Proceeding
Jogjakarta Communication Conference
Volume 3, No 1, pp. 487-499
ISSN 2988-5523

Analysis of Cyber Security Challenges in Bandar Lampung: Impact on Digitalization, Religion, and Society

Sri Choiriyati*, Immawati Asniar, Mike Meiranti, Ratu Sukma Rupawan

Communication Science Study Program, Universitas Muhammadiyah Lampung, 35142 Indonesia

*Corresponding author's email: srichoiriyaty@gmail.com

Keywords
Cybersecurity; digitalization; religion; society

ABSTRACT

This study aims to identify and analyze the challenges faced in cybersecurity in Bandar Lampung, focusing on its impact on the digital sector, religion, and society. This study uses a qualitative approach through interviews with a number of experts and practitioners in the field of cybersecurity, as well as related literature studies. The results of the study indicate that cybersecurity in Bandar Lampung faces various problems, such as lack of public awareness, lack of clear regulations, and challenges in protecting personal data and digital transactions. This study also found that cyber threats have the potential to disrupt religious activities and social interactions in society. In conclusion, increased awareness, education, and cooperation between the government, religious institutions, and society are needed to overcome these challenges.

1. Introduction

Cybersecurity is an important issue in the digital era, including in Bandar Lampung, which continues to grow in the use of information technology. As digitalization increases in the government, business and social life sectors, the challenges in protecting personal data, online transactions and digital interactions are increasingly complex. In response to this threat, the Lampung Provincial Government has established Computer Security Incident Response Teams (CSIRT) in six districts, including South Lampung, East Lampung and West Lampung. The CSIRT is tasked with preventing, detecting, and handling cybersecurity incidents so that their impact can be minimized.

Apart from the technical side, cybersecurity in Bandar Lampung also has social and cultural dimensions. Social and cultural factors can affect the level of public awareness of cyber threats, which varies from region to region (Davis, M., & Thomas, 2019). With the rapid use of the internet, especially in religious and social activities, there is a risk of misuse of technology that can affect community harmony. Several incidents such as the spread of hoaxes, hacking of religious figures' social media accounts, and theft of personal data have become major concerns. Lampung University (Unila) has even held a special workshop to raise public awareness of cyber threats and the spread of negative content.

Along with the increasing threats to personal data in cyberspace, people in Bandar Lampung need to get a deeper understanding of the importance of maintaining cyber security. (Amin & Patel, 2020). Although efforts to improve cybersecurity continue, challenges remain, especially in the readiness of human resources and supporting regulations. Based on data from the National Cyber and Crypto Agency (BSSN), by 2023 there will be more than 1.3 billion cyber-attacks in Indonesia, most of which target the government and public service sectors. Therefore, the Lampung Provincial

Government emphasized the importance of synergy between local governments, law enforcement officials, and the community in strengthening the cybersecurity ecosystem.

In a social context, digital security is not only limited to data protection, but also cultural adaptation in the use of technology. Public awareness in maintaining digital ethics, avoiding the spread of inaccurate information, and understanding the risks of cybercrime are crucial. Therefore, the approach to cybersecurity in Bandar Lampung should not only focus on technical aspects, but also on educating the public to be better prepared to face challenges in the digital world.This research offers a more comprehensive approach by combining digital, religious and community dimensions to analyze cybersecurity challenges in Bandar Lampung. By identifying broader and deeper issues, this research aims to provide a more thorough understanding of the challenges. It focuses on how cyber threats affect society, social interactions and religious activities in this area, which have often not received enough attention in previous studies.

This research is expected to contribute to creating more effective solutions to cyber threats at the local level. The approach used not only focuses on technical aspects but also considers the social and cultural characteristics of local communities. This is important because the effectiveness of a digital security strategy largely depends on the extent to which people can accept and implement protective measures in their daily lives.

The main objective of this research is to identify the challenges faced by the Bandar Lampung community in dealing with cyber threats. With the rapid development of digital technology in the region, cases such as theft of personal data, hacking of social media accounts, and spreading false information are increasingly prevalent. Therefore, this research also aims to develop policy recommendations that can improve the digital resilience of the community, both through stricter regulations and through increasing awareness of the importance of cybersecurity.

A number of previous studies have discussed steps to address cybersecurity issues through better policies and regulations. Most studies emphasize the importance of establishing a clear and structured legal framework to regulate various aspects of digital protection. Some of the proposed solutions include the implementation of encryption and double authentication technologies to improve the security of online transactions. With these measures in place, the risk of data leakage, which is often the target of cyberattacks, can be minimized. In addition to policy-based approaches, various training and education programs related to cybersecurity have also been implemented in several regions, including in Bandar Lampung. Communities need to be empowered through digital literacy programs to be better prepared to face the growing cyber threats. (Rachmat, W., & Nurhadi, 2021),

For example, Universitas Lampung (Unila) has organized a workshop to raise public awareness about cyber threats and the dangers of spreading negative content. This activity aims to equip individuals with a better understanding of personal data protection and how to recognize the evolving modes of digital crime. In this context, digital literacy is crucial, but previous research has highlighted that many people are still unaware of how to protect their personal data online. (Barker, D., & Lee, 2021)

While there have been many studies addressing policy and technical approaches, most still lack attention to the social and cultural impacts of using digital technologies. Many studies focus more on the technical aspects of personal data protection without considering how local communities and cultures adapt to these developments. In fact, the success of cybersecurity strategies largely depends on the acceptance and implementation of such measures by society.

One of the major shortcomings in previous research is the lack of exploration of how social and cultural factors influence user behavior towards digital security policies. For example, in the religious context, people often utilize digital platforms to share information and discuss religious teachings. However, their lack of digital literacy makes them more vulnerable to the spread of hoaxes or

technology-based extremism propaganda. Therefore, social and cultural factors need to be an integral part of a more comprehensive cybersecurity strategy.

Most previous studies have also relied more on quantitative methods, such as surveys, to measure the level of public awareness of cyber threats. While quantitative data can provide an overview of people's understanding, this approach often lacks depth in exploring the social factors that influence attitudes and behaviors in using digital technology. Therefore, a qualitative approach is needed to better understand how people in Bandar Lampung adapt to cybersecurity challenges in their daily lives.

Critics of previous research also point out that many studies focus only on technology and policy development without considering broader social aspects. Cybersecurity is not just a technical issue, but also relates to individual and collective behavior in a society. Policies that are too technical can be difficult to implement if they are not adapted to the social and cultural values prevailing in a particular community. Therefore, solutions that are more based on the needs of society are needed.

In addition, a lack of awareness of the importance of cybersecurity is often a major obstacle to digital protection. Many people do not realize that simple actions, such as using weak passwords or sharing personal information on social media, can increase the risk of becoming a victim of cybercrime. The role of religious leaders in providing education on digital ethics has proven to be significant in shaping public awareness of personal data protection in Indonesia, including in Bandar Lampung (Putra, F., & Suryadi, 2019). Therefore, more massive and community-based education is needed so that people are better prepared to face digital threats

Taking these factors into account, this research is expected to provide greater insight into how cybersecurity strategies can be tailored to be more effective at the local level. Through a more comprehensive approach-encompassing technological, social and cultural aspects-the resulting solution is expected to be widely implemented by the people of Bandar Lampung. This will not only improve the region's digital resilience but also create a safer and more inclusive digital environment for all.

In addition, most of the previous research has not examined how the religious sector can play a role in increasing community digital awareness and resilience. In many regions, religion has a powerful influence in shaping people's views and attitudes towards a range of issues, including technology and cybersecurity. Research that ignores this role tends to miss the potential for creating more adaptive and locally relevant solutions. Therefore, this research seeks to bridge this gap by integrating social and religious aspects in cyber threat mitigation efforts.

The concept proposed in this research is to look at cybersecurity through a more holistic lens, focusing not only on technology, but also on the social and cultural context of society. This approach aims to engage communities more actively in addressing cyber challenges, taking into account the social and religious factors that might influence how they respond to such threats. By introducing this concept, it is hoped that the resulting solutions can be more easily accepted and applied in people's daily lives, especially in areas that have cultural and religious diversity such as Bandar Lampung.

In addition, by including social and cultural elements in this research, we can expand the scope of a more in-depth analysis of people's behavior towards technology and cyber threats. This approach provides room for people to play a more active role in maintaining digital security, both in a personal and collective context. By taking into account existing religious beliefs and social values, the solutions developed will not only be relevant, but also more easily understood and accepted by the local community.

One of the things that sets this study apart from previous research is the emphasis on the importance of collaboration between the government, private sector and religious institutions in dealing with cyber threats. Previous research tends to focus on more technical solutions and policies, but not much on how to build partnerships between various parties in improving community digital resilience. By introducing a more inclusive approach, it is hoped that this research can pave the way for building more solid cooperation between various elements in society to deal with cyber threats.

The main objective of this research is to explore the challenges faced by the Bandar Lampung community in dealing with cyber threats, taking into account social, cultural and religious aspects. This research aims to provide a deeper understanding of how these three aspects interact with each other and affect the digital resilience of the community. In addition, this research also wants to identify emerging patterns in people's interactions with technology and how they can improve cybersecurity in ways that are more appropriate to the local context.

To achieve this goal, this research uses a qualitative approach with in-depth interviews with various relevant parties, including religious leaders, technology practitioners, and the general public. With this approach, a more holistic understanding of how cybersecurity challenges are faced at the local level is expected, as well as solutions that are more integrated with existing social and cultural conditions. The results of this research are expected to contribute to the development of more effective policies and strategies in dealing with cyber threats in the future, especially in areas that have distinctive social and cultural characteristics such as Bandar Lampung.

2. Method

This research used a survey approach with a qualitative descriptive research design to explore cybersecurity challenges in the digital, religious and community contexts in Bandar Lampung. The survey method was chosen because it allows researchers to collect data directly on people's perceptions and experiences in dealing with cyber threats. This research aims to explore how cyber threats affect the people of Bandar Lampung, especially in relation to digital, social and religious aspects.

This research was conducted in Bandar Lampung, which was chosen due to the rapid development of digital technology and the community's strong interaction with religion. The research subjects consisted of three main groups:

1. General public: Respondents who actively use digital technology in their daily lives.
2. Religious Leaders: Respondents from various religious organizations who have influence in delivering messages about cybersecurity.
3. Cybersecurity Practitioners: Technology and cybersecurity professionals who can provide perspectives on the technical challenges faced by communities at the local level.

The main instruments in this research were in-depth interviews and questionnaires. Interviews were conducted with religious leaders and cybersecurity practitioners to obtain their views on existing challenges related to cybersecurity. Meanwhile, a questionnaire was used to collect data from the general public regarding their understanding and attitudes towards cyber threats. The questionnaire combined closed and open-ended questions that allowed researchers to gather information regarding their awareness, actions and perceptions of digital security

The data collection procedure was carried out in several steps:

1. Preparatory Stage: Researchers conducted a preliminary study to understand the main problems faced by the Bandar Lampung community in the context of cyber threats and determine the right respondents.
2. Data Collection Stage: Interviews with religious leaders and cybersecurity practitioners were conducted face-to-face to gain a deeper understanding. For the general public, questionnaires were distributed both in person and through online platforms to reach more and diverse respondents.
3. Data Validation Stage: Data collected from interviews and questionnaires were validated by triangulation, which is comparing information from various sources to ensure the consistency and accuracy of the data obtained.

Data obtained from interviews and questionnaires will be analyzed using thematic analysis techniques to identify patterns and key themes that emerge in people's responses to cyber threats. Through this method, the researcher will be able to find linkages between various individual experiences in dealing with digital attacks, such as account hacking, data theft or online fraud. In addition, this analysis will also reveal the extent of people's understanding of cybersecurity and the barriers they face in protecting themselves from these threats. By understanding the themes that emerge, this research can provide a deeper picture of the problems faced by the people of Bandar Lampung in the context of the digital world.

The methods used in this study offer a useful contribution to future research, given the simple and flexible approach but still able to provide in-depth insights. This research can serve as a model for further studies in other areas with similar social and cultural conditions. One novelty is the integration of technical and social aspects in addressing cybersecurity challenges, which has not been widely studied in previous research.

In collecting data, this study used tools that are easily accessible and effective. Questionnaires were distributed in digital format through platforms such as Google Forms to facilitate data distribution and collection. All interviews were recorded using high quality digital voice recording devices to ensure the accuracy of the data collected during the interviews.

The novelty of this research lies in the application of a survey method that combines technical and social perspectives. Although the topic of cybersecurity has been extensively researched, most previous studies have emphasized on technical and policy solutions. This research focuses on how social and religious factors influence people's attitudes towards cyber threats. With this approach, this research provides new, more holistic insights, where solutions focus not only on technical aspects but also on deep social and cultural influences.

The methods used in this research are simple enough that they can be applied to other regions facing similar challenges. The results of this study can serve as a reference for further research that wants to examine the same topic in other regions with a more holistic approach and based on the local social and cultural context. Thus, this research can be replicated by other researchers in the future.

Through the use of a survey method combining in-depth interviews and questionnaires, this study managed to explore an in-depth understanding of cybersecurity challenges in Bandar Lampung. This approach provides a broader perspective by involving social and religious aspects in cybersecurity studies. This research offers solutions that are more comprehensive and relevant to local conditions, so they can be applied in other areas that have similar social and cultural characteristics.

3. Result and Discussion

This research aims to identify the challenges faced by the people of Bandar Lampung in dealing with cybersecurity issues, taking into account digital, religious and social factors. The results show some important findings that reflect the problems faced as well as people's attitudes towards cyber threats.

a. General Awareness of Cybersecurity

This research found that Bandar Lampung people's awareness of cybersecurity is still relatively low. Based on the survey results, 65% of respondents only have a basic understanding of the risks of cyber threats. Many of them assume that cyberattacks, such as hacking and identity theft, are more common among large companies than individuals. This lack of understanding shows that there are still many people who do not realize that cyber threats can happen to anyone, including individual internet users who are active on various digital platforms.

However, the study also revealed that the majority of respondents were more concerned about the threat of online fraud that often occurs on social media. Cases such as phishing, investment scams, and other crime modes are considered more dangerous because the impact is directly felt by the community. This phenomenon shows that digital security education needs to focus on threats that are closer to people's daily lives. By increasing understanding through socialization and more practical training, it is hoped that public awareness and readiness in dealing with cyber threats can increase significantly.

b. Understanding of Personal Data Protection

This research reveals that the level of understanding of Bandar Lampung people towards personal data protection in cyberspace is still relatively low. Only around 40% of respondents understand how to protect their personal information when using the internet. Many of them do not know the importance of privacy settings on social media or other digital applications. As a result, their sensitive information, such as addresses, phone numbers and online activity history, are vulnerable to being exposed and utilized by irresponsible parties. This lack of awareness risks increasing the number of personal data abuse cases, such as identity theft and unauthorized dissemination of personal information.

In addition to a lack of understanding about privacy settings, only a small percentage of respondents use security software, such as antivirus or encryption systems, to protect their data. Many internet users still rely on minimal protection methods, such as only changing passwords periodically, without realizing that other measures, such as two-factor authentication and data encryption, are also very important. This highlights the need for further education on practical ways to keep personal data safe in the digital world. With more widespread training and awareness campaigns, the public can better understand and implement effective measures to protect their personal information from increasingly complex cyber threats.

c. The Role of Religion in Raising Cybersecurity Awareness

Religion plays an important role in shaping people's awareness of ethics and responsibility in technology use. Based on the research results, 50% of respondents believe that religious teachings can help them understand how to use technology more wisely. Moral values taught by religion, such as honesty and prudence, often guide how people interact in the digital world. However, while the role of religion is recognized in shaping positive behavior, respondents

also highlighted that guidance from religious leaders on cybersecurity is still very limited. Most religious leaders emphasize the moral aspects of technology use, such as avoiding the spread of fake news or refraining from unethical behavior on social media, but have not provided much insight into technical protection, such as keeping personal data safe or avoiding cyberattacks.

This gap points to the need for further involvement of religious leaders in improving digital literacy among the public. By equipping religious leaders with basic knowledge on cybersecurity, they can play a more active role in providing education that not only focuses on moral values but also includes concrete steps in maintaining digital security. Through lectures, religious discussions and community forums, religious leaders can become agents of change who help people understand how to protect themselves from increasingly complex digital threats. With this approach, cybersecurity education can be delivered in a way that is more in line with the cultural background and values of the community, making it easier to accept and apply in everyday life.

d. Obstacles Faced by the Community

In addition to low awareness of digital security, this study also found that many people find it difficult to understand the technical aspects of cyber protection. As many as 55% of respondents revealed that they often feel confused and anxious when faced with cyber threats, such as identity theft or malware attacks. The lack of understanding of how digital threats work and their prevention measures means that many people prefer to rely on third parties, such as internet service providers or government policies, rather than taking their own initiative to improve their digital security. This indicates a high dependence on external protection, without sufficient effort from individuals to manage the security of their own personal data.

One of the factors that causes this difficulty is the lack of access to practical and easy-to-understand education about cybersecurity. Many of the available educational materials still use technical terms that are difficult for the general public to understand, making them feel intimidated or not interested in learning more. Therefore, a simpler, hands-on, experience-based approach is needed, such as community-based training, guidance in the form of educational videos, or apps designed to help users understand digital security risks in a more interactive way. With this approach, people can more easily understand the importance of cybersecurity and start taking proactive steps to protect themselves from growing digital threats.

e. Challenges Faced by Cybersecurity Practitioners

Cybersecurity practitioners in Bandar Lampung face various challenges in an effort to increase public awareness of digital threats. Based on the interviews conducted, the biggest challenge they encountered was the low level of public understanding of the importance of cybersecurity. As many as 70% of practitioners surveyed stated that the public still lacks adequate education about cyber threats, even though the use of technology continues to increase. The lack of access to training or information on digital protection has led to many individuals not being aware of the risks they face in cyberspace. This creates a significant knowledge gap, where people remain vulnerable to cyberattacks due to a lack of skills in protecting their personal data.

As a solution, cybersecurity practitioners emphasized the need for a more effective and easy-to-understand educational approach for the wider community. Interactive and hands-on experience-based training programs are considered more attractive to the community

compared to learning methods that are too theoretical. In addition, cooperation between the government, academia, and the private sector is considered important to expand the reach of cybersecurity education. By providing educational materials that are more relevant and accessible, it is hoped that the public can be more proactive in securing their personal information from various increasingly complex digital threats.

f. Utilization of Digital Security Programs by the Community

Although various educational programs on digital security are available, public participation in this type of training is still relatively low. Based on the survey results, only 30% of respondents have participated in training or educational programs related to cybersecurity. However, most of them feel that the material presented in these programs is less interesting or not in accordance with daily needs. As a result, few participants actually continued or applied the knowledge they gained after attending the training. Another factor that causes a lack of interest in digital security education is learning methods that tend to be theoretical and difficult for the general public to understand.

To increase the effectiveness of cybersecurity education programs, a more hands-on, experience-based approach needs to be implemented. The public is more interested in training that offers real simulations of how to deal with cyber threats in everyday life. In addition, the use of digital media such as educational videos, interactive webinars, and security-based applications can be a more relevant solution for modern society. In this way, education about digital security can be more easily applied and understood by various community groups, so that they are better prepared to face various threats in cyberspace.

g. Spreading False Information (Hoaxes)

One of the big challenges that the people of Bandar Lampung still face in the digital world is the rampant spread of false information or hoaxes. The survey results showed that 60% of respondents admitted to having been affected by hoaxes circulating on social media. Many of them have difficulty distinguishing valid information from fake news, especially because the spread of hoaxes occurs very quickly on various digital platforms. This unverified information often triggers panic, misunderstanding, or even social conflict in society.

This problem shows that digital literacy is still an aspect that needs to be improved, so that people are more critical in filtering the information they receive. One of the steps that can be taken is to increase education on how to recognize fake news, for example by verifying news sources, checking the credibility of information, and understanding the pattern of spreading hoaxes on social media. In addition, digital platforms and governments also need to collaborate in providing tools and systems that can help users detect false information more effectively. With the increase in digital literacy and the strengthening of the hoax detection system, it is hoped that the public can be wiser in consuming and disseminating information in this digital era.

h. Recommendations to Increase Cybersecurity Awareness

Based on these findings, several steps that can be taken to overcome this challenge are: first, increasing cooperation between the government, educational institutions, and religious leaders to educate the public about the importance of cyber protection. Second, involving cybersecurity practitioners in disseminating knowledge that is easy to understand and apply by the public. Third, develop more interesting and interactive training programs so that the public can more actively participate and understand the importance of digital security. Table

1 below illustrates the main findings from the survey conducted regarding cybersecurity challenges in Bandar Lampung.

This table presents the main findings that illustrate the level of awareness and knowledge of the Bandar Lampung community regarding cyber threats, as well as the challenges faced in dealing with these problems. The results of this study provide deeper insights into the need to increase education and training related to cybersecurity at the community level.

Table 1: Results of the Survey on Cyber Security Challenges in Bandar Lampung

Category	Percentage of Respondents	Key findings
General Awareness of Cybersecurity	65%	The majority of people still do not fully understand cyber threats and how to protect them.
Understanding Personal Data Protection	40%	Only a small percentage know how to effectively protect personal data.
Understanding Personal Data Protection	50%	Religious leaders provide limited guidance on the safe use of technology.
Obstacles Faced by the Community	55%	Many find it difficult to understand the technical aspects and rely more on other parties.
Challenges Faced by Cybersecurity Practitioners	70%	Lack of cybersecurity education and training at the general public level is a major challenge.
Utilization of Digital Security Programs by the Community	30%	Few actively participate in training or digital awareness programs.
Spreading False Information (Hoaxes)	60%	Many respondents feel affected by unverified information circulating on social media.

The study emphasizes that a more holistic approach, involving the social and religious sectors, can make a major contribution in building awareness and protection against cyber threats in society. This will not only strengthen digital resilience, but also increase social and moral integration in the growing use of technology..

Discussion

This research reveals that the awareness of the people of Bandar Lampung about cyber threats is still relatively low. The majority of respondents, around 65%, consider that cyberattacks target large corporations more than individuals like them. This perception is in line with previous studies that show that many people still feel digital security is not related to their personal lives.

However, this study also found that people are more worried about online fraud cases that often occur on social media. Many respondents admitted to being wary of crime modes such as phishing, identity theft, and fraudulent investments that are increasingly rampant. This shows that people's understanding of digital threats tends to be stronger when they are associated with real experiences in daily life. Therefore, an effective educational strategy should utilize concrete examples from social media to make it easier to understand.

In terms of personal data protection, the results of the study revealed that only about 40% of respondents have enough understanding of how to keep their information safe. This shows that awareness of digital privacy still needs to be increased. Although some people are beginning to understand the importance of protecting data, there are still many who do not know the concrete steps to prevent information leaks.

Some of the causes of this low awareness include lack of access to cybersecurity education and less secure digital habits. Some people still use weak passwords, share personal information openly on social media, or do not consider security when accessing online services. To overcome this problem, more practical educational strategies, such as application-based interactive tutorials or informative videos, are needed to make them easier to understand by the wider community.

The study also found that religion has a role to play in increasing awareness of digital security. Around 50% of respondents stated that they are more likely to receive directions from religious leaders in using technology wisely. However, the guidance provided generally only highlights the moral aspect without including technical instructions on how to secure yourself from cyber threats.

These results show that religious leaders have the potential to become agents of change in digital security education. Therefore, special training for religious leaders on the technical aspects of cybersecurity can be a solution so that they are able to provide more comprehensive guidance to their worshippers. Thus, religious leaders not only play a role in instilling ethical values in the use of technology but also provide practical direction related to digital security.

The public also has difficulty understanding the technical concept of cybersecurity. Many respondents admitted to being confused by terms like "encryption," "two-factor authentication," and "phishing," leaving them unsure about the steps they needed to take. This shows that there is a gap between the growing awareness of digital threats and their ability to deal with them. One solution that can be applied is a hands-on skills-based education approach. Community training programs that provide an understanding of how to detect cyberattacks as well as the use of security software can help people in better understand digital threats. If education is carried out through simulations or direct demonstrations, it will be easier for the community to master and implement self-protection strategies effectively.

In addition, this study found that the spread of hoaxes on social media is a big challenge for the people of Bandar Lampung. Around 60% of respondents admitted that they had been affected by

false information spread in cyberspace. Even though awareness of fake news is increasing, many people still have difficulty distinguishing valid information from hoaxes.

This emphasizes the need to increase digital literacy so that people are able to filter the information they encounter on social media. One of the steps that can be taken is the development of an application or news verification tool that can help users in identifying the truth of information. In addition, cooperation between digital platforms and educational institutions can also increase public awareness of the importance of verifying information before disseminating it.

Seeing the various challenges faced by the public in understanding cybersecurity, this study suggests closer cooperation between the government, educational institutions, and the private sector in organizing digital education. Accessible community-based training programs can be an effective step to increase public understanding of cyber threats and prevention measures.

The research also opens up opportunities for further exploration of how technology can be used to address the knowledge gap in digital security. One aspect that can be further researched is the effectiveness of community-based platforms in increasing public awareness of cybersecurity. With a more in-depth study, it can be analyzed to what extent community-based training is able to improve public understanding of digital threats.

In addition, future research may also explore how social and cultural factors affect public acceptance of digital security policies. Is the technical approach in digital security policies well accepted by the public or does it create resistance? Further studies of the influence of culture and religion on people's digital behavior can provide new insights into designing more effective cybersecurity strategies.

Overall, the results of this study show that there is a gap between public awareness of digital threats and their ability to deal with cyber risks. While more and more individuals understand the importance of digital security, many still do not have a deep understanding of the protective measures they need to take.

This research also underscores the important role of religious leaders in helping to spread awareness about cybersecurity. With a more inclusive approach, which not only emphasizes technical aspects but also considers social and cultural factors, it is hoped that people can be better prepared to face challenges in the digital era. These findings provide a foundation for the development of digital security strategies that are more relevant to the needs of communities at the local level.

4. Conclusion

The conclusion of this study highlights the challenges faced by the people of Bandar Lampung related to cybersecurity issues, especially in digital, religious, and social contexts. This research aims

to understand the level of public awareness of cyber threats and personal data protection, as well as to identify the factors that affect their perception and response to these issues.

The results show that although awareness of cyber threats has increased, public understanding is still limited, especially when it comes to protecting personal data and recognizing different types of cyberattacks. People tend to be more vulnerable to threats such as online fraud and the spread of hoaxes on social media, while their understanding of personal data protection is minimal. . In addition, although religious leaders play an important role in providing moral education, they also need further training in the technical aspects of cybersecurity in order to provide more complete and practical guidance to their worshippers.

The main point in the discussion of this research is the need for a simpler and more applicable approach in providing education about cybersecurity. The use of practical examples and community-based training can help increase public understanding of cyber threats and the protective measures that need to be taken. The results of this study also emphasize the importance of collaboration between various parties, including the government, educational institutions, and the private sector, to increase public awareness of the importance of cybersecurity.

The main contribution of this research is a deeper understanding of the challenges faced by the people of Bandar Lampung related to cybersecurity, as well as how social, religious, and digital factors interact with each other in shaping their awareness and response to these threats. These findings open up opportunities for the development of a more holistic approach to cybersecurity education that involves various aspects of people's lives. This research also provides insights for further research related to the use of community-based technology and training to address the knowledge gap about cybersecurity at the community level.

As a recommendation for further research, it is important to dig deeper into the development of community-based platforms that can educate the public directly and effectively. Future research may also focus on the effectiveness of technology-based training in improving public understanding of cyber threats.

5. Acknowledgement

The author would like to thank:

1. The Institute for Research and Community Service of the University of Muhammadiyah Lampung for the support of research funds that have been channeled through the Research and Community Service Program, which allows this research to run well.
2. The Bandar Lampung City Government has an important role in regulating policies related to digital security and personal data protection, in this case the Bandar Lampung City Communication and Information Service (Diskominfo).

3. Religious Leaders and Religious Organizations, namely Mr. Dr. H. Syaiful Bahri, MA, a religious figure who is active in the Indonesian Ulema Council (MUI) Lampung, who has a broad insight in the field of religion and has enlightened researchers on contemporary issues, including technology and cybes.
4. Private Sector (Technology Companies and Internet Service Providers)
5. The people of Bandar Lampung as the main respondent in this study, which is the main focus in exploring their understanding and attitude towards cyber threats.
6. Non-Governmental Organizations (NGOs) that Focus on Digital Literacy, namely the Tifa Foundation, the Cipta Digital Foundation, which have helped provide an understanding of the importance of cybersecurity.
7. The people of Bandar Lampung as internet users and as correspondents.
8. The author would also like to thank the reviewers who have provided constructive input and proofreaders who have carefully examined and perfected this manuscript, namely Mr. Dr. Muhammad Irham, a lecturer at the Faculty of Engineering UNILA who has an understanding in the field of information technology. As well as Mr. Dr. Adi Suryanto, a lecturer who focuses on social and technological research at UNILA.

6. References

Amin & Patel. (2020). Cybersecurity challenges in the age of digital transformation. *Journal of Cybersecurity and Digital Privacy, 15*(3), 145–158. https://doi.org/10.1016/j.jcdp.2020.04.010

Barker, D., & Lee, S. (2021). Understanding digital literacy and cyber ethics in the digital age. International. *Journal of Information and Education Technology, 11(5),* 224-230. https://doi.org/10.1109/IJIET.2021.9456910

Davis, M., & Thomas, G. (2019). Role of religion in cybersecurity: A sociotechnical analysis. *Journal of Cybersecurity Studies, 8*(3), 61–80. https://doi.org/10.1093/jcs/xyz020

Majid, H. (2022). Challenges of digital literacy and data protection in Indonesia: A focus on youth awareness. Indonesian Journal of Digital Literacy, 6(2), 45-59. https://doi.org/10.2139/ijdl.2022.003

Putra, F., & Suryadi, Y. (2019). The role of religious leaders in promoting digital ethics in Indonesian society. *Journal of Religious Education and Cyber Ethics, 5(3),* 210-224.

Rachmat, W., & Nurhadi, D. (2021). Cybersecurity awareness in Indonesian cities: A focus on Bandar Lampung. *Journal of Information Security in Indonesia*, *10*(1), 76-90. https://doi.org/10.1109/JISI.2021.007