computers

MDPI

Article

Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country

Adeel Ali *, Mahmood Shah *, Monika Foster and Mansour Naser Alraja

Newcastle Business School, University of Northumbria at Newcastle, Newcastle upon Tyne NE1 8ST, UK; monika.foster@northumbria.ac.uk (M.F.); mansour.alraja@northumbria.ac.uk (M.N.A.)
* Correspondence: adeel.ali@northumbria.ac.uk (A.A.); mahmood.shah@northumbria.ac.uk (M.S.)

Abstract: Technological advancements have helped all sectors to evolve. This advancement has widened the cyberspace and attack surface, which has led to a drastic increase in cyberattacks. Cybersecurity solutions have also evolved. The advancement is relatively slower in developing countries. However, the financial sector in developing countries has shown resistance to cyberattacks. This paper investigates the reasons for this resistance. Despite using legacy systems, the banking sector in Pakistan has demonstrated resistance to cyberattacks. The research used a qualitative approach. Semi-structured interviews were conducted with nine cybersecurity experts in the banking sector to illustrate the reasons for this cybersecurity resistance. The research focused on cybersecurity experts in the banking sector, recognizing that this industry is particularly prone to cyberattacks on a global scale. The study utilised a thematic analysis technique to find resistance factors. The analysis suggests that the opportunity cost of cyberattacks and lower attack surface in developing countries like Pakistan are the main reasons for the lower financial losses. The findings of this research will encourage the adoption of advanced technologies such as artificial intelligence (AI) and machine learning (ML) for cybersecurity in developing countries' banking and financial sectors.

Keywords: advanced technologies; cyber security; banking; resilience; cyberattacks; artificial intelligence; machine learning; financial sector

Academic Editor: Paolo Bellavista

Received: 30 December 2024
Revised: 17 January 2025
Accepted: 23 January 2025
Published: 27 January 2025

Citation: Ali, A.; Shah, M.; Foster, M.; Alraja, M.N. Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country. *Computers* **2025**, *14*, 38. https://doi.org/10.3390/computers14020038

1. Introduction

Financial institutions are an essential part of any economy. These institutions are vital in smooth economic operations [1]. In the last few decades, the use of technology has increased, and the recent pandemic (COVID-19) has accelerated this process [2]. Like all sectors, these advancements have also impacted banking operations. Banking organisations have also transformed operations [3]. Banking customers have shifted from branch banking to Internet banking and mobile banking. Omar, Sultan [4] suggested that customers prefer Internet banking over branch banking due to reliability, convenience, and other factors. Similarly, customers now prefer mobile banking due to ease of use [5].

These technological advancements have eased the use of the banking system. It has also increased the probability of cyberattacks [6]. Regarding the adoption of online banking in the developing world, the State Bank of Pakistan's payment system quarterly review report mentioned that in the third quarter of 2024, the country witnessed a 5.5% increase in Internet banking and a 4.5% increase in mobile banking [7]. The report also mentioned that businesses are increasingly shifting to digital payment methods, growing the country's digital ecosystem. With these advancements, cyberspace is also expanding, making the country more vulnerable to cyberattacks.

Globally, the situation has worsened in recent years. As mentioned in the global financial stability report, cyberattacks have been increasing drastically in recent years, and the share of the financial and insurance sector has doubled in the past decade [8]. The reason for this be could be the continuous increase in the use of AI and other advanced technologies [8]. Similarly, the cost of these attacks is also expected to increase. Figure 1 illustrates the cost of global cybercrime.

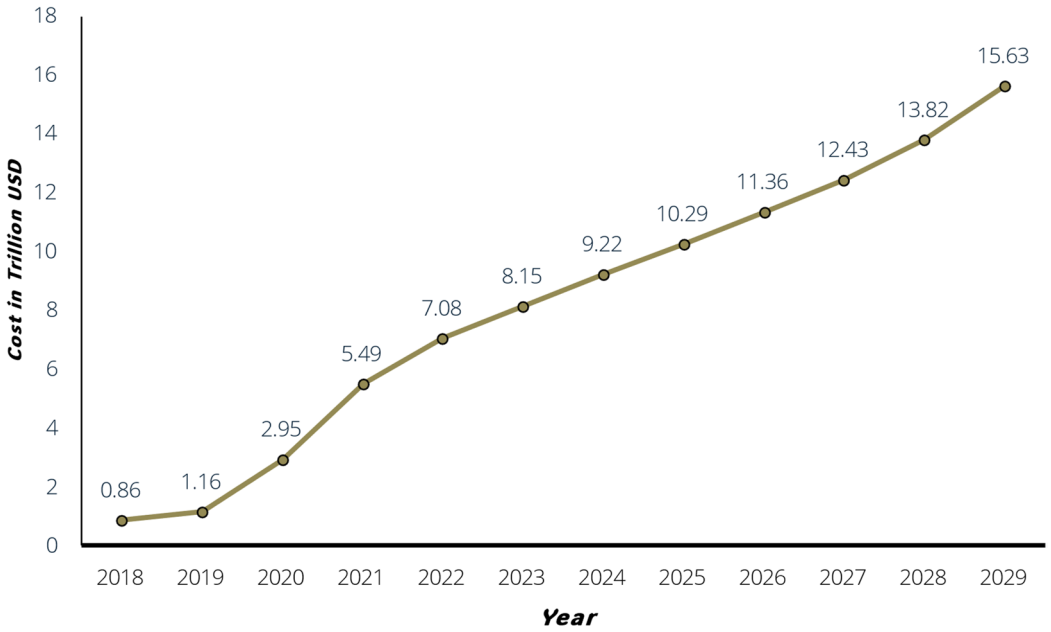

Figure 1. Annual cybercrime cost in 2018–2029 [9].

Figure 1 illustrates the increase in the cost of cyberattacks from 2018 to 2024 and shows that the cost is expected to increase further. Hence, the financial sector worldwide requires embracing advanced technologies such as AI and ML to ensure systems' cybersecurity.

Babajide Tolulope and Philip Olaseni [10] suggest that developed countries like the USA have employed robust techniques and resources to safeguard their infrastructure from cyberattacks; however, developing countries like Nigeria face challenges regarding resources, infrastructure, awareness, and expertise. At the same time, perpetrators are developing ransomware by utilising advanced technologies and using developing countries as a testing ground [11].

Cybersecurity is a global issue; developing and developed countries face financial losses due to these cyberattacks. However, Świątkowska [12] argues that developing countries face lower financial losses when compared to developed countries. Hence, the current study aims to investigate reasons for lower cyberattack costs.

RQ1: Which advanced technologies are used in the financial sector for cybersecurity?

RQ2: What factors can contribute to a lower rate of cyberattacks in a developing country?

The structure of the current paper is as follows. The following section presents a literature review of existing research. The material and method section contains the instrument used, instrument design, data collection techniques, demographics of participants, interview process and data analysis techniques and tools used in the research. The result section is presented in two parts. The first section analyses the current use of technology, and the second section presents the key factors. Similarly, the discussion section is organised into two parts: the first revisits the research questions, and the second addresses the study's limitations and provides recommendations for future research.

2. Literature Review

Technological advancement has advantages and disadvantages. Technological advancements have enabled financial institutions to reach the masses and allow individuals to use financial services and technology to carry out business efficiently. These facilities have substantially expanded cyberspace, making the financial sector more vulnerable to cyberattacks. The financial losses caused by these attacks are increasing globally. However, there is a substantial variation between developed and developing countries.

The disparities between developed and developing countries significantly impact their cybersecurity capabilities. The less developed countries struggle to repel attacks effectively [13]. Similarly, due to economic and organisational factors, developing countries face unique challenges in the cybersecurity context. While relying on legacy systems and lower reliance on advanced technological infrastructure may suggest lower cyberattack vulnerabilities, in reality, developing countries can be more susceptible to these attacks [13,14]. Due to a lack of advanced technologies, developing countries like Pakistan may struggle to repel sophisticated attacks. Although studies suggest a reduced vulnerability in developing countries due to low reliance on digital technology, the literature on other factors that can contribute to this variation is limited.

Mugari, Kunambura [15] conducted a study on the trends and impacts of cybercrime. The study found that card fraud in Zimbabwe is lower than in developed countries. The study suggested that developing countries like Zimbabwe faced fewer cyberattacks due to the lower adoption of information and communication technologies. This variance in developed and developing countries is due to the limited use of card payments in developing countries [15]. The deviation in different types of cyberattacks can be due to several factors, such as the economic condition of the country, overall development and internet usage [16].

Another important reason for lower financial losses in developing countries is low reporting. The number of attacks is lower as these attacks are not reported due to the absence of cybercrime law. Similarly, it is difficult to estimate the cost in developing countries due to a lack of reporting and systematic processes [17]. The existing literature suggests that the variation in cyberattacks can be due to economic factors, organisational factors, lower technological infrastructure and low reporting behaviour. However, the factors are not explicitly discussed in the literature.

Similarly, the literature discusses these factors as a supporting argument for the study's findings. Hence, the current study has employed a qualitative research method to bridge the gap in the literature.

3. Materials and Methods

The research method is an essential part of any research. The study's research methodology is illustrated in Figure 2 and the processes followed in the study are presented in detail in the following sections.

3.1. Instrument Design

The present study employed a thematic analysis technique to assess the factors contributing to the variation in cyberattacks in developed and developing countries. A systematic approach was used to conduct this study to avoid bias. The study used semi-structured interviews for qualitative data collection. A semi-structured interview provides robust findings [18]; hence, the study employed semi-structured interviews for data collection. A five-step guide was employed to develop the instrument. These steps included identifying the basis for using the instrument, finding literature, developing an initial draft, conducting a pilot study, and preparing the final draft [19]. Hence, three experienced academicians

were asked to review the designed instrument for reliability after developing the initial draft. The recommendations of these experienced researchers were implemented to enhance the instrument's reliability. In the next phase, a pilot study with two researchers was conducted. These participants had satisfactory knowledge of cybersecurity and advanced technology applications. Afterwards, the final draft was developed.

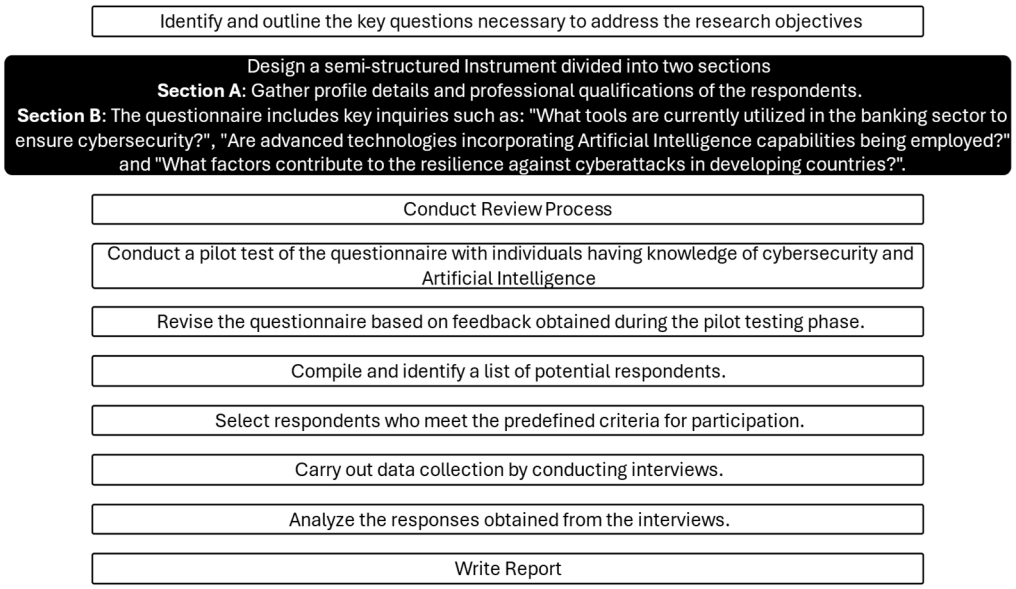

Figure 2. Schematic diagram of research design followed in the study.

3.2. Data Collection

After the instrument was developed, cybersecurity experts in Pakistan's banking sector were approached for semi-structured interviews. For qualitative data collection, purposive sampling is used extensively when a study requires information-rich participants [20]. Similarly, the snowballing technique is used after selecting a small number of participants who fit the criteria. The initially selected participants are asked to refer more participants who fit the criteria [21]. These techniques help in gathering data from the most appropriate participants. Hence, following Michał, Lee Zach [22], a purposive sampling technique was used to target experts who were selected based on their experience in the banking sector and cybersecurity. After conducting their interviews, they were asked to refer other potential participants. This approach led to the collection of nine interviews in total with cybersecurity experts.

This technique is beneficial when little is known about the subject under discussion. Table 1 illustrates the demographics of participants.

Table 1. Demographics of cybersecurity experts interviewed in the study.

No.	Designation
Participant 1	Chief Information Security Officer
Participant 2	Chief Information Security Officer
Participant 3	Head Information Security
Participant 4	Head Information Security
Participant 5	Head Cybersecurity
Participant 6	Head Enterprise Technology
Participant 7	Head Security Operation Center
Participant 8	Manager Identity Security Planning
Participant 9	AM Integration and Implementation

The sample included three cybersecurity experts from fintech and six from the banking sector. The study's sample size is in line with previous studies such as those by Hasija and Esper [23] who researched AI acceptance with seven interviews, Abdullah [24] who studied technology adoption in SMEs using six interviews and Alrashed, Ahmad [25] who studied technology adoption in medical education using thirteen interviews. In phenomenological research, the study explores lived experience regarding a particular phenomenon. As initially stated by Creswell and Morse, respectively, for phenomenological studies, five to twenty-five interviews or at least six interviews are necessary [26]. Similarly, Dworkin [27] also suggested that for a qualitative study, at least five interviews are required to reach a conclusion.

3.3. Interview Process

Before starting the interviews, the experts were briefed on the aim and objective of the study. Each participant signed a consent form prior to the start of the interview. Participants were also informed that the provided data would be anonymised and their identities would be protected. Participants were informed about the recording process. After discussing all elements of the research, the participants signed a consent form.

The interview started with questions about the participant's introduction and experience. The second question was about cyberattacks encountered. Similarly, the participants were asked about the current cybersecurity technologies they use in their organisations. Afterwards, the cybersecurity experts were asked about the differences between advanced technology and legacy systems in developing countries. After finding the variation in technology used for cybersecurity, experts were asked to point out the factors contributing to developing countries' resilience.

3.4. Transcription and Data Analysis

The shortest interview lasted four minutes and thirty-seven seconds, whereas the longest interview spanned eleven minutes and forty-two seconds. All interviews except one were recorded, as one participant did not consent to recording the interview.

Out of nine interviews, one was in Urdu. The interview was translated into English to proceed with the analysis. Other interviews were transcribed using the Microsoft Word transcription option. Each transcription was checked several times, and compared with the audio recording to remove errors. After verification, these transcripts were moved to software for analysis.

To analyse the transcripts, the study employed a thematic analysis approach. The study employed NVIVO 15 to analyse the interview data. NVIVO is a software that can help researchers with qualitative data analysis, previously known as NUD.IST Vivo [28]. NVIVO supports researchers in storing, managing and analysing unstructured data, including text, audio, video and other data files [29].

The study used a six-step thematic analysis outlined by Braun and Clarke [30]. These steps include familiarising with the data, initial coding, theme search, theme review, theme definition, and report production. During the managing and analysing phase, the current research used a coding process described by Williams and Moser [31], which enabled the research to conduct a systematic and structured data analysis. The first stage included finding themes from transcripts and generating open codes. In the second phase, axial codes are developed following the analysis of the open codes.

4. Results

4.1. Current Use of Advanced Technologies for Cybersecurity

Advanced technologies like AI and other technologies under the umbrella of AI, such as machine learning and deep learning (DL), are gaining cybersecurity experts' trust in developing countries such as Pakistan. The study received a mixed response from experts in the financial industry. Some experts suggested that they are using AI capabilities, and some suggested that they are considering using AI and ML. However, others suggested that they have not used any advanced technologies.

The financial sector uses security information and event management (SIEM) solutions, endpoint detection and response (EDR), extended detection and response (XDR), and firewalls to detect and mitigate cyber threats. The SIEM solution is a comprehensive tool that provides holistic view of the cybersecurity status of an organisation [32]. Pakistan's banking sector relies immensely on SIEM solutions due to their ability to perform real-time analyses and respond to various situations. EDR and XDR add another layer of protection to the system. EDR analyses all endpoint events and prevents cyberattacks as they arise [33]. A cybersecurity expert provided the following statement:

> *"We have an anti-malware solution or tool client deployed on every node in our organisation. Then, of course, we have EDR. We have next-generation firewalls. We have a privilege access management tool that is deployed. We have a SIEM solution deployed, which is also complemented by a SOAR solution, which is used for security orchestration and response. We are also using some breach and attack simulation tools which we use to validate our security controls".* (Cybersecurity Expert 2).

The expert mentioned several tools used in the financial sector for cybersecurity. Other cybersecurity experts in the study also endorsed the tools mentioned by expert 2. These tools can integrate machine learning tools to enhance cybersecurity. The experts made the following statements:

> *"It is not AI yet, but definitely machine learning".* (Cybersecurity Expert 7).

> *"Yes, we have started using it. So basically, one of the very use cases we are having is alert enrichment".*(Cybersecurity Expert 1).

As the above statement illustrates, the financial sector has started using AI and machine learning for cybersecurity. These advanced technologies enhance alert enrichment, which can help reduce the human effort in the process.

Cybersecurity experts 5, 8 and 9 mentioned that they have not started using AI or machine learning in their systems. However, other experts (6 and 4) have mentioned that they started exploring and testing new advanced tools for cybersecurity.

The analysis of different statements suggests that using advanced technologies in cybersecurity is inevitable. Financial sector organisations are evaluating different advanced technologies to enhance their cybersecurity.

4.2. Hierarchical Chart for Factors Affecting Cyberattack Incidents

Hierarchy charts make it easy to visualise coding. The reader can easily understand the reference frequency by viewing the hierarchy chart. This also educates the reader on the level of factors identified. Figure 3 illustrates the factors identified in the analysis of interviews. On the top left of the illustration, the figure provides the most discussed factor, and on the right, the least discussed factor.

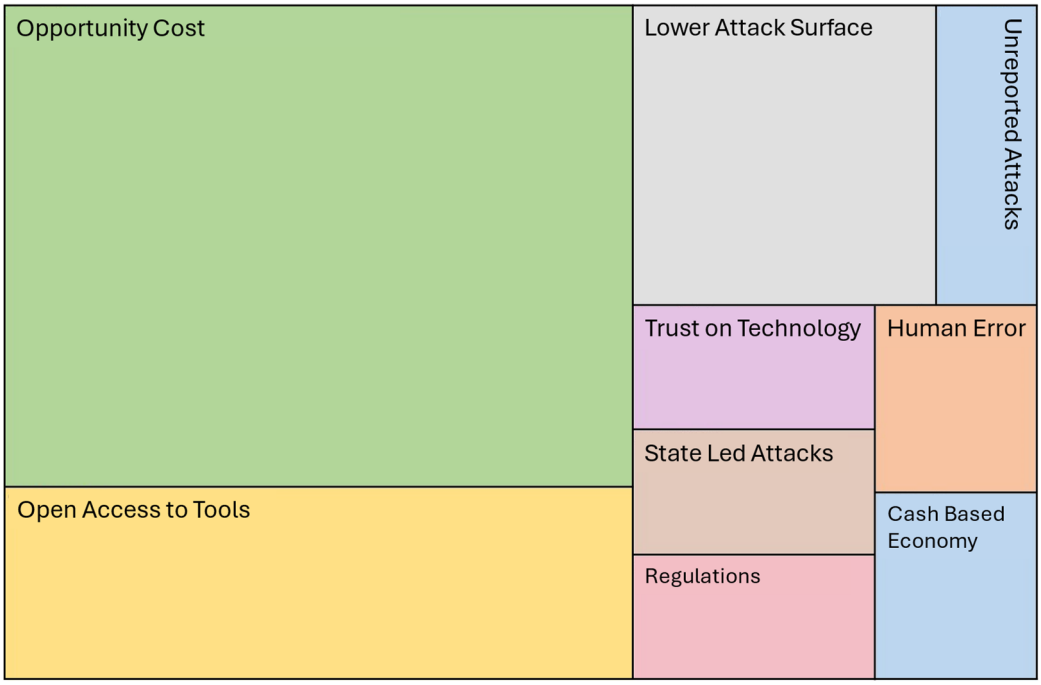

Figure 3. Hierarchy chart of factors identified.

The figure illustrates that opportunity cost highly influences cyberattacks in Pakistan. However, a cash-based economy is mentioned least. The following section will discuss the analysis results and factors identified in interviews with cybersecurity experts in the financial sector.

4.2.1. Opportunity Cost of Cyberattacks

Opportunity cost emerged as one of the key factors for lower cyberattack losses in Pakistan. Six out of nine cybersecurity experts in the financial sector mentioned the opportunity cost of cyberattacks as the main reason for the lower number of cyberattacks in Pakistan. The main reason for any cyberattack is financial gain. Hence, developing countries like Pakistan are not very lucrative for perpetrators when compared to developed countries. The majority of cybersecurity experts highlighted cost as the main reason. The expert made the following statement:

> *"The main reason is that, again, Pakistan is considered a less developed country, right? Hackers, or you can say attackers, look for rich people or developed countries where they have a lot of resources. They have a lot of financial transaction data available. For us, if they are going to be data, it will sell in the international market for just a few dollars. If there is some high target or international organisation data that will be sold in millions of dollars".* (Cybersecurity Expert 4).

In this regard, experts 1, 2 and 3 agree with the same statement. Data from developing markets or countries are not sold at higher values; hence, it is not lucrative for hackers. Regarding opportunity cost, another cybersecurity expert mentioned using credit cards and spending limits in developed countries. The expert mentioned the following:

> *"Suppose there is a UK or US platinum card on which there is a limit of fifty thousand dollars. Your card's limit is five lakh rupees. How much does it become? Twelve hundred dollars. If they compromise a card worth fifteen hundred dollars, what will they do with a fifteen-hundred-dollar card when they have the option of fifty thousand dollars?"* (Cybersecurity Expert 7).

Hence, hackers also carry out a cost–benefit analysis and look for opportunities that can give them more financial gain with less effort. Cybersecurity experts mentioned this as a return on investment for hackers, as outlined below:

> *"I would say that threat actors or, you know, the attackers go for data or, you know, breach those countries or have a financial impact on those countries where they get a lot of revenue or money because profitability or revenue is one of the factors which they have in their mind".* (Cybersecurity Expert 6).

To summarise, cybersecurity experts suggest that developing countries like Pakistan are not lucrative for hackers due to lower financial gain. Credit card fraud is also lower in developing countries due to lower card limits than in developed countries.

4.2.2. Lower Attack Surface

A lower attack surface is another substantial reason for lower cyberattacks in Pakistan. Three cybersecurity experts have mentioned lower attack surface as one of the main variables for lower cyberattacks. Experts mention one of the reasons for lower attack surfaces:

> *"The reason for this is that our attack surface is lower, and theirs is much higher. Okay, I will give you an example. We see this globally. If you google it, you will find hundreds of such shops within the UK that have an online presence as well as an on-premises presence. Here, how many shops in Urdu Bazaars do we have with an online presence? Nothing. It is nothing. It means it will be according to the salt in the flour". (Cybersecurity Expert 7).*

E-commerce and online shopping are not as widely accepted in Pakistan as in developed countries. In developed countries, most local businesses have an online presence; however, even flourishing businesses are not online in developing countries. Hence, customers and businesses are hesitant to have a significant online presence. This leads to a lower attack surface to infiltrate. As mentioned by one cybersecurity expert:

> *"Okay, so the reason is that wherever the cake would be, people would go there. So, these are the countries where they have more technology, and the number of users is higher. So, attackers like to attack more because they are more in number. They have more population online, using credit cards and while credit card adoption is still low in developing countries. So, these are a few reasons that we see more cyberattacks in developed countries than in developing countries".* (Cybersecurity Expert 8).

Developed countries have a more significant online presence, and the number of credit card users is higher in developed countries than in developing countries. Hence, the surface of attacks in developed countries is higher, which makes it lucrative for threat actors.

4.2.3. Access to Technology

Another reason for lower cyberattacks in Pakistan is access to technology. In developed countries, advanced technology is available to everyone. The cybersecurity expert from the financial sector mentioned the following:

> *"Attackers can also use this. If you are offering AI tools or any tool for the custodians, you cannot distinguish the either the recipient or the buyer of the product is an attacker or legitimate user, or a vendor or a businessman. So, as you are selling your product, you are selling your product to different people and now it is up to the people how they use this technology and these tools".* (Cybersecurity Expert 5).

Due to their unrestricted access, technologies like AI are not easy to control. Anyone can use the technology. Organisations can use it for their protection, and threat actors can use it to develop more complex attacks. Another cybersecurity expert mentioned the following:

"The young generations are even more likely to pursue ethical hacking or something similar……....they basically learn these things themselves". (Cybersecurity Expert 8).

The expert suggests that the young generation can be attracted to ethical hacking and similar activities due to their unrestricted access to these technologies. They learn them themselves, as the material is openly available to them. Threat actors can later use these facilities.

4.2.4. Unreported Attacks

The unreported nature can significantly change the point of view. Many cyberattacks go unreported in developing countries. It can happen due to a lack of regulations and victim blaming. A substantial number of cyberattacks on organisations in developing countries also go unreported. One cybersecurity expert mentioned the following:

"Another reason is that some of these cyber incidents, which even happen in developing countries, go unreported. There are not any regulations to make it a compulsion for the victim organisation to go public about the nature of the attack, the results of the attack and how it has impacted the information or the data of its customers". (Cybersecurity Expert 2).

The expert stated that developing countries have no restrictions on reporting cyberattacks. Organisations are not compelled to report cyberattacks and their implications, which may lead to misleading cyberattack figures in these countries.

4.2.5. Lack of Trust

Another reason mentioned by cybersecurity experts is a lack of trust in technology. Due to online scams, individuals in Pakistan do not trust digital platforms. The cybersecurity expert mentioned the following:

"A very big factor is that we get nervous. What is the reason? We hesitate so much. There are too many scams. If you buy something online here and you buy something online there, you will see the difference". (Cybersecurity Expert 7).

Due to online fraud, individuals in Pakistan hesitate to use new technology, reducing the cyberspace available for cyberattacks.

4.2.6. State-Led Attacks

Another prominent issue mentioned by one cybersecurity expert is state-sponsored attacks in developed countries due to rivalries, political gains and geographic issues. The cybersecurity expert in the financial sector mentioned the following:

"Most of these attacks are state-backed attacks, and there are rivalries within the country. In 2009, Barack Obama declared cyber at their fifth front after Sea, Air, Land and space, and their units within their defence within Europe, Russia and North America as well. So that is one of the reasons they are more attacked while we are not that much of a target now, the developing countries". (Cybersecurity Expert 2).

The cybersecurity expert emphasised that developed countries face more cyberattacks due to rivalries with other countries. Using the USA as an example, the expert mentioned that the USA has declared cyberspace the fifth most important security front due to these attacks.

4.2.7. Human-Technology Factor

Human–technology intervention is a key factor in cybersecurity. Human error can significantly influence the decision-making process. The cybersecurity expert mentioned the following:

> *"Everyone has installed top-notch like themselves and made frameworks, but still, it gets compromised. It means there is a gap somewhere, and the biggest gap that is near to me is the people's gap. People's investment is not there, and they invest in technology. Take any good tool you want; if the one that operates is not good, then it will not be effective".* (Cybersecurity Expert 7).

The expert emphasised that using advanced technology has a minimal impact compared to human experts. The performance of any technology depends on the operator. If the operator is not qualified, this can lead to drastic consequences. Hence, strategies should be focused on the development of people.

4.2.8. Lack of Regulations

Due to a lack of regulations, organisations are not bound to disclose cyberattacks. This leads to lower reporting of cyberattacks. The expert mentioned the following:

> *"So, any country which is less of regulatory data, privacy related laws implemented, they are probably not going to get that impacted. But in comparison, if you look at any European country, it is going to be a serious issue for them. So, it becomes a more high-value target as an organisation. Because I mean, the people over there are more aware of their laws' rights, and then they have the legal frameworks to call out".* (Cybersecurity Expert 1).

Developing countries lack regulations, leading to lower reporting and awareness than developed countries. Hence, organisations in Pakistan are not called out when they face cyberattacks.

4.2.9. Cash-Based Economy

Organisations and individuals in developed countries have more online presence, while Pakistan is more cash-based. Hence, Pakistan has a relatively limited cyberspace and is prone to cyberattacks. One cybersecurity expert mentioned the following:

> *"We are a cash-based industry. They are Credit-based or online, what they call it. How many such shops are there that have an online presence, but the on-prem is non-existent? All are online".* (Cybersecurity Expert 7).

The expert emphasised that developing countries like Pakistan are cash-based economies. Transactions in developed countries are carried out online and on cards, but few businesses in developing countries have an online presence. Hence, cyberattacks are lower in developing countries than in developed countries.

4.3. Word Cloud

During the analysis phase, the NVIVO-15 generates a word cloud from interviews, as illustrated in Figure 4. For clarity, frequently used words like developing, countries, and people were added to the stop word list.

The most repeated words in interviews are shown as bolder words. The cloud shows the most repeated words: online, dollars, data, credit card, presence, technology and financial. This cloud provides backing to our results discussed in previous sections.

Figure 4. Word cloud generated from analysis of interviews.

5. Discussion

The current study attempted to identify factors contributing to lower cyberattacks in Pakistan. It identified nine potential factors that explain why statistics show a lower rate of cyberattacks in developing countries than in developed countries. These identified factors are discussed in the following sections.

Opportunity cost is the most prominent factor identified and supported by a sizable number of cybersecurity experts. Experts suggest that the financial data of developing countries are not highly valued in the international market and that the developing market is not lucrative for threat actors. The threat actor compares the cyberattack's required costs and gains [34]. The decision to attack is based on a cost-and-benefit comparison [35]. Hence, regions with higher opportunity costs may face lower cyberattacks.

Another reason for low cyberattack figures is the lower attack surface. Advanced technologies like AI and ML have a black-box nature, further enlarging cyberspace and making it more vulnerable to cyberattacks [36]. Adopting advanced technologies is slow in developing countries [37,38]. Due to the lower adoption of advanced technologies like AI and ML, the attack surface is lower, leading to lower cyberattacks.

A further reason pointed out by experts for lower cyberattacks in Pakistan is restricted access to technology in Pakistan and other developing countries and open access in developed countries. Access to advanced technology has allowed thread actors to carry out more sophisticated attacks, and the attackers now offer cyberattacks as a service [2]. These are all repercussions of the open availability of advanced technologies.

An additional reason highlighted by cybersecurity experts is unreported attacks. The unreported nature of cyberattacks can drastically change the figures of cyberattacks. The literature suggests several reasons for this issue. Paul, Ali [39] suggested that cyberattacks can go unreported due to victim blaming, humiliation and guilt. Similarly, Nfuka, Sanga [40] suggested that cyberattacks are not reported due to a lack of regulations, awareness, and concern about customer attrition. These issues lead organisations and individuals not to report cyberattacks.

Another argument put forward by experts is the lack of trust in technology in Pakistan. Organisations in developing countries are providing digital solutions to their customers.

Capestro, Rizzo [41] suggest that trust significantly influences the adoption of digital technology. Due to online scams, the adoption of new technology has stalled [42].

Lower state-led attacks are another reason for lower attacks in Pakistan. Developed countries like the USA and China are actively involved in cyberattacks [43]. Adenuga and Abiodun [44] analysed the implications of cyberattacks on international security. The target countries were China and the US. The study suggested that high-level mutual discussions are the way forward. These state-led cyberattacks are motivated by political interests, economic interests, security concerns and technological capabilities [45]. This rivalry with advanced technologies at disposal is significantly lower in developing countries.

An additional reason highlighted is the human factor. Oladipo, Okoye [46] suggests that human-focused strategies can improve cybersecurity and user awareness. Developed countries are more focused on developing technology. However, due to a lack of technology, developing countries focus on human capability development.

Similarly, cyberattack data are impacted in Pakistan due to a lack of regulations. Both organisations and individuals are cautious to report cyberattacks due to a lack of regulations. Due to this lack of regulation and loopholes in laws, many cybersecurity incidents go unreported [47]. This can result in an incomplete data set of cyberattacks.

Another significant factor that can impact cyberattacks in Pakistan is that it is a cash-based economy. Shrestha [48] suggests that a cashless economy and cybercrime are negatively associated. This highlights that with more digitisation in the financial sector, more cybercrimes will follow. Although with a cashless economy, robberies can decrease, they will also increase money laundering, digital fraud and credit card fraud [49]. Hence, as the cybersecurity experts highlighted in the result section, a cash-based economy can result in fewer cyberattacks.

All the identified factors can significantly impact reported cyberattacks. Hence, it is essential to empirically test these factors in other developing countries. The next section presents a framework based on the findings of this research. The framework can be used for empirical research in developing countries.

Limitations and Future Recommendations

The study has considered several techniques to make the research unbiased. However, no research is free from limitations. The current research uses a qualitative method, limiting the results' generalisability. Hence, the following sections present a conceptual framework for future studies.

The study has highlighted several factors that can lower cyberattacks in developing countries. These factors include opportunity cost, lower attack surface, restricted access, unreported attacks, trust, state-led attacks, human–technology integrations, regulations, and a cash-based economy.

These findings have led to the development of a conceptual framework for future research to empirically test these findings in other developing countries. Figure 5 illustrates the conceptual framework.

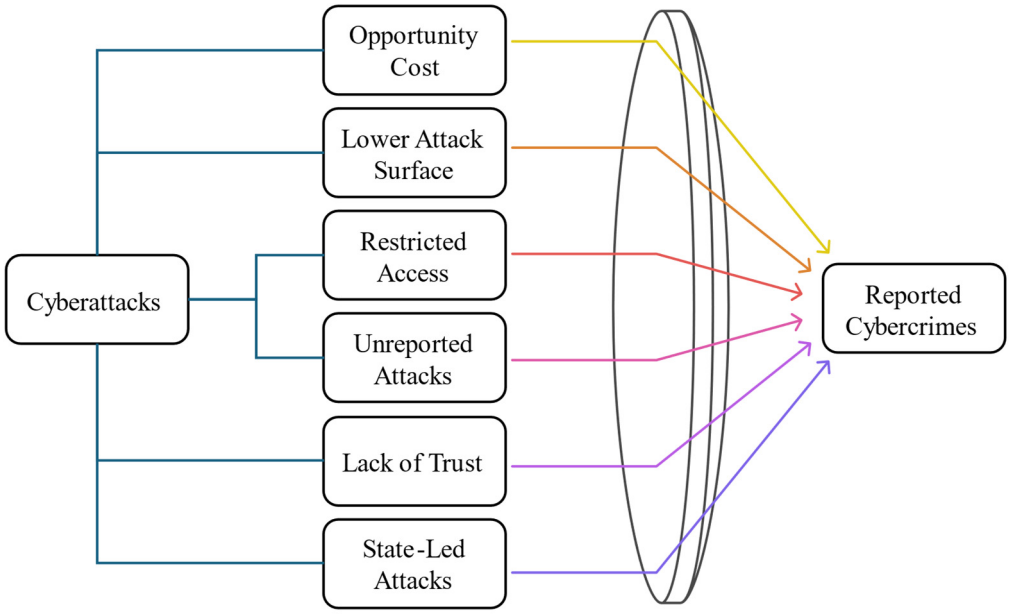

Figure 5. Conceptual framework for empirical testing of results.

6. Conclusions

The current study used a qualitative research method, i.e., semi-structured interviews, to find the key factors impacting cyberattacks in developing countries. The data were collected from cybersecurity experts working in Pakistan's financial sector. To the best of our knowledge, the study is unique as it explores factors that can impact the number of cybercrime incidents in developing countries.

The findings of the interview analysis are presented in the result section and are further supported by literature in the discussion section. This research has contributed to information security literature by identifying factors that can impact cyberattacks.

Author Contributions: Conceptualisation: A.A.; methodology, A.A.; software, A.A.; validation, A.A.; investigation, A.A.; data curation, A.A.; writing—original draft preparation, A.A.; writing—review and editing, A.A., M.S., M.F. and M.N.A.; visualisation, A.A.; supervision, M.S., M.F. and M.N.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Owing to privacy considerations, the data utilised could not be made publicly available, as they were directly associated with the anonymous participants.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Gulyás, O.; Kiss, G. Impact of cyber-attacks on the financial institutions. *Procedia Comput. Sci.* **2023**, *219*, 84–90. [CrossRef]
2. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* **2023**, *12*, 1333. [CrossRef]
3. Osei, L.K.; Cherkasova, Y.; Oware, K.M. Unlocking the full potential of digital transformation in banking: A bibliometric review and emerging trend. *Future Bus. J.* **2023**, *9*, 30. [CrossRef]
4. Omar, A.; Sultan, N.; Zaman, K.; Bibi, N.; Wajid, A.; Khan, K. Customer perception towards online banking services: Empirical evidence from Pakistan. *J. Internet Bank. Commer.* **2011**, *16*, 1–24.
5. Singh, S.; Srivastava, R. Understanding the intention to use mobile banking by existing online banking customers: An empirical study. *J. Financ. Serv. Mark.* **2020**, *25*, 86–96. [CrossRef]
6. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors* **2023**, *23*, 6666. [CrossRef]

7. SBP. Payment Systems Quarterly Review. 2024. Available online: https://www.sbp.org.pk/psd/reports/index.htm (accessed on 17 December 2024).
8. IMF. *Global Financial Stability Report*; IMF: Washington, DC, USA, 2024; Available online: https://www.imf.org/en/Publications/GFSR/Issues/2024/10/22/global-financial-stability-report-october-2024 (accessed on 17 December 2024).
9. Statista. Global Cybercrime Estimated Cost 2029. Statista 2024. Available online: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (accessed on 18 December 2024).
10. Babajide Tolulope, F.; Philip Olaseni, S. Cybersecurity in the financial sector: A comparative analysis of the USA and Nigeria. *Comput. Sci. IT Res. J.* **2024**, *5*, 850–877. [CrossRef]
11. Kissin, E. Hackers use developing countries as testing ground for new ransomware attacks. *Financial Times*, 24 April 2024.
12. Świątkowska, J. Tackling cybercrime to unleash developing countries' digital potential. *Pathw. Prosper. Comm. Backgr. Pap. Ser.* **2020**, *33*, 2020-01.
13. Gamreklidze, E. Cyber security in developing countries, a digital divide issue. *J. Int. Commun.* **2014**, *20*, 200–217. [CrossRef]
14. Kshetri, N. Diffusion and Effects of Cyber-Crime in Developing Economies. *Third World Q.* **2010**, *31*, 1057–1079. [CrossRef]
15. Mugari, I.; Kunambura, M.; Obioha, E.E.; Gopo, N.R. Trends, impacts and responses to cybercrime in the Zimbabwean retail sector. *Safer Communities* **2023**, *22*, 254–265. [CrossRef]
16. Boussi, G.O.; Gupta, H.; Hossain, S.A. A Machine Learning Model for Predicting Phishing Websites. *Res. Sq.* 2023; *preprint*.
17. Chang, L.Y.C.; Coppel, N. Building cyber security awareness in a developing country: Lessons from Myanmar. *Comput. Secur.* **2020**, *97*, 101959. [CrossRef]
18. Ruslin, R.; Mashuri, S.; Rasak, M.S.A.; Alhabsyi, F.; Syam, H. Semi-structured Interview: A methodological reflection on the development of a qualitative research instrument in educational studies. *IOSR J. Res. Method Educ. (IOSR-JRME)* **2022**, *12*, 22–29.
19. Kallio, H.; Pietilä, A.M.; Johnson, M.; Kangasniemi, M. Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *J. Adv. Nurs.* **2016**, *72*, 2954–2965. [CrossRef]
20. Palinkas, L.A.; Horwitz, S.M.; Green, C.A.; Wisdom, J.P.; Duan, N.; Hoagwood, K. Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Adm. Policy Ment. Health Ment. Health Serv. Res.* **2015**, *42*, 533–544. [CrossRef]
21. Parker, C.; Scott, S.; Geddes, A. Snowball sampling. In *SAGE Research Methods Foundations*; SAGE Publications Ltd.: New York, NY, USA, 2019.
22. Michał, K.; Lee Zach, W.; Chan Tommy, K. Blockchain technology and trust relationships in trade finance. *Technol. Forecast. Soc. Change* **2021**, *166*, 120641.
23. Hasija, A.; Esper, T.L. In artificial intelligence (AI) we trust: A qualitative investigation of AI technology acceptance. *J. Bus. Logist.* **2022**, *43*, 388–412. [CrossRef]
24. Abdullah, N.H.; Wahab, E.; Shamsuddin, A. Exploring the Common Technology Adoption Enablers among Malaysian SMEs: Qualitative Findings. *J. Mgmt. Sustain.* **2013**, *3*, 78. [CrossRef]
25. Alrashed, F.A.; Ahmad, T.; Almurdi, M.M.; Alderaa, A.A.; Alhammad, S.A.; Serajuddin, M.; Alsubiheen, A.M. Incorporating Technology Adoption in Medical Education: A Qualitative Study of Medical Students' Perspectives. *Adv. Med. Educ. Pract.* **2024**, *15*, 615–625. [CrossRef]
26. Mason, M. Sample Size and Saturation in PhD Studies Using Qualitative Interviews. *Forum Qual. Sozialforschung/Forum Qual. Soc. Res.* **2010**, *11*, 8. [CrossRef]
27. Dworkin, S.L. Sample Size Policy for Qualitative Studies Using In-Depth Interviews. *Arch. Sex. Behav.* **2012**, *41*, 1319–1320. [CrossRef]
28. Welsh, E. Dealing with Data: Using NVivo in the Qualitative Data Analysis Process. *Forum Qual. Sozialforschung/Forum Qual. Soc. Res.* **2002**, *3*. [CrossRef]
29. Phillips, M.; Lu, J. A quick look at NVivo. *J. Electron. Resour. Librariansh.* **2018**, *30*, 104–106. [CrossRef]
30. Braun, V.; Clarke, V. Using thematic analysis in psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [CrossRef]
31. Williams, M.; Moser, T. The art of coding and thematic exploration in qualitative research. *Int. Manag. Rev.* **2019**, *15*, 45–55.
32. Sheeraz, M.; Durad, M.H.; Paracha, M.A.; Mohsin, S.M.; Kazmi, S.N.; Maple, C. Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection. *Sensors* **2024**, *24*, 4901. [CrossRef]
33. Arfeen, A.; Ahmed, S.; Khan, M.A.; Jafri, S.F.A. Endpoint Detection & Response: A Malware Identification Solution. In Proceedings of the 2021 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 23–25 November 2021; pp. 1–8.
34. Bederrna, Z. Financial Perspective Thought Experiment on Russian Cyber Threat Actors. *Int. J. Econ. Finance* **2023**, *15*, 1–10. [CrossRef]
35. Cremonini, M.; Nizovtsev, D. Understanding and influencing attackers' decisions: Implications for security investment strategies. *Sch. Bussiness Work. Pap.* **2006**, *68*, 1–26.

36. Ruzomberka, E.; Love, D.J.; Brinton, C.G.; Gupta, A.; Wang, C.C.; Poor, H.V. Challenges and Opportunities for Beyond-5G Wireless Security. *IEEE Secur. Priv.* **2023**, *21*, 55–66. [CrossRef]
37. Rana, M.M.; Siddiqee, M.S.; Sakib, M.N.; Ahamed, M.R. Assessing AI adoption in developing country academia: A trust and privacy-augmented UTAUT framework. *Heliyon* **2024**, *10*, e37569. [CrossRef] [PubMed]
38. Ikpe, E.O. Adoption and implementation of artificial intelligence in small businesses in selected developing countries. *J. Health Appl. Sci. Manag.* **2024**, *8*, 26–34. [CrossRef]
39. Paul, F.A.; Ali, A.; Dar, D.R.; Saikia, P.; Ganie, A.U.R. Unmasking the Shadows: Battling the Cyber Crime in the Digital Age. In *The Palgrave Handbook of Global Social Problems*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 1–25.
40. Nfuka, E.; Sanga, C.; Mshangi, M. The rapid growth of cybercrimes affecting information systems in the global: Is this a myth or reality in Tanzania? *Int. J. Inf. Secur. Sci.* **2014**, *3*, 182–199.
41. Capestro, M.; Rizzo, C.; Kliestik, T.; Peluso, A.M.; Pino, G. Enabling digital technologies adoption in industrial districts: The key role of trust and knowledge sharing. *Technol. Forecast. Soc. Change* **2024**, *198*, 123003. [CrossRef]
42. Kotzias, P.; Roundy, K.; Pachilakis, M.; Sanchez-Rola, I.; Bilge, L. Scamdog Millionaire: Detecting E-commerce Scams in the Wild. In Proceedings of the 39th Annual Computer Security Applications Conference, Austin, TX, USA, 4–8 December 2023; pp. 29–43.
43. Hill, R. Dealing with cyber security threats: International cooperation, ITU, and WCIT. In Proceedings of the 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, Tallinn, Estonia, 26–29 May 2015; pp. 119–134.
44. Adenuga, A.O.; Abiodun, T.E. China-US cyber-attacks and international security. *Nnamdi Azikiwe J. Political Sci.* **2023**, *8*, 86–97.
45. Azubuike, C.F. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. *Nnamdi Azikiwe J. Political Sci.* **2023**, *8*, 101–114.
46. Oladipo, J.O.; Okoye, C.C.; Elufioye, O.A.; Falaiye, T.; Nwankwo, E.E. Human factors in cybersecurity: Navigating the fintech landscape. *Int. J. Sci. Res. Arch.* **2024**, *11*, 1959–1967. [CrossRef]
47. Marotta, A.; Madnick, S.E. Regulating Cyber Incidents: A Review of Recent Reporting Requirements. In Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023), Rome, Italy, 10–12 July 2023; pp. 410–416.
48. Shrestha, S. Moving from cash to cashless economy: Factors affecting digitalization in Nepal. *Nepal. J. Manag.* **2024**, *11*, 56–73. [CrossRef]
49. Passas, N. Report on the debate regarding EU cash payment limitations. *J. Financ. Crime* **2018**, *25*, 5–27. [CrossRef]