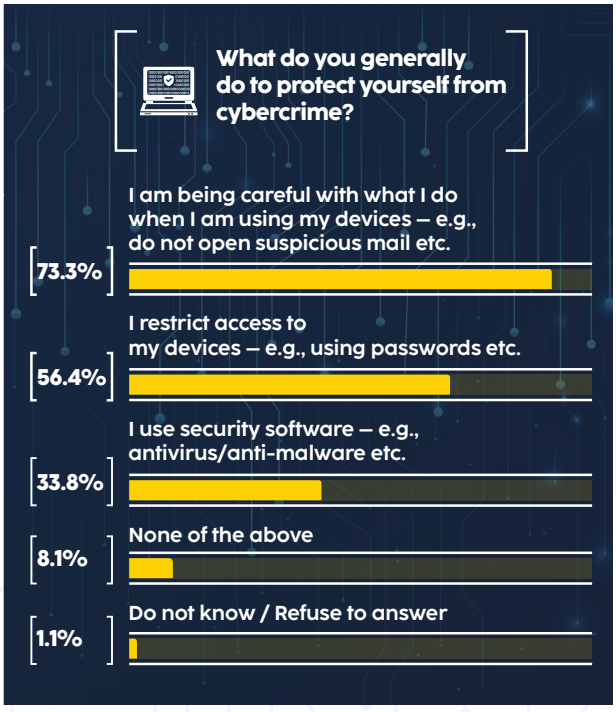
Additionally, 68.7% of respondents use the Internet for spending time on social networks, 66.4% read news in online newspapers and magazines, 39.7% for searching information about products, vacancies or services, 28. 7% use it to play or download games, and 26.4% use it for online banking.

Analysis of the survey by several categories shows that the sale of goods or services through websites or applications, the use of e-government services, and online banking are more often chosen by male respondents. While sending or receiving email is common among student students, making calls over the Internet, spending time on social networks or doing work, playing games, or downloading was among respondents with upper secondary education.



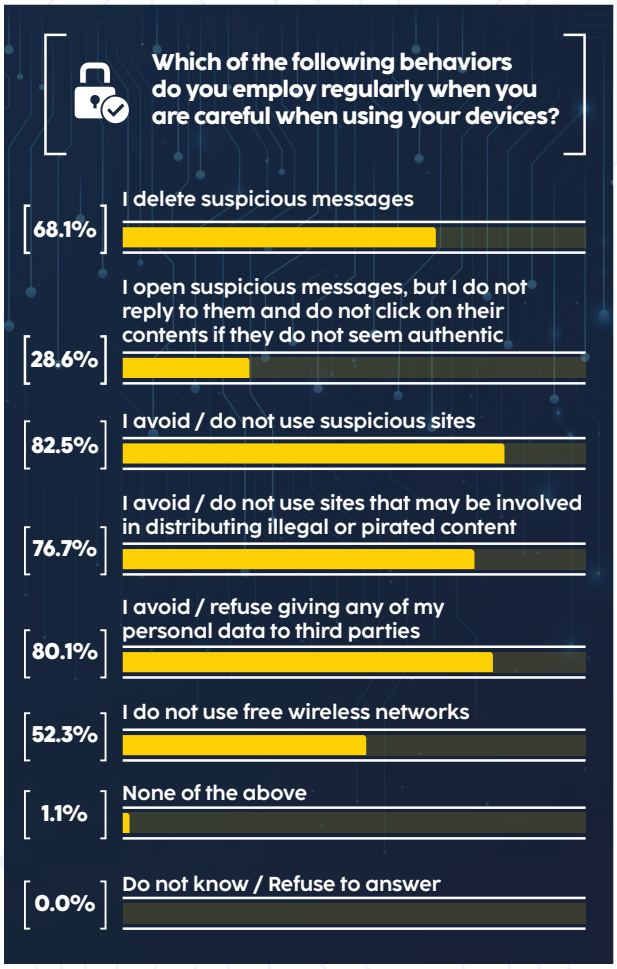
Concerning the possibility of victimization, 73.3% take some careful measures with what they do when using their devices. Restricting access to the devices was the most widespread measure (56.4%) and it was most prevalent among the 18–24 aged sample. While looking at correlations with demographics, gender appears to have significance, with men being more likely to take all protective measures listed on the questionnaire. Those spending 4+ hours online were more likely to take all the protective measures listed on the questionnaire. The same applies to the respondents with vocational/professional education and bachelor's degrees.

As mentioned, such as cybercrime protection techniques 56.4% of respondents restrict access to their personal devices (e.g. using a password), while 33.8% of them used security applications (for example, antivirus, etc.)

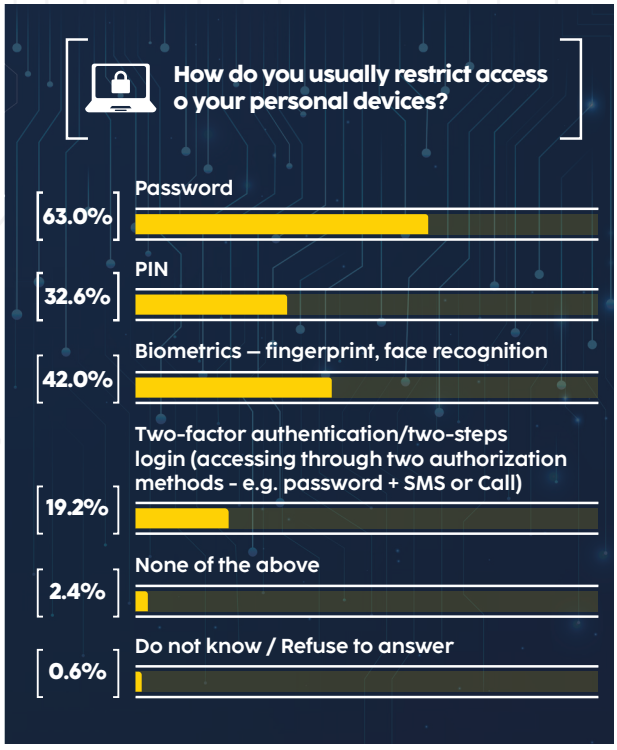


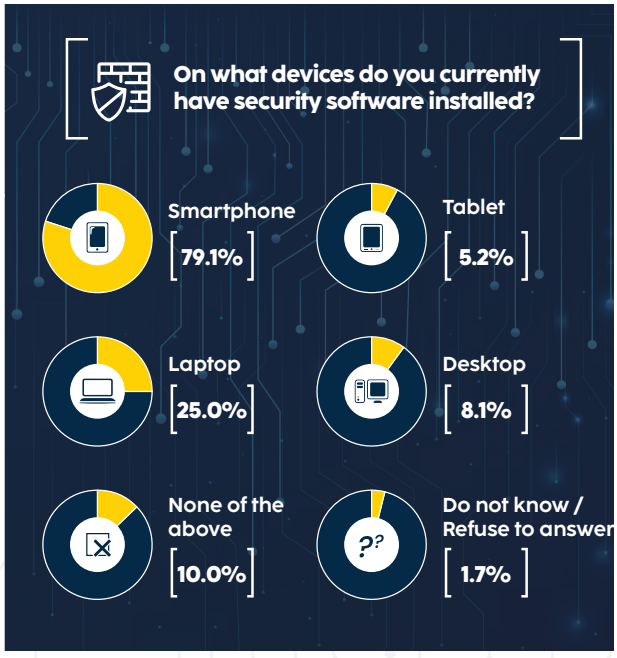
The most widely reported behaviour employed regularly when using devices is the avoidance of suspicious sites (82.5%). The fact that only one-third of the sample uses antivirus/anti-malware software is a concerning finding and points to the need for raising awareness in this regard. No important difference was observed in the questions above between the focus group and the survey sample.

Furthermore, as a precaution when using the devices, 80.1% of respondents do not transfer their personal data to a third party, 68.1% delete suspicious communications, 76.7% do not visit sites that may spread unlawful or pirated content, and 52.3% do not use free wireless networks (eg Wi-Fi).



It should be noted that the respondents were given the opportunity to choose several answer options. When it comes to personal devices, the most often used access restriction/protection approach is the use of a password. Other methods mentioned by respondents include biometrics (fingerprint, facial recognition) (42.0%), PIN code (32.6%), and two-factor authentication (19.2%), which requires an eye, finger, or face print in addition to a password. The use of two-factor authentication was more often mentioned by those with complete secondary education and by male respondents.

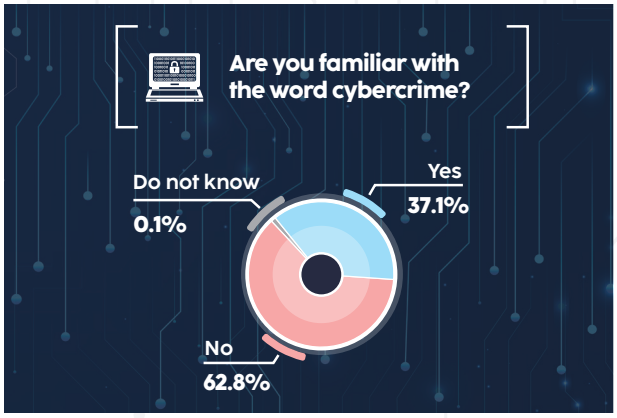


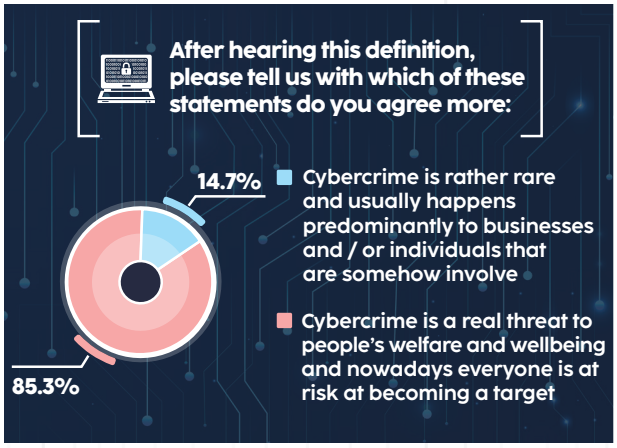


Password is the most used access restriction/protection method for personal devices. Data from the focus groups largely confirm this result, though while a third of the survey participants mentioned PIN, it was barely noted among other population sample. Most of respondents who are smartphone users (79.1%) neighbour have security software installed in their smartphone.

5.4.2. Knowledge, awareness, and attitudes towards cybercrime

5.4.2.1. Level of knowledge





A relatively larger proportion (62.8%) of the sample was not familiar with the word "cybercrime". The level of awareness about this term among the respondents is only 37.1%. Once they were provided the definition, 85.3% chose the "Cybercrime is a real threat to people's welfare and wellbeing, and nowadays, everyone is at risk of becoming a target" option. Male urban dwellers and those with bachelor's or master's degrees, as well as those who are using both smartphones and computers, were more likely to be familiar with the word cybercrime.

All participants in focus groups had heard of cybercrime (in a different context, including school, banking, journalism, war with Armenia in 2020), as well as the majority of the other crime categories described. However, phishing and ransomware were hardly ever mentioned, despite the fact that the former was widespread in terms of victimization. Respondents mostly recognized them once an explanation was given.

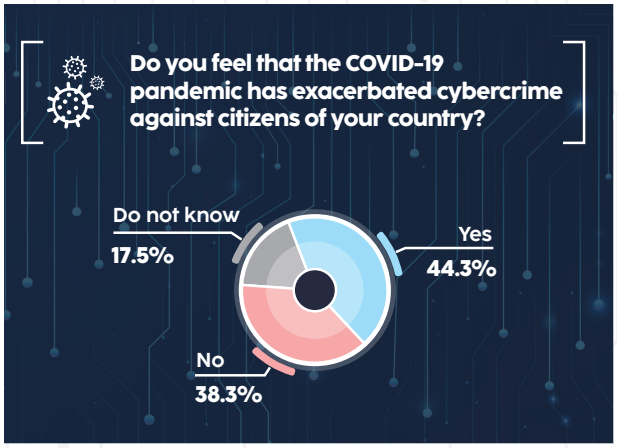
In terms of the perception of cybercrime, the phrases “internet crimes” and “information crimes” were frequently noted as all-encompassing phrases among GPGs as well as NGO representatives. However, the perception of cybercrime among IT professionals and law enforcement representatives differed radically from that of the general population. For the former participants, cybercrime is any crime that achieves its target, not just an attempted one. Also, these participants spoke of very elaborate and intricate details of cybercrime. Thus, participants had in-depth knowledge of all the offence categories discussed. For law enforcement representatives, cybercrime meant hacking access to information stored on other devices and damaging the integrity of information systems.

“For me, a true cybercrime consists of the one that penetrates all the systems – antivirus programs and firewalls we have built. I consider a true cybercrime that renders us helpless and desperate. If it is something we or our system deal with every day, like those trivial, minor attacks or problems, it is nothing for us.” (IT professionals & NGO group)

“I see cybercrimes, or potential for that, everywhere. On the internet, ATMs, card payment post terminals, buses… for me, if there is a human being on top of the system, I mean, as a responsible person, then this system is certainly prone to compromise. Nothing is safe” (IT professionals & NGO group)

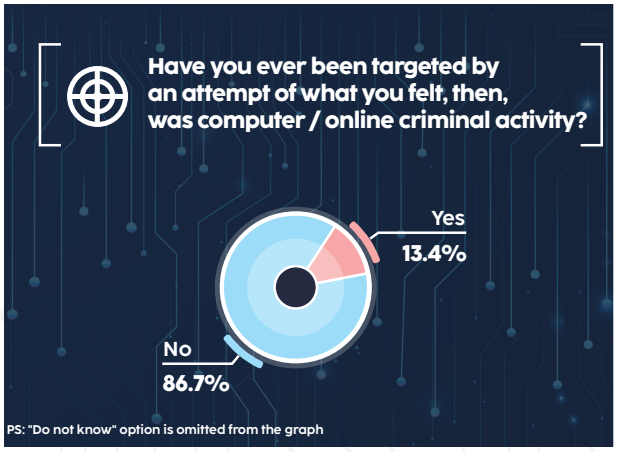
“For us, it is loss of profit and reputation. When the system goes down due to attacks, our phones do not stop ringing. I have seen cases where companies had to cease operations for hours.” (ISP)

For GPGs, cybercrime consisted mostly of attacks against people intending to steal their money and personal details.



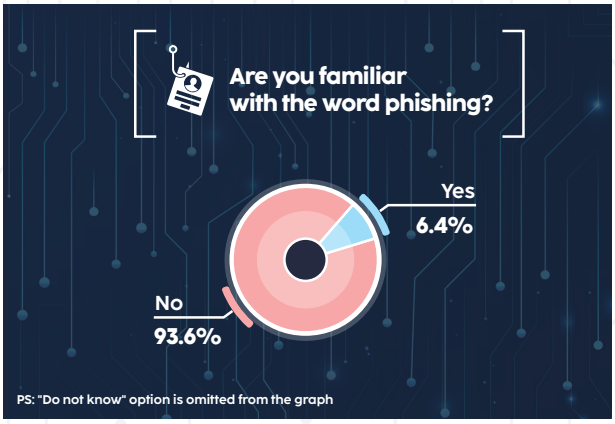
The majority of people (44.3%) feel that the COVID-19 pandemic has exacerbated cybercrime against citizens. Respondents from the 18-24 age sample were more likely to agree with the previous statement.

5.4.2.2. Phishing



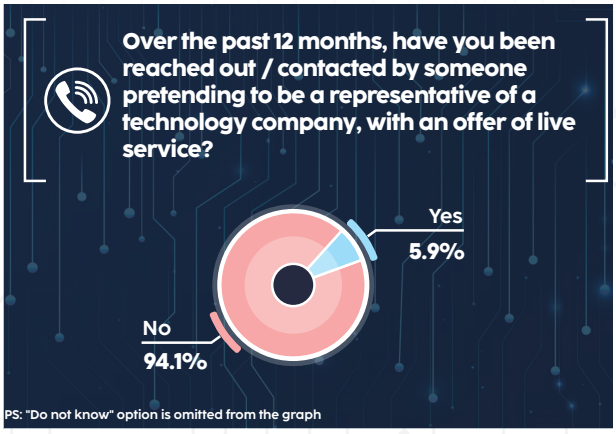
Most respondents (86.4%) believe that they have not been targeted by an attempt to do what they felt, then, was computer or online criminal activity. This result is significant in the sense that phishing is probably not a serious concern on a national level. Also, the fact that no significant correlation was observed between attempts and demographics, suggests that there is no specific group with a higher likelihood of being attempted.

Only 13.4% of respondents claim to have ever been the subject of online or computer-related crimes. According to the study results, only a small percentage of respondents (6.4%) are aware of the term "phishing." The number of people who have no knowledge of this term is fairly high (93.6% in total).



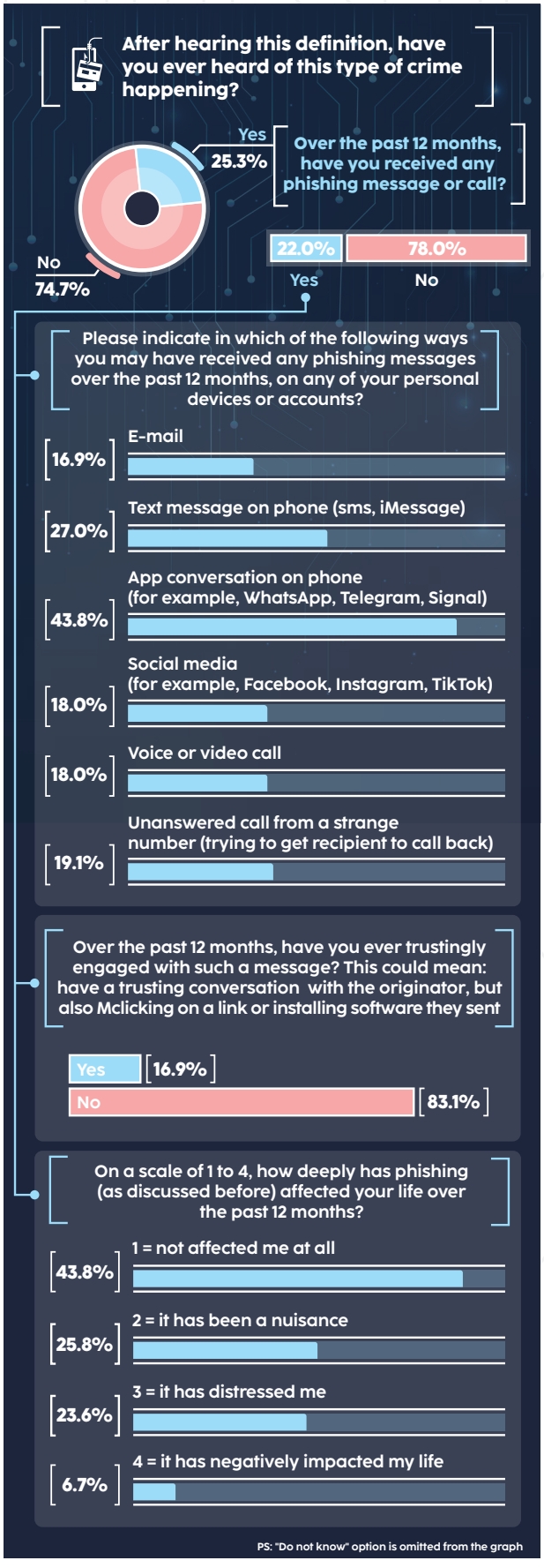
In terms of familiarity with the word "phishing", only a very small part of the sample recognized it. Due to the correlations, there were more aware people among those holding master's degrees, as well as people using both smartphones and computers. Approximately a third and a half of those holding bachelor's and master's degrees, respectively, have never heard of this type of crime happening. No significant correlation was observed in terms of receiving any phishing messages or calls.

According to the responses to the relevant question, the vast majority of respondents (94.1%) were not contacted by someone posing as a representative of the technology company on the live service offer.

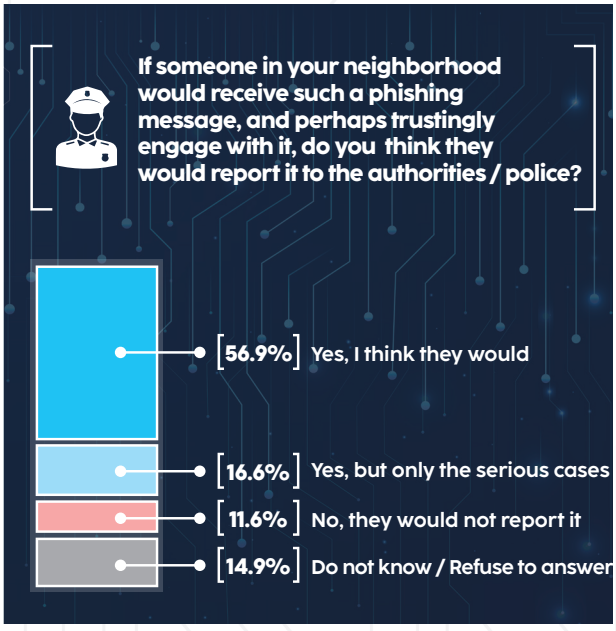


Once they were provided the definition, 74.4% said that they have heard of this type of crime happening. A small proportion has received any phishing messages over the past 12 months.

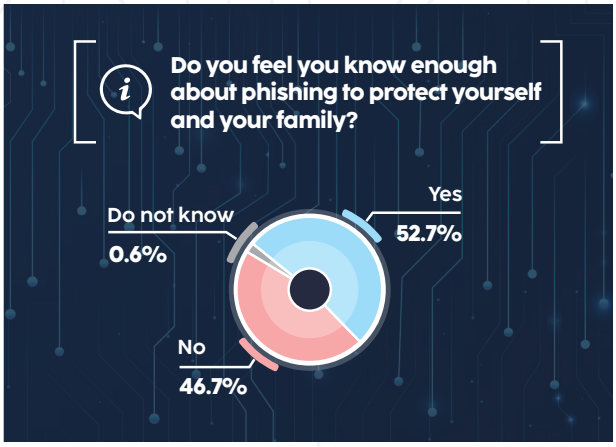
Even after explaining the relevant definition, 74.7% of respondents claimed they had not heard about the occurrence of this type of crime. However, a part of the respondents indicated receiving communications containing the aforementioned content (particularly via e-mail and social media) in the previous 12 months. According to the findings, the majority of the victims' lives were not substantially affected by such occurrences, or they did not perceive it as a concern.



More than half (56.9%) feel that if someone in their neighbourhood would receive a phishing message, they would report it to the authorities / police. No significant correlation was identified with socio-demographic characteristics. Almost half of the sample feel very concerned, and 22.1% feel concerned about phishing criminal activities in the country. As the age of respondents gets younger, the likelihood that he/she is to some extent concerned about phishing-related criminal activity increases. The higher the degree of concern about phishing criminal activities, the more probable it is to use all of the protective measures indicated on the questionnaire.



52.7% know enough about phishing to protect themselves and their family. The opposite was stated by 46.7% of respondents.



Among focus group respondents, nearly all said they had seen phishing attempts. The fact that only five cases of victims are known in the GPG indicates a high level of awareness about how people can protect themselves and their workplace. Nonetheless, sharing some stories of victims may be useful in shedding light as to how they were victimized and what their experience was in relation to reporting, or absence thereof.

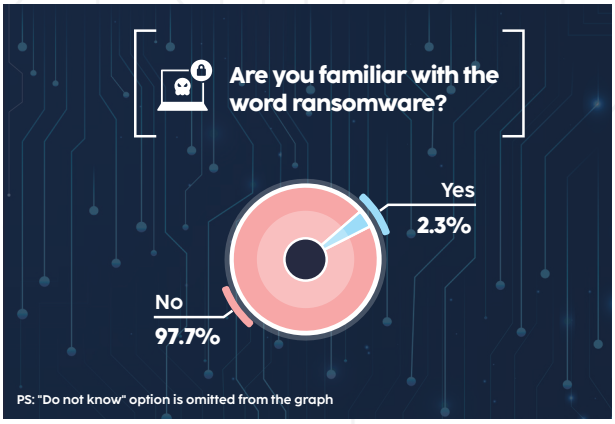
"I registered my interest in one of the recruitment companies. Someone called me, asking whether I look for a job. He was not from the recruitment company I was registered at. He said a name, [some interjections due to emotions], sorry I forgot. Anyway, he asked for AZN 150 deposit. I initially hesitated and insisted to meet him in person and give money. But you know what, he convinced me really well. That is why I perceive cybercrime as an act where conviction is used to steal something from someone. Yes, I deposited AZN 150. A few days later, when I wanted to contact him, he did not respond." … I went to the police. Thankfully, they found them, though the money was gone. More precisely, transferred to an account of foreign country, and the police failed to get it back. (Male, victims' group)

"I was looking for a cheap mobile phone. I saw a discounted one on TAP.AZ [it is a well-known e-commerce platform in the country], an online e-commerce website. They asked for AZN 50 deposit, which we did. Then, we could not contact him…Me and my daughter went to the police, but they showed no reaction. They simply said that it is not our business. Go to another district police, even though they certainly were wrong, they just wanted to get rid of me" (female, victims' group)

"My son actually was the reason why I lost money to this kind of fraud. He was led by strangers in America to believe that if he pays money to them, he will get good gifts in return for his videogame. You will earn $800, things like that. I am an old woman and i do not really know all these details. I gave him $200, and he lost it to fraudsters." (GPG)

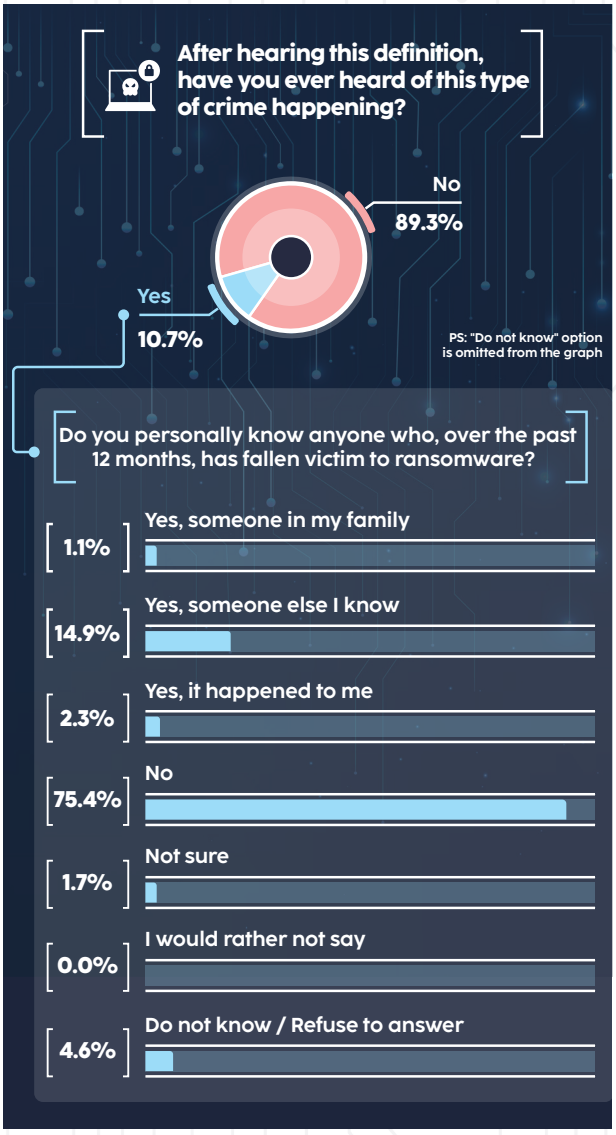
5.4.2.3. Ransomware

Ransomware is a type of malware used by cybercriminals to block access to a system or encrypt data. (In return, they demand a ransom from the victims - ed.).



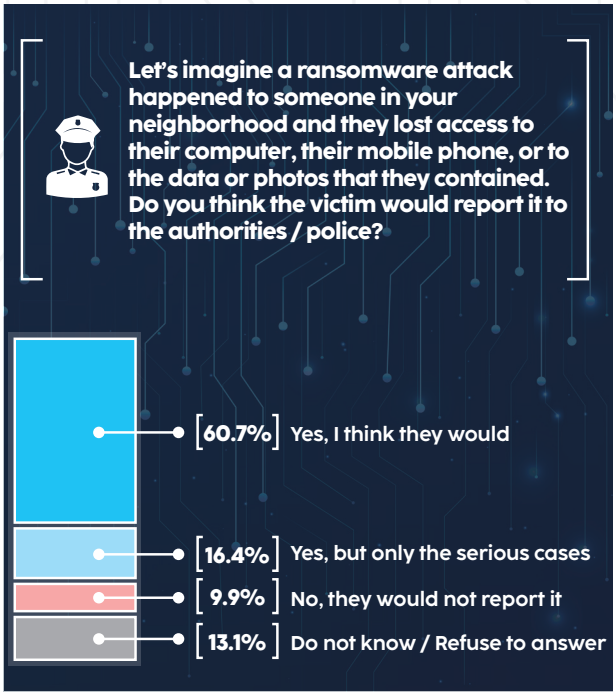
In general, 97.7% of the sample's participants reported they were unfamiliar with the term "ransomware" (a cyberattack that uses malicious software to hold data hostage), and only 2.3% claim that they have knowledge about this term.

Following an acceptable explanation, 89.3% of respondents stated that they had never heard of such a crime, while 10.7% responded that they had. In the last 12 months, 14.9% of respondents reported that someone they know, 1.1% of their family, and 2.3% of themselves had been victims of ransomware. 4.6% of the respondents found it difficult to answer this question.



Furthermore, 60.7% of respondents feel that if a neighbour is attacked in this way and loses access to their computer, mobile phone, photographs, or other information, the victims will notify authorities/police. If this type of incident occurred, 16.4% of respondents stated they would only report to authorities/police in extreme situations, while 9.9% said they would not apply under any circumstances.

13.1% of respondents did not give an opinion on this question.



The term "ransomware" is unknown to 97.6% of respondents. Once the definition was provided, 89.1% said they had never heard of this type of crime happening.

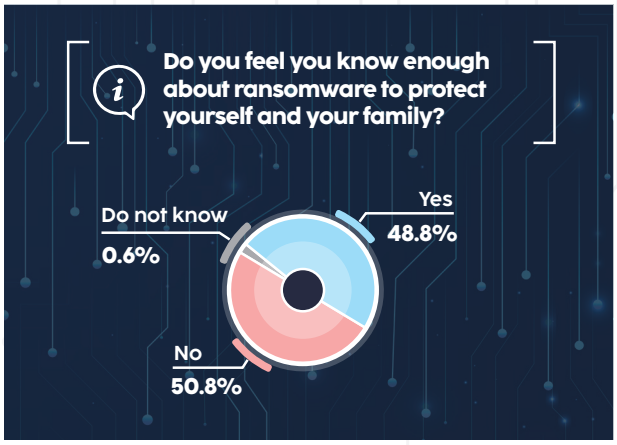
Over the last year, 2.3% of people have become victims of ransomware.

In the case of a ransomware attack on someone in their neighbourhood, 60.7% believe that if they lost access to their computer, mobile phone, or the data or images stored on them, they would notify authorities/police.

For the majority (85%), the event of a ransomware attack would either distress or negatively impact their lives. Almost half of those polled are very concerned about the level of ransomware in Azerbaijan. In order to protect themselves and their family, 48.8% of people think they are knowledgeable enough about ransomware. However, considering the extremely limited cases of ransomware attempts among the sample (both across the survey and focus groups), one wonders whether their risk perception is accurate and whether they are really protected enough.

Ransomware (hostage attacks), according to the majority of respondents, can cause annoyance or negatively impact people's life. In this context, over half of the respondents are extremely concerned about the frequency of such instances in Azerbaijan. Following the findings, 48.8% of respondents believe they are well-informed enough to defend themselves and their family from such circumstances.

Half of those respondents (50.8%) said they were not well-informed about the Ransomware program.



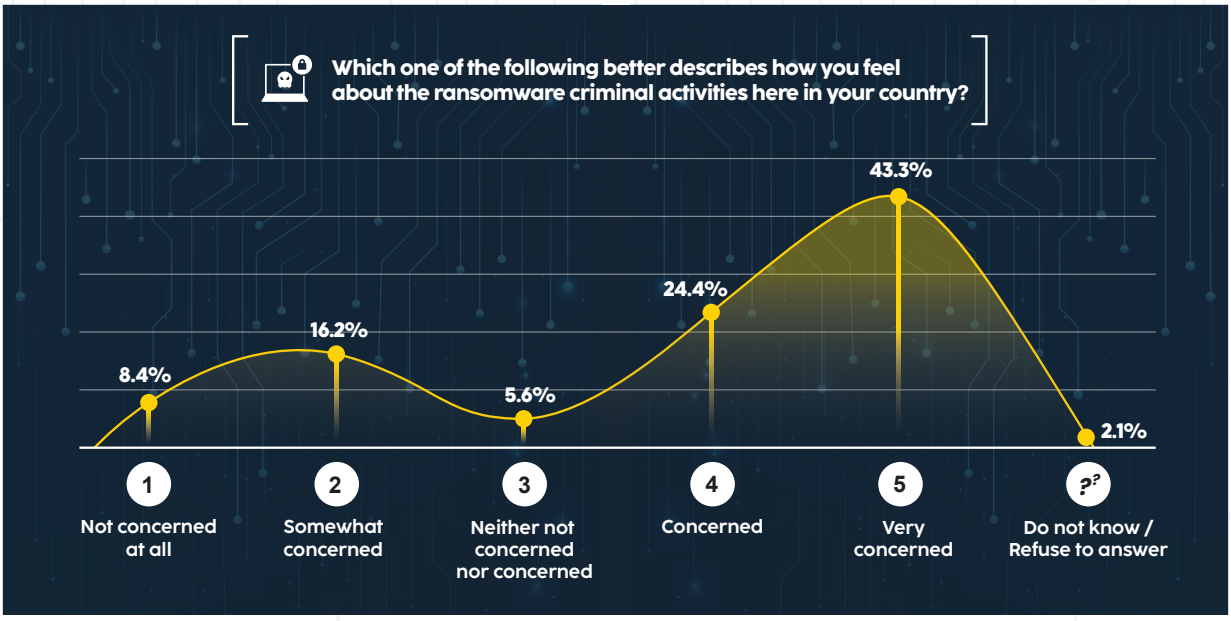
Across all GPGs, there was almost no one (except for one female in Group 3 who used to work at a bank and attended regular seminars on this problem, and one student in Group 1 who was victimized) who had heard of ransomware before being provided with the definition. Overall, across all three groups, only 4 recognized it later on. The primary reasons may be (1) the English version of the name and (2) little prevalence of this offence in the local context. Moreover, ransomware was unheard of among victims' group as well.

In terms of ransomware, only two victims and one vicarious victim were identified across all three groups. However, none of these victims paid the ransom. Rather, they either bought a new device or formatted the existing one.

"I have not been victimized, but my close relative's phone was blocked. He could not make ransom payment, and the repairman could not repair it. So, he had to buy a new device" (GPG)

"My Instagram was blocked about 10 years ago. I did not know how much they asked for it. I went to a software engineer, and he suggested me to change my device. So, I did" (GPG)

Overall, all groups pointed to a very limited prevalence of ransomware. Interestingly, CERT representative drew attention to the increased prevalence of ransomware during the pandemic:



"I totally agree with the idea that phishing became more widespread, and many of them contained messages about how to protect yourself from COVID-19 virus. Some of them, as we observed, resulted in ransomware. We also discovered several fake profiles posing as health institutions".

In Azerbaijan, 43.3% of respondents are extremely concerned about the spread of ransomware crimes, while 24.4% are mainly concerned. 8.4% of respondents claimed that it does not matter at all.

5.4.2.4. Intimidation and Abuse

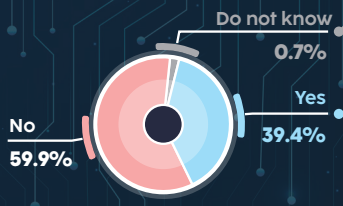
Almost two-thirds of the respondents (59.9%) declined to answer the intimidation/violence-insult questions. Approximately 39.4% of survey respondents agreed to respond to such questions. A relatively small percentage of this sub-sample (18.2%) reported seeing hate, prejudice, or violence directed at individuals of a particular race online, whereas 81.3% claimed they had not.

In addition, 95.3% of respondents agree that the authorities/police should do more to protect children from the Internet environment and online environment. However, 3.4% of respondents exposed the disagree.

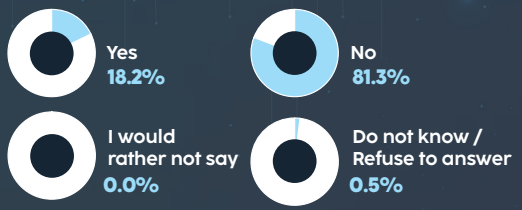
The statements of 91% of the respondents about these questions were that they did not face any cases of online violence. Furthermore, 7.2% of the survey participants said that someone familiar, 0.2% someone from their family, and 1.1% themselves have experienced cases of online violence.

68.5% of the respondents think that if someone in their neighbourhood was victimized by online violence, they would definitely report the law enforcement agencies. Though, 17% of the survey participants said that in such cases, someone in their neighbourhood would apply to the relevant authorities only in serious cases, while 5.6% said that they would not apply in any case. And, 8.9% of survey participants claimed they had difficulty answering this question.

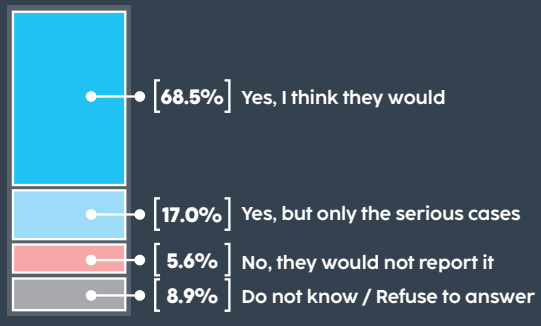
Would you be willing to answer a few questions about intimidation and abuse?



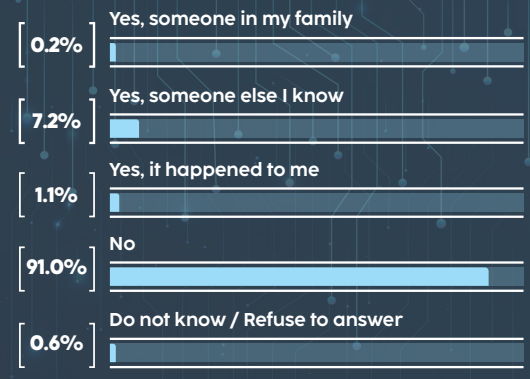
In the past 12 months, have you yourself witnessed any online promotion of hatred, discrimination, or violence against people of a certain race, color, descent or origin?



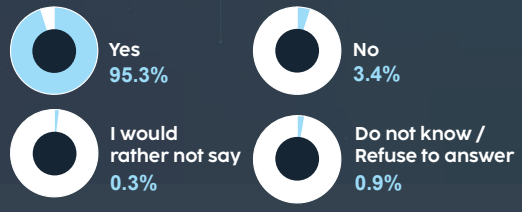
If someone in your neighborhood would receive such a phishing message, and perhaps trustingly engage with it, do you think they would report it to the authorities / police?



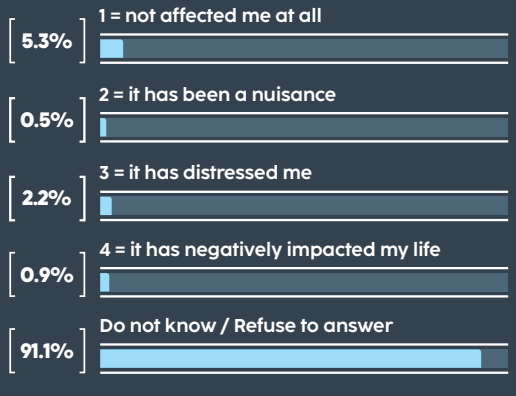
Yes, someone in my family: Some online interactions can be very intimidating Has anyone that you personally know been insulted, bullied, blackmailed, or intimidated online, in the past 12 months?

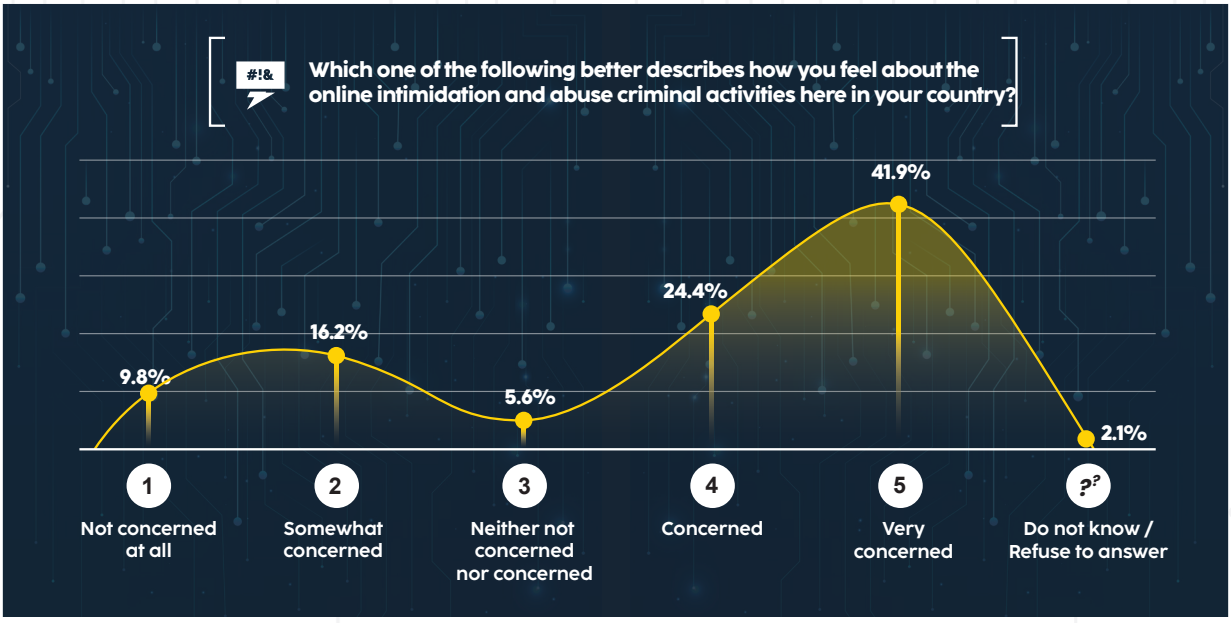


Unfortunately, the internet can sometimes be an unsuitable place for minors. Do you think authorities / police should do more to protect them online?



On a scale of 1 to 4, how deeply have online intimidation or abuse affected your life over the past 12 months?



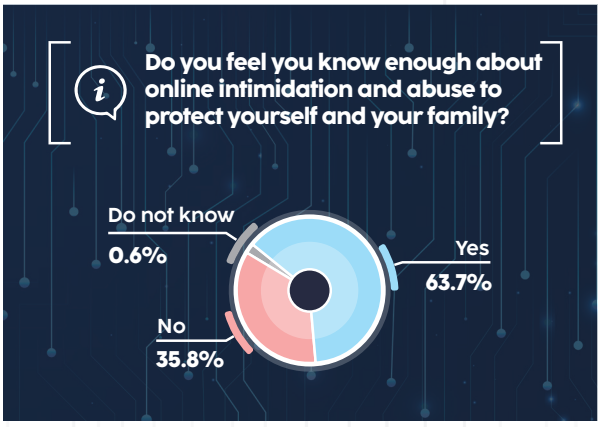


Almost two-thirds refused to answer the questions about intimidation/abuse. A relatively smaller part (18,2%) of that subsample has witnessed the online promotion of hatred, discrimination, or violence against people of a certain race, while 95.3% think authorities / police should do more to protect minors online. According to 91% of respondents, they have never been the victim of internet harassment.

41.9% feel very concerned about the online abuse in the country. Although 63.7% believe they know enough about online harassment and abuse to protect themselves and their family, the figure indicates that there is still an opportunity for further awareness and preventative action.

41.9% of respondents said that there are many cases of online threats, violence-insults/violence in the country, and 24.4% reported that they were mostly concerned. 9.8% of survey participants said that such cases do not matter to them.

In order to protect themselves and their family, 63.7% of respondents indicated they have sufficient information about internet threats and violence-harassment/abuse, while 35.8% did not have any information. It should be highlighted that this figure also indicates the potential for enhanced awareness and preventive actions.



Younger individuals are more likely to feel educated enough to protect themselves and their family against online abuse and intimidation. Residents from urban areas were more likely to have sufficient knowledge to protect themselves and their families. The higher the educational level, the more likely people are to have sufficient knowledge in this regard.

Focus groups provided unique insights into the issue of online abuse. That is, both NGO representatives and GPGs showed one commonality – those actively engaged in a political discussion or debate had been abused at some point due to their opinions.

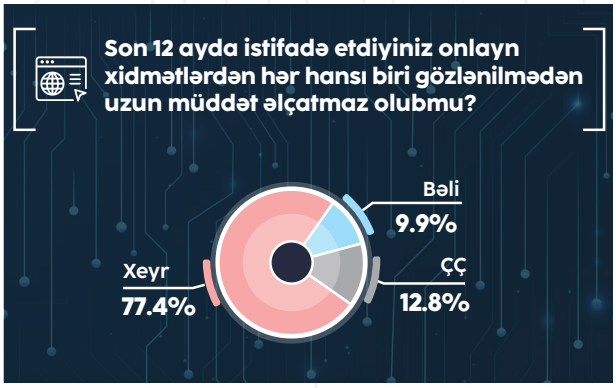
"I was the target of a smear campaign for a week because of one particular activity I was involved in. Then it stopped when I revealed them publicly" (IT professionals & NGO group)

5.4.2.5. Interference (services made unavailable)

77.4% of respondents have seen at least one of the online services that they rely on been unexpectedly unreachable for a prolonged time,

while 9.9% said they had. It was difficult for 12.8% of respondents to reply to this question.

Focus groups provided unique insights into this issue, in the sense that it became apparent that online banking systems tend to go down very often, even though it is not necessarily due to external attacks.



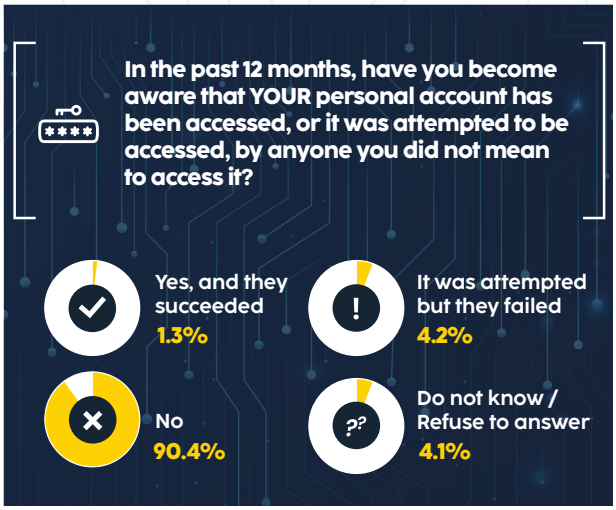
5.4.2.6. Data breaches and online identity theft

The majority have not become aware that login credentials to a personal account of them have been exposed online in the past 12 months.

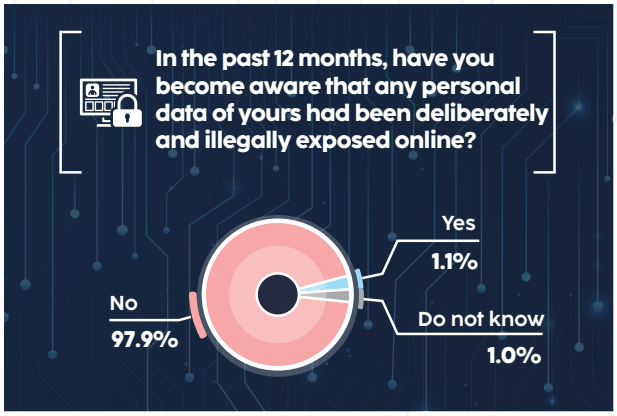
In the previous 12 months, 9.6% of people were unaware that their personal account had been accessed, or attempted to be accessed, by someone they did not intend to access.

In the past year, 97.9% have not experienced any personal data of them been deliberately and illegally exposed online.

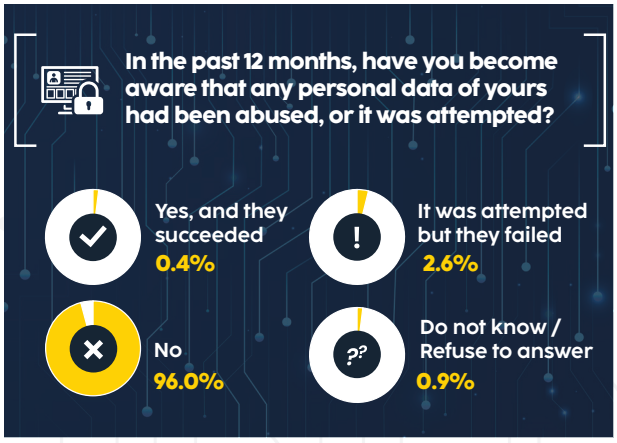
According to the survey results, the majority of respondents (90.4%) did not experience cases of someone accessing or attempting to access their personal account in the previous 12 months. However, 4.2% of respondents believe it was attempted but failed.



97.9% of respondents reported that their personal information was not intentionally or illegally captured or distributed over the Internet in the last 12 months. Only 1.1% of those respondents stated they had experienced such incidents.



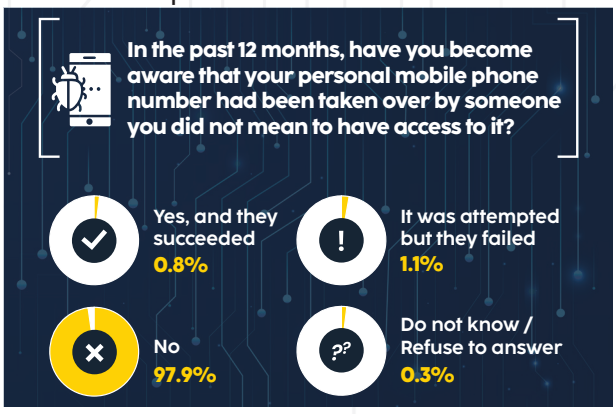
In the past 12 months, 96% have not experienced any personal data of them been abused/attempted. Whereas, 2.6% of respondents indicated that there was failed attempts.



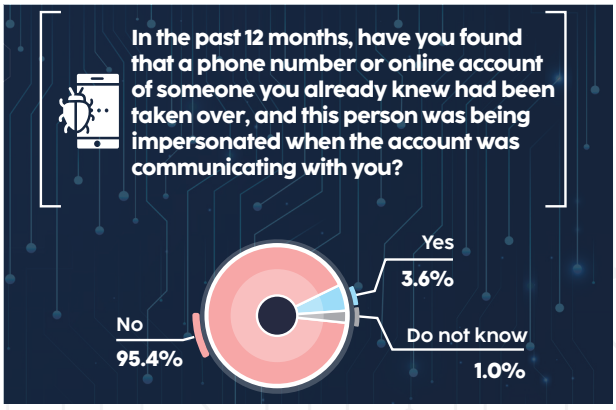
89.4% of respondents had not witnessed their bank, online payment or credit card information being shared online. 9.8% of respondents found it difficult to answer this question.

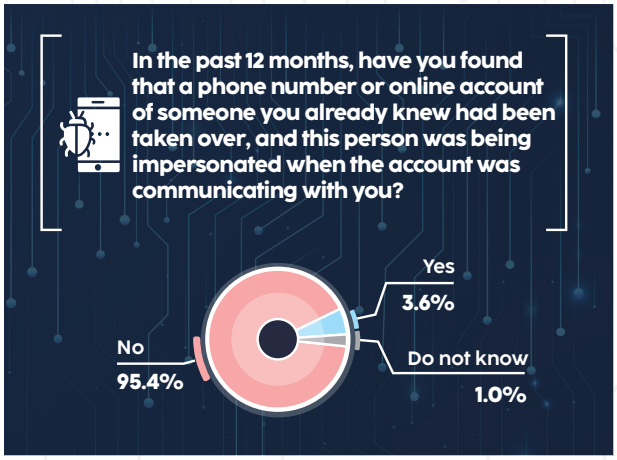
Almost no one have seen their personal mobile phone number taken over by a stranger.

The majority of respondents did not experience the acquisition of their personal mobile phone number by an unknown individual. Only 1.1% of respondents claimed about failed attempt.



Impersonators have contacted 3.6% of people using their phone number or online account. However, 95.4% of the respondents reported that they have not encountered such cases.



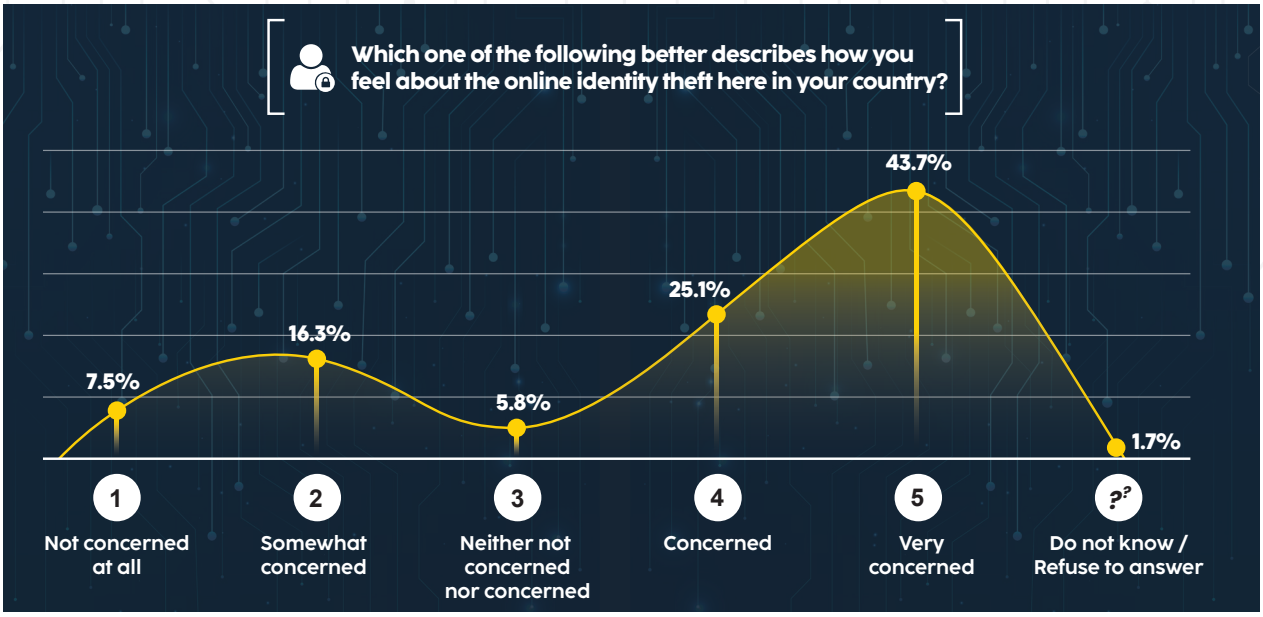


63.9% think if someone in their neighbourhood would fall to victim to online identity theft, they would report it to the authorities / police.

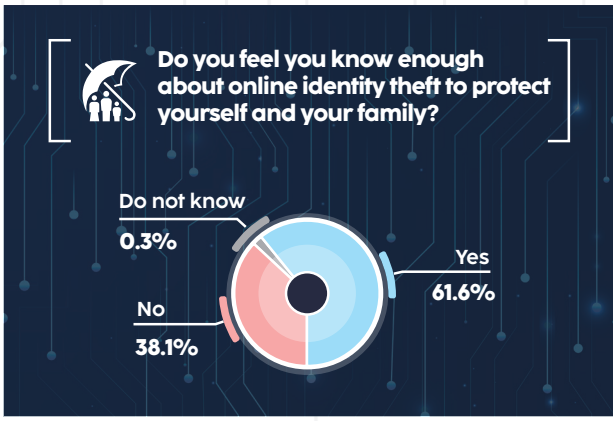
Due to very limited prevalence, nearly 90% has not been impacted by online identity theft.

Approximately 16.8% of survey participants believe they will provide information only in exceptional cases. 9.7% of respondents have stated that they will not report it. The difficulty in answering this question was reported by 9.6%.

According to the findings, 43.7% of the sample is very concerned about online identity/ identity theft in the country, while 25.1% is moderately concerned. 7.5% of respondents felt it was unimportant to them.



While 61.6% feel they know enough about to protect themselves and their family from online identity theft, only 38.1% did not know enough.



Identity theft was widely discussed among focus groups (4 respondent had suffered from bank card theft and 3 from social media account hacking). Some of the victims' stories are useful in shedding light as to how they were victimized:

"I lost $500 when a foreign company whom I made a payment to failed to protect its system effectively. The hacker apparently had attacked system of that company and obtained all customers' details. Despite my efforts, no one restored the money. I also had an intimidating call. Ringer knew exactly how much I had in my bank account. So, I immediately blocked it." (GPG) (NOTE: this respondent did not file a police report due to lack of trust)

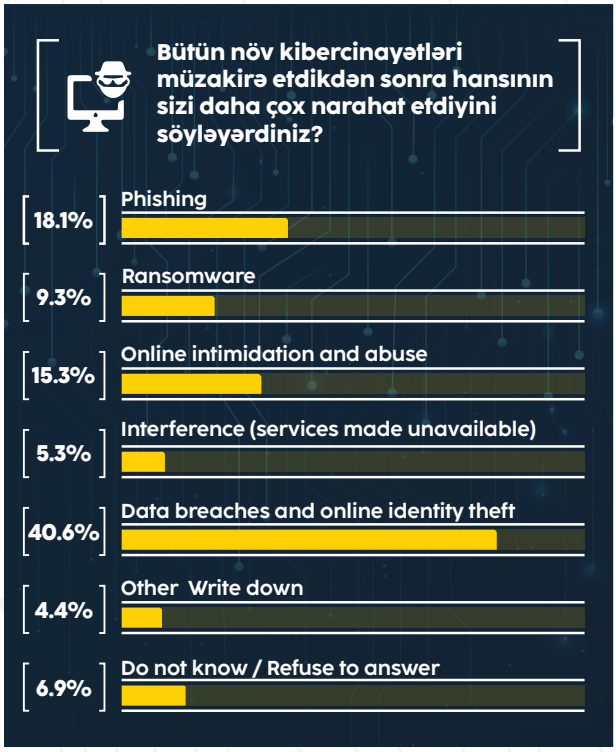
"I once deposited $1 into my child's card so he can make online purchases for himself. But it was quickly gone [about a month later]. Then, later some time, I deposited $20-30, but the same happened again. In total, as a family, we have lost $100 before we deleted the account and set up a new one." (GPG)

"My brother lost 200 AZN, I mean, it was stolen. He used that card to make $2-3 online payment. About a month later, 200 AZN was stolen. He did not report it to the police due to lack of trust. You know why we do not trust [she presumably feared to criticize the police in front of everyone]" (Female, victims' group)

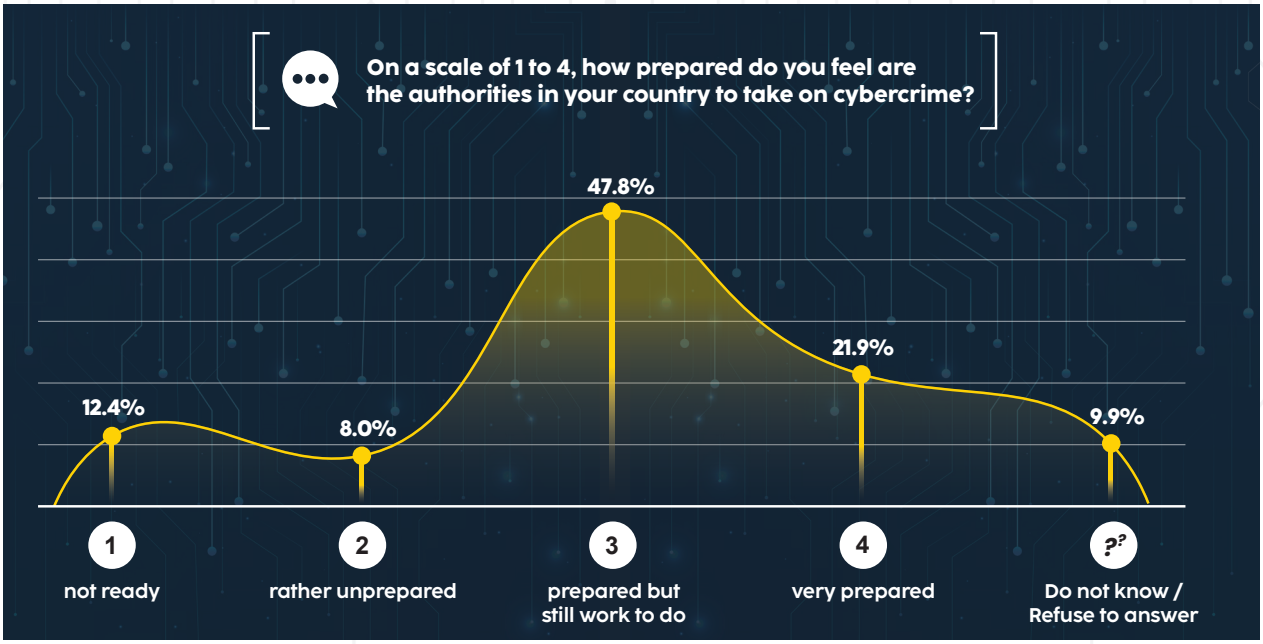
"My son's gaming account was stolen. He cried a lot, so it affected all of us. You know, he had those points, bonuses, things like that in his account. He lost it all" (Female, victims' group)

5.4.2.7. Cybercrime – concerns and expectations

While data breaches and online identity theft are the most concerning offenses for 40.6%, it is interesting to note that only a very small percentage have actually suffered from them. A similar point applies to phishing as well.



47.8% feel that the national authorities are prepared but still have some work to do in order to take on cybercrime. Even so, 12.4% of respondents believe they are not prepared at all.



The sample was almost equally divided as to their expectations about the future of the scale of cybercrime. Urban dwellers, active internet users, and women were more likely to think of an increase in cybercrime. It is rather intriguing, given that World Economic Forum's (WEF) experts have called 2021 the year of the cyberpandemic: "We are in the middle of a "cyber pandemic". COVID-19 accelerated a transition towards remote working and the software being used for these attacks has become easier to execute, ransomware attacks have risen rapidly and continue".

Focus groups were very useful on this issue due to the comments they have generated. Without exception, all groups agreed that cybercrime would worsen in the future, due to the increased use of electronic services (e-gov and e-commerce), as well as digitization of previously paper-based data.

"These days everything is digitized, and we are on the cusp of the digital revolution, thus, it is all too clear that this problem will become more widespread. State authorities now pay more attention than ever in preparing the cadres to combat cybercrimes…In fact, we may see decline in the crimes resulting in physical harm due to increase in online thefts." (GPG)

"At the time when all of our data are in digital form, we have no power to protect ourselves" (GPG)

"Smart devices, 5G, greater use of fiber optics, virtual reality – we do not know what they will bring [when he said that his face expression turned sceptical] ((IT professionals & NGO group)

"The more we use smartphone and computer, the level of danger will rise accordingly. In this case there is neither insurer nor the insured. Everyone's suspicion towards each other increasingly grow day by day. Everyone can be a threat." (IT professionals & NGO group)

While the victimization rate for many of the cybercrimes listed was fairly low, 36.6% of individuals viewed cybercrime as the most concerning offense, indicating that a sizable portion of people feel rather concerned about this offense category in general.

5.4.3. Conclusions

- According to the quantitative data, not all types of cybercrime have gained traction in Azerbaijan, and even those with a higher prevalence (phishing and data breaches, online identity attempts for ordinary citizens, and ransomware/DDoS attempts for organizations) have a relatively low "success" rate.

- The fact that data breaches and online identity theft are the most concerning crimes for the greater part of the sample may be a cause of concern, but the very low victimization rate for these types of crime might suggest a good level of awareness and protection.

- The fact that more than one-third of the population perceives cybercrime as the most worrying offense indicates understanding of the potential of this crime category.

- One rather interesting point that warrants further investigation is that a considerable division has emerged with regards to expectations about the future of the scale of cybercrime.

- In terms of protection, the data suggests a somewhat positive picture, but nonetheless, a considerable portion of the sample feel not sufficiently equipped to protect themselves, which may indicate a need for awareness programs such as the ones organized by CERT.

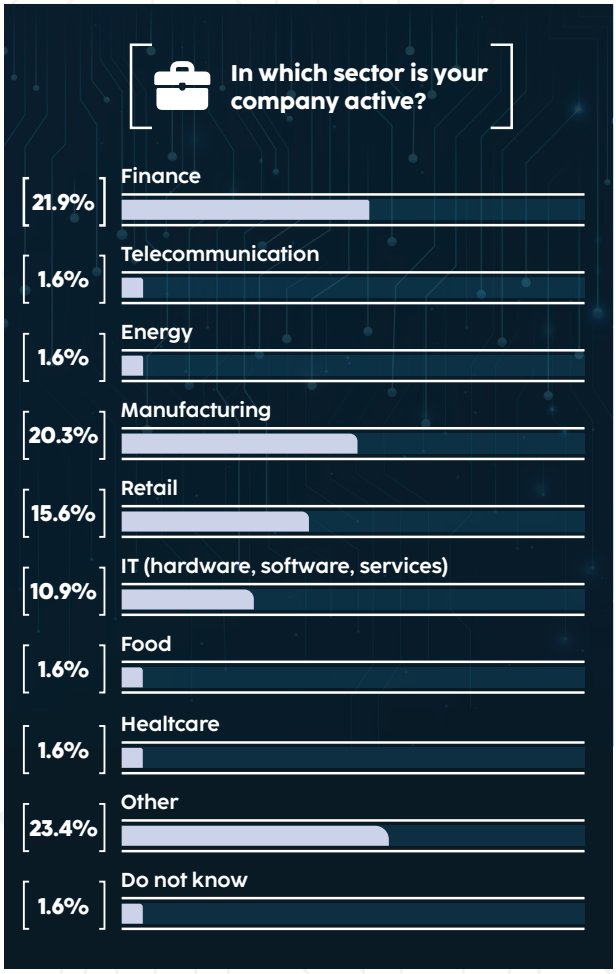
- The data suggests that, assuming the respondents are accurate in their responses, many cybercrimes would go unnoticed in their neighbourhood.

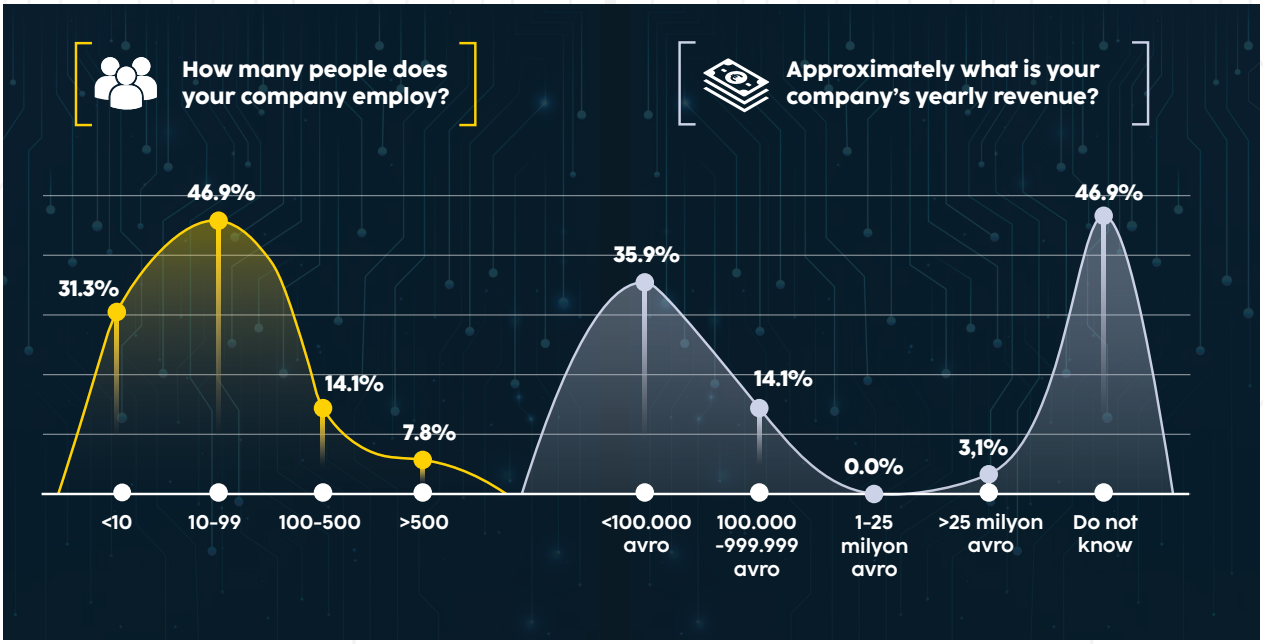
5.5. ENTERPRISES

5.5.1. Organisational Information

Relatively more companies in the sample represent the financial, manufacturing, and trade sectors. Thus, the data must be interpreted in light of this limitation. In terms of geographical representation, the capital city of Baku and the peninsula it is located on make up a significant proportion (81,8%). Similarly, the predominant part of the sample comes from cities, which is understandable since it is mostly companies in urban regions that heavily rely on the internet for business. Several economic regions are not represented at all.

Based on the results, it is clear that 21.9% of the surveyed enterprises (institutions/companies) are in finance, 20.3% are in production, 15.6% are in retail, 10.9% are in IT (hardware, software, and services), 1.6% are in healthcare, telecommunications, energy, and food, and 23.4% are in other sectors.

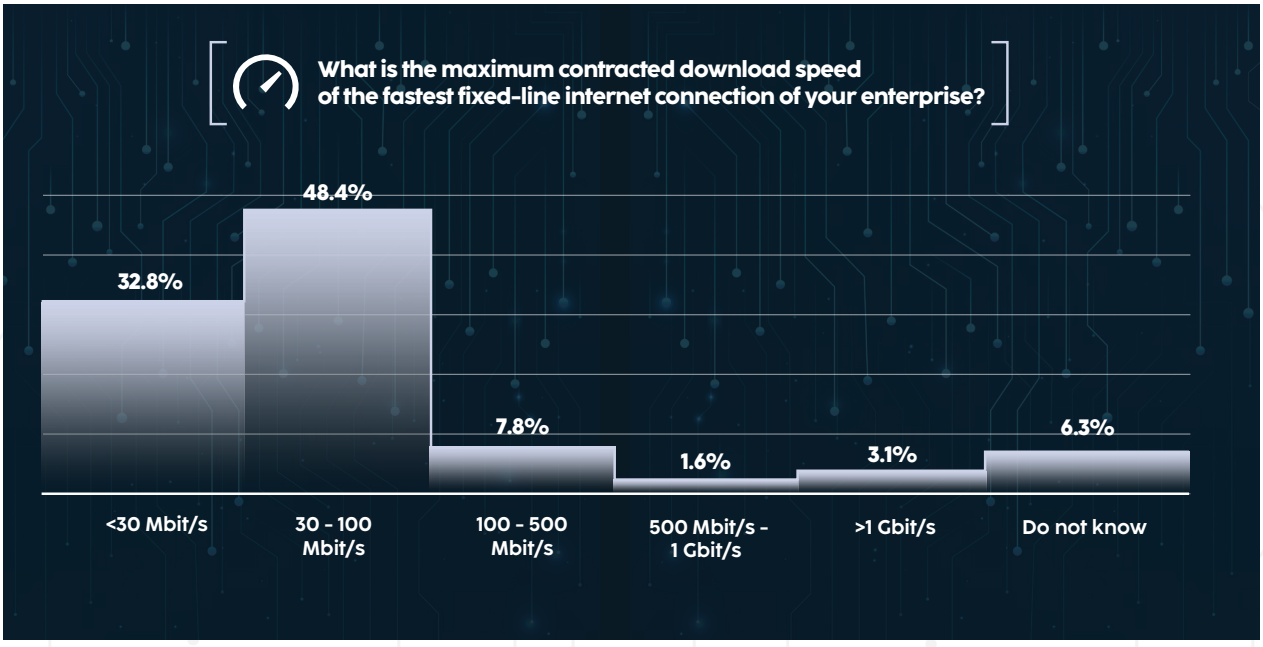




The majority of the companies in the sample have less than 100 employees, while only 7.8% have over 500 employees. A third of the companies' annual revenue is less than €100,000. A similar number of respondents either did not know (for example, because they worked in IT) or intentionally did not disclose the figure.

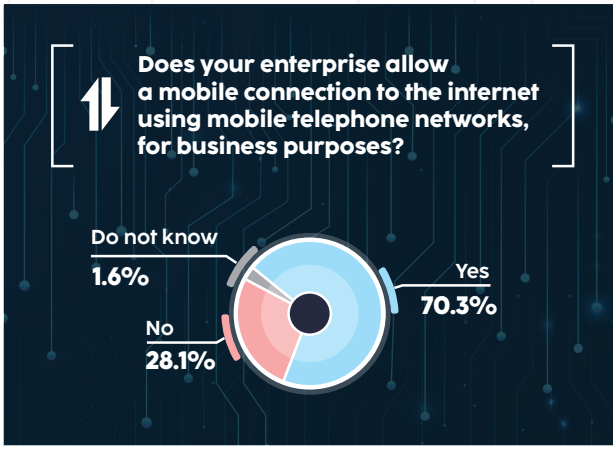
5.5.2 Use of Internet

All companies have some type of fixed line connection to the internet. The maximum contracted download speed of the fastest fixed-line internet connection is generally slower than 100 MB/S.

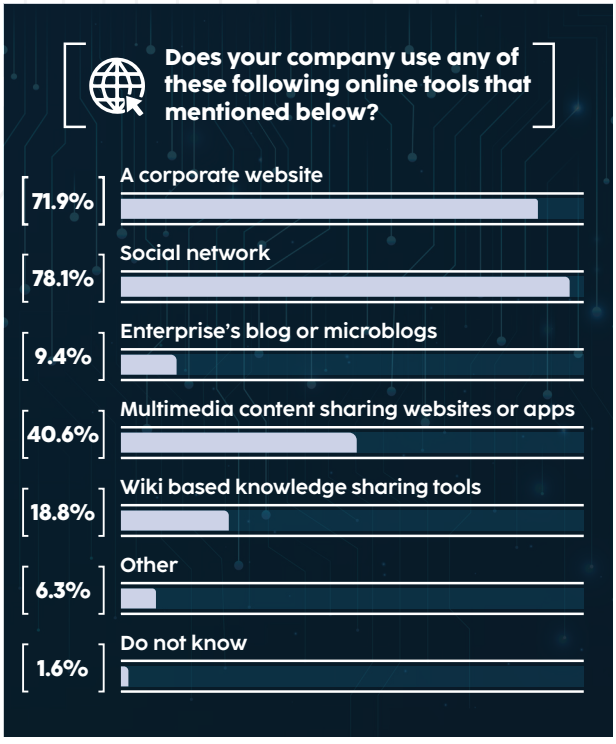


A considerable number of enterprises (70,3%) allow a mobile connection among their employees to the internet using mobile telephone networks for business purposes, which may be a source of concern due to increased vulnerability to cybercrime via employees' devices. In fact, a considerable proportion of companies allow employees to use their personal devices for business purposes all the time.

According to the study results, 28.1% of businesses (institutions) do not allow their workers to connect to the Internet for work reasons using mobile phone networks.



The majority of organizations and enterprises (71.9%) have a website or social media profiles (78.1%). In this regard, among the replies to the related question, blogs or microblogs are the least prevalent tool/platform (9.4%).



Most of enterprises have at least either a website or a social media account, while a blog/microblog is the least prevalent medium of the ones researched.

5.5.3. Knowledge, awareness, and attitudes towards cybersecurity

5.5.3.1. Cybersecurity role

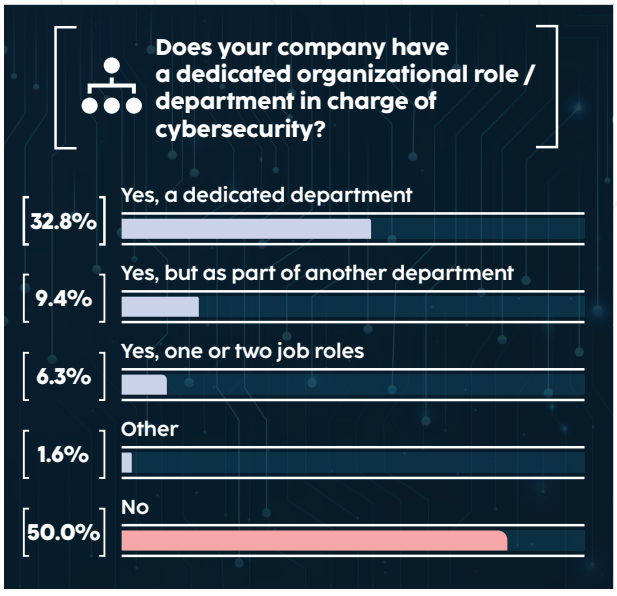
It is concerning that a significant number of enterprises and organizations (50.0%) do not have a specialized department or division for cybersecurity. While financial concerns are significant, it is essential to highlight that not all organizations handle sensitive/confidential information that (according to respondents) would "attract" the attention of cybercriminals.

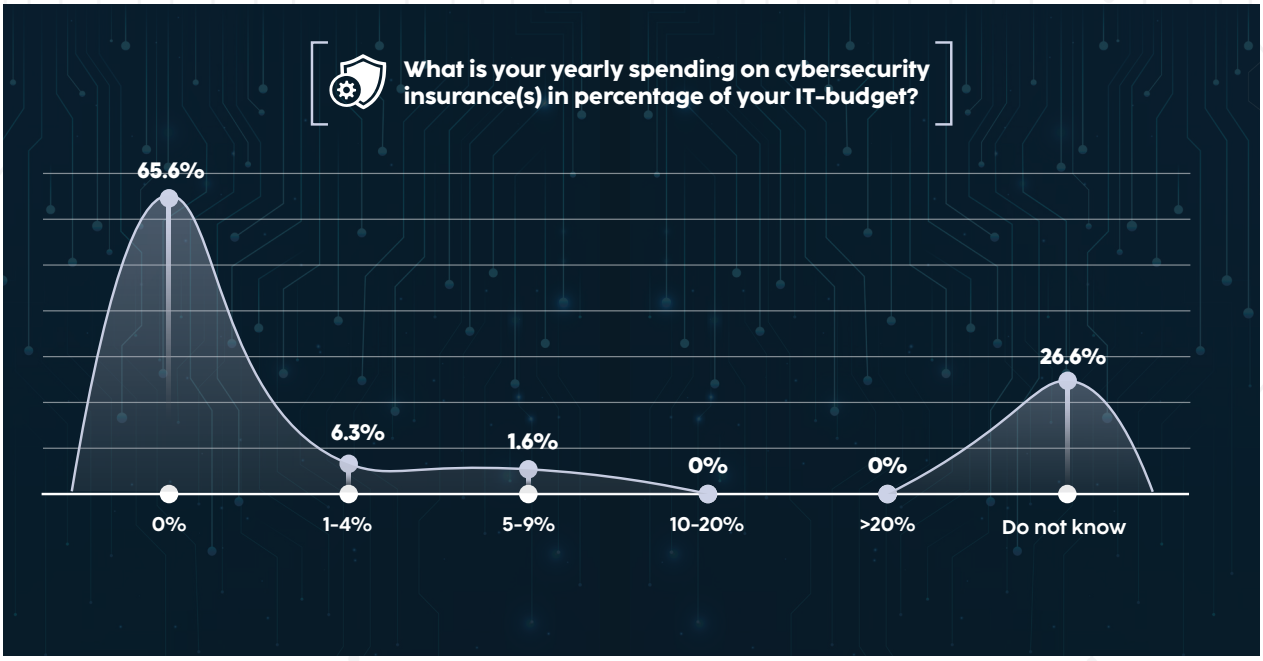
It is a rather concerning fact that a significant number of enterprises do not have a dedicated role or department in charge of cybersecurity.

32.8% of respondents noted that the organization (enterprise) they represent has a special department responsible for cybersecurity, 9.4% reported that a division of another department is working.

6.3% noted that one or two employees are engaged in this work separately.

While financial issues may play a role in this, one should also keep in mind that not all enterprises (in their opinion) deal with sensitive data that would "attract" the attention of cybercriminals. In the financial sector, 64% of organizations have a specialized job or department in responsibility of cybersecurity, whereas in manufacturing and information technology, the statistics are 23.1% and 57.2%, respectively. The size of the company is important as well; the larger the organization, the more likely it is to have cybersecurity professionals. For instance, only 20% of the enterprises with fewer than 10 employees responded positively to this question, while the figure for those with a workforce of 100-500 and 500+ is almost 100%.



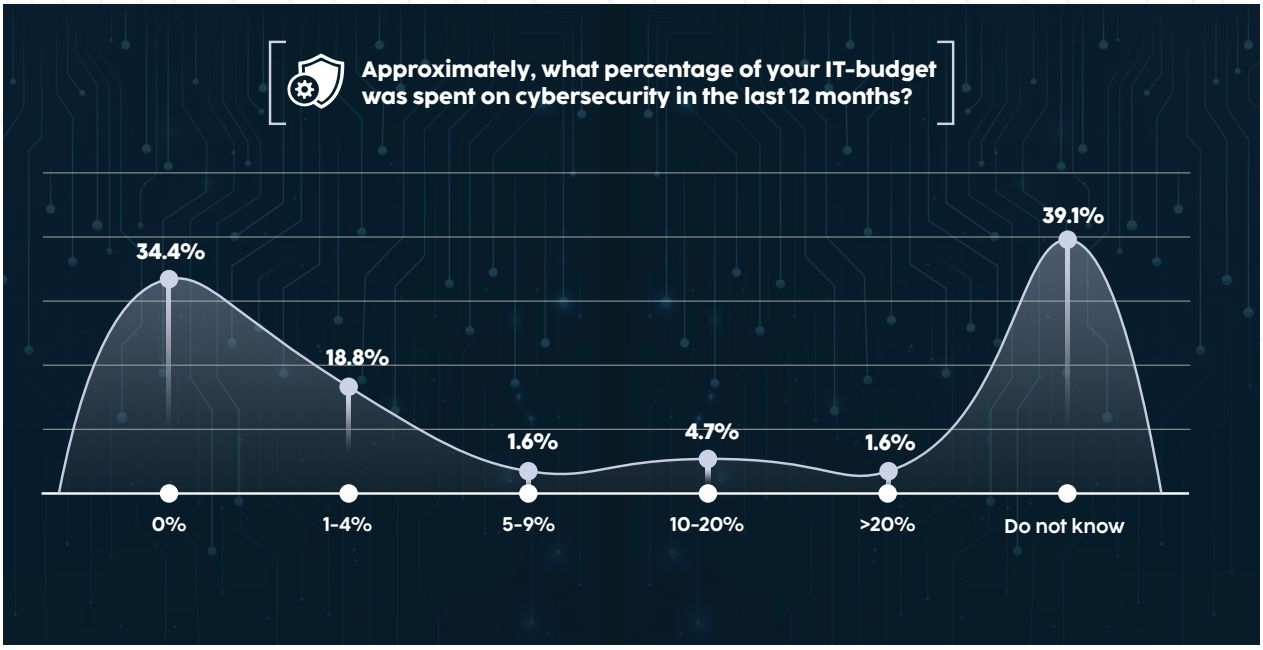


When respondents were asked to state cybersecurity insurance' expenditure weight within IT budget, it became apparent that most of the enterprises (65.6%) do not have insurance.

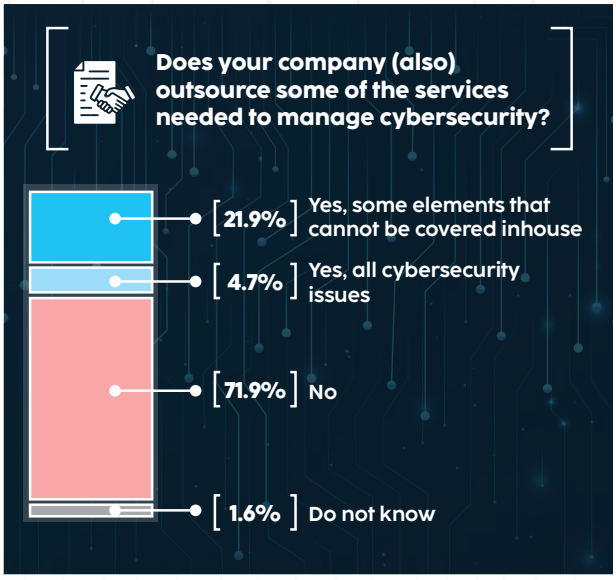
In fact, since the remaining respondents were unaware of it, despite being in IT department, one may conclude that cybersecurity insurance is extremely limited in Azerbaijan, which has implications for the insurance sector (i.e. a market to penetrate in the future).

26.6 % of businesses outsource part or all of the services required to manage cybersecurity.

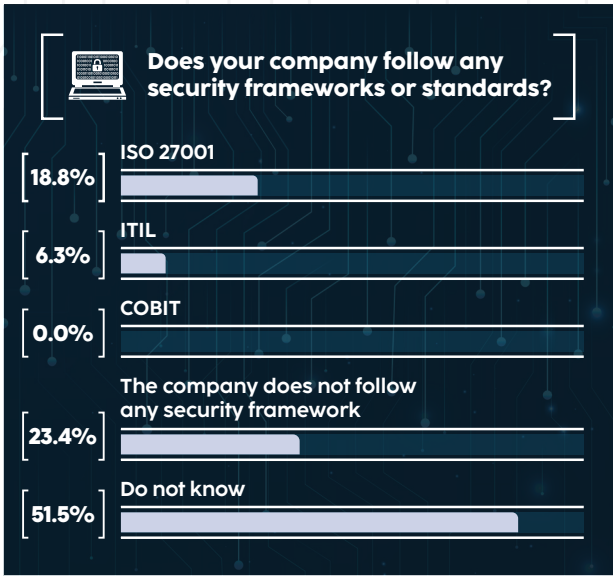
The weight of expenditure on cybersecurity within their IT budget is generally low, while an important proportion of the respondents (39,1%) either did not know (e.g. due to being from IT department) or intentionally, or not disclose the figure. 21.4% of the companies in the financial sector spent 1-4% of the IT budget, while the rates for retail and manufacturing were slightly higher (one has to keep in mind the important difference in the number of companies representing sectors).



71.9% of survey respondents do not rely on any external organization for some of the services required to manage the cybersecurity of the enterprise (organization) they represent. According to 21.9% of respondents, some components that are not entirely provided internally by the organization they represent are entrusted to other organizations for this purpose. Also, 4.7% of respondents claimed their organization employs the services of other organizations to manage all cybersecurity risks.



ISO 27001 is the most prevalent safety framework followed in the sample (18.8%), but one has to bear in mind that a noticeable number of people (51.5%) were unaware or unsure of the framework in place. It is also important to note that ISO 27001 is a regulatory mandate in certain sectors (i.e., banking sector). The enterprise (organization) they represent, according to 23.4% of respondents, does not use any security framework.

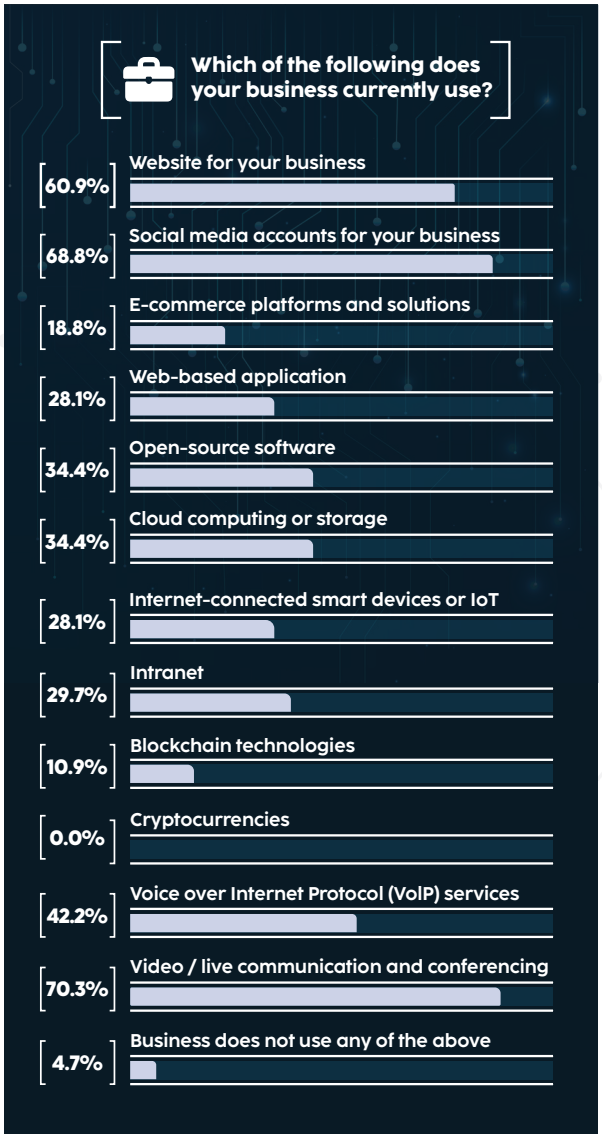


The ISO 27001 standard is mainly applied by companies operating in the capital Baku and having 100-500 employees.

When asked about technologies used in enterprises and organizations, video conferencing/meetings (70.3%), social media accounts (68.8%) and websites (60.9%), cloud computing (34, 4%).

When asked about technologies in use at the company, open source program, cloud computing, VoIP and online video conferencing/meeting came up relatively more frequently.

Cloud computing users store more commercially sensitive data (18,8%), workforce data (15,6%), and non-sensitive data (20,3%) than other categories of data.

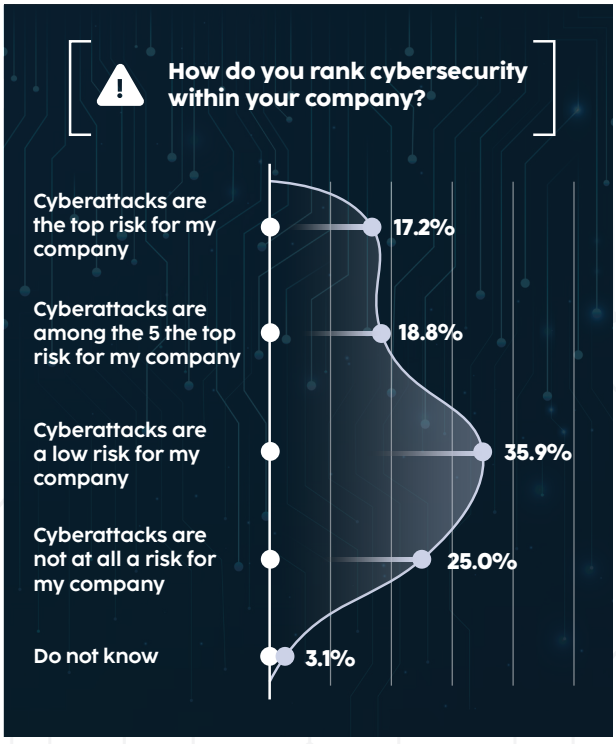


5.5.3.2. General Priority and Confidence

More companies rank cybersecurity within their organisations either low or non-existing. More than 80% of the enterprises with a workforce of 100-500 and 500+ rank cybersecurity as either the biggest or among the top 5 biggest risks, while the figure for smaller companies is more than threefold lower. 64% of financial sector enterprises rank cybersecurity either the biggest or among the top 5 biggest risks.

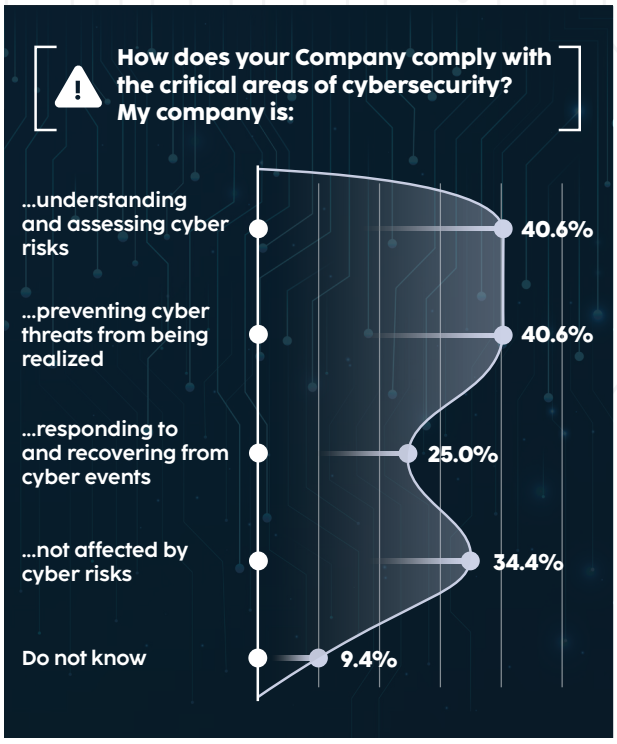
According to 35.9% of respondents, cyberattacks are a low risk for the institution (enterprise) they represent, 18.8% consider it to be one of the five most significant threats, and 17.2% believe it is the most serious risk.

25% of survey respondents believe that cyberattacks pose no risk to the organization (enterprise) they represent. The difficulty in answering this question was reported by 3.1% respondents.

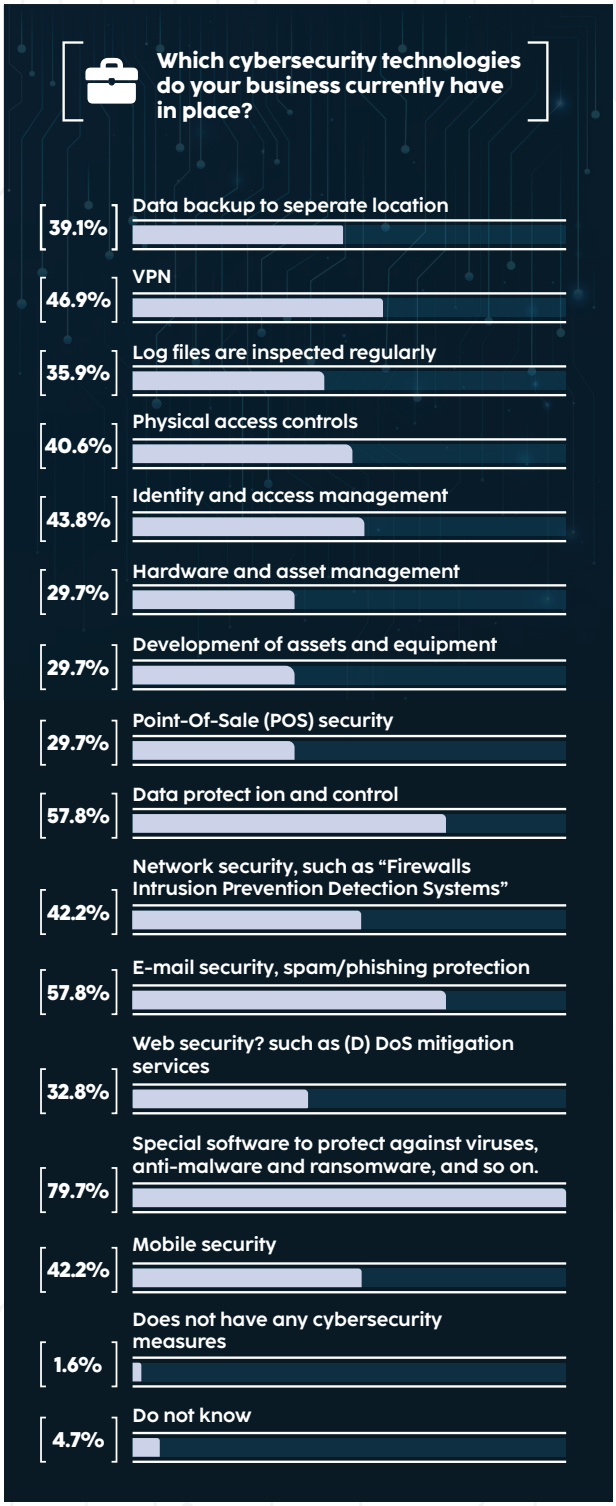


When questioned about the essential areas of cybersecurity for organizations (institutions), the perception and evaluation of cyber risks, as well as the prevention of their implementation, are all at the same level (40.6%).

According to the answers, the use of anti-malware solutions (programs) for protection



against viruses, spyware and other types prevails among the cybersecurity technologies available in the organizations (79.7%). In this respect, data protection and control measures (57.8%), e-mail security, anti-spam/phishing (57.8%), VPN (46.9%), mobile security (42.2%), separately for backup transferring a copy of data to the database (39.1%), regular checking of log files (35.9%) and others comes after them.



When asked about what the critical areas of cybersecurity are for them, understanding and assessing cyber risk and preventing cyber threats from being realized came up almost the same number of times.

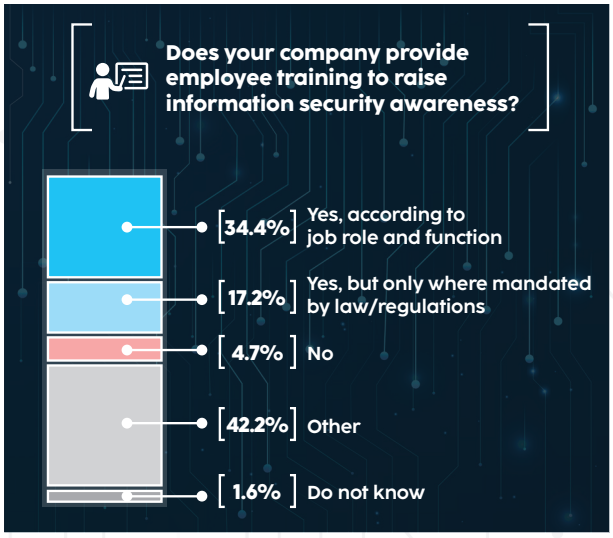
Among cybersecurity technologies currently in place, anti-malware software to protect against viruses, spyware and others was noted by the majority, while spam/phishing filtering and data protection and control came next.

5.5.3.3. Awareness Raising

Enterprises and organizations provide several levels of training to workers (based on position and function) in order to raise information security awareness.

According to 34.4% of respondents, the organization (enterprise) they represent organizes training for this purpose based on roles and functions.

Due to 17.2% of survey respondents, trainings are held in specific locations in accordance with the guidelines. Although just 4.7% of respondents said no training was provided for this purpose, 42.2% gave other explanations.



Around half of the companies provide employee training (according to job role and function) to raise information security awareness. Training is provided by all enterprises with a workforce of 100-500 and 500+ people, while only over half of companies with 10-99 employees do so. In sectoral terms, it is very intriguing that a third of the financial sector companies do not conduct training. One explanation for that level of training may be attributed to the sampling approach adopted (non-random sampling

was used). Another reason may be due to the perception among those enterprises that their activities are not risky enough to require training. It may also be partly due to lower prevalence of cybercrime in Azerbaijan compared to more developed economies where more enterprises rely on the internet, though this point is based on personal observations.

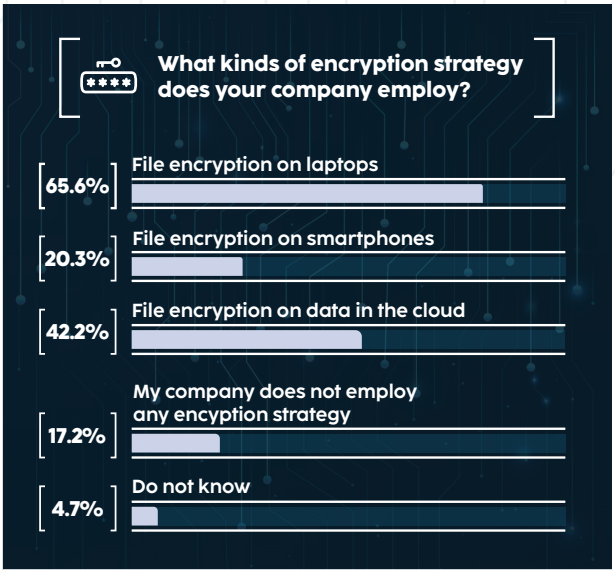
Greater budgets and the use of advanced security technologies, according to 45,3% and 46,9% of respondents, respectively, can boost organization's security standards. It's worth noting that the least popular option was "increased security department staff numbers"(25%). When asked about major challenges or barriers to effective cyber risk management, the most common responses were a lack of resources and cyber risk not being a top priority.

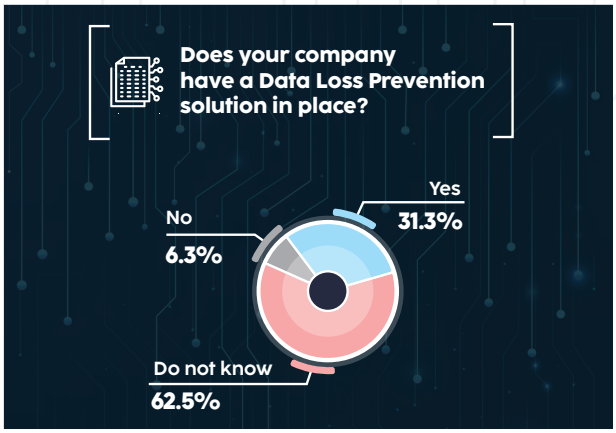
5.5.3.4. Authentication and Encryption

The results of the study prove that 65.6% of enterprises implement file encryption on laptops within the organization. File encryption on the Cloud (42.2%) was followed by file encryption on smartphones (20.3%). Due to reports from 17.2% of the organizations (enterprises) participating in the survey, they do not use an encryption strategy.

File encryption on laptops is used by 65,6% of enterprises.

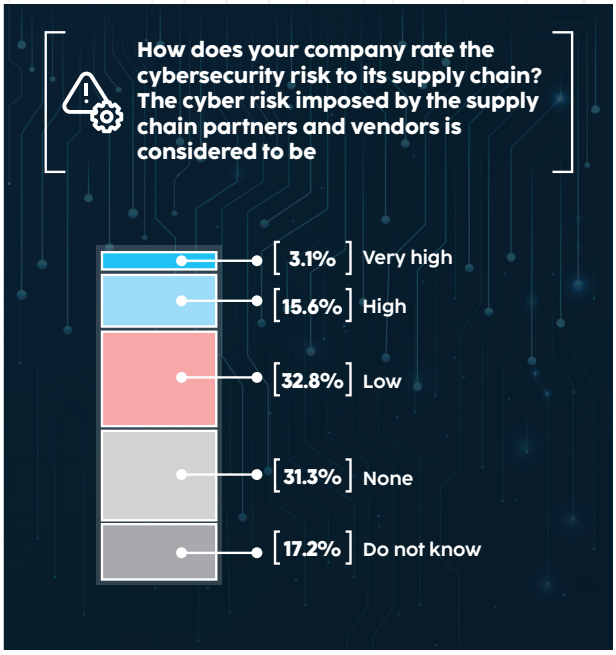
While Data Loss Prevention solution is not that prevalent (62,5% not having it), two-factor authentication is used slightly more (42,2% having it). The larger the company is, greater the likelihood of having Data Loss Prevention solution becomes. The absence of this solution in 43% of financial sector organizations is an intriguing finding.





5.5.3.5. Supply Chain

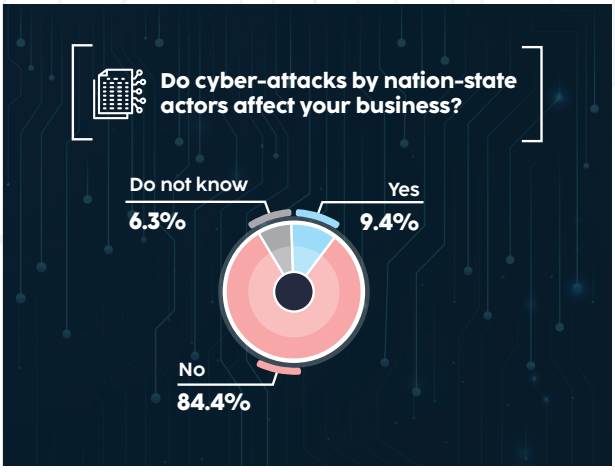
Overall, the cybersecurity risk to the supply chain is rated rather low among the sample. Addressing information security issues in a contract and signing confidentiality and/or non-disclosure agreements are the most used protection methods/tactics in this regard.



5.5.3.6. Government role

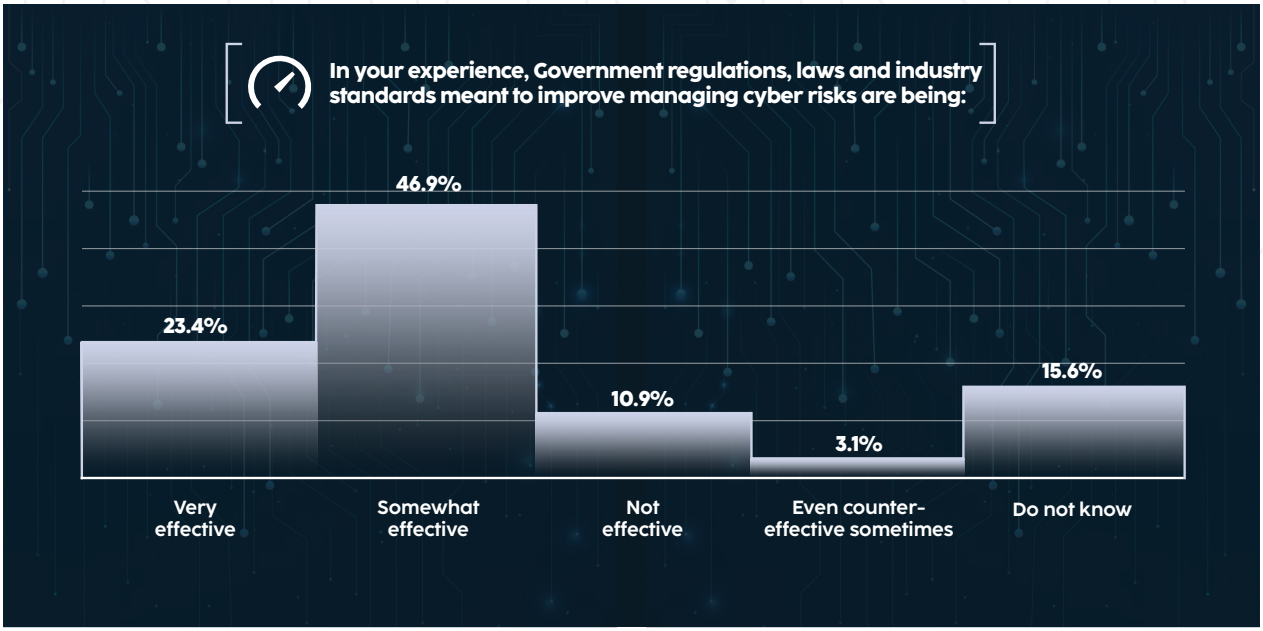
Cyberattacks by nation-state actors have affected a very small proportion of the sample.

According to the survey findings, cyberattacks by nation-state actors harmed a very small portion of the sample (9.4%).



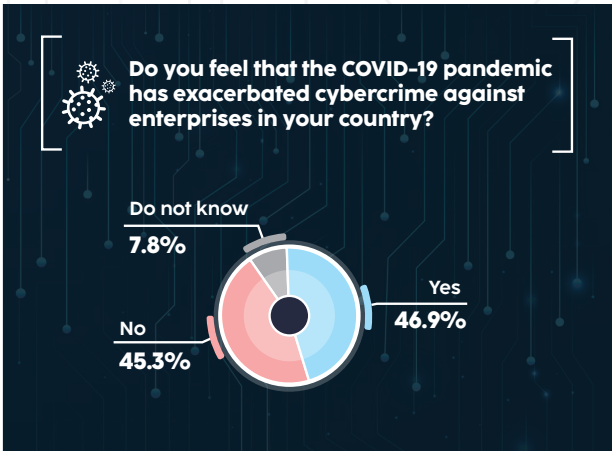
Respondents' attitudes about government-promoted policies, laws, and industry standards aimed at improving cyber risk management are generally favourable. Due to the reports, 23.4% of respondents believe it is extremely successful, while 46.9% believe it is somewhat effective. Also, 10.9% of respondents took the opposite position.

In general, there is a rather positive attitude towards government regulations, laws and industry standards aimed to improve managing cyber risks.

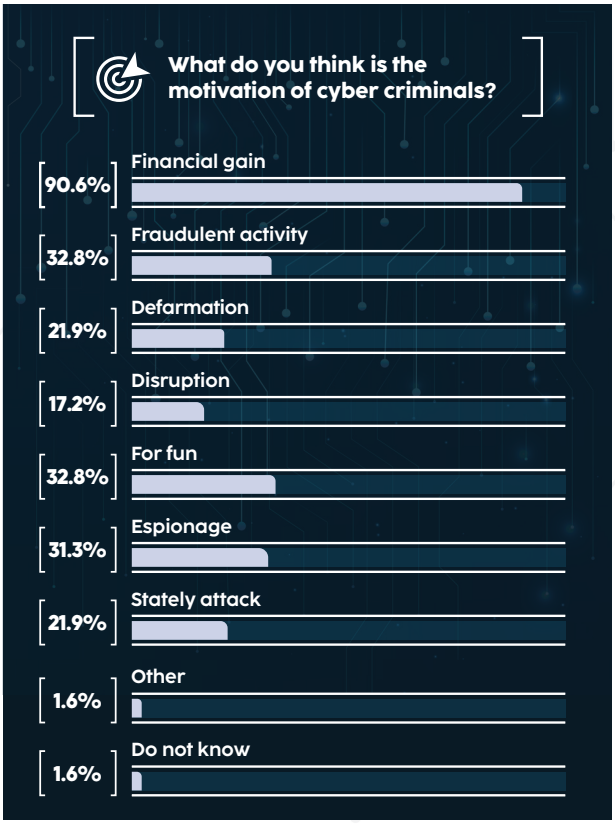


5.5.3.7. Cybercrime state of affairs

Remarkably, the responses with regards to whether the COVID-19 pandemic has exacerbated cybercrime against enterprises are almost equally divided between “yes” and “no” (46.9% and 45.3% respectively). While 64.3% of the enterprises in the financial sector have observed an increase, the figure among manufacturing entities is 30.8%.

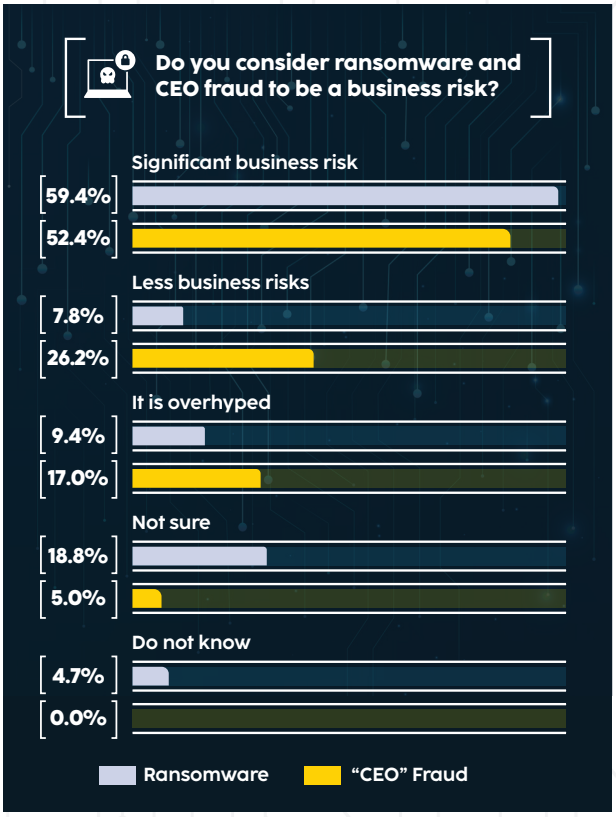


The term "financial gain" (90,6%) stands up as the most startling response as a motivation to commit cybercrime.



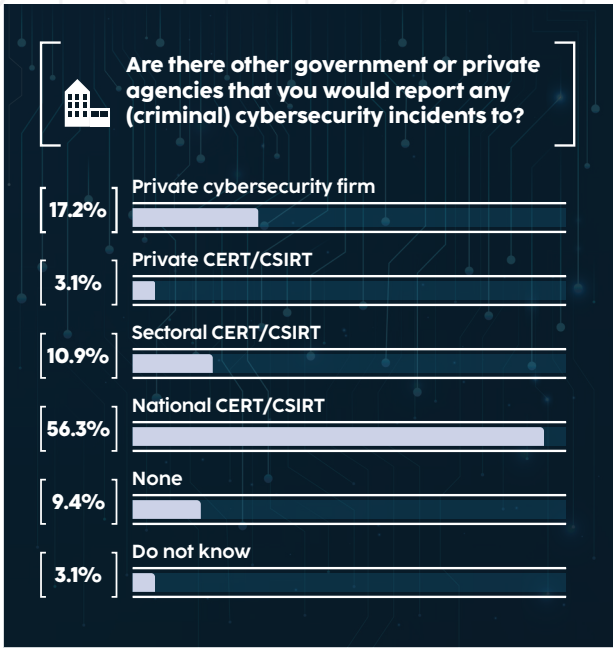
Fraud (fraudulent) activities (32.8%), entertainment (32.8%), espionage (31.3%), large-scale attack (21.9%), defamation (slander) (21, 9%), and system disruption (17.2%) are among the most common.

According to the responses to a number of questions about cybercrime victimization, enterprises have a very low rate of victimization. Nonetheless, there was a general agreement regarding the high-risk levels of ransomware (59,4%) and CEO-fraud (52,4%).



In the event of a potential or successful attack, relatively more organizations (57.8%) would contact law enforcement for assistance and/or to investigate or stop the source of the attack.

The most frequently chosen law enforcement organisation was the National CERT(56.3%).Similar to focus groups' results, a greater proportion of the sample expects the cybercrime scale to increase in the future.



5.5.4. Conclusions

The responses to several questions on cybercrime victimization indicate a very low rate of victimization among enterprises. To some extent, this is unexpected considering the widespread prevalence of various cybercrimes, such as phishing and bank card theft, among individuals. However, during survey interactions, some respondents informed us about many failed attempts by cybercriminals, which points to the effectiveness of the defence systems in place. In fact, no company reported they had lost any money due to cybercrime in the last 12 months.

It is a rather concerning fact that a significant number of enterprises do not have a dedicated role or department in charge of cybersecurity. While financial concerns may play a role, it is also important to remember that not all businesses (in their perception) deal with sensitive data that would "attract" the attention of cybercriminals. Furthermore, it is a widespread practice in Azerbaijan to not have anyone or anything responsible for cybercrime or security, especially among small and medium enterprises.

A similar picture emerged when respondents were asked to state the cybersecurity insurance's expenditure weight within their IT budget, as most enterprises do not have such insurance, which has implications for the insurance sector (i.e., a market to penetrate in the future). Overall, one thing is clear from our data: expenditure on cybersecurity tends to comprise a very small proportion of the IT budget among the companies covered.

One of the noteworthy discoveries is about victimization and staff training. Not all enterprises conduct training on cybersecurity.

While the fact that cyberattacks by nation-state actors have affected a very small proportion of the sample may be a cause for celebration, several respondents highlighted the severity and intensity of cyberattacks during the war with Armenia in 2020. As a result, it would be too premature to conclude that Azerbaijani companies are not vulnerable to foreign state-sponsored attacks.

On the question of contacting law enforcement for assistance, every company would report to the national CERT/CSIRT, with other options not chosen. Once again, the responses to this question mean that a significant number of attacks have gone unreported.

NOTE: The number of respondents perceiving certain questions too sensitive was not low (28,1%). A partial explanation for this is related to the questions on budget, where many respondents decided to not respond due to confidentiality.

6. QUALITATIVE RESEARCH

6.1. Summary

- Among GPGs, only three offences came up at varying frequencies - online abuse, identity theft and phishing.
- In terms of cybercrime victimization, identity theft stood out both in terms of frequencies and scale of impact. Among GPGs although online abuse was slightly more prevalent (9 cases) than identity theft (4 bank card and 3 social media account theft), the former had no impact on victims. The fact that all participants received phishing calls and emails but only two victims were identified suggests a high level of awareness of and protection from this particular cybercrime.
- All other cybercrimes (i.e. ransomware, exposure of personal details) were extremely limited or even unheard of.
- The majority felt unsafe while online, as well as due to use of smartphones. “Nothing and nowhere is safe” statement was dominant. Regarding safety, one of the most important insights gained from focus groups is came from ISP representatives. Despite all the strict measures taken, they did not feel fully secure because the devices and software used are imported or produced abroad.
- Regarding perception of cybercrime, the phrase of “internet crimes” and “information crimes” were noted frequently as all-encompassing phrase among GPGs, while markedly different responses were recorded particularly among IT professionals and ISP representatives.
- In terms of seriousness of cybercrime in relation to other offences, cybercrime is seen potentially more dangerous. It was felt that cybercrime can impact wider society, while violent crimes and property crimes tend to be on an individual or community level. IT professionals, ISP representatives and some of the law enforcement officials went further, pointing to the possibility of easily hacking someone else’s vehicle or smart home system to cause harm.
- While phishing was mentioned as the most concerning cybercrime among most of the GPG and victims, various responses (DDoS, attack on critical infrastructure areas) were recorded in other groups.
- All respondents had heard of the word cybercrime, as well as most of the crime types mentioned, but phishing and ransomware were almost unheard of. Respondents mostly recognized them once explanation was given.
- Among victims only group, all respondents had been victims of phishing, but interestingly, no one knew what the term of phishing is.
- While one group (18-21) view the police as the agency they would report their future cybercrime victimization to, other GPGs in general, as well as NGO representatives would go to IT expert, though they did not eliminate the possibility of the police. That is, while they had little trust in the police ability to handle their report, they would report to them as the last resort. This and the relevant finding previously mentioned above point to a need for more cooperation between IT sector and the police in clearing up and recording cybercrimes.
- Without any exception, all groups’ dominant view was that cybercrimes will intensify in the future, particularly due to more and more use of electronic services (e-gov and e-commerce), as well as digitization of everything.

6.2. Technical Information – all in charts to provide an overview of the structure of the respondents

See Table 2 and 3

6.3. Research Methodology - as presented in the ToR and all country specifics to be included

Data collection method

To learn the views of participants in their own words, open-ended questions and a flexible discussion environment were necessary, which were made possible by the focus group format. By using such a format, it enabled this study to obtain far more detailed and insightful responses from participants than the traditional survey method. In fact, across all groups, especially among general population, the group environment was very effective in eliciting responses which would have not been gathered otherwise. That is, there were many cases where question initially produced one

or two responses, but once those responses were expressed, others followed immediately.

Participants were assured of their anonymity and confidentiality of their responses. Written informed consent was obtained before starting the interview. All discussions were audio-recorded and attended by an assistant of the moderator.

While 4 discussions (all GPGs, ISP representatives) were conducted face-to-face in a hotel conference room, 3 were organized over Zoom. Due to the geographical spread of victims, Zoom appeared to be a more viable option, while the for other two groups, their work schedule prevented them from leaving their office and visiting our Centre.

Group sizes varied on some occasions due to last-minute dropouts (especially among potential participants who had lower than higher educational attainment) in all GPGs. As a result, quotas for specific groups were not entirely met. Regarding other groups, only such a problem was observed in IT professionals/ NGO representatives group where 3 IT professionals failed to join due to unexpected problem in their company.

Sample

Participants for GPGs were recruited primarily through two channels(using the snowball technique): a) students of universities where the research group teaches and b) personal and professional connections established during the cooperation with other agencies. The survey was used to identify victims. Their mobile numbers were written down during the survey and contacted by Centre's survey team afterwards. An official invitation letter was sent to multiple law enforcement agencies. Professionals in IT sector and NGO representatives were recruited through both official invitation letter and personal connections of the IT/media department of the Social Research Centre.

Due to accessibility and cost considerations, only Baku was chosen. Except for two victims, Zoom participants were all from Baku. As a result, it is important to recognize the geographical limitation of this study, and we urge readers to keep this in mind when interpreting the findings.

Only face-to-face groups' list with signature is available, while others are Zoom screenshots and one WhatsApp group call. Whole list will be compiled once all analysis and etc finished. Please note that in law enforcement group, no one activated their camera due to privacy. These photos/ lists with signature can be provided upon request. For the list of gender and age, please see the respective table.

Challenges

In terms of challenges in the qualitative data collection, Regarding GPG, since most of them were unaware of many offences covered, there were many occasions when group was largely passive. This issue was observed particularly in the group with the youngest age. Among victims, out of 11 invitations, although 6 participants joined, one of them had poor internet connection, due to which he had to leave conversation a bit later. Thus, we acknowledge sample-size related limitation.

Despite the ease of contacting law enforcement agencies, it took a long time to obtain official approval from relevant ministries so that their employees could participate in focus groups. Secondly, since law enforcement is dominated by male workforce, only one female participant was recruited into this group. A similar point can also be made about other groups where no female participant attended. Once again, this can be explained by the larger portion of the workforce being made up of male, of which the reasons are beyond this study to explore. Third, only two enterprises took part.

Overall, we failed to recruit 70 participants due to a) last minute dropouts; b) lack of incentive and c) many victims' unwillingness to participate due to a lack of budget to cover their costs of travel, since not everyone was comfortable with Zoom or other similar applications

While the topic did not cause reluctancy of the citizens, gender breakdown was an issue only among professionals and enterprises.

The lack of IT departments or IT-related activities did shape and impact the process. This was a huge problem in rural areas, so we focused only on Baku. Due to the lack of incentive provided that would suffice them, it was difficult to recruit. Only two enterprises took part and they were contacted personally.

There were cases of refusal to answer some of the questions among state security

services and ISP providers who found them too sensitive and intrusive. Also, the group with the youngest age were unaware of many offences covered, so there were many occasions when group was largely passive

Analysis

"Nvivo" qualitative analysis software was used for this research addition to its potential to facilitate the quick and easy creation of categories and the ease with which it provides in terms of managing large datasets.

Once prepared, all interview transcripts were analysed by the moderator (manager of qualitative research part of the project). Abridged transcription method was used, whereby only relevant parts of the conversation are transcribed. The interview transcripts were analysed through thematic analysis (Braun & Clarke, 2006). Thematic analysis has been conceptualized as a method for identifying, analysing, and reporting patterns and themes within data. In each transcript, keywords were marked and each theme that emerged was given a code, which was eventually "checked" to see whether they appear in other transcripts. The results found individually were then clustered together to discover the main responses to each question.

To exemplify the point of respondents, quotations are used. Each quotation has pseudonyms (in abbreviation) attached to it. To maintain anonymity, only group number (for GPGs) or ID number (for other groups) is shown.

6.4. GENERAL POPULATION

Group observations

Group 1 – mostly dominated by 5-6 members. Several questions produced a very limited answer only. Group was made up of students mostly.

Group 2 – A highly active group. Group was made up of people with mixed professions

Group 3 – A highly active group. Group was made up of people with mixed professions. Only one lady was passive, who was the eldest and had no higher education. She also had a much more limited internet use than others

6.4.1. Online Activities (usage in general)

Respondents differed greatly from each other in terms of the social media platforms they use, and their daily use duration. Journalists and scientists, in particular, reported a very high level of online activities (in excess of 10 hours a day) due to their work requirements. In fact, for them, social media was one of the media through which they do their work (i.e. sharing their research, interviews, etc.). Students, on the other hand, used it almost equally for both education and social media interactions and sharing posts. News reading was cited across all groups, with social media use coming the second.

Many (n=12, 46%) participants expressed concerns about security when being online, and those individuals were constantly fearful of being victimized. The remaining participants did have some concerns too, but due to various reasons (e.g., not providing too much personal data, not visiting certain websites, taking precautionary measures), they did not feel equally fearful. Thus, the general sentiment was somewhat sceptic when it came to sense of security. In other words, almost no respondent felt fully protected.

Among Group 2 and Group 3 there were many statements along the lines of "nothing is safe", "nowhere to hide" and "anything that is posted or available online has dangers" indicating the somewhat powerlessness of respondents in maintaining sufficient protection. While not all respondents discussed where protection could/should come from, there was slightly more people thinking that it is only users themselves who can protect themselves (i.e. by not providing too much private data). In fact, two respondents equated the current cyberspace with Orwellian description of the society. The general sentiment as to where protection could/should come from was that both users and providers (i.e. Facebook) must play their part. Still, however, many respondents would not feel 100% secure at all.

"I have time and again tested and seen how artificial intelligence operates on social media. Whatever I think of and search for start to come up on my screen frequently. So, they read our mind [her face expression and voice tone showed how worrisome she felt when saying that]" Group 3

"Everyone in possession of a smartphone or smart device is vulnerable. They cannot feel safe." Group 3

"The only platforms where I feel safe when using are the ones that do not require account. So, news agencies are prime examples." Group 2

"No social media platform provides a guarantee to security of our data. So, one cannot feel safe there, but it is a human need, one must be present there." Group 1

"One can impose blocks, freeze bank card details in case of threat, and do that and do this to protect himself, but, there are things beyond our control [he nodded his head in despair]." Group 3

"Let me give my answer a bit indirectly. When we set up an account or accept cookies, we give them an access to our data. But we never read them. Our individual data on its own may not matter hugely to them, but once all users' data are collected, then it matters. For me, it is not a big threat, for the reason I just mentioned" Group 2

"An interesting thing is that we may want to limit access technological companies have to our data, but, if we deny it, apps or social media programs simply will not work. Moreover, since I am in the politics as a journalist, I always feel vulnerable to cybercrime every time I go online or download an app" Group 2

"We, as individuals, have given all the access to others, I mean, companies, to gather all data about us". Group 3

"All of our bank and salary cards are on our phone. We make payments through there. We make online purchases through there. So, yes, that makes me feel scared a bit" Group 3

"E-gov" services had a very limited use both in terms of use motives and frequency of visits among Group 1, but it was used by all other respondents regularly. The majority used it for quarterly tax and earning declarations, while some also use it for checking and printing certain documents (i.e. personal data). Among Group 1, the dominant motive was to make tuition fee payments. It was widely noted in the whole sample that due to its state ownership, those (n=10, 38%) using its services felt highly safe about its security system. Only four users had concerns, as expressed below:

"No one can provide 100% guarantee to security. In the early period of the pandemic, foreign hackers recently stole and exposed the list of all COVID-19 infected patients, even though it was a part of e-gov." Group 3

In terms of e-commerce, nearly all respondents (with one exception in Group 1) use it, though at varying frequencies. Rather interestingly, however, when asked about the sense of security, many users struggled to provide answer, claiming that they had not thought about it yet. During the discussion, nearly all respondents said that they see little or no risk in this regard, though six respondents reported taking precautionary measures specifically for e-commerce. Those precautionary measures involved keeping little or no money in the card and using two cards (one of them being used specifically for e-commerce). That is, the card used specifically for e-commerce is usually deposited with the amount required for transaction only. The primary concern voiced was the possibility of paying money and getting no item or substandard item in return.

"It boils down to amount. If I have 100 manats(AZN) (€49) in my account on the e-commerce platform, I feel, like, ok, if I lose it, it is just 100 manats(AZN). I can recover it soon. But, if it was 400-500 manats(AZN) (€201-250), which may be an irreversible loss, that would definitely make me feel worried all the time." Group 2

"I keep a separate card solely for e-commerce, and the amount I spend through it is usually low." Group 2

In terms of measures of protection taken when online a variety of techniques came up on different platforms, so looking at them separately would be useful. Looking at social media, half of the respondents (n=13; 50%)

adopt explicit measures, with some of them being displayed below:

"In my social media account, I have set up two-factor identification. So, when someone wants to access it, I get a message on my phone alerting me." Group 1

"I do not have full confidence in what I do in terms of protecting me, but nevertheless, I regularly change my password" [when he said that, his facial expression turned hopeless, verifying what he said about lack lack of trust]. Group 2

"I use long, complex passwords. 15-20 characters, symbols, words. Moreover, I adopt two-factor identification for all my social media accounts." Group 2

"I do not message with someone over Facebook on important, sensitive matters. I do not even use certain emojis, such as heart." Group 3

Finally, regarding device related measures, the term of "I use a password" was the dominant answer in all groups, while only four participants use extra measures (e.g. two-factor identification).

6.4.2. Level of knowledge on cybercrime & cybersecurity

The majority of the respondents struggled with the question as to dynamics of cybercrime pre- and post- pandemic, though a few have observed an increase based on what they have heard (particularly in group 36-65). Thus, only 5 respondents answered this question, with all of them confirming that they have seen an increase in cybercriminal activity over the last 2-3 years.

All respondents had heard of the term "cybercrime", but at different contexts (school, bank training, journalism). There were two exceptions who heard of it just a year ago during the war with Armenia. Thus, 11 respondents (42%) first saw or heard of this term while at school or university (9 of these were in Group 1, where it was predominantly students), while remaining, elder respondents first heard of this phrase either at work, on news or during the war with Armenia in 2020.

Cybercrime & cybersecurity – specific

When the meaning of cybercrime was asked and how would they define a cybercrime, only 2 male and 1 female participant spoke, while others either agreed or did not react in Group 1. For the participants who spoke in this group, cybercrime was a criminal act committed on virtual sphere, and anything can constitute cybercrime as long as it meets this criterion.

However, in general, the phrase of "internet crimes" and "information crimes" were noted frequently as all-encompassing phrase. Some (n=3) also view it as a digital version of traditional offences. However, only some Group 3 members (n=3) mentioned videogames as a kind of cybercrime, since it harms their or relatives' children. More than half of the respondents (n=16; 62%) immediately provided cybercrime examples, such as bank card theft, DDoS, and access to social media accounts, as well as all online frauds.

The crimes most heard were theft of bank card details (n=14; 53%), spam mails (n=4; 15%) and online abuse towards children (n=3; 11%). When it comes to seriousness of cybercrime in relation to other offences, inter-group, as well as intra-group differences were noted. Overall, however, only three respondents view cybercrime as less serious than other offences (and here, only violent crimes were mentioned by them), thus, indicating a rather greater degree of seriousness attached to the former offence. While not all of the remaining respondents did talk about it, 18 of them (69%) believe that cybercrime can easily surpass other offences in terms of the impact it can inflict. A rather frequently noted idea (n=20, 77%) was that cybercrime can impact wider society, while violent crimes and property crimes tend to be on an individual or community level.

"Cybercrime has consequences which can be repaired, but in case of violent crimes, its damage is irreversible." Group 1

"In certain cases, cybercrime is more serious than others. For instance, stealing military secrets to defeat one country in a war could have far more serious consequences than individual offences." Group 1

All crimes are equal to me. Speaking of cy-

bercrime, theft of personal data may in fact result in that victim's suicide. Same with online intimidation." Group 3

"Cybercrime can have ideological consequences en masse scale. I heard a fake news yesterday saying that our national hero military general was burglarized. It has serious consequences on nation's psychological state." Group 3

"Sometimes deliberate spread of fake news can harm nation psychologically and morally." Group 2

"Let me give you a very recent example. We are having a narcotics crisis these days. Their sale is done on Instagram, as well as on other social media platforms. Our Ministry of Internal Affairs said that all those transactions were done via cryptocurrencies on cyberspace. See, many people suffered due to these opportunities provided by cyberspace." Group 3

There was also a consensus that the motives of cybercrime are not different from those of traditional crimes. Two more prevalent answers emerged - making profit (n=7; 27%) and getting a revenge (n=7; 27%) were prime motives cited. Not all participants responded to this matter.

"It is the same thing; it has just become more modern. The medium has changed… Also, it renders offenders invisible, thus, provides extra advantage". Group 3

"Self-actualisation. So, if someone in a family is frowned upon, bullied or anything like that, he says to them that 'let me show you what I can do', and then use cybercrime as an instrument to prove himself" Group 2

"I have seen some people doing it purely due to personal hostility. I mean, for instance, boys would do it over a girl to steal her account, see what she is doing and all that. Also, just like a hired killer, he, I mean, a hacker does it on the request of customers who hire him to break accounts, attack someone and all that." Group 2

"For those who want to earn money with ease and quickly, it is a good medium." Group 3

The responses to the question of what other crimes cybercrimes resemble were similar to previous one. That is, the general statement was that cybercrimes are not much different in terms of nature – rather, it is a different medium to commit "old" offences. However, as noted elsewhere in this report, two-thirds of the whole sample point to a unique feature of cybercrimes – their ability to impact wider society. A very few participants also added the word of "invisibility of an offender" when comparing cybercrimes to others.

While majority in group 1 had no idea as to whom are more vulnerable to cybercrime victimization, respondents in group 3 were particularly aware of this issue. It was widely accepted that it was primarily entities in possession of secret data (i.e. mainly military and intelligence agencies) that were vulnerable to cybercrime victimization. In general, a few respondents (n=3; 11%) also added the vulnerability of children since they do not understand the consequences of what they share online and they are likely to receive bullying messages. Group 2's dominant view was that due to the nature of cyberspace, everyone in possession of a smartphone or smart device is vulnerable. It was also added by a few participants that state actors and banking industry are highly vulnerable to cybercrime victimization due to the data they hold. Several examples of cyberattacks between states were noted. Interestingly, unlike almost all groups, the elderly was not mentioned by these respondents.

6.4.3. Phishing

In Group 1, 2 and 3 only one person from each of them knew it before definition. However, four respondents from Group 1, eight from Group 2 and eight from Group 3, recognized it after definition. In fact, phishing was the most recognized offence among all discussed, though almost none of them was victimized.

All (n=24; 92,3%) those who were contacted but did not actively engage shared their experience. Many reported receiving WhatsApp messages (with texts such as "if you don't send it to 10 people, you will die") and email (with texts such as "you have inherited mil-

lions of dollars, send us your card details so we can deposit the cash"). Another noteworthy feature for Group 2 and 3 was that phishing calls received were primarily from Russia, Ukraine, and Europe, while instant messages and emails were predominantly from within the country. Many also reported cases where the item they wanted to sell attracted a fake customer. Then, fake customer asks for a bank account. Almost no attempt has been successful, except for one middle aged lady in Group 2, who lost money (80 manats (AZN), more than 1/10th of the monthly average wage) to a fake online seller, and one elder lady in Group 2, whose son lost her money to fraudsters.

"I do receive tons of suspicious mails, but since I have good knowledge of IT things, I am from media, and I have studied it, I can detect them and do not open or respond to them" Group 2

"I have received a lot of messages in Russian language but keep ignoring it. Also, many calls made in the early morning hours, who I think want to get some money from me or so. I have never responded to them" Group 3

"My son actually was the reason why I lost money to this kind of fraud. He was led by strangers in America to believe that if he pays money to them, he will get good things in return in his videogame. You will earn $800, things like that. I am an old woman, do not really know all these details. I gave him $200, and he lost it to fraudsters." Group 3

"I am a mother. My daughter's teacher actually spreads phishing mail in class by sharing one of those messages, you know, someone mentioned earlier [referring to intimidating fake messages]. So, I strongly suggest the authorities to do awareness campaigns in schools." Group 3

Only three participants knew someone else who suffered from this offence.

Almost all group participants see no precautionary measure apart from ignoring calls or emails. Overall, almost all of them felt fully aware of how to protect themselves. This is slightly different from the result obtained in the discussion among professionals, who used additional methods such as installing spam filters.

While the youngest group (18-21) had no idea as to what they can learn about phishing, the group (22-35) saw no need for dedicated webinars/seminars that would consume a lot of time. Instead, they prefer handy briefings to be shared online. Other group's only suggestion was nationwide and schoolwide awareness programs, and all those suggestions came from three women and one man who were either parents or working in the education sector. This may indicate the severity of the problem across schools, hence, a need for parent-only focus groups. In fact, as noted by a female in Group 3, teachers can, unintentionally play a role in spreading phishing mail.

6.4.4. Ransomware

Across all three groups, there was almost no one (except for one female in Group 3 who used to work at a bank and attended regular seminars on this problem, and one student in Group 1 who was victimized) who had heard of ransomware before definition. Overall, across all three groups only four recognized it later. The primary reasons may be (1) the English version of name and (2) little prevalence of this offence in the local context.

Only two victims and one vicarious victims were identified across all three groups. However, none of these victims paid ransom. Rather, they either bought a new device or formatted the existing one.

"I have not been victimized, but my close relative's phone was blocked. He could not make ransom payment, and repairman could not repair it. So he had to buy a new device" Group 2

"My Instagram was blocked about 10 years ago. I did not know how much they asked for it. I went to a software engineer, and he suggested me to change my device. So I did" Group 2

6.4.5. Intimidation and Abuse

In comparison to other offences, online abuse's victims were slightly more prevalent. While three respondents in group (18-21) had suffered from online abuse, the number was

two and four for those aged 36-65 and 22-35 respectively. Almost all online abuse and intimidation cases were related to political topics (due to disagreement with other social media users) and war with Armenia (with Armenian user accounts). Thus, a person was unlikely to have been online abuse's victim unless he or she was actively engaged in a discussion or debate.

Several female participants in Group 2 or 3 (no male participant touched on this) voiced concerns about online bullying they have observed among their pupils or children. Without elaborating, they suggested schoolwide programs in this respect.

6.4.6. Identity theft

Identity theft was the crimes participants knew most about straight away. Among offences related to identity theft, attempts to access social media account by strangers and bank accounts were almost only offences reported. 3 participants (all in Group 2) experienced successful attack to access to his or her social media account, while in two cases (Group 1 and Group 3), the attempt was failed.

Regarding the attempts targeting people's bank accounts, out of 8 attacks (30%), half have been successful.

"I once deposited $1 into my child's card so he can make online purchases for himself. But it was quickly gone [about a month later]. Then, later some time, I deposited $20-30, but the same happened again. In total, as a family, we have lost $100 before we deleted the account and set up a new one." Group 3

"A close relative of mine, grandparents suffered from bank card details theft. It turned out it was actually their grandson who took it. More than $1000. They had reported to the police immediately when cash was spent, but it took a long time to discover the identity of person who siphoned money constantly." Group 3

"I lost $500 when a foreign company whom I made a payment to failed to protect its system effectively. The hacker apparently had attacked system of that company and obtained all customers' details. Despite my efforts, no one restored money. I also had an intimidating call. Ringer knew exactly how much I had in my bank account. So, I immediately blocked it." Group 3 (NOTE: this respondent did not file a police report due to lack of trust)

No single case of the exposure of bank details was reported. No single case of mobile phone number theft was identified, but two respondents (Group 2 and 3) reported failed attempts to create WhatsApp and Instagram accounts by others through their numbers. Due to notification message by WhatsApp, they understood what was happening and did not allow the offence to materialize.

6.4.7. Interference (DDoS)

While many participants had experienced dysfunctional online services in banking services, it was due to technical fault, rather than cybercrime. All journalists (n=3) reported it happening to either their website or another well-known news platform.

Given that less than half of the participants (20 cases reported by 10 respondents) have actually been victims of cybercrime, the data on reporting to the law enforcement and other relevant actors after cybercrime victimization should be treated with care. Nonetheless, the analysis shows that only one contacted the police (though the ensuing experience was unsatisfactory), while four contacted IT expert, hacker or their company's relevant department (their experience was relatively more satisfactory).

"When I lost $500, and went to the bank, they said you should contact the company where you used your card to make payment. I did what they asked but did not work out." Group 3

"I once went to the police when I suffered from phishing, but they said that they can do only so much. After certain point, they are incapable of pursuing criminal, because he or she leaves no trace" Group 2

Overall, there were serious complaints about banks' reluctance to deal with these matters, and police's inability and lack of expertise in pursuing criminals. This can be understood when one looks at what participants what par-

ticipants would do if they were victimized.

Thus, different responses were observed across groups when asked whether and whom they would contact if victimized. Overall, 12 cited the police in this question, while the remaining 14 would go to a non-police actor (e.g. IT expert). Those aged between 22-35 almost unanimously would prefer private companies or IT experts, citing the lack of staff in law enforcement agencies in the country. However, the participants in group 36-45 hold a more optimistic view of the law enforcement agencies, hence, would report cybercrime victimization to them, though some admitted their unwillingness in doing so. That is, some participants would do so only because they see no alternative to the law enforcement agencies in finding the offender and restoring damage. In other words, they do not genuinely see the police trustworthy and capable enough to solve the matters. A very similar picture emerged for Group 1, though they somewhat refrained from elaborating on their points. In fact, everyone in this group chose the police.

"I agree with many people here, I may not trust them in the fairness and ability of their investigation, but still, I would contact the police." Group 3

"Banks do not fulfil their responsibility of finding the source of the attack, maintaining their security and restoring the damage. So, I would skip banks and go to police. If they cannot handle it, then other law enforcement agencies. If an offence involves phishing, for instance, it is unambiguously bank's responsibility. If I am customer, then they should resolve this matter." Group 3

"I would prefer IT expert over the police in terms of reporting. Our police officers generally have poor knowledge of IT stuff. Even if I do, irrespective of whether the police do its job, I would go to IT expert." Group 2

"If someone takes my phone or account as a hostage, I would go to IT expert." Group 3

6.4.8. Cybercrime – concerns and expectations

In terms of the most worrisome cybercrime, in group 3 nearly all attendants mentioned phishing as the most concerning cybercrime.

"No doubt, phishing, because most of the crimes discussed here, and by the way, according to my observations, have an element of phishing." Group 3

In terms of fight against cybercrime, unfortunately, only 8 attendants (30%) mentioned their opinion, and the rest struggled to respond. It may be explicable by the fact that cybercrime is a relatively new phenomenon in this society. They were equally divided – for the half, fight against cybercrime is quite evident, but still more to be done. For the rest, almost nothing is done, and lack of expertise is the biggest obstacle.

"Yes, there are measures taken, but not sufficient. In our phishing case, we contacted the police, but, no result. They cannot find who did it... They said that we do follow some measures, but after some point, investigation cannot go, it is impossible for us." Group 3

"Let me add to your [referring to other respondent] concerns about the police being unable to find who did those things. The reason is that even within the relevant state organ, there is no expertise." Group 3

The general sentiment about which government agencies should deal with cybercrime was that more need to be done and expertise should be improved. In Group 1, one participant suggested an inter-agency organ that would deal with cybercrimes. The similar, but the more concrete suggestion was put forward by a finance expert in Group 2, who thinks that all law enforcement agencies must collaborate and set up a special commission in this regard.

Without any exception, all groups' dominant view was that cybercrimes will intensify in the future, particularly due to more and more use of electronic services (e-gov and e-commerce), as well as digitization of once-paper-based data.

"These days everything is digitized and we are on the cusp of the digital revolution, thus, it is all too clear that this problem will become more widespread. State authorities now pay more attention than ever in preparing the cadres to combat cybercrimes…In fact, we may

see a decline in the crimes resulting in physical harm due to increase in online thefts." Group 1

"At the time when all of our data are in digital form, we have no power to protect ourselves" Group 3

6.5. CYBERCRIME VICTIMS

Group observations

Out of 11 invitations, although 6 participants joined, one of them had a poor internet connection, due to which he had to leave conversation a bit later. Three respondents were from capital city, while two were from rural areas. There were three male and two female participants.

6.5.1. Online Activities (usage in general)

While two participants used in the Internet during the whole day (9 am-6 pm) due to their work, others exploited it mainly for communication and social media.

While everyone uses "e-gov", its intensity was particularly high among two participants since it had to do with their work (i.e. checking, sending documents, doing interactions). Others used it only occasionally. All except for one (female) used e-commerce.

In terms of measures taken to protect themselves when using platforms, one male participant stood out as he used complex passwords, SMS notification system and a filter for his email. Others mentioned not opening spam messages, using two cards in e-commerce and blocking any person sending suspicious message. One female participant working in a private company informed us of the special department in their company where every spam message is directed to.

Except for one male participant, others did have some sense of concern, and as it became clear later, it was primarily due to their own, as well as others' victimization. In fact, one lady was so concerned after her friends lost money to fraudsters that she stopped buying items online.

6.5.2. Level of knowledge of cybercrime & cybersecurity

The only thing that changed in group's online routines during the last year were increased use of e-commerce and use of internet due to working from home. No one acknowledged any increase in cybercrime dynamics recently.

Everyone had heard word cybercrime after school, which is understandable given the relatively higher age average of this group.

In terms of meaning and perception of cybercrime, a male participant responded "I perceive cybercrime as an act of masterful deception and manipulation. They convince you and make you fall into trap." Another male respondent views theft of private materials (video, pictures) of other people is what constitutes cybercrime, and it is very widespread. A woman's response was as follows: "Deceiving someone that he or she will earn a prize and eventual online appropriation of someone else's money from his or her card". The remaining participants' answers were along the lines of online card theft, but they did not talk in detail. In fact, almost all participants' answers correlated directly with their past victimization experience. In terms of cybercrime examples given, online card theft was the most prevalent response.

Regarding motives, profit making was the dominant response. However, no specific group was mentioned when it came to vulnerability. Rather, the consistently voiced term was "people", referring to everyone. In terms of seriousness of cybercrime, some viewed violent crimes as more serious, while relatively few viewed cybercrime as equally or more serious due to its psychological impact.

6.5.3. Phishing

All respondents had been victims of phishing, but interestingly, no one knew what phishing is. To make it easier to follow, the experiences of victims in terms of reporting are added as well. Experience of 3 respondents are shown below in their own words:

"I registered my interest in one of the recruitment companies. Someone called me, asking whether I look for a job. He was not from the recruitment company I was registered at. He said a name, then "some interjections", and sorry I forgot. Anyway, he asked for AZN 150 deposit. I initially hesitated, and insisted to meet him in person and give. But, you know what, he convinced me really well.

That is why I perceive cybercrime as an act where conviction is used to steal something from someone. Yes, I deposited AZN 150. A few days later, when I wanted to contact him, he did not respond." / / "I went to the police. Thankfully, they found them, though the money was gone. More precisely, transferred to an account outside country, and police failed to get it back." (Male)

***MODERATOR:** Can I ask what job it was?*
"Driver in a private company. And the salary was around AZN 800-900." (Male)

"I was looking for a cheap mobile phone. I saw a discounted one on TAP.AZ, online e-commerce website. They asked for AZN 50 deposit, which we did. Then, we could not contact him." / / "Me and my daughter went to the police, but they showed no reaction. They simply said that it is not our business. Go to another district police, even though they clearly were wrong, they just wanted to get rid of me" (Male)

"Lost money to a person impersonating as a recruitment company" /// I thought that the police officers will frown upon me since I am woman. Also, I did not want to lose my time there (Female)

Overall, only one victim has been satisfied with the police's reaction, and only one (female) has not contacted the police.

Regarding why it happened, the male respondent blamed it on two factors – falling victim to masterful speech of the fraudster and his need for finding work. It was interesting because initially, this respondent had rejected to do what fraudster asked from him, but the way the latter spoke changed his opinion. The lady suffering almost from the identical case blamed it on her lack of knowledge of such criminal schemes, since she was "too young" to know those things. Other respondents also pointed to lack of knowledge and "trustworthy" image of the fraudsters.

In terms of impact, the old lady whose son lost his gaming account had started to use two cards in e-commerce, while one lady was so concerned after her friends lost money to fraudsters that she has stopped buying items online. The male respondent suffering from person impersonating as recruitment company responded that way: "I still cannot believe it. It had one big impact on me, since I understood severity of cybercrime, and thus, I always try to inform other people of being careful of those cybercriminals."

6.5.4. Ransomware

No one knew it before definition, and after definition, only one recognized it. No one has been victimized.

6.5.5. Intimidation and Abuse

Only one case of online intimidation and abuse was reported, and it was vicarious victimization case.

"My son received online intimidation. He received emails from some adult websites saying 'you will die', 'go and harm yourself', and 'heaven awaits you afterworld'. He immediately reported to me and I realized it is fake messages. It was frightening to him" (Female)

6.5.6. Identity theft

One victim (male) had his bank card attacked and money taken (AZN 45 - €22) but, in his own words, "Since it was not a big deal, so did not report it to the police". A female victim's brother's card was attacked and money stolen (AZN 200), but they did not report it either due to lack of trust. Two other similar cases of vicarious victimization were reported, both involving female victims whose sons' gaming accounts had been stolen or attempted to be stolen. Only one respondent noted use of 3-D security with his cards, which is interesting. In fact, as he put it, ""It [referring to bank card theft] has not happened to me, and I think has to do, partly, with use of 3-D security in my card". One person had failed attempt to hack his social media account.

"My brother lost 200 AZN (€98), I mean, it was stolen. He used that card to make a $2-3 online payment. About a month later, 200 AZN was stolen. He did not report it to the police due to lack of trust. You know why we do not trust [she presumably feared to criticize the police in front of everyone]" (Female)

"My son's gaming account was stolen. He cried a lot, so it affected all of us. You know,

he had those points, bonuses, things like that in his account. He lost it all" (Female)

6.5.7. Interference (DDoS)

No case reported

6.5.8. Cybercrime – concerns and expectations

From all the types of cybercrimes discussed, phishing was cited as the most frequently occurring, as well as the concerning one in the country. As to reasoning behind responses, it was once again previous victimization experience, as well as observation of others' victimization that shaped responses.

In terms of whether they would report their future victimization, group was almost united. Except for male respondents, everyone would prefer not to go to the police. Interestingly, they would just oto reportting. Trust was the overarching reason here. In the discussion of reporting future victimization, two female victims came up with a suggestion:

"In my opinion, the state must set up a website dedicated to cybercrime, where people can report their own, as well as others' victimization. This way, more people would become aware of dangers." (Female)

"Yeah, yeah, I agree. Also, such a program [referring to other female's comment above] can be launched via social media. Also, I have seen example of website in Russia." (female)

Moreover, like some parents/educators in other groups, two female participants and one male with children emphasized the need for schoolwide awareness program, since they see children as a risky group with high probability of victimization.

Apparently, one of these female victims said that instead of reporting, she would engage in awareness activities: "I follow social media accounts and pages where people share their experience of fraud, like the ones we are talking about. I regularly share informative posts there to raise awareness"

As was the case in all groups, there was agreement that cybercrime will become more prevalent with the development of technology.

6.6. IT PROFESSIONALS

Group observations

All participants were equally active. Group was made up of people with different positions within their organizations. The group consisted of four people from three IT companies, one from media organization (TV station). Unfortunately, due to 5 people, diversity of the opinions of IT experts was narrower than it could have been otherwise. Other 3 invitees failed to come up and notified us in the last minute, citing the collapse of the internet network in the organization they work at. Concerning three representatives of NGOs on human rights, two of them were well-known figures and heads of NGO in the country. The other one is specialized on the internet and IT sector.

6.6.1. Online Activities (usage in general) NA

6.6.2. Level of knowledge on cybercrime & cybersecurity

On average, these participants' first contact with the word of cybercrime was about 20-22 years ago, though in different contexts (internet clubs and work). While two NGO representatives heard of the term when the Internet was established in Azerbaijan in the early 1990s, for IT professionals, it was almost all during their school or work.

There was unanimous agreement as to phishing being the most prevalent in the country. while discussing phishing, nearly everyone cited recent examples where banking industry has been targeted by phishing scams.

The perception of cybercrime among IT experts differed radically from that of general population. For these participants, cybercrime is any crime that achieves its target, not an attempted one. Also, these participants spoke of very elaborate and intricate details of cybercrime. Thus, participants had in-depth knowledge of all offense categories discussed.

"For me, a true cybercrime consists of the one that penetrates all the systems – antivirus programs, and firewalls we have built. I consider a true cybercrime that renders us

helpless, and desperate. If it is something we or our system deal with everyday, like those trivial, minor attacks or problems, it is nothing for us." R1

I see cybercrimes, or potential for that, everywhere. On the internet, ATMs, card payment post terminals, buses… for me, if there is a human being on top of the system, I mean, as a responsible person, then this system is certainly prone to compromise. Nothing is safe" R2

"Wherever there is data input and output, there is a potential for cybercrime." R3

However, NGO representatives' perception of cybercrime was mostly similar to that of general population. The word of "internet-mediated offences" was dominant in their speeches.

Regarding the vulnerability, group was divided, with three participants seeing the elderly as more vulnerable to cybercrime victimization, while the other one cited the youth. For the former, those participants refer to lack of knowledge of many elderly in detecting cyber dangers. For the latter, it was the high level of online activity of the youth that made them vulnerable to cybercrime victimization. For all, however, it was all about awareness of cyber dangers. Differing from them was an IT expert and all NGO representatives who see lack of awareness and education as the key determinant of vulnerability, irrespective of the. However, despite their focus on education, age was noted as a natural correlate. That is, since it is generally younger people using internthe et more intensively, they tend to have more awareness, and vice versa.

"In my opinion, vulnerability is not related to the age. It has to do with knowledge. Therefore, people must be educated, and trainings and conferences must be held in this regard." R2

"I think it is not related to the age. In my view, which, by the way, differs from the other participant, it is the youth that is at risk most. I do not see lack of knowledge as the reason for victimization. Rather, they are online and are likely to commit some mistakes, and thus, suffer" R3

"In general, the level of knowledge and users' new habits are crucial issuethe in ICT field. Children the and elderly are more vulnerable. If we look at gender divide, women comprise more of the victims." NGO

How do respondents feel about themselves in terms of vulnerability? Despite the measures taken, all had a sense of fear, and they view it as an inevitable product of the online space.

"As a protection measure, we separate broadcast devices from the network to make sure it is fully offline. We attach them to the network only for short periods when needed. We use VLAN, optic fiber to send signals". R4

"Of course, the more I understand cybercrime, the more vulnerable I feel. My duty involves the protection of company's server, workforce, myself and company's infrastructure…All software programs are regularly updated due to their shortcomings. Thus, one always feels in danger." R1

"In our company, everyone is sensitive to these matters. No matter what, there are always gaps. We update software programs, but after some time, we see gaps there. Thus, we must use as latest technologies as possible to maintain protection." R3

"The more we use smartphone and computer, the level of danger will rise accordingly. In this case there is neither insurer nor the insured. Everyone's suspicion towards each other increasingly grow day by day. Everyone can be a threat." NGO

In terms of general measures of protection taken, a large number of measures were identified, which makes this group a fundamentally different one from all GPGs. There were many statements along the lines of "there is a danger everywhere." Smart devices and smart home systems, as well as digitization, they argued, have rendered everyone vulnerable and created danger for all of us. The following statements are worth looking at:

"We get lots of updates. Every time it happens, I have to explain it to our employees.

For instance, let's assume that Microsoft's existing program has been produced by 500 professionals. It is just a hypothetical number I say. It means that there are 10 billion people among whom potential hackers try to break the system. Irrespective of the perfection of these programs, every update means indicates the presence of issues, loopholes. That is how I explain these updates to them". R2

"There are elementary measures of protection one must take. Spam filters, not visiting certain websites, not answering suspicious email. I do all that, and so far, I have experienced no problem" NGO

All respondents agreed with the idea that dynamics of cybercrime have changed post pandemic. It was their personal observations that lead them to think so, rather than concrete data.

Group was united in terms of its perception of cybercrime seriousness in relation to other offences – the former is potentially far more dangerous than the latter. Similar to the points raised by many participants in all groups, the unique features of cybercrime were referred to in order to show its seriousness. In fact, two respondents used the phrase of "incomparable" when comparing different crimes with cybercrime. The following statements exemplify their points:

"Cybercrime tend to be much more serious, because terror act can be committed with this. In modern countries passenger railways are operated based on digital system. One can cause a train collision through an interference … These criminal acts, if done physically, would require huge amount of financial power, whereas it is much more convenient to do cybercrime." R3

"You can nick one or two persons' wallet, but by gaining access to one website would allow you to steal card details of 200-300 customers at one go… or, if one wants to destroy an electric station, physically, he can harm only 3-5% of it, wher,eas through cybercrime, he can shut down the whole area. R4

"The impact it can have is incomparable to that of normal offences" NGO

Different motives as to cybercrime offences were noted. 2 participants argued that not everyone, in particular some youth (aged 18-21) see it as a crime. Rather, cybercrime represents them an opportunity to show off themselves to others without getting caught by the police (e.g., hacking social media accounts on behalf of others' requests). There was also a consensus that the motives of cybercrime are not different from those of traditional crimes – making profit, getting a revenge and etc.

"Those aged 16-22 commit cybercrime more often. And it is because since they are somewhat minor or teens, they have a desire to earn money quickly, and cybercrime offers an opportunity." R1

"Stealing from someone's wallet is the same as stealing from bank card. They are the same, and deserve same punishment." R4

Three participants, all being from companies talked in-details about company policies, such as modifying access for each employee individually, setting strict bans on joining Wi-Fi through personal device and etc. In fact, these participants also spoke of complaints of their staff due to the strictness of those policies. However, none but one participant's company organizes regular seminars on cybersecurity. Rather, they are delivered only when an employee joins the company. All those companies had a set of clear rules on how and whom to report suspicious e- mail or mail/invitation. No participant expressed a need for more information on how to avoid cybercrime victimization, but they strongly suggested for nationwide awareness program, especially among the elderly.

6.6.3. Phishing

One of the participating companies had around 12,000 phishing emails in spam box, while another had almost none. In fact, within the group, phishing was the sole offence mentioned, though it had never had any impact on the company. Thus, there was no victim in any of these companies. All companies have spam filters in their mail systems to filter out suspicious mails.

However, one NGO representative has suffered from phishing, which was followed by his social media account and email account both

being hacked. While he did not suffer financial damage and managed to restore his account through IT expert's assistance, almost all his emails were deleted.

In terms of NGO representatives, the primary defence mechanism is to not read suspicious emails and block people on social media who launch online abuses against them.

6.6.4. Ransomware

No direct victim was identified. Despite being in IT sector, only two respondents had ever heard of ransomware happening to someone else. No ransomware has happened to participating NGO representatives.

6.6.5. Intimidation and Abuse

No participant from IT side had experienced online abuse, while all NGO representatives have suffered from this offence several times. To them, it was normal due to their political presence and participation, which, at times, have clashed with others. This point was similar to what was observed among GPGs. Among them, just like NGO representatives, it was those actively engaged in political discussion or debate that were abused.

"I was the target of a smear campaign for a week because of one particular activity I was involved in. Then it stopped when I revealed them publicly" NGO

6.6.6. Identity theft

No participant or employee working with them had experienced identity theft, except for one NGO representative (noted already above). Only one participant (one NGO representative who also suffered from phishing) has experienced both successful and failed attempts to steal his social media account. No single case of exposure of btok details was reported. No single case of mobile phone number theft was identified.

6.6.7. Interference (DDoS)

No participant from IT side had experienced DDoS, and they linked it with the fact that their companies have no strategic importance.

6.6.8. Data Breach

No participant had experienced a data breach

6.6.9. CEO fraud/ Business email compromise (BEC)

No participant had experienced CEO Fraud

6.6.10. Cybercrime – concerns and expectations

Overall, IT specialists did not report any corporate victimization. Among three representatives of NGOs on human rights, several cases of victimization (except for online abuse, which was experienced by all of them) were reported by only 1 respondent.

There was unanimous agreement on the question of whether participants would report cybercrime victimization to anyone in the future. The phrase "it depends" came up in all answers. That is, participants divided crimes into two categories: ones they can solve on their own (such as DDoS) due to their skills and the ones that is beyond their capacities (such as stealth of personal data or online intimidation). It suggests that it is more a question of whether police can resolve it, and if not, they see little need to contact them.

NGO representatives were almost united in their preference of non-police actors in reporting their cybercrime victimization, though they still did not fully eliminate possibility of contacting the police in very serious crimes. One particular comment, however, stood out for at least two reasons. First, it was unique to one respondent (NGO representative) in the whole study, and second, it shows the role of informal social control on the fight against cybercrime. That particular NGO representative said that he reports cybercrime attempts to several agencies, in particular Cybersecurity Service (CERT) in order to inform them of the new techniques employed by cybercriminals. Thus, in his opinion, he plays a role in the implementation of more and more preventive measures by the relevant agencies.

"We deal with minor issues, like online threat, by blocking those people. Things like that are handled easily on your own" NGO

"I just consult with IT experts when I see some danger or suspicious activity" NGO

Among all cybercrimes, NGO representatives cited data theft and stranger camera intrusion, while DDoS and data theft were more prevalent responses among IT sector members. NGO representative citing data theft argued that since they are in constant negotiation with multiple actors and state agencies, they send and receive sensitive documents frequently, hence, the fear of losing them to cybercriminals. In addition to the similar argument put forward by IT sector respondents, the reason why DDoS was mentioned was that it would cease their operations for an unknown period. Interestingly, however, they all deemed DDoS unlikely to happen.

Without exception, all groups agreed that cybercrimes will intensify in the future, particularly due to more and more use of electronic services (e-gov and e-commerce), as well as digitization of once-paper-based data. This was exactly what was observed in all GPGs.

"The whole world is currently transitioning from the analogous system to the digital system. All sorts of activities, ranging from administering the drugs to patients to security system have now been digitized. Over time, one will be able to harm others from distance with ease." R1

"The more digitized we become, the more widespread it will become" NGO

"Smart devices, 5G, greater use of fiber optics, virtual reality – we do not know what will they bring [when he said that, his face expression turned sceptic] R3

6.7. ISP PROFESSIONALS

Group observations

Here were represented 4 entities (3 private companies and 1 state agency). Private companies came from telecom and internet provision sectors, while other participants all represented the government agency responsible for the online security maintenance. All respondents were male.

All participants were equally active. Group was made up of people with different positions within their organizations. With the exception of a few questions (i.e. the storage of their backup data, since many saw it as too secretive to share), participants were quite happy to discuss the matters.

6.7.1. Online Activities (usage in general) NA

6.7.2. Level of knowledge on cybercrime & cybersecurity

The perception of cybercrime of this group differed significantly from that of the general population, and one can explain it with the fact they represent organizations, and are the people tasked with protecting their entities from cybercrime. One phrase stood out among those in the private sector: loss of reputation and profit. The phrase expressed almost by all participants was loss of data, which meant the theft or stealth of valuable data from their database. When asked to elaborate on these points, the following statements were given:

"For us, it is loss of profit and reputation. When the system goes down due to attacks, our phones do not stop ringing. I have seen cases where companies had to cease operations for hours." R1

"Cybercrime is just the commission of traditional offences on the virtual sphere. You can kill someone via cybercrime, such as through intimidating them to the level where they commit suicide, provoke people to do illegal things and purchase illegal items, just like you do offline." R2

"I view it as a leak of data, confidential data more precisely." R3

The issue of how safe participants felt in terms of the security of their organization produced a variety of responses, some of which clashed with each other, though everyone felt the constant threat. The phrase "we are protecting ourselves 24/7" was widely expressed.

One main issue expressed by everyone emerged while discussing sense of security. It was felt that despite all the measures taken, all entities in Azerbaijan have one Achilles heel – the devices and software used here are all imported or produced abroad. Private

sector representatives, unlike those from the state, frequently referred to lack of finances to further improve their security. Overall, many attendants used the phrase of "50/50" to describe their sense of security. That is, they said that they have done many things (or, in their words, 50% of the possible things) to protect themselves, but another 50% is beyond their control.

"Given that even company like Facebook has suffered from gaps in its system, of course, we can also suffer in the same way, such as via data breach. The operation system we use is not our own product, so are the devices we use. So, we assess risk level at 50%." R3

There was a wide range of ideas as to the most prevalent offences of this sort in the country. While only two respondents noted phishing, no other crime was mentioned more than once.

However, in terms of sectors, all but one agreed that banking industry faces the biggest risk and the highest number of attacks. The increasing phishing e-mails/calls made on behalf of banks and financial companies were also noted. The only respondent who disagreed added telecommunication sector as the most vulnerable sector.

Different motives as to cybercrime offences were noted. Profit-making was argued to be the main motivation by 3 participants, while the other 3 viewed it as an instrument for committing traditional crimes. Unlike other groups, one response stood out (n=4) – espionage and secret data gathering between nations.

Regarding the vulnerability to victimization, group was divided. For 4 participants, education and awareness level determine one's vulnerability. Thus, in their opinion, since the elderly were relatively less informed, they were more likely to suffer. For other 5 participants, the youth aged 12-16 are viewed as in severe risk. Those participants reasoned their argument by the following statements:

"Irrespective of gender, the likelihood of victimization increases at the age of 12-16. Those people are likely to devein lop interest in the content that is available on risky websites, let's put it that way. They may be required to open their microphone, camera, location, etc. Since they are somewhat minor, they cannot conceive the potential threats." R2

"Teenage boys have huge interest in gaming. Often, they fall into traps in the games set by cybercriminals." R5

Unlike other groups, the issue of devices was noted in the discussion of vulnerability (n= 3). Speaking of the vulnerability of corporations, those respondents believe that many entities lack financial resources to purchase necessary equipment for their protection. As other factors regarding the vulnerability to victimization, being female (n=1), working with vendors (n=1) and using smart devices (n=2) were noted. The rationale given for "working with vendors" response was that those people may work with vendors, but they do not know their cybersecurity measures/level and risks.

In terms of general measures of protection taken by the respondents' organizations, a large number of measures were identified, though nearly all were reluctant to dig into deep. Similar to the group consisting of IT experts/professionals, firewalls, anti-virus programs and spam filters were noted. However, this group's distinctive feature is that they all talked about physical security of their servers and equipment in addition to their virtual protection system. A similar point was made about physical destruction of devices that are no longer used:

"We have both virtual and physical protection, because our servers are located in a specific place, which is monitored 24/7. Whoever comes in and leave, login passwords, passwords credentials and all that are important elements we monitor, and they form our protection." R7

"Getting rid of electronic data is one thing. But we also conduct physical destruction of devices in a special room in our building." R6

The group's perception of cybercrime seriousness was one of relativity. That is, respondents felt that no crime can be judged by its seriousness on its own – rather, one must assess specific cybercrime's seriousness in relation to specific violent or property crime. Several participants gave examples where cybercrime such as online abuse has led to

suicide of the victim, thus, indicating the overlapping of two crimes at some cases. Only one respondent viewed violent crime as unambiguously more serious when compared to cybercrime which does not involve physical harm. Overall, this response was very similar to that of provided by all other groups.

All participating companies conduct regular penetration testing. In fact, the representative from the state security service mentioned that it is their mandatory duty, and they do it for all state entities at least twice a year.

"In our Data Centre, there is a special software. It regularly monitors and analyses system users. Let's say that user X has a pattern of login and logout everyday, and his password is this or that. If any of these parameters about user X change, it flags it as a suspicious activity." R5

6.7.3. ISP Specifics on cybercrime & cybersecurity

Apparently, the only data collected by the participating companies consist of "source and destination" – where the traffic originates and which website it visits. No data on user profiles are collected. In terms of data deletion, it is deleted every 3, 6, 12 months – depending on the company. No participant said that they delete data upon request, since no such request has ever been received. It was also shared by some respondents that these data have been helpful for the law enforcement to identify criminals. No company in the group sells customer data, and according to them, doing so would go against the law. Indeed, speaking of data storage, all companies said that even if they want to store data, they simply would not be able to do so due to lack of storage facilities.

"Providers' gathering data is not a right thing to do, because it requires substantial amount of investment. What can be collected, and what we do is the followings; which IP addresses joined when, which website was visited and when he or she left online. I believe more details must be collected, because as it stands, whenever which state agency requires data on someone, ISPs fail to respond them properly." R5

"Data collection and management is not an easy thing, both financially and technologically. Also, 90% of ISPs in this country do not do that." R3

"We do collect certain data. The data [meta-data] is categorized into two groups. One reason we collect certain data has to do with state security, so in cases of crimes, we can find the criminal. The other category is about customers' logging traffic and duration."

Only one participating entity (state sector) followed ISO/IEC 27001. However, they also follow their own internal standards produced by themselves.

6.7.4. Phishing

No victims were identified.

6.7.5. Ransomware

No victims, several attempts have been made many years ago.

6.7.6. Intimidation and Abuse (Privilege escalation/malware)

While no participant (with the exception for one from private sector) had experienced privilege escalation attack, it worries many. In fact, only DDoS and this crime generated group-wide concern which was vividly seen in their body language and face expression. Their concerns are exemplified by the following statements:

"Of course, it is [refers to privilege escalation] a serious thing. They join our system as an ordinary "user", rise all the way to administrator level and try to do whatever they want."

"We at state security service protect ourselves from privilege escalation via auditing team. This team monitors, or scans both our internal system and government websites twice a year. However, privilege escalation can occur internally, from within, which is quite likely."

6.7.7. Identity theft

Only one participant (private sector) suffered from data breach, and his experience is shown below;

"Yes, data breach has happened to us. It can happen through one careless act. Let me share our bad experience. One of the employees in our company, an accountant, used her personal USB flash once. She inserted it into one of the company computers. A day later, our CTO called me immediately. Every employees' password and username was on his table. You see how quickly it happened? That one USB managed to breach our security"

6.7.8. Interference (DDoS)

Nearly all participants said that they experience DDoS on a regular basis, and they linked it with the fact that their companies or organization are a target for foreign agents. In fact, DDoS was noted by all as the most frequent attack received. That was understandable, since 6 participants came from companies responsible for telecom and internet provision, while other 3 participants represented a government agency responsible for the online security maintenance of all state bodies in the country. Based on long work experience, participants drew attention to one particular change in DDoS – their enormous growth in size. Thus, while, it was mentioned, that DDoS size rarely reached 1 gigabyte until 10-12 years ago, it can now easily exceed 1 terabyte. It was also a widely shared view that prior to mega sport or cultural or political events, DDoS attacks increase in frequency and seriousness.

"One of the DDoS attacks we had recently stopped our internet provision to customers. My phone did not stop ringing, CEO, CTO all kept calling. It took several minutes to bring it back. But one internet provider I know recovered in 6 hours."

"DDoS causes a big financial loss, and also, reduces customer satisfaction because the service they use goes down. So, it always keeps us on our toes"

6.7.9. Cybercrime – concerns and expectations

In terms of reporting cybercrime victimization, it is important to note that three participants (all from the state organization) said that they are the entity where reports can be made to – they themselves do not report to any other entity in case of victimization. Other participants (all from private sector) came up with two answers – resolving the matter internally or reporting to the very state organization who was represented in the focus group. In fact, before, during and after the discussion, a very close relationship between them was observed. And it was acknowledged by respondents themselves that they constantly get in touch with each other.

The response to the question of whether participants would report cybercrime victimization to anyone in the future was almost identical to the one provided by IT experts/professionals. The phrase of "it depends" came up in all answers. That is, participants divided crimes into two categories: ones they can solve on their own (such as DDoS) due to their skills and the ones that is beyond their capacities (such as theft of personal data or online intimidation).

The group's dominant viewpoint was that cybercrimes will intensify in the future, owing to the increasing use of smart devices in all spheres of our lives. Smart homes were referred to by many attendants, one of whom said that one can "blow up someone's house from distance if they can and want" [explanation: through hacking controls of devices, one can do any kind of damage to others] to demonstrate how dangerous it has become. Another source of concern was the growing severity of DDoS attacks and the difficulty in protecting yourself from them.

The most concerning cybercrime most widely noted was an attack from within. When asked to elaborate on this point, two kinds of responses were given – an employee who conspires with an outsider to obtain and share confidential data, and employee's mistake that exposes and compromises internal security. Trojan horse was the second concerning cybercrime. Here, those voicing this concern referred to Microsoft and Cisco to explain that if those companies suffered from the Trojan horse, their own companies can easily be victimized too.

"A big problem among ISPs in this country is the obsession with protecting the system from external threats. They tend to ignore internal threats. For instance, an employee

might join the network via his personal phone, which could create a threat. R3

"As state security service, we maintain protection of systems of government agencies and their communication lines from external threats. Doing so is easy, because you have set up your defences, and waiting for an attack to happen, and you can fend it off. However, internal factors can create threats. We protect parameters of government agencies and their communication lines, but we cannot maintain control over what is happening to or what is being done with each agency's own network" R2

"Yes, we have experienced problems caused by internal sources. For instance, an employee has changed "soft" without informing us, thus, it operated for quite some time before we knew and tested it." R4

6.8. LAW ENFORCEMENT

Group observation

A limited range of organizations (State Security Service – 5, CERT – 1, Ministry of Internal Affairs – 1, Special Communication and Information Security Agency – 1) were represented.

6.8.1. Online Activities (usage in general)

In aspects of the most dangerous online activities for the general population from a cyber risk perspective, e-commerce and phishing stood out as the riskiest online activity and cybercrime respectively. A representative from CERT stated: "based on the incident reports reported to us, online trade and sales on Instagram and other e-commerce platforms. Their accounts are hacked regularly. Banking companies also report incidents frequently". An identical point was made by the Ministry of Internal Affairs' representative. In addition to these points, a member of the State Security Service draw attention to smaller enterprises, because in his view, their online defensive mechanisms are more limited and less strong than their larger counterparts, and thus, they are targeted more frequently". More remarks were made about the online activities considered to be most dangerous for general population in the discussion of pandemic and cybercrime.

An interesting point made by State Security Service is worth sharing:

"Cybercrime is not perceived seriously by large, when compared to many foreign countries, with banking being exception to some extent. In foreign countries, there are many cases of insider cooperation with cybercriminals, whereas we do not really have them here as much as it is there"

In terms of sector vulnerability, all respondents mentioned critical infrastructure, with two also adding the banking industry. In fact, attacks on critical infrastructure were the most terrifying crime for all participants. A representative from the Ministry of Internal Affairs noted phishing and e-commerce (getting bank details or asking for a deposit) most prevalent offences, while Special Communication and Information Security Agency's response was "every sector where there is data and money to be made, they are more likely to be victimized." A participant from CERT said, "as I said before, and as mentioned by other participants, online trade and sales on Instagram and other e-commerce platforms, as well as banking companies are quite vulnerable."

6.8.2. Level of knowledge on cybercrime & cybersecurity

Group participants had a single definition of cybercrime, which came from the legal code – cybercrime is about "Hacking computer systems and obtaining or damaging computer-stored data." Some also added that malware production and circulation are also cybercrimes, and they generate profit for its producers.

Nonetheless, unlike all other groups, this group noted an issue in the definition of cybercrime. That is, one of the biggest problems in the cybercrime combat is the lack of commonly accepted definition. For instance, despite the widespread use of the phrase of cyberfraud, it is not legally defined as a cybercrime. It is a fraud committed via ICT means.

There was unanimous agreement as to a change in cybercrime's nature and intensity after COVID-19 pandemic. Several examples were given.

"We identified three important changes during COVID-19 pandemic. First, working from home meant that employees became deprived of the secure network of their company. So, every time they join company network, it creates threats to their systems. Secondly, increase in online trade meant more online data becoming available. Third, phishing became more widespread, and here, I would like to note "pandemic map" trap. Organizations posing as a health institution sent maps that depicted updated picture of COVID-19's spread. Anyone who opened them fell into their trap. In fact, this attack targeted many government agencies." SCISA

"I totally agree with the idea that phishing became more widespread, and many of them contained messages about how to protect yourself from the COVID-19 virus. Some of them, as we observed, resulted in ransomware. We also discovered several fake profiles posing as health institutions." CERT

"I observed an increase in cybercrime in the banking sector. Many fake profiles of banks were set up, and offered people to set up accounts and do their operations without leaving home. Those trusting them then engine with a dialogue, where bank credentials were then provided by the client to the so-called bank. In our Ministry, we receive huge amount of bank-related reports by victims." MIA

Cybercrime & cybersecurity – general

In terms of the main types of cybercrime that participants have heard of, phishing stood out. However, participants from state security service drew attention to "man in the middle" offences targeting business dealers, and fake call made on behalf of banks as not only increasingly widespread offences, but also difficult ones for victims to understand.

Participants noted a wide variety of phishing crimes as this type is the main one they usually deal with in their activity. As just noted, though, more and more cases of "man in the middle" are being reported, at least to state security service. These offences, as said by participants from state security service, cost millions of dollars or euros to victims.

Concerning cybercrime's seriousness, it is almost unequivocally seen as potentially more dangerous. Since cybercrime can target critical infrastructure areas, it can cause massive damage which cannot be done by traditional offences, hence, potentially more dangerous. However, what is intriguing is how the local criminal code has set the sentence for such cybercrimes. A participant from state security service noted that despite attacking critical infrastructure areas is regarded as the most serious form of cybercrime by law, offender can get maximum of 6 years in prison.

In the matter of reporting cybercrime victimization, there was a widespread agreement that Azerbaijani citizens are generally unaware of where to report their cybercrime victimization since we do not have one dedicated body to dealing with cybercrime victims. Rather, there are multiple of them. For instance, both the Ministry of Internal Affairs and the State Security Service can launch investigations. Other reasons were also noted for not reporting by citizens:

"One of the issues creating problems for us in investigations is that we receive all sorts of reports, including very minor crimes to investigate, which increases our workload. For instance, a crime that can be handled by the authorities responsible for financial crime investigation is directed to us by those very authorities since they deem us more capable of handling it. We have a problem of "first responder" here." SSS

"Based on my experience, one of the main problems in investigations is the increased level of knowledge of cybercriminals. They have figured out how to lose the trace of the money they have stolen, such as by transferring them to foreign wallets" MIA

"Some [referring to victims] do not even report, and some do it too late. In some cases, since report is not made to the right address, it takes lots of time for that body or agency to relay the case to us. We also sometimes receive victimization reports over our social media accounts. Ok, now let me tell you some things that happen when victim comes to our office. We ask them some details, he or she says I do not have it, or I did not "screenshot" it. All these cause delays in the investigation." SSS

However, representatives of two agencies noted a positive thing in reporting cases, where some victims have immediately contacted them based on suspicion without even an actual crime commission.

All respondents agreed that the reporting mechanism should be much clearer (i.e., know where to report) and less bureaucratic in order to make it simpler for victims to fill out their reports and have successful results.

Cybercrime & cybersecurity – specific

The motives of cybercrime mentioned in this group almost matched those of provided by others - self-actualisation, profit, sabotage, espionage and revenge (i.e., by a disgruntled employee). An interesting response that came up widely was related to the opportunities offered by cyberspace – anonymity and larger pool of potential victims.

The question on vulnerability level of different groups generated a wide range of opinions. In fact, there was hardly a commonality between responses, which is the opposite of many groups in this study. Three respondents agreed on level of awareness as being key to low/high vulnerability level. Two of them also linked the level of awareness to age factor, saying that the elderly is more vulnerable due to poorer knowledge of cyber “traps”. Two respondents see level of online activity as an important correlate of vulnerability level – the more one uses, the more likely he or she can suffer. Again, these respondents linked level of online activity to age factor, saying that young and middle-aged people are more prone to cybercrime victimization.

“Of course, those with lower level of awareness are more prone to cybercrime victimization. Those using computer and ICT more become more familiar with things like which email to respond, trust and open. Therefore, new users, like elderly in particular, have higher likelihood of cybercrime victimization, since they tend to trust everything they read on the internet. In fact, we have seen lots of fake news unintentionally spread by elderly.” SSS

“Our data suggests more cybercrime victimization in urban areas, and we reason it with level of awareness. More awareness means more likelihood of reporting. In the capital city, we see more reporting than rural areas, so I guess I responded to your question on vulnerability.” SSS

“There are many people who do not understand bank cards. I will explain my point in a slightly different way. If you give all your credit card credentials, including its security number on the back of bank card and OTP code sent to your phone, what can your bank do to protect you?” MIA

6.8.2.1. Attribution

NOTE: identities of quotation authors are hidden due to internal nature of these questions

It turned out that all of the participating entities used a prioritization mechanism for addressing cases, except for one. Since they are obliged by law to take every case equally seriously, the phrase "the fact that critical infrastructure has been targeted does not reduce the seriousness or importance of less significant reports by one citizen or victim" shows the approach of this entity. However, other participating bodies do have a prioritization mechanism. Thus, while one respondent described their policy as "our approach to cases depends on the target of the cybercrime... as well as how critical and what type it is," another respondent put it that way:

“When we receive information about an incident, we need immediate intervention to prevent damage. Priorities must be set. This is taken into account in cybersecurity agencies. Appeals must be answered within the period specified by law. If any damage is to be prevented, we list those appeals according to their importance. Sometimes there are certain groups that are more sensitive. We identify these groups to respond to more sensitive groups as soon as possible. Sometimes we see that the consequences of the damage are not great, but the citizen considers it great.”

All participating organizations expressed issues with collecting the cybercrime information they needed. While there were certain positive comments, many challenges do hamper information collection. One of the common themes that emerged was that organiza-

tions facing cybercrime may opt to not inform relevant government agencies, which, in the words of one respondent, "can be improved through awareness programs." Since many cybercrimes go unreported due to this problem, it could weaken the deterrence effect of law enforcement. Another respondent drew attention to victims' inability to cooperate with them. Since many victims do not know where to report and do not keep traces of their communication with the offender, it makes their [respondent's organization] investigative job difficult. Some of the quotations below exemplify the situation:

"There are two issues here: one is to collect internal data. There is no difficulty in this regard, we can get it. For example, bank information. However, there are some issues that go beyond the country. For example, an IP belonging to another country has been detected and its identity needs to be clarified. This is not always successful. Sometimes it is possible to find it on the basis of an application, and sometimes the IP disappears in the middle because it comes through several networks, and it is very difficult to find. At the same time, other countries do not always respond to our requests. For example, if 10,000 manats(AZN) were stolen, it is not so important for them. In this case, they cannot answer. In contrast, if there is a fact of aggression, human death, then they can answer. In fact, it is very difficult to get information from abroad because the theft of 30,000-50,000 manats(AZN) is not considered a serious crime at the international level."

"There are difficulties in both areas: both technical and legal. From a legal point of view, the difficulty is that our legislation does not contain separate cyber-specific provisions for the implementation of procedural legal measures necessary for the investigation of cybercrime. We are forced to apply traditional procedural legal norms to the investigation of cybercrime. Cybercrime is difficult to categorize because it is a less serious crime that does not pose a threat to society. We are obliged to obtain a court decision, obtain information and review the content. We must have a court decision to disclose the information. Legislation on legalization imposes restrictions on us, which makes it difficult to investigate cybercrime. There are also some technical difficulties."

"We can only collect information if there is a court order. We face other difficulties. First of all, it is necessary to classify the data obtained. They can be divided into two parts: fixed and variable data. After receiving the information and investigating, it is possible to determine by whom and for what reason the crime was committed. We also face natural obstacles, e.g. may be encrypted. It can take a long time to decrypt data by any means. As well as, there is information that its processing takes a short time. In other cases, too much information can be a problem (which could amount to terabyte). Only a small portion of this information is relevant to the investigation and operation. As a result, we can say that we can collect data, but there are difficulties in obtaining results."

Cooperation with other countries / EU countries was noted by all participants. One participant's organization has cooperation with more than 20 centres globally and become full members of 6 international organizations. According to the participant, while they learn a lot from participating in discussions and working with those organizations (i.e. indicator exchange, prioritization of threats, global trends, new cybercrimes and so on), they do not have an authority in partaking in criminal investigation. A similar point was made by another respondent. Unlike these two, another participant did not specify the number of organizations/states they have a cooperation with, but they do have an authority in partaking in criminal investigation and request information about crime from their international counterpart whenever needed. However, this participant complained about extreme delay in responses, which can hamper their investigation. In fact, it was noted that such a reaction (apart from delay, they have seen cases where little assistance was provided) is against Budapest Convention. In addition, there was one common theme voiced by participants, which is succinctly summarized by one quotation below:

"Some countries are very indifferent to requests for information. They do not comply

with the requirements of the Convention or do not pay attention to its provisions. There are also some superficial approaches to the implementation of the survey. For example, we want information about several cases, sometimes they give only one, and it does not allow to get a comprehensive answer. No convention can regulate this. It refers to the domestic legislation of each country and is based on its own legislation. They do not pay much attention to the International Convention. The weakest link in cybercrime is legal aid inquiries. While we find a lot of information on the technical side, the relevant agencies of the opposite side create problems during the investigation…The conventions do not set a specific deadline for the execution of inquiries. It would be good for the parties to make a commitment on time, for example, to implement a simple problem within a month, or in the case of complex issues for a longer period. Sometimes the answer may not come for months."

In terms of Big Data repositories, one entity uses "feeding" centers, who compiled Big Data in certain ways and present them to them. This information tends to be around threats and new trends. It was also revealed that each government agency is provided regularly with relevant information to protect themselves from cybercrime and Big Data play an important role here. Other entity uses "online tubes" (some are free, some paid) to decipher data significant for criminal investigation. Other entities (n=2) do not use Big Data repositories.

While Azerbaijan falls outside jurisdiction of GDPR and thus, none of these organizations follow it as a guideline, they all follow local criminal code and regulations (NOTE: one respondent informed us that the work is underway to adapt local regulations in line with GDPR). However, it was noted that despite the presence of regulations/laws on dealing with individuals' private data, it is not as encompassing and detailed as GDPR. In fact, one participant expressed a wider problem in complying with human rights laws in case of cybercrimes:

"We have a law on the protection of privacy. However, it is still not as comprehensive as the GDPR. This is due to insufficient training of both the private sector and third party staff. For example, there is a control log: I got the proof and passed it on to the next employee, who also passed it on to someone else. Employee X also sends him to court. This is done for security reasons. The control journal reflects the date, by whom, and with what change the information was given to the other party. All of these are human rights issues. What causes it? In the approach of the judges in the courts, the prosecutor's office, the investigating party and the operational side. In general, we do not fully reflect the challenges of the time at the level of law enforcement agencies, courts and prosecutors. When cybercrime becomes a threat, we will start to fight it. Then the process must be carried out in strict compliance with the requirements. I hope something will change."

Another issue voiced was related to the Criminal Procedure Act. It was noted that despite the adaptation the of criminal code in line with the Budapest Convention, Criminal Procedure Act has not been modified. Thus, it creates challenges for treating electronic evidence.

"I want to talk about the technical aspects of data acquisition and storage. It is a fact that the information is changeable according to our internal rules. The main principle in taking information is that the information should not be changed or corrected. Therefore, the information itself is never taken directly. Usually its image is taken, a byte copy is taken. When, where and how much information was taken, etc. These are regulated by a number of internal rules."

As already mentioned, information provision to relevant state agencies by the private sector is voluntary. Thus, while participating entities do receive information from the private sector, they express their intention of raising awareness among the latter. However, one respondent noted their close working relationship with the Central Bank, who acts as something of an intermediary between relevant government agencies in the fight against cybercrimes and private banks. That is, the central bank provides information to

private banks and financial institutions as to how to protect themselves from cybercrime. Cooperation with "backbone" ISPs was also mentioned, as the latter "does the necessary work in the event of the spread of incidents throughout the country." It was also mentioned that many organizations in the financial sector exchange information with CERT regularly. All these comments were shared by all participants. However, one entity representative added that their organization also conducts seminars and publishes journals annually to raise awareness. In fact, CERT and the State Security Service have awareness programs at schools and for the general population to explain phishing and other risky activities.

When it comes to using specific law enforcement/judicial powers in investigations, two participating entities said that due to not having investigative authority, they direct some cybercrime cases to the state security service. Thus, it was only the state security service that used law enforcement and judicial powers in investigations.

6.8.2.2. Disrupting Cybercrimes

In terms of investigations, preliminary investigations can be carried out by the State Security Service or the Ministry of Internal Affairs, depending on whoever initiated it first. The State security service, Ministry of Internal Affairs, and CERT can all receive reports from citizens, but the latter cannot initiate an investigation. Therefore, they divert it to the relevant agencies mentioned. However, CERT plays an important role in raising awareness among victims and non-victims alike.

It was argued that since the Criminal Procedure Act had not been modified in accordance with the specification of cybercrime, the state security service had to resort to classic criminal intelligence and investigation techniques in the realm. The statement below explains the point:

"Because our procedural legislation is not sufficiently cyber-specific, we are forced to use classical investigative measures. However, after becoming a party to the Convention on Cybercrime, there is also the authority to apply directly to freeze data, especially in order to provide the speed we need. The data is frozen and stored. Then we get a court decision and take the frozen information and use it. Of course, it does not apply to other classic crimes. It is cyber- specific. Since our procedural code itself provides us with classical techniques, we also have to use those techniques."

It was noted that despite the use of classic criminal intelligence and investigation techniques in the realm, one always must be extremely careful in treating electronic evidence due to its different nature from other crime evidence. An interesting example was given in this regard:

"The investigator can never decide on behalf of the specialist. He only consults with a specialist, evaluates his tactics and works with a specialist in whatever form he needs. A large group of offenders may have been arrested. It is a traditional way to look at a computer system (DNA, fingerprinting). It is also possible to know from certain user data in the internal system what this person used. However, DNA and fingerprint tests are performed to confirm the evidence. This is the classic method. In cybercrime, specific methods prevail. An investigator unfamiliar with the field may not be aware of the method of their removal. Because a person does not know, for example, what information is stored in RAM, turns it off to take the computer to the control room and analyse it. The main evidence is considered to have been destroyed on the spot. Because the basic information stored here may not be written to permanent memory. The investigator must be informed to know how to act in such scenarios."

In terms of thwarting ongoing cybercrimes, one participant gave an ongoing example where they have noticed and flagged the registration of the "gov.az.info" domain as a suspicious activity. He also said that they have the technical and legal capacity to follow and analyse phishing messages sent to government agencies and take measures against them. Another respondent spoke of "malware" and "mining" processes originating from foreign countries. As soon as they noticed it, they started to collect evidence and identify the IP to thwart attempts, which succeeded. In

general, this respondent pointed to the ease of disrupting cybercrimes so long as an IP address is identified, as well as through putting blocks into a country's "wall".

6.8.2.3. Caring for victims

All respondents take care of victims in various ways and to different extents. As already noted, one entity representative noted that their organization conducts seminars and publishes journals annually to raise awareness. Schools are also covered, and TV broadcast is used as well. Another respondent spoke of cyber hygiene project they have started in collaboration with two other bodies, where 10,000 people are to be targeted as a part of awareness campaign. Another respondent mentioned their consultative talks with every victim they receive to increase their awareness. However, no case of any other proactive measure was noted. Whether victims feel confident that law enforcement can and will do something with their information was not covered due to time limit.

6.8.2.4. Cybercrime prevention

Three participating entities spoke of their special interest in and using the skills of younger first offenders of cybercrimes. Across whole group, the general view was that relevant agencies must make good use of their skills before they become so-called career criminals. The quotes below exemplify their views:

"We have a special interest in cases involving minors. First of all, we are interested in whether the juvenile committed this crime using IT knowledge, his "hacking" knowledge, or the lack of knowledge of the other party in this area? In most cases, this is not due to the presence of IT knowledge. It is a scammer who takes advantage of people's ignorance."

"It is more convenient to direct the knowledge of young people in the right direction, than those who are professionals in the field, who take purposeful steps. At a young age, it is easier to identify them and direct their knowledge in the right direction."

6.8.2.5. Cyber capacity

One participant mentioned general difficulties in recruiting talent, and lack of talent across the country in fight against cybercrimes. Nonetheless, the academy within state security service, as well as universities providing law courses were noted as main sources of talent. Once recruited, they undergo several trainings and tests. One respondent mentioned contests where talents can be discovered. A quotation from another respondent below succinctly shows finance-related issues in recruiting talent:

"It is very difficult to find staff in our country. The reasons are also known. First, a person can normally ask for a higher salary, but salaries do not depend entirely on the institution, but on the Ministry of Finance, and for many reasons do not always turn out as desired. There are people whose salary is not a problem, but they want freedom, they demand a work schedule. Although it is difficult to find a ready staff, it is relatively easy to find a staff that can be trained. These may be people with high scores in universities, which means that this person has a good perception and ability to take. It should be prepared by the department itself, involved in courses (external or internal courses)."

6.8.3. Cybercrime – concerns and expectations

As is the case with other groups, there was unanimous agreement that cybercrime will intensify in the future, due to increasing number of devices connected to the internet, digitization, and technological development in general.

6.9. CONCLUSIONS

❖ While every focus group respondent knew what cybercrime is, only one-third of the survey population recognised cybercrime, which is one of the differences between the results of survey and focus groups and can be explained partly by different sampling methods employed in each of them.

❖ Regarding the perception of cybercrime, the phrases "internet crimes" and "information crimes" were frequently noted as all-encompassing phrases among GPGs as well as NGO representatives. However, the perception of cybercrime among IT professionals and law enforcement representatives differed radically from that of the general population. For the former participants, cybercrime is any crime that achieves its target, not an attempted one. The implication is that there are apparently a large number of unreported cybercrime attacks across the IT sector. Also, these participants spoke of very elaborate and intricate details of cybercrime. Thus, participants had in-depth knowledge of all the offence categories discussed. For law enforcement representatives, cybercrime meant hacking access to information stored on other devices and damaging the integrity of information systems.

❖ Only a limited form of cybercrime (certain forms of identity theft, phishing, and DDoS mainly) have penetrated the cyberspace of the country. Nonetheless, as indicated both by focus group and survey data, cybercrime victimization is quite low despite the sheer number of attempts our respondents (especially phishing-related) have faced. In fact, there were comments among both IT professionals and law enforcement representatives that cybercrime has yet to become a concern for the general society in Azerbaijan due to its nascency and lower use of online activities compared to more developed countries. Nevertheless, one might imagine it becoming a concern not in so distant future given the greater use of technology and online interactions.

❖ Both survey population and focus group had very little knowledge of ransomware, though slightly more people for both target groups had heard of this crime happening. Exposure of personal details was rarely identified across both target groups, despite it being considered as the most worrying one in the survey.

❖ Unlike focus groups, not all respondents in the survey population have experienced phishing attempts. Only 22% have experienced it.

❖ Another important difference between the results of survey and focus groups is related to online abuse. While around one-third of general population in focus groups have suffered from it, almost no one mentioned this crime in the survey. It can be partially explained by the nature of the sample in focus groups, since there were many political scientists, journalists, and activists whose ideas led to online abuse from others who disagreed with them.

❖ In terms of defence against cybercrime, our data point to reasonable defensive awareness at least among our sample, though several cases of cybercrime victimization were noted. While GPGs had mostly sceptic view of the law enforcement in dealing with their victimization reports, law enforcement focus groups revealed several serious problems with victims themselves, such as late notification and not reading or following safety instructions provided by banks (it was noted in the context of phishing and bank card theft). Nonetheless, law enforcement representatives did acknowledge delays and problems in investigation. As reported by all victims, as well as those in victim-only focus group, they have faced many problems when contacting the law enforcement, such as paying lip-service to their report, not taking it too seriously or acknowledging their inability to investigate and find. Thus, while reporting itself is not a problem, it is the reaction that either deters people from reporting or getting a satisfactory outcome.

❖ The question of vulnerability generated three prominent, somewhat interrelated themes: age, level of education or awareness of cybercrime, and level of online activity. For some participants, it was primarily their level of education or awareness of cybercrime that determined their vulnerability. Nonetheless, it intersects with a person's age, according to the participants, since the young tend to have more knowledge of potential threats online

than the elderly. However, there was also a view that irrespective of awareness and age, a person's level of online activity was more important than anything else.

❖ The point made above brings to the fore the issue of children. Several participants in focus group were parents, and they generally did acknowledge their concern for children, since they spend lots of time in front of screen and with gadgets.

❖ As noted by some in GPGs, and almost all respondents in other groups, banking industry is highly vulnerable to cybercrime victimization.

❖ Speaking of vulnerability, it is worth noting the risks facing school children. One focus group's suggestion was nationwide and schoolwide awareness programs, and all those suggestions came from three women and one man who were either parents or working in the education sector. This may indicate the severity of the problem across schools, hence, a need for parent-only focus groups in the future. In fact, as noted by a female, teachers can, unintentionally play a role in spreading phishing mail. Considering a high use of smartphones and tablets among pupils, it is possible that there is a significant "dark figure" (unknown) of cybercrime among this subgroup.

❖ Appertaining to the seriousness of cybercrime in relation to other offences, cybercrime is seen potentially more dangerous by all groups. Cybercrime can impact wider society, while violent crimes and property crimes tend to be on an individual or community level. For law enforcement respondents a particularly concerning feature of cybercrime is its ability to damage critical infrastructure and thus, cause mayhem. Across some groups, there was also a widespread agreement that cybercrime can result in suicides in certain cases, such as intimidation.

❖ In terms of reporting past cybercrime victimization, while extremely few have contacted the police, their ensuing experience was unsatisfactory. There was greater propensity to contact IT experts in case of cybercrime victimization, except among the youngest focus group. Unfortunately, our data do not allow us to ascertain whether the IT experts also refer cases/people to the police eventually.

❖ IT professionals, IST representatives and NGO representatives were less likely in comparison with GPGs to notify the police.

❖ As admitted by some law enforcement representatives and victims, the local agencies have faced many cases where tracing the offender becomes almost impossible.

❖ Without exception, all groups agreed that cybercrime would worsen in the future, owing to increased use of electronic services (e-gov and e-commerce), as well as digitization of previously paper-based data. Nevertheless, perhaps the most striking difference between the results of the survey and those of the focus groups is related to the expectations related to cybercrime. While almost every focus group respondent anticipates an intensification of cybercrime in the future, nearly half of the survey population thinks the opposite. This striking difference can be explained, perhaps, by the selection criteria. When selecting participants for focus groups, certain criteria (e.g., active use of the internet, working in the IT or ISP sector and so on) were applied, and thus, bias played a role. For the survey, though, it was random.

7. GENERAL CONCLUSIONS

1. Raising cybersecurity awareness, perception gap and need for advanced and comprehensive cybersecurity policy.

The relevant government agencies of Azerbaijan in the field of cybersecurity must be particularly engaged in protecting the 8.26 million internet and 11.30 million mobile users across the country.

Bare in mind that the research project's primary objective was to conduct a quantitative and qualitative analysis of Azerbaijanis' attitudes toward cybercrime and cybersecurity. The findings are provided in chapters and include surveys of two primary target groups: individuals and enterprises, as well as five focus groups (FG) comprised of the general population, cybercrime victims, information technology professionals, internet service providers, and law enforcement. The sections that follow summarize key findings in these areas.

The study reveals the formation of different attitudes towards cyber threats among different target groups of the population, depending on age, gender, occupation, education and other. We observe it in terms of cybercrime perception, since the phrases "internet crimes" and "information crimes" were commonly used as all-encompassing phrases among GPGs and NGO representatives. However, the perception of cybercrime of IT professionals and law enforcement representatives differed radically from that of general population, as well as some results of survey and focus groups differed.

An example of this-the most remarkable difference regarding awareness between survey and focus group results related to expectations of cybercrime. While almost every focus group respondent expected cybercrime to increase in the future, almost half of those surveyed anticipate a decrease. Although this remarkable difference is explained by the selection criteria for participants for focus groups from participants for the survey.

A key barrier to the adoption of new "online-cybermindsets" is the significant perception gap between what the public thinks about cybercrime and the reality of the threat. As a result of this perception gap, many members of the public put themselves and their organizations at considerable danger of becoming victims of cybercrime by delaying or deprioritizing online security.

The fact that the term "cybercrime" has not yet been widely adopted and clearly used among the population indicates that a lot of educational and informational work remains to be done in this area. As previously stated, the incident exposed an international fraud crypto-pyramid (Ponzi scheme) in Azerbaijan, committing fraud against about 10,000 citizens, which is contrary to full awareness of cybercrime. At the same time, the fact that cybercrime is considered as one of the most important threats, with a low victimization rate and growing concern, provides a basis for effective countermeasures.

Research summarises key results and identifies a large and growing gap between the nature of the cyber threat from one side, public perceptions from the other, and the importance of measures to be taken accordingly. One of the reasons could be that not all forms of cybercrime have gained traction in Azerbaijan, and even those with a greater prevalence (phishing and data breaches, for example), may not have reached dangerous levels of prevalence yet.

According to the results of research, it has been established that there are both improvements, as well as problems with the providing of cybersecurity and combating cybercrime compared to the time elapsed. Survey results of individuals target groups has highlighted an increase in awareness of cybercrime amongst general population.

Since the beginning of the pandemic cybersecurity gained further significance, online activities accelerated and thus, has increased public awareness.

In terms of protection, the data suggest somewhat positive picture, but nonetheless, considerable portion of the sample feel not sufficiently equipped to protect themselves, which may indicate need for awareness programs such as the ones organized by CERT.

2. Results of the survey of other target groups -enterprises demonstrates that there is a completely cybersecurity and threat perception gap.[29]

As of October 1, 2021, the number of business entities in Azerbaijan was 1,306,490. Of the registered statistical units, 136,743 are micro (93%), 6,832 are small (4.7%), 2,652 are medium and 603 (1.8%) are large business actors.

Regarding knowledge, awareness, and attitudes towards cybersecurity a large proportion of the public and Small and Medium-sized Enterprises (SMEs) vastly underestimate the risk of cybercrime and feel powerless to protect themselves against it. There is a widespread belief that "size matters" and cybercriminals focus only on big businesses and celebrities rather than small "ordinary" people; a misconception that there are few consequences of being a victim of cybercrime; and an array of inconsistent advice that leads to dangerous inertia.

However, in terms of sectors, all but one agreed that banking industry (as large business actors) faces the biggest risk and the highest number of attacks. The increasing phishing mails/calls made on behalf of banks and financial companies were also noted.

When asked about the main challenges or barriers to effective cyber risk management, the most frequently cited were the lack of resources and cyber risks that were not top priorities. SMEs believing that applying advanced security technologies and increasing budget will help improve organization's security level shows that the role of the human factor, the importance of the personnel problem is not understood, and technological solutions are considered key.

The fact that a significant number of enterprises do not have a department in charge of cybersecurity, or any one responsible for cybercrime or security, as well as lack of cybersecurity insurance especially among small and medium enterprises can cause major problems.

At the same time expectation of cybercrime scale to increase in the future indicates the need for more publicity of the problem.

As a result of the perception gap, millions of people are leaving themselves, businesses, and infrastructure vulnerable by failing to follow even the most basic secure online behaviours. Whether targeting global corporations or micro-SMEs, criminals frequently exploit the weak cybersecurity of individuals to facilitate their attacks. International experiences show that companies can be publicly blamed for breaches resulting from the poor cybersecurity (and subsequent data theft) of other organisations or the poor cybersecurity of their customers.

There will be most impact if to work together to bridge dangerous perception gap, encouraging individuals and SME to take simple actions to protect themselves, businesses and society at large.

Another point to consider is the expectations of different target groups, that all issues will be resolved by the state. Important majority feel that the state or national authorities are prepared but still have some work to do to take on cybercrime. This is the result of the fact that the place and role of civil society, each person in the joint fight against cyber threats in society is not seen in the process.

3. Analysis of perception, level of knowledge on cybercrime and cybersecurity- cybercrime concerns and expectations of İT and ISP Professionals reveals results that are both general and country-specific.

As already emphasized in the study, a general principle, attitude to national cybersecurity capacity development must be approximately on the same level as ICT development in the country. If a country is interested in ensuring strong security, forming society with cyber threat awareness and informational culture, it has to pay equal attention to all direction. These areas must be balanced. At the moment, Azerbaijan has a gap between ICT development and cybersecurity development;

[29] As is known, the perception gap is based on three key myths: "Cybercrime isn't something that I need to be concerned about"; "Cybercrime is not 'real' crime "; "It's nothing more I can do to protect myself". Rather than accepting cybersecurity as a personal responsibility, many feel that it is "someone else's problem" and absolve themselves of responsibility through an overly passive interpretation of common expectations. https://www.sciencedirect.com/ science/article /abs/ pii/ S0278691512000981

the state needs to pay attention to minimize this gap. A suggestion for the e-governance transition process is to develop services and solutions that ensure Security by Design to minimize the risks of security breaches and vulnerabilities. It is cheaper and easier to design systems from the start that consider the present legal framework in ICT and cybersecurity.

When analysing the threat background, the cybersecurity strategies of the past decade and the actual legal framework in the country, it is crucial to take some serious steps to develop cyber-reforms, ensure the continuity of e-transformation and e-governance in Azerbaijan that will fulfil the requirements and needs of current day cyber-landscape.

Malware operators have been observed evolving their tactics to hack into sensitive targets. This is because developing of capacity building of IT and ISP professionals entire systems should be made a priority of the cybersecurity governance in Azerbaijan.

Fighting cybercrime is fundamental to both effective criminal justice and cybersecurity policy. Even organized crime, economic crimes, and crimes against individuals require an effective framework to deal with cybercrime, for example regarding access to electronic evidence or criminal proceeds on the Internet. In this regard, cooperation between criminal justice authorities and private organizations, including service providers, is essential. Strong cybersecurity must go hand in hand with an open, free and secure cyberspace in which the rule of law are fully applied.

We see that both law enforcement agencies and ISPs want to make the Internet safe for users. However, providers have a different mindset, not focused on investigation and prosecution, but on customer satisfaction. They have a common interest, but approaches may differ - it is important to keep this in mind when discussing cooperation.

One of the main points in cybersecurity is capacity building. New cyber threats, tools, and methods are emerging depending on technological developments. New policies, laws, standards, products, solutions may be needed in the new situation. In this respect, the capacity of software, hardware and application developers have to be developed, and new possible security problems and solutions should be designed.

In other words, IT and SSP professionals' cybersecurity capacity building has become an essential requirement for institutions and commercial companies as well as states today. Nowadays, in numerous progresses of cybersecurity volume, there are severe problems in raising qualified human resource capacity in this area as well. It is necessary to prepare national and international developed programs in order to develop qualified human resources required in the field of cybersecurity. The establishment of graduate and postgraduate level programs in cybersecurity, research institutes and test centers and certification programs should be encouraged by the state. Additionally, cybersecurity training courses have to be organized and provided from low to high-level knowledge and skills to the people.

Ensuring cybersecurity is impossible if only through the introduction of modern equipment and software, but it is possible by taking into account the analysis of the human (regarding IP & ISP) factor, technologies, and processes. "A big problem among ISPs in this country is the obsession with protecting the system from external threats while ignoring internal threats." For instance, an employee might join the network via his personal phone, which could create a threat.

The results showed that homeland defence and economic well-being were the dominant aspects of cybersecurity policy, whereas capacity building and infrastructure were the main concerns of cybersecurity elements for Azerbaijan. This study recommends that Azerbaijan strengthen both infrastructure and capacity-building to efficiently develop and implement national cybersecurity policy. In terms of infrastructure, there is a need for more improvement in the cybersecurity architecture of the country, the financing of information security, the information sharing mechanisms and so on. It is required to enhance security awareness through cybersecurity education and training of citizens, as well as trust and working culture.

4. Talking about result of law enforcement focus groups attitudes and opinions regarding cybersecurity and measures taken, general conclusion can be characterized followed actions:

- ❑ There is need to raise awareness about cybersecurity: more information about current risks and specific measures should be made available to the general public.
- ❑ It is important to take a holistic view of all topics related to values: we do not have to choose between (cyber)security and privacy or any other value.
- ❑ Most of the data found relates to general security and privacy issues; therefore, further empirical research is needed to cover other values as well as to explore specific issues.
- ❑ According to the standard data protection model, main new protection objectives as-confidentiality, integrity, availability- should be added. Thus, privacy and security, individual and general directions must complement each other.

Other important conclusions regarding to the results of the study we can relate to the following issues:

- An analysis of the available national legal frameworks reveals insufficient unification of "predicate" cybercrime offences, investigative powers and the admissibility of electronic evidence.
- The impact of international fragmentation and differences in national laws on the international cooperation
- Reliance on traditional means of formal international cooperation on combating cybercrime and the use of electronic evidence for all crimes
- The role of "location'" of evidence
- Unification of the national legislation of the countries
- Capacity of law enforcement and criminal justice authorities

Efforts to prevent cybercrime need to be stepped up based on a comprehensive approach that further raises awareness builds partnerships between public and private organizations and integrates Strategies for fighting cybercrime in the broader issue of ensuring cybersecurity. Strengthening international, regional and national partnerships, including with the private sector and academic institutions, in order to provide effective technical assistance in the field of preventing and combating cybercrime in country would be appropriate.

As revealed in research, when it comes to cybercrime's seriousness, it is almost unequivocally seen as potentially more dangerous. Since cybercrime can target critical infrastructure areas, it can cause massive damage which cannot be done by traditional offences, hence, potentially more dangerous. However, what is intriguing is how the local criminal code has set the sentence for such cybercrimes. A participant from state security service noted that despite attacking critical infrastructure areas is regarded as the most serious form of cybercrime by law, offender can get maximum 6 years in prison.

Another example applies GDPR issue. The specialist also proposed to toughen the punishment for petty fraud, while today criminal prosecution begins in case of damage in the amount of more than 500 AZN (currently, € 260). With a small amount lost, citizens do not file a complaint, which is what such actions of cybercriminals are designed for. Unfortunately, in terms of the length of the process and the loss of time, citizens are reluctant to complain. However, it would be useful for citizens to complain, regardless of whether the damage is small or large.

Together with local regulations on personal data in Azerbaijan, international regulations should also be taken into consideration. As per GDPR having come into force on May 25, 2018, emphasis is made on the protection of EU residents' data, not considering the residence of the entity processing, obtaining, or operating such data. Such an extraterritorial effect of said regulation needs to be understood by entities having multinational business activities, especially by entities providing services worldwide no matter their place of business.

Research revealed that only a small proportion of the banks were aligned with GDPR requirements, while the vast majority violated certain requirements. The legislation of the Republic of Azerbaijan does not oblige le-

gal entities that provide financial services to comply with GDPR requirements. However, paragraph 2 of Article 3 of the GDPR, which covers the territorial scope, states that even companies established outside the EU are subject to GDPR requirements if they offer goods or services to real people (data subjects) living in the EU or monitor the behaviour of such people, irrespective of whether a payment is required from the data subject. In other words, if any bank is storing the data of at least one customer from Europe, it automatically falls under the GDPR. Moreover, compliance with GDPR requirements may be a decisive factor for prospective organizations (especially those from the EU) that are looking for a partner for financial services.

Capacity building of law enforcement institutions, effective security mechanisms, and active surveillance systems of the virtual world while considering the applicable fundamental human rights, are helpful in preventing the dangers to cyberspace in Azerbaijan, but everything is based upon the intentions of policymakers and stakeholders. The digital legislation, along with a potential cyber-force, will not only prevent the probable cyberattacks on Azerbaijan, but it will also reduce the growing cyber-skirmishes between Azerbaijan and other states. Consequently, the multifaceted cyber threats can be neutralized by establishing robust cyber-deterrence. The cyber-power of Azerbaijan will enhance cybersecurity.

5. Regarding social and cultural context which might have an impact in shaping of the respondent's perception/attitude toward issues the study. It may be claimed that Azerbaijan is in the process of evolving from a traditional to a modern society and moving towards a postmodern stage.

The processes taking place in Azerbaijan can be characterized as the completion of the transition from traditional to modern society, while entering the postmodern phase.

The global information revolution is having an important impact here, even in the form of undesirable cyber threats. Increasing transparency criteria of the information society are becoming imperative. Identified during the survey, some answers about insufficient funding, the non-transparency of the cybersecurity budget, and a lack of understanding of its importance are due to the fact that transparency in the country has not yet been fully formed.

Same idea is to say regarding opinion differing scale and impact of cybercrime and real crimes, vulnerability and victimization. “A rather frequently noted idea (n=20, 77%) was that cybercrime can impact wider society, while violent crimes and property crimes tend to be on an individual or community level”.

Research sample was almost equally divided as to their expectations about the future of the scale of cybercrime. Urban dwellers, active internet users and women were more likely to think of increase in cybercrime.

Rapid urbanization in Azerbaijan with a population of over 10 million people, continues to increase. 56% of the total population lives in urban areas or cities (World Bank, 2020) while unofficially this number could be higher. Moreover, economic and social disparities among capital and regions are another problem. Baku-the capital city accounts for 70% of GDP due to the oil and other business sectors. This has an impact on the perception of urban and rural population.

Traditional family values in Azerbaijan can be considered as social and cultural contexts that might have an impact on the formation of the respondent's perception/attitude toward issues. This brings to the fore the cybersecurity issue of children. Several participants in the focus group were parents, and they acknowledged their concern for children, since they spend lots of time in front of screens and with gadgets during the pandemic. Recall that it was noted that there was a need for parent-only focus groups in the future.

It is a known fact that the forces interested in foreign religious and ideological propaganda among the youth of Azerbaijan use new technologies. This is not surprising if we remember that it is the virtual space that is the stronghold of the various protests. As a female participant pointed out, teachers can unintentionally play a role in spreading phishing mail. Given the high use of smartphones and tablets among pupils, there may be a significant "dark figure" of cybercrime among this subgroup. However, many facts indicate

that this is an intentionally purposeful activity mainly directed from Iran. Fake news has serious consequences for the psychological state of the country. Sometimes the deliberate spread of fake news can harm a nation psychologically and morally. "

As seen, the threats of foreign state sponsored cybercrimes have potential to create political instability, social unrest, and economic havoc and to damage the digital infrastructure of any state. Therefore, the national security in the digital age is difficult to strengthen against the cyberattacks, because the vulnerable cyberspace of a country may not only lead to economic crisis, political instability and security degradation but it can also cause a social unrest by providing incentives of hybrid PSYOP (Psychological Operations) to the rival forces. The counter measures to eliminate or minimize the likelihood of cyberattacks have become an essential ingredient of cybersecurity in all states' politics.

Another social and cultural context influencing the respondent's perception of issues will be "honour cybercrimes" characteristic of the mentality and related to online abuse of personal pride, insults, infringements of dignity, and so on, which can lead to suicide. In relation to cybercrime, theft of personal data may in fact result in a victim's suicide, which can also be the case with "online intimidation". Finally, journalists may also face difficulties when they express their political opinions online.

The consensus that the "motives of cybercrime are not different from those of traditional crimes" was also widely agreed upon should be emphasized. It is the same thing; it has just become more modern. Only the medium has changed. Also, it renders offenders invisible, thus providing an extra advantage". The difference is that cybercrime can impact wider society, while violent crimes and property crimes tend to be on an individual or community level.

6. To summarise research results, one of the important areas for improving awareness of cybersecurity is training, enlightenment, education, and academic research programs.

Educational institutions, private and public entities have a great responsibility to educate society in the field of cybersecurity. In order to augment the cyber-strength of Azerbaijan, there is a need for strong promotion of cybersecurity studies, educational and informational activities along with the cybersecurity discipline in universities and academia. The establishment of cybersecurity centers in academic institutions can assist policymakers in the formulation of cyber-defence and contingency policies. Hence, the cybersecurity oriented academia with research-oriented feedback can improve the performance of the cybersecurity experts of Azerbaijan. A comprehensive plan for the research and development of the IT industry, consisting of the advancement of ICT education, virtual training centers, and promotion of computer software engineering centers at a national level, is needed to be implemented effectively.

Yet, as we can see from this study, higher education institutions in Azerbaijan do not offer any bachelor or master's degree programs related to cybersecurity, and cybersecurity is not included in the existing programs. This is one of the first problems in training new cybersecurity professionals in this country. Many private education companies are providing various lectures and courses in Azerbaijan. These include both local and foreign courses.

7. Regarding cybersecurity policy, the results show the unbalanced approach of cybersecurity policy development in Azerbaijan and there is an urgent need for national cybersecurity strategy. Azerbaijan has a national policy and strategy to specifically guide the cybersecurity approaches within the country. However, there is no national cybersecurity strategy or policy document on the legislative basis of Azerbaijan. Nowadays, national cyber policy decisions are made without objective policy evaluation by stakeholders and cybersecurity experts. But, difficulties arise when many aspects need to be considered equally at the same time when making the best decisions to satisfy all stakeholders. Therefore, different aspects of research should be considered properly for devel-

oping an effective cybersecurity policy and strategy in Azerbaijan. Cybersecurity policy must be strongly adhered to so that each country and organization can recognize and prepare for different forms of growing cybersecurity threats in the future.

The conclusion on the natural character of the delay in implementation of the objectives of the National Cybersecurity Strategy in Azerbaijan leads us to the recognition of the need for a clearer trajectory determination towards ensuring security in the country. It is obvious that after so much delayed drafting, we can state that in tackling strategy, a considerable uncertainty has emerged. The recommendation for draft revision by the new officials required has seen slow implementation, and, again, one of the reasons for that is, in part, a lack of clear awareness of the urgency of the issues to be addressed by the law and that these issues have a direct relationship with national cybersecurity problems. In other countries without national strategies, the situation is connected with increasingly complex and rapidly changing social, political, and economic conditions. However, in Azerbaijan, political conditions are stable and unchangeable, so there is a stable situation.

The analysis's findings indicate that capacity development and infrastructure development should be balanced against strategy and legislation. Authorities should conduct periodic reviews of the effectiveness of their cybersecurity policies and strategies. The devastating effect of cyberattacks has endangered the national security strategies of many countries, including Azerbaijan. The traditional national security framework of Azerbaijan requires its own cyber-reforms by incorporating new security mechanisms in order the secure the rapidly increasing e-infrastructure of the state.

In conclusion, the combination of cyber laws, technological advancement, adoption of adequate security standards, establishment of cybersecurity centers, and strengthening of the security apparatus can help Azerbaijan develop a cyber-shield capable of effectively countering adverse cyberattacks and enhancing the country's position in the growing global cyberspace.

8. LIST OF ANNEXES

8.1. Demographics

Table 1: Sample profile of survey

Economic region	Frequency	Valid Percent
Baku	400	25,0
Absheron	100	6,3
Gence-Qazax	220	13,8
Sheki-Zaqatala	120	7,5
Lankaran	160	10,0
Quba-Xacmaz	100	6,3
Aran	360	22,5
Daglıq Shirvan	60	3,8
Yuxarı Qarabag	80	5,0
Total	1600	100,0
Settlement type		53,7
Urban		46,3
Rural		
Gender	788	49,3
Male	812	50,7
Female		
Education	7	0,4
No qualifications	331	20,7
Vocational/ Professional Education	99	6,2
Middle school	734	45,9
High school	385	24,1
Bachelor’s Degree	35	2,2
Master’s Degree	7	0,4
Doctoral studies	1	0,1
Postdoctoral studies	1	0,1
Dont know /prefer not to say		
Age		
18-24	201	12,5
25-34	366	22,8
35-44	474	29,6
45-54	285	17,8
55-65	274	17,1

Table 2: Sample profile of focus groups

Results focus group - IT experts & NGO		
		Gender
	30	Male
	35	Male
	30	Male
	35	Male
	31	Male
	53	Male
	50	Male
	45	Male
	Group 1 (18-21) results	
	18	Male
	20	Male
	21	Female
	19	Male
	20	Male
	19	Female
	22	Male
	20	Female
	19	Male
	19	Female
	Group 2 (22-35) results	
	25	Male
	23	Female
	27	Male
	32	Male
	35	Female
	33	Female
	24	Female
	26	Male
	Group 3 (36-65) results	
	55	Female
	35	Female
	45	Male
	40	Female
	39	Female
	50	Male
	38	Female
	38	Male
	Law enforcement/NGO	
	NA (not applicable)	Male
	NA	Male

	NA	Male
	NA	Male
	NA	Male
	NA	Male
	NA	Male
	NA	Female
	ISP	
	NA	Male
	NA	Male
	NA	Male
	NA	Male
	NA	Male
	NA	Male
	NA	Male
	NA	Male
	NA	Male
	Victims	
	54	Male
	65	Female
	45	Male
	40	Male
	29	Female

Table 3: Group composition and duration of discussions

	Group type	Group size	Duration	Gender	
Group 1	General population (18-21)	10	1 h 00 mins	6 M	4 F
Group 2	General population (22-35)	8	1 h 16 mins	4 M	4 F
Group 3	General population (36-65)	8	1 h 15 mins	3 M	5 F
Group 4	Victims	6	45 mins	2 M	4 F
Group 5	ISP	9	1 h 40 mins	9 M	0 F
Group 6	Law enforcement	8	3 h 14 mins	7 M	1 F
Group 7	IT and information security experts/ human right lawyers/advocate	8	1 h 38 mins	8 M	0 F
Average duration					
Total		57	73 mins / 14 secs		

8.2. Organisational Info

8.3. Questionnaire

CYBER SECURITY AND CYBER CRIME BAROMETER QUESTIONNAIRE

Basic Management Information

M-1. Month of the Interview_____

M-2. Date of the Interview_____

M-3. Region_____

1. 2. 3. 4. 5. 6. 7. 8.

M-4. Settlement: 1. Rural Zone 2. Urban Zone

M-5. Code of the region/municipality

1. Capital	9.	17.	25.	33.
2.	10.	18.	26.	34.
3.	11.	19.	27.	35.
4.	12.	20.	28.	36.
5.	13.	21.	29.	37.
6.	14.	22.	30.	38.
7.	15.	23.	31.	39.
8.	16.	24.	32.	40.

M-6. Interviewer Code _____

M-7. Length of the Interview _____

SAMPLE PROCEDURE

1. Once you have selected a household for interview follow the next steps:
2. Select the person who has the birthday closest to the day/month in which the interview is being conducted.
3. In case the selected person refuses to be interviewed or someone obstructs the interview, the attempt should be stopped and you should continue in the other household.
4. Ask about the names, gender and age of family members who are over 18 years old. When this is done ask about their birthday too:

No.	Initials	Gender	Age	Birthday (dd/mm/yy)
1.				
2.				
3.				

4. _____ _____ _____ _____ _____
5. _____ _____ _____ _____ _____
6. _____ _____ _____ _____ _____
7. _____ _____ _____ _____ _____
8. _____ _____ _____ _____ _____
9. _____ _____ _____ _____ _____

How to introduce ourselves?

Good morning / Good Afternoon

I am _____ and work for the _____. We are an independent project and do not represent governmental, political or international bodies.

First, thank you for accepting to take part in this research. The purpose of this research project is to collect data on national attitudes towards cybersecurity and cybercrime. This is a research activity being conducted in the framework of the Cyber East and Cybersecurity East project, a joint activity of the Council of Europe and the European Union.

Your participation in this survey is voluntary. You can choose not to participate. If you decide to participate in this survey, you have the option of withdrawing at any time. The procedure involves providing answers to the survey questions that will take approximately 30 – 40 minutes.

The projects will treat all personal information with strict confidentiality and in accordance with EU's General Data Protection Regulation (GDPR) and national data protection legal framework. Only the company and the projects that collect data will have temporary access to your contact information. Your name and other contact information will be deleted before the survey data is published and no later than 2 February 2022. All your responses are confidential. Any personal identification data is stored separately from the rest of your responses. Rest assured: these results are only used on an aggregate level and for research purposes only. There is no link between your answers and your identity!

Results of the surveys will be shared only with your respective country (regional publication will be discussed separately) and are meant to be used to further contribute to other reporting efforts (e.g. IOCTA) as well as for shaping future policies, strategies and capacity building responses on cybercrime, cybersecurity and electronic evidence in the near and mid-term.

If you agree with these conditions, please check (or say) YES to proceed.

Thank you very much!

Technographics intro

Q1. Do you in your household have access to the internet? **DO NOT READ**
a. Yes
b. No
c. Do not know/ Refuse to answer (do not read: for the purpose of database only)

Q2. Do you regularly use for personal needs any of the following devices? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED**
a. Smartphone
b. Tablet
c. Laptop
d. Desktop
e. Smart TV
f. Game Console
g. Other: […….....] WRITE DOWN ANSWER
h. Do not know/ Refuse to answer

Q3. How much of your personal time in a day do you spend on your devices, ONLINE and OFFLINE? – please estimate the total time for all – smartphone, tablet, computers
a. Less than one hour
b. 1 to 2 hours
c. 2 to 3 hours
d. 3 to 4 hours
e. 4 to 5 hours
f. 5 to 6 hours
g. 6 to 7 hours
h. 7 to 8 hours
i. 8 to 9 hours
j. 9 to 10 hours
k. More than 10 hours

Q4. How much of your personal time in a day do you spend ONLINE on your devices? – please estimate the total time for all – smartphone, tablet, computers
a. Less than one hour
b. 1 to 2 hours
c. 2 to 3 hours
d. 3 to 4 hours
e. 4 to 5 hours
f. 5 to 6 hours
g. 6 to 7 hours
h. 7 to 8 hours
i. 8 to 9 hours
j. 9 to 10 hours
k. More than 10 hours

Q5. What are the activities you do online regularly? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED**
COMMUNICATION
a. Sending / receiving E-mails
b. Online Communication (including video calls) over the internet (e.g. via Zoom, Skype, Messenger, WhatsApp, Facetime, Viber, Snapchat etc.)
c. Participating in social networks (e.g. creating user profile, posting messages or other

contributions to Facebook, Twitter, Instagram, Snapchat, TikTok etc.)

ACCESS TO INFORMATION

d. Finding information about goods, work, or services

e. Reading online news sites / newspapers / news magazines

CREATIVITY

f. Sharing or publishing self-created videos, photos, music, texts etc. on a website or via app

USE OF ENTERTAINMENT

g. Listening to music (music streaming) or downloading music (e.g. Spotify, Apple Music, YouTube music etc.)

h. Watching internet-streamed TV (live or catch-up) from TV broadcasters (e.g. [national examples])

i. Watching Video on Demand from commercial services (e.g. Netflix, HBO GO, Amazon Prime etc.)

j. Watching video content from sharing services (e.g. YouTube, TikTok, Facebook, Instagram etc.)

k. Playing or downloading games

OTHER ON-LINE SERVICES

l. Online shopping via a website or app (e.g. local apps, Amazon, EBay, AliExpress, etc.)

m. Online Banking

n. E-government services

General Usage and Attitudes 1

Q6. Are you familiar with the word cybercrime?

a. Yes

b. No

c. Do not know / Refuse to answer

For this interview, cybercrime refers to the criminal activity that either targets or abuses a computer, a computer network, or a networked device.

Q7. After hearing this definition, please tell us with which of these statements do you agree more:

a. Cybercrime is rather rare and usually happens predominantly to businesses and / or individuals that are somehow involved with dubious activities; it is not a serious risk for 'normal' people.

b. Cybercrime is a real threat to people's welfare and wellbeing and nowadays everyone is at risk at becoming a target.

Q8. What do you generally do to protect yourself from cybercrime? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-c**

a. I am being careful with what I do when I am using my devices (e.g. do not open suspicious mail etc.) **CONTINUE @ 9**

b. I restrict access to my devices (e.g. using passwords etc). **CONTINUE @ 10**

c. I use security software (e.g. antivirus/anti-malware etc.) **CONTINUE @ 11**

d. None of the above **CONTINUE @ 12**

e. Do not know / Refuse to Answer

Q9. ASK ONLY FOR 8.a Which of the following behaviors do you employ regularly when you are careful when using your devices? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-f**

a. I delete suspicious messages
b. I open suspicious messages, but I do not reply to them and do not click on their contents if they do not seem authentic
c. I avoid / do not use suspicious sites
d. I avoid / do not use sites that may be involved in distributing illegal or pirated content
e. I avoid / refuse giving any of my personal data to third parties
f. I do not use free wireless networks
g. None of the above
f. Do not know / Refuse to Answer

Q10. ASK ONLY FOR 8.b How do you usually restrict access to your personal devices? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-d**
a. Password
b. PIN
c. Biometrics – fingerprint, face recognition
d. Two-factor authentication/two-steps login (accessing through two authorization methods - e.g. password + SMS or Call)
e. None of the above
f. Do not know / Refuse to Answer

Q11. ASK ONLY FOR 8.c On what devices do you currently have security software installed? READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-d
a. Smartphone
b. Tablet
c. Laptop
d. Desktop
e. None of the above
f. Do not know / Refuse to Answer

Q12. ASK ONLY FOR 8.d Is there a reason why you don't use any of these means of protection from cybercrime? (If so: what is the reason?) **OPEN ANSWER**
a. [……] **WRITE DOWN ANSWER**

Q13. Have you ever been targeted by an attempt of what you felt, then, was computer / online criminal activity?
a. Yes
b. No
c. Do not know / Refuse to Answer

Q14. Do you feel that the COVID-19 pandemic has exacerbated cybercrime against citizens of [country]?
a. Yes
b. No
c. Do not know / Refuse to Answer

Phishing

Q15. Over the past 12 months, have you been reached out / contacted by someone pretending to be a representative of a technology company, with an offer of live service?
a. Yes
b. No
c. Do not know / Refuse to Answer

Q16. Are you familiar with the word phishing?
a. Yes
b. No
c. Do not know / Refuse to Answer

For this interview, phishing is when criminals use remote contacting to impersonate other parties – through phone, e-mail, text messages or social networks. The criminals pretend to be someone else and will attempt to trick the recipient into installing malicious software or sending them money or private information.

Q17. After hearing this definition, have you ever heard of this type of crime happening?
a. Yes
b. No **CONTINUE @ 22**
c. Do not know / Refuse to Answer **CONTINUE @ 22**

Q18. Over the past 12 months, have you received any phishing message or call?
a. Yes
b. No **CONTINUE @ 22**
c. Do not know / Refuse to Answer C**ONTINUE @ 22**

Q19. Please indicate in which of the following ways you may have received any phishing messages over the past 12 months, on any of your personal devices or accounts? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED**
a. e-mail
b. text message on phone (e.g. Sms, iMessage etc.)
c. app conversation on phone (e.g. WhatsApp, Telegram, Signal etc.)
d. social media (e.g. Facebook, Instagram, TikTok etc.)
e. voice or video call
f. unanswered call from a strange number (trying to get recipient to call back)
g. other [.....] **WRITE DOWN ANSWER**
h. Do not know / Refuse to Answer

Q20. Over the past 12 months, have you ever trustingly engaged with such a message? This could mean: have a trusting conversation with the originator, but also clicking on a link or installing software they sent. **READ CHOICES**
a. Yes
b. No
c. Do not know / Refuse to Answer

Q21. On a scale of 1 to 4, how deeply has phishing (as discussed before) affected your life over the past 12 months? **READ CHOICES**
a. 1 = not affected me at all
b. 2 = it has been a nuisance
c. 3 = it has distressed me
d. 4 = it has negatively impacted my life
e. Do not know / Refuse to Answer

Q22. If someone in your neighborhood would receive such a phishing message, and perhaps trustingly engage with it, do you think they would report it to the [authorities/police]? **READ CHOICES**
a. Yes, I think they would
b. Yes, but only the serious cases
c. No, they would not report it
d. Do not know / Refuse to Answer

Q23. Which one of the following better describes how you feel about the phishing criminal activities here in [country]? R**EAD CHOICES**
a. 1 = Not concerned at all
b. 2 = Somewhat concerned
c. 3 = Neither not concerned nor concerned
d. 4 = Concerned
e. 5 = Very concerned
f. Do not know / Refuse to Answer

Q.24 Do you feel you know enough about phishing to protect yourself and your family? **READ CHOICES**
a. Yes
b. No
c. Do not know / Refuse to Answer

Ransomware

Q25. Are you familiar with the word ransomware?
a. Yes
b. No
c. Do not know / Refuse to Answer

For this interview, ransomware is an illegal application that criminals use to block access to computers, mobile phones and to the data and photos that they may contain. The criminals will then ask the victim for money to release the computer, mobile phone, data or photos.

Q26. After hearing this definition, have you ever heard of this type of crime happening?
a. Yes
b. No **CONTINUE @ 29**
c. Do not know / Refuse to Answer **CONTINUE @ 29**

Q27. Do you personally know anyone who, over the past 12 months, has fallen victim to ransomware? **READ CHOICES, MULTIPLE ANSWERS**
a. Yes, someone in my family
b. Yes, someone else I know
c. Yes, it happened to me
d. No **CONTINUE @ 29**
e. Not sure **CONTINUE @ 29**
f. I would rather not say **CONTINUE @ 29**
g. Do not know / Refuse to Answer **CONTINUE @ 29**

Q28. I am sorry to hear this. I have one very technical question about this. Do you happen to know the type(s) of ransomware involved? **OPEN ANSWER**
a. [……] **WRITE DOWN ANSWER**

Q29. Let's imagine a ransomware attack happened to someone in your neighborhood and they lost access to their computer, their mobile phone, or to the data or photos that they contained. Do you think the victim would report it to the [authorities/police]? **READ CHOICES**
a. Yes, I think they would
b. Yes, but only the serious cases
c. No, they would not report it
d. Do not know / Refuse to Answer

Q30. Let's say for a minute, that a ransomware attack happened to you. Your favorite computer, phone, data or photos would be permanently inaccessible, unless you pay a significant amount of money. On a scale of 1-4, how deeply would this affect you? **READ CHOICES**
a. 1 = not affected me at all
b. 2 = it has been a nuisance
c. 3 = it has distressed me
d. 4 = it has negatively impacted my life
e. Do not know / Refuse to Answer

Q31. Which one of the following better describes how you feel about the ransomware criminal activities here in [country]? **READ CHOICES**
a. 1 = Not concerned at all
b. 2 = Somewhat concerned
c. 3 = Neither not concerned nor concerned
d. 4 = Concerned
e. 5 = Very concerned
f. Do not know / Refuse to Answer

Q32. Do you feel you know enough about ransomware to protect yourself and your family? **READ CHOICES**
l. Yes
m. No
n. Do not know / Refuse to Answer

Intimidation and abuse

I have a few questions in front of me about online intimidation and abuse. I won't ask about any details. Still, please don't feel any obligation to answer.

Q33. Would you be willing to answer a few questions about intimidation and abuse? **READ CHOICES**
d. Yes
e. No **CONTINUE @ 39**
f. Do not know / Refuse to Answer **CONTINUE @ 39**

Q34. Some online interactions can be very intimidating. Has anyone that you personally know been insulted, bullied, blackmailed, or intimidated online, in the past 12 months?
a. Yes, someone in my family
b. Yes, someone else I know
c. Yes, it happened to me
d. No
e. Do not know / Refuse to Answer

Q35. In the past 12 months, have you yourself witnessed any online promotion of hatred, discrimination, or violence against people of a certain race, color, descent or origin?
o. Yes
p. No
q. I would rather not say
r. Do not know / Refuse to Answer

Q36. Unfortunately, the internet can sometimes be an unsuitable place for minors. Do you think [authorities/police] should do more to protect them online? **READ CHOICES**
a. Yes
b. No
c. I would rather not say
d. Do not know / Refuse to Answer

Q37. I have asked you a few questions about online intimidation and abuse. If someone in your neighborhood fell victim to such crimes, do you think they would report it to the [authorities/police]? **READ CHOICES**
a. Yes, I think they would
b. Yes, but only the serious cases
c. No, they would not report it
d. Do not know / Refuse to Answer

Q38. On a scale of 1 to 4, how deeply have online intimidation or abuse affected your life over the past 12 months? **READ CHOICES**
a. 1 = not affected me at all
b. 2 = it has been a nuisance
c. 3 = it has distressed me
d. 4 = it has negatively impacted my life
e. Do not know / Refuse to Answer

Q39. Which one of the following better describes how you feel about the online intimidation and abuse criminal activities here in [country]? **READ CHOICES**
s. 1 = Not concerned at all
t. 2 = Somewhat concerned
u. 3 = Neither not concerned nor concerned
v. 4 = Concerned
w. Very concerned
x. Do not know / Refuse to Answer

Q40. Do you feel you know enough about online intimidation and abuse to protect yourself and your family? **READ CHOICES**
a. Yes
b. No
c. Do not know / Refuse to Answer

Interference (services made unavailable)

Sometimes, online services can be unreachable due to a malfunction. At other times, criminals are blocking access to them.

Q41. In the past 12 months, has any of the online services that you rely on been unexpectedly unreachable for a prolonged time? **READ CHOICES**
a. Yes
b. No
c. Do not know / Refuse to Answer

Data breaches and online identity theft

Q42. In the past 12 months, have you become aware that login credentials to a personal account of yours had been exposed online?

a. Yes
b. No
c. Do not know / Refuse to Answer

Q43. In the past 12 months, have you become aware that YOUR personal account has been accessed, or it was attempted to be accessed, by anyone you did not mean to access it?
a. Yes, and they succeeded
b. It was attempted but they failed
c. No
d. Do not know / Refuse to Answer

Q44. In the past 12 months, have you become aware that any personal data of yours had been deliberately and illegally exposed online?
a. Yes
b. No
c. Do not know / Refuse to Answer

Q45. In the past 12 months, have you become aware that any personal data of yours had been abused, or it was attempted?
a. Yes, and they succeeded
b. It was attempted but they failed
c. No
d. Do not know / Refuse to Answer

Q46. In the past 12 months, have you become aware that any of your bank accounts, online payment accounts or credit card details had been exposed online?
a. Yes
b. No
c. Do not know / Refuse to Answer

Q47. In the past 12 months, have you become aware that any of your bank accounts, online payment accounts or credit card details had been abused by a stranger, or it was attempted?
a. Yes, and they succeeded
b. It was attempted but they failed
c. No
d. Do not know / Refuse to Answer

Q48. In the past 12 months, have you become aware that your personal mobile phone number had been taken over by someone you did not mean to have access to it? [e.g. Somebody received a message or call appearing to be from your mobile phone that you did not send/initiate; or A company (or bank) warned you that your phone number might have been hijacked to try and take over your account with that company (or bank)]
a. Yes, and they succeeded
b. It was attempted but they failed
c. No
d. Do not know / Refuse to Answer

Q49. In the past 12 months, have you found that a phone number or online account of someone you already knew had been taken over, and this person was being impersonated when the account was communicating with you?

a. Yes
b. No
c. Do not know / Refuse to Answer

Q50. We have discussed several ways criminals can try to pretend they are someone else. This is called online identity theft and it is a major component in cybercrime. If someone in your neighborhood falls victim to online identity theft, or to a scam abusing a stolen identity, do you think they would report it to the [authorities/police]. **READ CHOICES**
a. Yes, I think they would
b. Yes, but only the serious cases
c. No, they would not report it
d. Do not know / Refuse to Answer

Q51. On a scale of 1 to 4, how deeply has online identity theft affected your life over the past 12 months? **READ CHOICES**
a. 1 = not affected me at all
b. 2 = it has been a nuisance
c. 3 = it has distressed me
d. 4 = it has negatively impacted my life
e. Do not know / Refuse to Answer

Q52. Which one of the following better describes how you feel about the online identity theft here in [country]? **READ CHOICES**
a. 1 = Not concerned at all
b. 2 = Somewhat concerned
c. 3 = Neither not concerned nor concerned
d. 4 = Concerned
e. 5 = Very concerned
f. Do not know / Refuse to Answer

Q53. Do you feel you know enough about online identity theft to protect yourself and your family? **READ CHOICES**
a. Yes
b. No
c. Do not know / Refuse to Answer

General Usage and Attitudes 2

Q54. Now that we have discussed all these types of cybercrime which one would you say it worries you most? **READ CHOICES**
a. Phishing
b. Ransomware
c. Online intimidation and abuse
d. Interference (services made unavailable)
e. Data breaches and online identity theft
f. Other [.....] **WRITE DOWN ANSWER**
g. Do not know / Refuse to Answer

Q55. Comparing cybercrime with other types of crime present in our society please tell us which one worries you most and which ones worries you the least? **READ CHOICES, RANDOMIZE LIST**
a. Cybercrime

b. Violent crime (e.g. robbery, assault etc.)
c. Property crime (e.g. burglary, auto-theft etc.)
d. White collar crimes (excluding cybercrime - e.g., fraud, bribery etc.)

Q56. On a scale of 1 to 4, how prepared do you feel are the authorities in your country to take on cybercrime?
a. 1 = not ready
b. 2 = rather unprepared
c. 3 = prepared but still work to do
d. 4 = very prepared
e. Do not know / Refuse to Answer

Q57. Looking at the next 5 years, do you expect the cybercrime activities in YOUR country to?
a. Decrease drastically
b. Relatively decrease
c. Relatively increase
d. Increase drastically
e. Do not know / Refuse to Answer

Demographics fade out

D1. What is your gender? **DO NOT READ**
a. Male
b. Female

D2. What is your age? **DO NOT READ**
y. [……] **WRITE DOWN ANSWER**

D3. What is highest level of education you have completed? **READ CHOICES**
a. No qualifications
b. Vocational/ Professional Education
c. Middle school
d. High school
e. Bachelor's Degree
f. Master's Degree
g. Doctoral studies
h. Postdoctoral studies
i. Don't know /prefer not to say **DO NOT READ**

Please end the interview with this statement: "Thank you for participating in this survey. Do you have any questions for us? My supervisor might contact you to confirm if I conducted this interview. Can you give us any of your contact numbers for this purpose? "

Name and Surname: _____

Phone Number: _____

TO BE COMPLETED BY THE INTERVIEWER:

Were any of the questions difficult or sensitive to answer?
1. Yes 2. No
Did the respondents complain about the duration of the interview: _____

'I confirm the accuracy of this interview'
Name and surname _____
Signature _____

TO BE COMPLETED BY THE FIELD SUPERVISOR

Has the process of conducting interview been supervised _____
If yes, in what way?

1. By telephone;
2. Being present during the interview

Name _____
Signature _____

Enterprises

CYBER SECURITY AND CYBER CRIME BAROMETER QUESTIONNAIRE

Basic Management Information

M-1. Month of the Interview_____

M-2. Date of the Interview_____

M-3. Region_____

1. 2. 3. 4. 5. 6. 7. 8.

M-4. Size of the Enterprise: 1. Large 2. Medium 3. Small

M-5. Code of the region/municipality_____

1. Capital	9.	17.	25.	33.
2.	10.	18.	26.	34.
3.	11.	19.	27.	35.
4.	12.	20.	28.	36.
5.	13.	21.	29.	37.
6.	14.	22.	30.	38.
7.	15.	23.	31.	39.
8.	16.	24.	32.	40.

M-6. Interviewer Code_____

M-7. Length of the Interview_____

How to introduce ourselves?

Good morning / Good Afternoon
I am _____ and work for the _____. We are an independent project and do not represent governmental, political or international bodies.

First, thank you for accepting to take part in this research. The purpose of this research project is to collect data on national attitudes towards cybersecurity and cybercrime. This is a research activity being conducted in the framework of the Cyber East and Cybersecurity East project, a joint activity of the Council of Europe and the European Union.

Your participation in this survey is voluntary. You can choose not to participate. If you decide to participate in this survey, you have the option of withdrawing at any time. The procedure involves providing answers to the survey questions that will take approximately 30 – 40 minutes.

The projects will treat all personal information with strict confidentiality and in accordance with EU's General Data Protection Regulation (GDPR) and national data protection legal framework. Only the company and the projects that collect data will have temporary access to your contact information. Your name and other contact information will be deleted before the survey data is published and no later than 2 February 2022. All your responses are confidential. Any personal identification data is stored separately from the rest of your responses. Rest assured: these results are only used on an aggregate level and for research purposes only. There is no link between your answers and your identity!

Results of the surveys will be shared only with your respective country (regional publication will be discussed separately) and are meant to be used to further contribute to other reporting efforts (e.g. IOCTA) as well as for shaping future policies, strategies, and capacity building responses on cybercrime, cybersecurity and electronic evidence in the near and mid-term.

If you agree with these conditions, please check (or say) YES to proceed.

Thank you very much!

Organizational Intro & Info

Q1. In which sector is your company active? **READ CHOICES**
a) Finance
b) Telecommunication
c) Energy
d) Automotive
e) Logistics and Transport
f) Manufacturing
g) Retail
h) Information Technology (Hardware, Software, Services)
i) Food
j) Healthcare
k) Real Estate
l) Other […] **WRITE DOWN ANSWER**
m) Do not know / Refuse to Answer

Q2. Does the CORE STAFF in your company/enterprise has access to the internet for business purposes? (this includes a fixed line and/or a mobile connection) **DO NOT READ**
a. ,Yes
b. No
c. Do not know / Refuse to Answer

Q3. Does your company/enterprise use any type of fixed line connection to the internet? (ADSL, SDSL, VDSL, fiber optics technology (FTTP), cable technology, etc.) **DO NOT READ**
a. Yes
b. No
c. Do not know / Refuse to Answer

Q4. What is the maximum contracted download speed of the fastest fixed-line internet connection of your enterprise? **READ CHOICES**
a. less than 30 Mbit/s

b. at least 30 but less than 100 Mbit/s
c. at least 100 Mbit/s but less than 500 Mbit/s
d. at least 500 Mbit/s but less than 1 Gbit/s
e. at least 1 Gbit/s
f. Do not know / Refuse to Answer

Q5. Does your enterprise allow a mobile connection to the internet using mobile telephone networks, for business purposes? **DO NOT READ**
a. Yes
b. No
c. Do not know / Refuse to Answer

Q6. Does your enterprise use any of the following online tools? **READ CHOICES/ MULTIPLE ANSWERS**
a. A corporate website
b. Social networks (e.g., LinkedIn, Facebook, TikTok, Odnoklassniki, Vkontakte, Xing, etc.)
c. Enterprise's blog or microblogs (e.g., Twitter, etc.)
d. Multimedia content sharing websites or apps (e.g., YouTube, Flickr, SlideShare, Instagram, Pinterest, Snapchat etc.)
e. Wiki based knowledge sharing tools
f. Other: […] **WRITE DOWN ANSWER**
g. Do not know / Refuse to Answer

Cybersecurity role

Q7. Does your company have a dedicated organizational role / department in charge of cybersecurity? **READ CHOICES**
a. Yes, a dedicated department
b. Yes, but as part of another department
c. Yes, one or two job roles
d. Other: […] WRITE DOWN ANSWER
e. No
f. Do not know / Refuse to Answer

Q8. Does your company (also) outsource some of the services needed to manage cybersecurity? **READ CHOICES**
a. Yes, some elements that cannot be covered inhouse
b. Yes, all cybersecurity issues
c. No
d. Do not know / Refuse to Answer

Q9. Approximately, what percentage of your IT-budget was spent on cybersecurity in the last 12 months? **READ CHOICES**
a. 0%
b. 1 - 4%
c. 5 - 9%
d. 10 - 20%
e. > 20%
f. Do not know / Refuse to Answer

Q10. What is your yearly spending on cybersecurity insurance(s) in percentage of your IT budget? **READ CHOICES**

a. have no cybersecurity insurance
b. 1 - 4%
c. 5 - 9%
d. 10 - 20%
e. > 20%
f. Do not know / Refuse to Answer

Q11. Does your company follow any security frameworks or standards? **READ CHOICES, MULTIPLE ANSWERS**
a. ISO 27000
b. ITIL
c. COBIT
d. The company does not follow any security framework
e. Other […] **WRITE DOWN ANSWER**
f. Do not know / Refuse to Answer

Q12. Which of the following does your business currently use? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. Website for your business
b. Social media accounts for your business
c. E-commerce platforms and solutions
d. Web-based application
e. Open-source software
f. Cloud computing or storage CONTINUE @13
g. Internet-connected smart devices or Internet of Things (IoT)
h. Intranet
i. Blockchain technologies
j. Cryptocurrencies (such as bitcoin)
k. Voice over Internet Protocol (VoIP) services
l. Video / live communication and conferencing
m. Business does not use any of the above
n. Do not know / Refuse to Answer

Q13. ASK ONLY FOR 12f. What type of data does your business store – on cloud computing or storage services? Include data that are backed-up. **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. Confidential employee information
b. Confidential information about customers, suppliers, partners or other third parties
c. Confidential business information
d. Commercially sensitive information
e. Non-sensitive or public information
f. Business does not store data on cloud computing or storage services
g. Do not know / Refuse to Answer

Q14. Does anyone in your business use personally owned devices such as smartphones, tablets, laptops, or computers to carry out regular business-related activities? **READ CHOICES**
a. Yes, all the time
b. Yes, but rarely, as an exception
c. No
d. No, and this is explicitly forbidden by company policy
e. Do not know / Refuse to Answer

General Priority and Confidence

Q15. How do you rank cybersecurity within your company? [In the NIST Cybersecurity Framework, there are Five Functions: Identify, Protect, Detect, Respond and Recover - They represent the five primary pillars for a successful and holistic cybersecurity program. In addition, they aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions.] **READ CHOICES**
a. Cyberattacks are the top risk for my company
b. Cyberattacks are among the 5 the top risks for my company
c. Cyberattacks are a low risk for my company
d. Cyberattacks are not at all a risk for my company
e. Do not know / Refuse to Answer

Q16. How does your Company comply with the critical areas of cybersecurity? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED FOR a-c**
My company is:
a. understanding and assessing cyber risks
b. preventing cyber threats from being realized
c. responding to and recovering from cyber events
d. not affected by cyber risks
e. Do not know / Refuse to Answer

Q17. Which cybersecurity technologies do your business currently have in place? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. Mobile security
b. Anti-malware software to protect against viruses, spyware, ransomware, etc.
c. Web security, such as (D)DoS mitigation services
d. E-mail security, spam/phishing protection
e. Network security, such as firewalls, Intrusion Prevention Detection Systems
f. Data protection and control
g. Point-Of-Sale (POS) security
h. Software and application security, including vulnerability management
i. Hardware and asset management
j. Identity and access management
k. Physical access controls
l. Log files are inspected regularly
m. VPN
n. Data backup to separate location
o. Business does not have any cybersecurity measures in place
p. Other […] **WRITE DOWN ANSWER**
q. Do not know / Refuse to Answer

Awareness Raising

Q18. Does your company provide employee training to raise information security awareness? **READ CHOICES**
a. Yes, according to job role and function
b. Yes, but only where mandated by law/regulations
c. Other […] **WRITE DOWN ANSWER**
d. No
e. Do not know / Refuse to Answer

Q19. What do you think will help improve your organization's security levels? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. Senior management commitment
b. Larger budgets
c. Increased security department staff numbers
d. Better employee security awareness
e. Advanced security technology
f. Other […] **WRITE DOWN ANSWER**
g. Do not know / Refuse to Answer

Q20. What are your organization / enterprise major challenges or barriers to an effective cyber risk management? **READ CHOICES**
a. Lack of mandate
b. Lack of resources
c. Lack of support by executives
d. Prioritization
e. Other […] **WRITE DOWN ANSWER**
f. Do not know / Refuse to Answer

Authentication and Encryption

Q21. What kinds of encryption strategy does your company employ? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED FOR a-d**
a. File encryption on laptops
b. File encryption on smartphones
c. File encryption on data in the cloud
d. Other […] **WRITE DOWN ANSWER**
e. My company does not employ any encryption strategy
f. Do not know / Refuse to Answer

Q22. Does your company have a Data Loss Prevention solution in place? **DO NOT READ**
a. Yes
b. No
c. Do not know / Refuse to Answer

Q23. Does your company use Two-Factor Authentication? **READ CHOICES**
a. Yes, deployed to most / all users
b. Yes, deployed to a minority of users
c. We are considering / planning to deploy it
d. No
e. Do not know / Refuse to Answer

Supply Chain

Q24. How does your company rate the cybersecurity risk to its supply chain? **READ CHOICES**
The cyber risk imposed by the supply chain partners and vendors is considered to be
a. very high
b. high
c. low
d. none
e. Do not know / Refuse to Answer

Q25. How does your company ensure an adequate and appropriate level of information security over third parties? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. Identifies risks related to third parties as part of information risk assessments
b. Addresses information security issues in a contract
c. Signs confidentiality and/or non-disclosure agreements
d. Imposes corporate security policy and controls on third parties
e. Where permitted, performs background verification checks
f. Controls third-party access to systems and data
g. Regularly monitors and reviews third party services
h. None of the above
i. Other […] **WRITE DOWN ANSWER**
j. Do not know / Refuse to Answer

Government role

Q26. Do cyberattacks by nation-state actors affect your business? **DO NOT READ**
a. Yes
b. No
c. Do not know / Refuse to Answer

Q27. In your experience, Government regulations, laws and industry standards meant to improve managing cyber risks are being:
a. very effective
b. somewhat effective
c. not effective
d. even counter-effective sometimes
e. Do not know / Refuse to Answer

Cybercrime state of affairs

Q28. Do you feel that the COVID-19 pandemic has exacerbated cybercrime against enterprises in [country]? **DO NOT READ**
a. yes
b. no
c. Do not know / Refuse to Answer

Q29. In the past 12 months, have criminals obtained and/or abused payment information from your company or its customers? **DO NOT READ**
a. yes
b. no
c. Do not know / Refuse to Answer

Q30. Over the past 12 months, has your business been affected by deliberate DDoS attacks? **DO NOT READ**
a. Yes: we couldn't rely on services that we need
b. Yes: we couldn't deliver services that we provide
c. No
d. Do not know / Refuse to Answer

Q31. Do you consider ransomware to be a business risk? [Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert.] READ CHOICES

a. Significant business risk
b. Less business risks
c. It is overhyped
d. Do not know / Refuse to Answer

Q32. Do you consider business e-mail compromise (CEO Fraud) a business risk? [CEO Fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wire-transfers, or sending out confidential tax information.] **READ CHOICES**
a. Significant business risk
b. Less business risks
c. It is overhyped
d. Do not know / Refuse to Answer

Q33. In the past 12 months, how many times has your company been victim of cyber-crime? **READ CHOICES**
a. never **CONTINUE @ 36**
b. 1 time
c. 2-5 times
d. more than 5 times
e. Do not know / Refuse to Answer

Q34. ASK ONLY FOR 33b-33d. Over the past 12 months, which types of cybercrime have affected your organization? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. DDoS Attack/Interference
b. Hacking attempt
c. Phishing Email
d. Malware & Trojans
e. Spyware / Stealth software
f. Fraudulent Emails (e.g. CEO Fraud)
g. Helpdesk / Tech scam
h. Ransomware
i. CEO Fraud (business e-mail compromise)
j. Identity Theft
k. Other […] **WRITE DOWN ANSWER**
l. Do not know / Refuse to Answer

Q35. ASK ONLY FOR 34a-34j. How did the crime(s) affect the organization? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. Website or other online services were taken offline
b. Information being leaked in relation to the organization
c. Funds were transferred to an unknown bank account
d. Unintended payments were made
e. Information about IP or staff were leaked online
f. Personal data was leaked
g. Blackmail attempt was made
h. Do not know / Refuse to Answer

Q36. What do you think is the motivation of cyber criminals? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
a. Financial gain
b. Fraudulent activity

c. Defamation
d. Disruption
e. For fun
f. Espionage
g. Stately attack
h. Other […] **WRITE DOWN ANSWER**
i. Do not know / Refuse to Answer

Q37. Over the past 12 months, how much money has your organization lost due to cybercrime? **READ CHOICES**
a. none
b. < 0.1% of our yearly revenue
c. < 1.0% of our yearly revenue
d. < 10% of our yearly revenue
e. < 100% of our yearly revenue
f. more than our yearly revenue
g. Do not know / Refuse to Answer

Q38. Over the past 12 months, what impact has your organization suffered from cybercrime? **READ CHOICES**
a. none
b. it was a nuisance
c. it has impeded our processes
d. it has seriously impacted our business
e. Do not know / Refuse to Answer

Q39. Over the past 12 months, have criminals tried to extort money from your company through cybercrime? **READ CHOICES**
a. YES, via Ransomware: blocking access to devices
b. YES, via Ransomware: encrypting data
c. YES, buy threatening to publish stolen data
d. YES, by asking for money to stop a prolonged DDoS attack
e. YES, by exploitation of sensitive personal images
f. Other […] **WRITE DOWN ANSWER**
g. NO
h. Do not know / Refuse to Answer

Q40. ASK ONLY FOR 39a-39f If so, how much money went to the criminals? **READ CHOICES**
a. none
b. < 0.1% of our yearly revenue
c. < 1.0% of our yearly revenue
d. < 10% of our yearly revenue
e. < 100% of our yearly revenue
f. more than our yearly revenue
g. Do not know / Refuse to Answer

Q41. In the event of a potential or successful attack, would the organization contact Law Enforcement for assistance and/or to investigate or stop the source of the attack? **DO NOT READ**
a. Yes **CONTINUE @ 43**
b. No **CONTINUE @ 42**
c. Do not know / Refuse to Answer **CONTINUE @ 43**

Q42. ASK ONLY FOR 41b If No, what is the reason(s)? **READ CHOICES**
a. Don't know who to contact
b. Have not been helpful in the past
c. Handle the issue internally
d. Didn't know this is something they can help with
e. Do not know / Refuse to Answer

Q43. Are there other government or private agencies that you would report any (criminal) cybersecurity incidents to? **READ CHOICES**
a. Private cybersecurity firm
b. Private CERT/CSIRT
c. Sectoral CERT/CSIRT
d. National CERT/CSIRT
e. None
f. Do not know / Refuse to Answer

Q44. Looking at the next 5 years do you expect the cybercrime activities targeting businesses to? **READ CHOICES**
a. Decrease drastically
b. Relatively decrease
c. Relatively increase
d. Increase drastically
e. Do not know / Refuse to Answer

Organizational Info & Fade out

O1. How many people does your company employ? **READ CHOICES**
a. < 10
b. 10 – 99
c. 100 – 500
d. > 500

O2. Approximately what is your company's yearly revenue? **READ CHOICES**
a. < 100,000 €
b. 100,000 – 999,999
c. 1 Mio € - 25 Mio €
d. > 25 Mio €
e. Do not know/ Refuse to Answer

Please end the interview with this statement: “Thank you for participating in this survey. Do you have any questions for us? My supervisor might contact you to confirm if I conducted this interview. Can you give us any of your contact numbers for this purpose? ”

Name and Surname: _____

Phone Number: _____

TO BE COMPLETED BY THE INTERVIEWER:

Were any of the questions difficult or sensitive to answer?

1. Yes 2. No

Did the respondents complain about the duration of the interview: _____

‘I confirm the accuracy of this interview’

Name and surname _____

Signature _____

TO BE COMPLETED BY THE FIELD SUPERVISOR

Has the process of conducting interview been supervised _____

If yes, in what way?

1. By telephone;
2. Being present during the interview

Name _____

Signature _____

NOTES

A Joint Project of The European Union,
The Council of Europe and The Social Research Center

CYBERCRIME AND CYBERSECURITY BAROMETER IN AZERBAIJAN
Regional quantitative and qualitative analysis of the attitude towards cybercrime and online security.

Editor: Nailakhanim Rustamova
Designer: Qurban Jalilov
Babak Jafar

Address:
Republic of Azerbaijan, AZ 1073, Baku city,
Yasamal district, Ismayil bey Kutkashinli street, 18.
Social Research Center

Phone: (+994 12) 510-70-78
(+994 12) 510-23-75
(+994 12) 510-70-69

Email: info@stm.az
Internet address: www.stm.az

Anchor signed:
Physical print sheet:
Order:
Circulation: 500

It was printed in the printing house of "MM-S" enterprise.
Address: Republic of Azerbaijan, AZ 1102, Baku city,
Nasimi district, A. Taghizade street, house 13.
Phone: (+994 12) 431 11 00
(+994 50) 314 09 37

Republic of Azerbaijan, AZ 1073, Baku, Yasamal district, Ismayil Kutgashinli str., 18

Phone: (+994 12) 510 70 78; (+994 12) 510 23 75; (+994 12) 510 70 69

info@stm.az www. stm.az