Dissertation

by Xxx Xxx

Submission date: 30-Dec-2021 07:51AM (UTC-0800)
Submission ID: 1736488547
File name: Dissertation.pdf (386.68K)
Word count: 16236
Character count: 92718

Cyber Security Strategies and Challenges Faced by Financial Institutions

[STUDENT'S ROLL NUMBER]

[NAME OF THE INSITUTE]

ABSTRACT

The purpose of the study is to prevent and mitigate the attack that has already taken place in Pakistan. The aim is that the cybercrime training could be utilized in the prevention of corporate financial management training. The task of the financial management is to create a situation where every employee of the company gets a sufficiently good overall picture of the cyber threats and clear instructions for action. Investment is the financial market for the buying and selling of long-term loans or investments. This type of capital market helps organizations and governments pay their bills while protecting them from fraud. Commercial electronic commodities have replaced these significant markets . These resources include currency exchanges, investment banks, treasurers, and government departments. It shows that some online businesses and financial services are being used in Pakistan. It all started in mid-October 2018, when some Islamic bank clients received warning messages about monetary transactions they were not receiving .Due to unprecedented $ 2.6 million exchanges, Islami Bank closed its global rate cap on October 27, 2018. The scammers traded through ATMs around the world. Use of bank statements .When PakCERT investigated cybersecurity, it was determined that the 20,000 bank card data could be tampered with. With a high data high-data-rate, organisations need credit protection for data breaches. The control system must require the financial component to provide the appropriate information and data storage measures to ensure the reliable delivery of the product and the service component, protect the data services and its processes, and the efficient use of facilities. With advanced businesses covering the financial system through numbers and remote financial solutions, it is also responsible for supporting the group in risk management. As non-partisans, international organisations and development workers can promote public-independent dialogue, support

constitutional initiatives, and help build support structures that enable the sector to move forward with the rapid change of environment.

Table of Contents

CHAPTER ONE: INTRODUCTION

Background

In the 21st century, non-traditional threats have become more important than traditional ones. This period is called the "age of data"; as mechanical advances, data transformation, and correspondence have contributed to the rise of digital warfare. As a result, the violent movement of war zones from land, air and sea can be detected on the Internet. Digital conflicts are a real threat to public influence and protection, as they have far-reaching consequences that are exacerbated at home, around the world and abroad. Just as there is no digital activity between countries, this makes it difficult to identify an opponent. In the case of Pakistan, the Internet has spread to banking institutions, education as well as the military, as well as to the government (Salahdine and Kaabouch, 2019). In any case, Pakistan is lagging behind when it comes to limiting its position.

A large part of Pakistan is facing problems with illegal access. Pakistan has yet to establish a modern base to defend itself against digital threats. This has now jeopardised the security of the public in Pakistan due to the information insecurity of governments or individuals. In the interests of public and private protection, various laws have certainly been passed, and they are not very cost-effective. They are rude in Pakistan, So far, the project has been planned and proposed, but the parliament has not yet approved it (Hussain, 2019). This is certainly a disappointment for the government and other partners to ignore this issue. Pakistan needs to work effectively in this particular region. Pakistan's financial sector has expanded the excellent quality of its computer network and started putting financial offices online, but executives are not encouraged to try illegal transfers. In the financial district, ATM fraud has become commonplace. Programmers are introducing ATMs to hack into the card economy and extort other documents.

The website of the Pakistani Bank Allied Bank Limited was hacked, and programmers left their website, which their framework cannot do. In fact, even several different banks have been victims of digital attacks and lost huge sums of money. However, they ensure that defensive measures are in place. As a result, they do not specify their extent, but constant attacks have a serious impact on Pakistani society as a whole. The public seems suspicious of online banking services. The Pakistani authorities have developed a small plan to spend on research and innovation (Valasai et al., 2017.). The government does not see a significant need in this area, and therefore, they do not spend more on it. As a result, Pakistan has been experiencing a sharp economic downturn for some time. At the time, Kamran Ali Qureshi, the director of the Office of Science and Innovation, told the Pakistani Commission that Japan was burning a 25% budget for research and innovation, while Pakistan was spending less than 1%.

At that time, the advisory group came to the conclusion that we now hope to eliminate the enemy of scientific behaviour and give this area more economic importance. Digital warfare is more complex than traditional traps in Pakistan and India. Pakistan does not focus on innovation; however, India invests more in its mechanical state and inhibits Pakistan's digital warfare. Israel supports India against Pakistan. As a result, Pakistan lags far behind India in terms of research and innovation. India has more complex innovations than Pakistan. This factor undoubtedly makes our country unstable (Rahman and Shurong, 2017). Digital countries have two equivalent countries that protect them. However, Indian programmers are much better than Pakistani programmers and exceed the protected limits of digital delimiters. As a sovereign state, Pakistan must take prudent measures to defend itself against digital threats.

In both countries, digital information attacks or breaks each other. With India in such a position, it creates a dangerous situation for Pakistan as it does not have the right basis to know

about digital threats. To control Pakistan, some countries say, requires powerful digital forces to prevent digital attacks. Unfortunately, Pakistan's digital military is lagging behind incomplete innovation. There are few companies in Pakistan that reduce digital awareness. The Pakistan Information Security Organization has launched a cyber-security campaign to raise public awareness. If NGOs can pay attention to the population, the government seems to have little interest in such activities. At this point, Hussein Sayed's secret agent Mushin introduced Pakistan's first digital protection bill, called the 2014 Security Council Bill, which aims to manage traditional risk rather than risk (Awan et al., 2017). This poses a natural threat to Pakistan's public security.

However, this law has not yet been passed because it is not interested in the government. Pakistan currently has some laws on cybersecurity, but many of them are not strict, and others are not enforced. This is a major reason for Pakistan's digital warfare. Pakistan has a digital platform called Public Cybercrime Response Point. Its main task is to combat digital hidden words related to data collection, financial problems and illegal stimuli. In fact, it is not very economical due to the digital ignorance of the Pakistani people. People have no idea how to break crutches, and others think it could make it harder for them, so they get stuck (Awan et al., 2018). However, government research institutes also cover Facebook, Twitter, Google, Skype and other similar cybercrime. It is gratifying to draw attention is not so realistic.

Pakistan faces growing cybersecurity challenges. Due to Pakistan's increasing reliance on the Internet, explore more weaknesses in information technology. Here are some of the challenges. Pakistani authorities have restricted the number of destinations that are sterilised due to offensive information available (such as YouTube and streaming) available through various applications. Thus, it created a dangerous situation for the state as it clearly shows that the administration is not energetic enough to adequately avoid this fate. Pakistan Telecommunications Agency is a

government agency that establishes or maintains telecommunications (Afshan et al., 2018). Handle all correspondence and circumvent illegal or disruptive sites to multiply the reasons for digital protection.

In 2012, 2013, the PTA closed 15,380 websites/subscriptions because they contained frightening information, but is this office not as good at banning places like YouTube? It remains open in Pakistan, a testament to the government's greatest disappointment. This will lead to an embarrassing situation regarding public safety in Pakistan. In addition, the US National Security Agency monitors Pakistan through online correspondence. They seized 13.5 billion emails, telephones and faxes, making Pakistan the second most important country the NSA has seen after Iran. It is a matter of concern for Pakistan to properly address this issue and take appropriate measures to verify its knowledge or framework for such espionage activities (Al-Muhtadi et al., 2019). The financial sector is improving online addiction and providing the public with a bankruptcy office in Pakistan, but the structure is insecure, so they are losing public confidence in the online financial system.

The private financial companies in Pakistan do not offer their customers legal protection, and therefore, people are more willing to store and save money at home than in banks. Manual credit transfer of funds from branches to different branches takes too long, say five to ten days, due to slow cash flow and due to one company or another this ton is left. People quit big contracts because they do not get their money properly (Noor et al., 2019). Nowadays, many frightened business relationships and mysterious meetings take place all over the world. They have more sophisticated digital innovation and highly skilled people. When people are involved and connected, they work independently. No law can be given to them, as their observation is also an

important criterion. As a result, these anonymous companies and parliaments create a very dangerous environment for public safety in Pakistan.

The Pakistani framework cannot fight against or prevent illegal entry. In addition, there are a number of panicked organisations operating in Pakistan that point to a more difficult security situation in Pakistan. Lack of attention to digital technology in humans is also becoming an increasingly serious challenge. People do not know how to protect their information against hackers or illegal access because they are being abused. Many Pakistani programmers claim that Pakistan's official database and registration authority are insecure. NADRA information is, in fact, public and therefore, it must take effective steps to keep website secure (Glavee-Geo, Shaikh and Karjaluoto, 2017). Because Pakistan is such a convenient place, there is a unique knowledge of Pakistan and, therefore, a real threat to NADRA. This requires existing methods to ensure the security of the information they develop. Hacktivism is not controlled in Pakistan, programmers in the current plan are destroying many official destinations in the Pakistani administration, and it is completely inappropriate for a government agency to do so as they lack innovations to prevent these digital attacks.

Research Aim

The purpose of the study is to prevent and mitigate the attack that has already taken place in Pakistan. The aim is that the cybercrime training could be utilized in the prevention of corporate financial management training. The task of the financial management is to create a situation where every employee of the company gets a sufficiently good overall picture of the cyber threats and clear instructions for action. The training material is intended mainly for small and medium-sized

enterprises, but it can also be used by public authorities and larger companies, where applicable. The training material can be used to improve the company's cybersecurity management, management's cybersecurity awareness and the company's competitiveness, as well as to secure the company's reputation and business continuity.

Research Objectives

- To analyses the effectiveness Cyber Security Strategies and preventing cyber threats by Financial Institution in Pakistan.
- To improve the company's cybersecurity and financial institution in Pakistan.
- To provide recommendations for improving cybersecurity in Financial Institutions in Pakistan.
- To identify the risks, arise in Financial Institutions in Pakistan regarding cyber-attacks.

CHAPTER TWO: LITERATURE REVIEW

Risks in Financial Institutions in Pakistan Regarding Cyber-Attacks

With the increasing use of internet services to increase integration, governments are transforming their centralized services into internet services. The use of Internet services in government programs has increased the risk of destroying security systems from the inside out. Based on published reports (Department of Homeland Security 2014, Reddy, Reddy 2014, Jang-Jacquard, Nepal 2014, Elmagrabi, Losavio 2014, Sebastian Bortnik 2012, APWG 2013, Osterman Research White Paper 2015.) and a conference held in the United States. Found that online experts may have the ability to build networks, slow down, or reduce attacks on cyber services or services linked to government documents (Zhou et al., 2019). The security, stability, and integrity of State property and the public service are also a concern for institutions, as the increasingly severe attacks on privacy information are another threat to the economy and national security. In Salahdine and Kaabouch, (2019), the cyber services organization faced a significant data security crisis following Hamas leader Mahmoud al-Mabh. Assassins used their three Europeans to steal from British citizens in Israel. According to a New York Times report, the malware (Stuxnet, Flamer virus) infected the Iranian nuclear agency and nuclear facilities before fleeing and destroying the website. Also, along with another report published on October 16, 2014, the phishing campaign Gcaza and Von Solms, (2017) created several people who discovered Dyre / Dyreza bank malware's use to create user / authentic accounts. And send the information collected to the attackers. Dyre / Dyreza

banking malware brings a new problem to developing countries and is often created by senders, installers, users, themes, and payers.

Digital Financial Services (DFS) has an excellent opportunity to see the integration of financial resources and help improve people's lives. Thus, cybercrime has emerged as a significant problem in developing countries' financial markets and threatens to undermine developing countries in other sectors, including finance (Al-Muhtadi et al., 2019). In recent years, financial markets in Sub-Saharan Africa, East Asia and the Pacific, Latin America, and South Asia have been hit by the rapid growth of severe Internet and data - and markets with high DFS1 trading volumes have been severely affected. Although the Asian market has the highest use of mobile phones and phone numbers, they are also at risk of being attacked by cyber attacks on office fees. In 2016, financial institutions in Bangladesh, Indonesia, Japan, the Philippines, Taiwan, and Vietnam were hit by a series of attacks (Awan et al., 2017a). Cybercrime is also growing in sub-Saharan Africa and Latin America, with criminals growing faster in these two regions than in any other region. One explanation for this situation may be that DFS applications are often used to use insecure and unsafe methods to protect financial transactions' security, making DFS work with clients. Buy it easily. Also, as governments develop more robust defenses against cyberbullying, hackers seem to have shifted their focus simply from looking at the DFS market in the future with their fragile use.

Many countries are adopting radio services, and Pakistan is one of the developing countries where many organizations are using information technology in their facilities. Top governments

are showing their willingness to use these. types of art and services in their design. Buildings. NADRA (National Database and Registration Authority) is Pakistan's official state-of-the-art certification body used by banks, passport offices, electoral departments, telephone, and the FBI (Federal Bureau of Investigation), among others. Maintain population information (Wolf, 2020). According to the report (Threat Track Security 2014), NADRA is one of the world's leading organizations due to its use of advanced service technologies. Currently, European countries are using the SCAP (Security Content Automation Protocol) algorithm for their NVDs (National Vulnerability Database), which data that allows risk assessment, security measurement, and compliance (Awan et al., 2018). Experts have observed attempts to breach confidential information (CyberSecurity - Stanford, CA, USA 2014, Pro Pakistan 2013). Meanwhile, NADRA may be the target of a terrorist attack to close down or harm its central services, violate people's confidential information, and use it for their purposes.

Investment is the financial market for the buying and selling of long-term loans or investments. This type of capital market helps organizations and governments pay their bills while protecting them from fraud. Commercial electronic commodities have replaced these significant markets (Venkatachary et al., 2018). These resources include currency exchanges, investment banks, treasurers, and government departments. It shows that some online businesses and financial services are being used in Pakistan.

Pakistan is also a developing country that is starting to promote cyber security. Therefore, confidentiality is a critical issue for organizations. For example, social networking sites provide a

platform that allows users to communicate freely and share personal information with friends. But cybercriminals create these websites to steal personal information, including location (Gcaza and Von Solms, 2017). According to security experts (Threat Track Security 2014), the expected cyber threats in 2015 are shown in Figure 4. A high number of APTs, and a minimal number of harmful cell threats. And again, the worst attacks gave 23%, while non-days of attacks and internal threats were 13.5%. The percentage of potential network threats in 2015 is shown in Figure 5. 28% are RCP (remote call method) and SQL injection, the second is about 23% chance, and the other - 25%, browse 17%. Cross-site scripting - 7% It was also found that most online services were captured in 2015, as shown in the pictures above (Shah, 2018). And again, Pakistani politicians need to lay the groundwork for a secure future.

Cyber threats and policies in Pakistan

Following the theft of confidential information by the US. The National Security Agency (NSA), the National Telecommunications and Information Technology Security Council (NTISB) have recommended laws to protect governments, agencies, and their operations from attack. On the line. The Cabinet statement states that "these views raise serious concerns about the implementation of all laws and regulations," and "the United States, a leading country in communication and technological know-how, the use of tools, various electronic means of communication (Awan et al., 2017b). Aerial studies such as satellites, telecommunications, power surveillance via email surveillance, radio surveillance, information transmission, vulnerabilities in IT network confidential information and another complex, hidden or past methods" (Glavee-Geo et al., 2017). In 2014, a report Rahman and Shurong, (2017) stated that cyber hackers had launched attacks on Pakistani websites that have in-depth knowledge of security and the government through

the promotion of DDoS. Investigation Agency (DDoS) According to an official document from the National Cybercrime Response Center Awan et al., (2017b), the group cannot investigate FIA air crimes (Valasai et al., 2017). An attack occurred. And surprise users through proxy agents such as TOR, free software programs that keep the website from being ignored.

Cyber Protection Policies in Pakistan

At present, no law enforcement law in Pakistan can effectively address cyber threats. Law enforcement in Pakistan, however, is inadequate and insufficient to communicate with threats on the Internet (Gcaza and Von Solms, 2017). This time it has eliminated all cybercrime and created all sorts of cybercrime and cybercrime issues such as hacking (access to information), interference with information and technological systems, especially false online line attacks against ICT facilities, illegal fraud by members of the public, identity theft and viral exploitation and risk in testing ICT system (uddin Ahmed et al., 2019). These criminal offenses cannot be adequately reported or punished before the law. These unique and unusual crimes require a new and comprehensive approach that will focus on the character of individuals/organizations on the Internet (Glavee-Geo et al., 2017). The Tanzanian ambassador-initiated Pakistan to establish a Cybercrime Unit (CCU) to deal with crime, create appropriate legislation, and set up a Computer Emergency Response Team (CERT) to facilitate its operations (Salahdine and Kaabouch, 2019). Tanzania has lost $ 6 million to various air courts, forcing them to upgrade CCU and CERT. Angels officials discussed the $ 455 million lost each year due to cybercrime and computer theft (Gupta, 2018). It has been observed that hundreds of millions of data records from developed countries have been violated. In this regard, developed countries such as Pakistan should promote anti-crime laws in developing countries (Rahman and Shurong, 2017). In January 2015, the

National Assembly of Pakistan introduced the Prevention of Crime Act 2015, unveiled by the Minister of Information Technology and Communication Afshan et al., (2018), which addressed the following key issues.

We are improving the right to use new search opportunities, which are not available, such as searching and retrieving international evidence using selected methods. Instructions for the manufacture of electronic certificates, orders for the maintenance of electronic certificates, delivery of road information (Hussain, 2019). The collection of factual information under certain circumstances and other powers is required to thoroughly investigate online offenses. The very nature of the new power required to investigate and remedy these offenses requires compliance with their functions and the protection of the people to freedom of expression under the constitution (Noor et al., 2019). It can be achieved by strengthening defenses and establishing new defenses, especially with the new power and emergency.

The introduction of this new law will effectively protect crime and provide national security by providing and building a secure investment environment in ICT, Governor, and e-commerce (Noor et al., 2019). And again, it also includes important protections for the disclosure of these measures and for many measures to protect citizens' privacy. Thus, it did not work to expose citizens to remove threats from all cybercriminals at home and abroad. It is the first major government initiative to prevent cybercrime and promote national security on the Internet (Irfan et al., 2017). However, other requirements need to be added to protect the government and the citizens of Pakistan.

Effectiveness of Cybersecurity Strategies in Preventing Cyber Threats in Financial Institutions

When we think of cybersecurity, the first thing that strikes me is cybercrime. Illegal activity in the context of cybercrime, where computers are used as a primary source of training and theft (Wolf, 2020). Cybercrime is often defined as a crime which involves using a computer and the Internet to steal personal information, track down searchers, and search for information (Awan et al., 2017b). As modern technology is so essential to human life, crime in the technology sector grows together. Malware attacks co-occur between tools, software objects, and communication components, and improper use of an existing image. Cyber attacks are a direct attack on the Internet against an organization that uses the Internet to disrupt, hacking, crippling, and illegally use large IT devices (Gupta, 2018). Understanding cybersecurity has a positive effect on organizational performance. Excessive computers are a severe problem in many lands.

It is widely believed that cyber terrorists are intelligent and have been able to launch attacks on the privacy, accessibility, and organization of various technical services, such as data management agencies (Salahdine and Kaabouch, 2019). The security, mobility, and stability of IT resources and government services in the country is another administrative challenge, as the increasing number of attacks has been a threat. national security, resulting in financial losses and other vital data. It is estimated that by the year 2020, 38.5 brick-making technology will be connected to the Internet to create and distribute confidential information worldwide (uddin Ahmed et al., 2019). In this case, two new problems arise, such as information unrelated to multiple scenarios' availability. A complex database is a database that changes depending on the type of

product and uses standard rules and different rules for sharing information (Al-Muhtadi et al., 2019). At the same time, many events are a set of facts and actions that flow into information and communication systems.

The data and records on 19,864 cards, which belong to 22 Pakistani banks, show the dark side, a survey conducted by Pakistan Emergency Response on the PakCERT Budget. It all started in mid-October 2018 when some Islamic banks customers received warning messages about currency exchange, which they did not receive (Rahman and Shurong, 2017). Due to unparalleled transactions amounting to 2.6 million (USD 18,584.70), Islami Bank closed its global payment system on October 27, 2018. The scammers have made international transactions through ATMs. Using documents issued by the bank (Hussain, 2019). When PakCERT surveyed cyberattacks, it found that the information on 20,000 bank cards could be compromised. And again, the news might explain that some of you recently received from your banks. The card has been blocked from international trade for security reasons. On October 26, 2018, a copy of the data and information from more than eight thousand bank cards was posted on a dirty website (Gcaza and Von Solms, 2017). When everyone thought the storm was severe on October 31, 2018, the world's second round was given more than 12,000 Darknet cards, including 12,000 cards from Pakistani banks. Islamic Bank was the largest bank to go public, but the statement said most of the control cards from the 24 banks were available to buy over the counter (Shah et al., 2018).

The dirty website is a hotspot for criminals and cannot be fixed without software, anonymous communication (Noor et al., 2019). The news came after an airstrike at Pakistan's

Islamic Bank last week, but $ 20,000 was withdrawn from their server. These papers' retail price increased from $ 100 to $ 180 (from $ 13 million to $ 440). Of all the banks, HBL, the world's largest bank, was hit hardest by more than 8,000 cards, followed by UBL, Standard Chartered Bank, MCB, and Meezan Bank, each with a thousand cards (Shah, 2018). Alfalah Bank, Islami Bank, and Punjab Bank were among the banks to view more than 500 of their cards on the website or the Internet. Depending on the packet, copies of credit card information can be obtained in two steps (Valasai et al., 2017). First, signs such as full name, address, phone number, card number, and expiration date can be used by any order to purchase online. The second instruction is represented in an attempt to be abandoned (Noor et al., 2019). It means that the offender would have wanted to read the card information at the ATM or on the business computer or unlicensed trading equipment.

The Electronic Crime Prevention Act views the Internet as a place for modern communication. The law also states that cyberattack control should be done to promote information security and value (Zhou et al., 2019). In this regard, the Act promotes CERT as a legal mechanism for accountability. CERT's primary goal is to control and reduce any injuries, preserve evidence, respond quickly and effectively, prevent similar incidents in the future, and obtain information about threats to the organization. To this end, the Pakistan Telecommunications Authority (PTA) has developed an implementation plan called "CERT (Computer Emergency Response Team) - Pakistan Telecommunication Sector Implementation Plan" (Glavee-Geo et al., 2017). The format is suitable for parts of the national network and advises PTAs on building those sections. It is a form that describes the functions and functions of CERT. Telephony in Pakistan is 70 percent, with 140 million mobile users, and among them, three to five million users connect via the Internet every hour (Salahdine and Kaabouch, 2019). Because of these numbers, breaking and

destroying, increasing breach of privacy and security in the Pakistani communications community, can control the country. With its users from electrocution, CERTs come first.

Pakistan has faced cyberattacks in recent years. On the eve of the 70th anniversary of Pakistan's independence, the Ministry of Defense's websites, the Ministry of Water and Energy, the Ministry of Information, the Ministry of Environment, and the Ministry of Food Security were attacked (Awan et al., 2018). Those events took a long time to shame and expose the scarcity of the world. In 2010, it was a similar pattern, but several attacks were recorded, including the collapse of 36 visitor websites (Zhou et al., 2019). In 2018, the attack was not only on government departments but Careem's request, designed to call travelers, was made on the website. As a result of the attack, information on the database of 14 million users from different countries, including Pakistan, was compromised. The information indicates that email ID, customer information, traffic, and phone numbers have changed (Noor et al., 2019). Similarly, cyberattacks at many banks have emerged and are frequently increasing in Pakistan.

The Federal Investigation Agency (FIA) has reported that almost all Pakistani banks were attacked by cyberattacks in 2018, resulting in financial losses in their accounts (Valasai et al., 2017). Thus, the State Bank of Pakistan, which regulates all banks' activities, has voted and said cybersecurity been violated. It is not known what bullying means and how to deal with it (Noor et al., 2019). A final agreement for all banks operating in Pakistan is at risk of cyberattacks.

The global financial sector is facing two key issues. First, differentiate the data, which the machine converts using different modes and different communication rules. Second, many processes require a lot of knowledge and experience to get into data and communication (Wolf, 2020). The Delegation of Tanzania Pakistan has recommended creating a Cybercrime Unit (CCU) to address offenses, create standards and establish a Computer Emergency Response Team (CERT) to facilitate its implementation (Salahdine and Kaabouch, 2019). Tanzania has lost $ 6 million to several air courts that have forced CCU and CERT to grow.

Officials say they lost $ 450 million last years from cybercrime and online theft (Awan et al., 2017a). Also, hundreds of millions of documents from developing countries have been produced incorrectly. In this regard, developed countries such as Pakistan should encourage and the more prominent countries a plan to fight crime. To save the lives of innocent people, we encourage you to make proper international orders based on real life. Also, new protections are needed to protect global privacy (Noor et al., 2019). It is an essential step in communicating with IT. In countries that use a wide range of equipment, especially electronic location monitoring, surveillance, and aircraft such as voice recording, satellite measures can be taken as required (Venkatachary et al., 2018). Open the message and delete the emails. Leakage, radio surveillance, and weak IT communication secretly or openly transmit confidential information and other complex media (Irfan et al., 2017).

Pakistan's financial institutions include banks, financial development (DFI), microfinance banks (MFB), non-banking companies (NBFCs), insurance companies, Modarabas, and other

financial institutions. Pakistan's financial institutions are mainly made up of banks because they hold most of its monetary value as a percentage of GDP (Zhou et al., 2019). Pakistan's State Bank (SBP) controls banks, DFIs, companies listed by MFBs, while Pakistan's Securities and Exchange Commission (SECP) regulates NBFCs, insurance companies, and Modaraba companies.

Recommendations for Improving Cybersecurity in Financial Institutions in Pakistan

With the increasing use of the Internet and its widespread availability, the web is expanding, making it easier for attackers to target the various services (Gcaza and Von Solms, 2017). To prevent attacks from the website, CERT (Computer Incident Response Team) plans to participate in the Electron Crime Prevent Act. Organizations should strive to build good computers. It is a must-have for any Affiliate promoting any program. Between 30 and 35 percent of that bandwidth is lost because the datasheet does not go directly to the data centre (Noor et al., 2019). On the other hand, they do so with different access to 'different locations' and thus require more time and bandwidth. To address this, Pakistan needs a Class Internet Exchange Point (IXP).

The department is currently discussing rules on internet security. The role of educators, military and students in combating air threats are essential (uddin Ahmed et al., 2019). Co-operation is needed for the public and military to organize cybersecurity monitoring and response. Protection is at the national, group, and system level, and the response also needs to be multi-component and multi-component. There is a need to improve world-level advice to address the website's problems, which need to be evaluated and implemented through national and industrial CERTs (Shah, 2018). First and foremost, national law or constitution defines the purpose,

objectives, and government objectives to ensure online security (Gupta, 2018). The drafting law for cybersecurity is under the Ministry of Information Technology and should be considered finalized and published.

While cybersecurity requires action and initiative, it requires a balance between security and civil rights. Any law enforced on the Internet will fail if you violate copyright laws. The role of education and training in cybersecurity is essential in problem-solving (Zhou et al., 2019). The situation should take precedence in school. Even at low levels and with graduation degrees, the type is not suitable for providing cybersecurity leaders and experts (Zhou et al., 2019). The quality of the programs should be upgraded to meet the existing challenges. Even the Pakistani Telecommunications Authority does not have the requirements for people to work in cybersecurity (Gcaza and Von Solms, 2017).

In a report released on July 5, the State Audit Office stated that the threat of intimidation has become more complex and challenging and that the prices of banks and other financial institutions have already suffered" lost hundreds of millions of dollars (Salahdine and Kaabouch, 2019). "This statement contains guidelines on how banks and financial institutions can improve online security, and it begins to address the failure of many organizations to value data security until the outcome (Al-Muhtadi et al., 2019). He also warned that the growing number of mobile operators should be secure, and regulators should hire IT experts to monitor small and medium-sized enterprises. to reduce risk; therefore, good preparation or response requires timely knowledge " (Shah et al., 2018).

In emerging markets, online attempts by governments or government agents often undermine the private sector as consumers. Due to limited capabilities and resources, International internet security governments often focus on serving government officials with serious complaints - the most important factors for stability and integrity (Zhou et al., 2019). Thus, even with establishing its offices and significant markets, skills and resources are often inadequate to properly train and train civil servants, hire professionals, and replace them (uddin Ahmed et al., 2019). From the support required by judges and administrators. Organized National Computer Security Event Response Team (CERTs) or National Computer Security Event Response Team (CSIRTs) to assist in combating IT or data (Salahdine and Kaabouch, 2019).

More and more countries are building such structures in Africa, and some of them are already in place. As such, CERTs and CSIRTs are often less able to cope with the rapid changes in the cyber threat environment, undermining the advice and support they can provide to the industry (Gcaza and Von Solms, 2017). Only a few countries have CERT, which specializes in responding to threats and financial events. In general, the amount of service provided by these groups is minimal, services are not available per hour, and it is rare to include an emergency cable (Rahman and Shurong, 2017). Key job opportunities include central security, industry-wide and smart threat circuits, service consulting systems, financial equipment consulting services, and business training programs for individuals (Gcaza and Von Solms, 2017).

In many developing countries, with few emerging markets and developing countries, NGOs work together to share the threat of knowledge and work together to combat financial scandals and cybercrime (Venkatachary et al., 2018). In many cases, paid organizations have been at the forefront of resolving the cyber threat exchange. Sometimes only a handful of participants agree to work together to form a partnership, and over time other parties join them (Noor et al., 2019). Donors come in various locations and are not usually limited to group funding; it also included companies from experience information, communication, and intelligence components (Zhou et al., 2019). Recently, there has also been a dramatic increase in the number of internet and financial services companies (called FinSec companies), often small in size, are seeing a rock in the market in product offering and service FSP communications with fintech (uddin Ahmed et al., 2019). Another boost is the increase in the number of insurers, especially in large insurance companies around the world.

As you work to make online aid aids available in developing countries, two significant challenges arise. First, these countries have a limited amount of cybersecurity expertise, especially experts who understand threats on the air in DFS. Second, there is the possibility that the economies of developing countries may not be able to meet the need for families to take full advantage of the low-cost telecommunications system (Al-Muhtadi et al., 2019). Therefore, an excellent solution to a shortage of telecommunications may be to build practical online communication circuits that can increase the knowledge available in the region and build in more significant crisis, serving the needs of many countries (Irfan et al., 2017). These regional states can be viable financial and communication partnerships, are capable of serving both the public and

private sectors, and can serve as a platform for non-support for public-private partnerships and exchanges, including exchanges for sensitive threats (Shah et al., 2018).

With stops in many countries, these areas can facilitate cross-border, rapid system management and share regional practices, threats, and best practices with other regions of the world (Rahman and Shurong, 2017). Another benefit of regional sites is their ability to connect to the Internet in many developing countries, providing support, information, and tools that may not be available at the regional level. For example, the central cybersecurity zone in West Africa could pose a serious threat to cyber support in Europe (Gupta, 2018). Several European and African participants are working to create and improve such " natural resources'. At present, there are very few attempts to support workers in many countries and facilitate dialogue and sharing borders (Noor et al., 2019).

One example is the FS-ISAC Threat Distribution Network, which expands globally to form regional regions in Asia and Europe. Most of the world's efforts seem to be globalization and the sharing of industrial services; they are very familiar with the type of services provided (Irfan et al., 2017). Young and middle-aged donors and governments with limited resources and capacity are critical of these efforts to address. They need a general store that allows them to access professional services and share information with their community affiliates (Gcaza and Von Solms, 2017). To effectively support the DFS sector's growth in developing countries, more international efforts are urgently needed to provide costly and efficient services to the (digital) financial services sector (Venkatachary et al., 2018).

With a high data high-data-rate, organizations need credit protection for data breaches. A well-thought-out strategy may include protecting your website with single security that includes all protections - firewall, antivirus, anti-spyware, and malware - as security software from multiple clients can ultimately work together (Irfan et al., 2017). Also, employees should be trained to prevent cybercrime - for example, not to open emails, radio, or media from suspicious or anonymous people. Combining good security with business insurance helps to protect the company's financial position and its reputation and public trust (Salahdine and Kaabouch, 2019). Moyle saw buyers and sellers of accurate money information. He saw security leaders advising on stupid water conservation methods. "Understanding best practices for data management and data storage is important for everyone, not just IT staff, with knowledgeable experience,"

Banking services are beginning to count faster and are increasingly being used by low-income, low-count counts in developing countries (Valasai et al., 2017). However, at the same time, as this progresses, event teams face growing risks from computers trying to attack their systems and customers. If this group continues to build and maintain loyal customers in the financial systems, it needs to strengthen its defenses and have the ability to respond and recover from potential attacks (Salahdine and Kaabouch, 2019). Maintaining a financial component and overseeing global financial progress involves relying on FSPs to promote the security of their operations and requiring an all-encompassing approach (Zhou et al., 2019).

Governments and services should work together within their jurisdiction and staff around the world to share expertise and support each other in the fight against criminals (Al-Muhtadi et al., 2019). The top six moves need some of their weak teammates' support as this will bring benefits in terms of listening and help keep their teammates and confidence in the team. Also, discussions

about cybersecurity and data security in the financial sector should go hand in hand and be included in discussions about data security and your data's proper use (Salahdine and Kaabouch, 2019). Information protected by the rules will not work if the information and information contained in it are not protected from unauthorized access.

The control system must require the financial component to provide the appropriate information and data storage measures to ensure the reliable delivery of the product and the service component, protect the data services and its processes, and the efficient use of facilities (Awan et al., 2017b). With advanced businesses covering the financial system through numbers and remote financial solutions, it is also responsible for supporting the group in risk management (Shah et al., 2018). As non-partisans, international organizations and development workers can promote public-independent dialogue, support constitutional initiatives, and help build support structures that enable the sector to move forward with the rapid change of environment (Glavee-Geo et al., 2017).

Records are vital for financial institutions. As online banks increase the amount of information generated by businesses, they need to store it. Classified courses are encouraged because they help organizations prioritize their risk reduction risks to their current threats (Zhou et al., 2019). Organizing information by type, value, and understanding not only informs you of the security you are using but can also be used to test your compliance. If you work with third-party products, you should check their cybersecurity as much as you can (Venkatachary et al., 2018). Third-party risk analysis models can help identify customer protection holes. Comparing your types of customers with your risk and personal history and patient data can continue to help you rank customers based on the threats they make to your business. From there, you can take

appropriate steps to reduce any risks (Salahdine and Kaabouch, 2019). You also need to create an internal set of tasks for the supervisor representative to facilitate the process and keep customers compliant at all times.

CHAPTER THREE: METHODOLOGY

Research philosophy

The current research has chosen pragmatism as its research philosophy. The research philosophy is defined to explore the problem through multiple approaches (Hayes, and Heit, 2018). Pragmatism states that there can be various solutions to a problem and that there can be multiple reasons for a particular situation (Seo, et al., 2019). Therefore, this philosophy is used for mixed-method research. This philosophy explores the research through various approaches and strategies; through the evaluation of these approaches, there are many aspects to a problem or issue (Mobily, and Morris, 2018). The current research has focused on exploring the issues that are faced by financial institutes regarding cybercrime and the role that cybersecurity institutions play in preventing these cybercrimes.

The need of selecting pragmatism as its research philosophy is to ensure that the research is analysing the research aim through both primary and secondary data available (Seo, et al., 2019). Pragmatism evaluates the research question with the approach that the research has further solution or concepts that can be explored through it (Yao, et al., 2018). The aim behind opting pragmatism for the research philosophy is to understand the overall aspects of the selected research problem (Hayes, and Heit, 2018). Therefore, the research had included a mixed-method approach for its methodology to understand various sources of information through which the data can be generated and analysed in order to reach a conclusion (Kennedy, 2019).

The potential ways in which this can be done is through the application of both types of data analysis tools (Barclay, et al., 2017). Thus, the current study has incorporated questionnaire distribution and secondary data that is available on the research aim (Seo, et al., 2019). Through the questionnaire distribution, the researcher shall be incorporating various opinions of the options

that are available to financial institutions regarding cybersecurity and the extent to which these institutes are protected (Kennedy, 2019). Another approach that the researcher shall take is to incorporate the secondary method, which is to gather and analyse literature present on the strategies used by cybersecurity institutes to protect financial institutes.

Design of experiments

The current study has opted for a mixed-method design for its research. The qualitative design is a part of the chosen research design (Kennedy, 2019). Qualitative design is a research design that evaluates the research through a theoretical approach. This approach shall be using a broad and theoretical approach in evaluating the research aim through exploring various theories (Kral, et al., 2019). The current research shall be exploring research objectives by gathering information related to cybersecurity strategies (Hayes, and Heit, 2018). The data that is present on the approaches that are available on the approaches that are being used by cybersecurity for financial institutes (Kennedy, 2019).

The second part of the research design is a quantitative design that will be evaluated through numerical data. The data have been evaluated through a survey conducted by financial institute's representatives (Seo, et al., 2019). The cybersecurity options that are available to the financial institutes will be helpful to understand the challenges that are faced by financial institutes (McAbee, et al., 2017). The reason for the selection of these research design is due to the broad overall analysis that they provided to the researcher. Through qualitative design, a more broad and wide aspect of the answer to the research question was gathered. On the other hand, through quantitative design, more rigid, reliability and valid design have been understood to reach the

research objectives effectively (Yao, et al., 2018). Through mixed-method research design, the aim of exploring the research problem through multiple means was accomplished. The qualitative and quantitative design enabled the process of discovering the research elements with the aid of broad and theoretical means (Kral, et al., 2019). This was done by gathering various literary articles that are published regarding the approaches that have been used by cybersecurity. Similarly, the quantitative design was evaluated as well through a survey application that enabled the researcher to gather and evaluate data through numerical means (Yao, et al., 2018).

Implementation

The current research has used an inductive approach for the current research. Through inductive reasoning, the concepts research shall be collecting generalised data and move towards specific reasoning (Kral, et al., 2019). Through the approach, the researcher shall be moving towards exploring strategies that are opted by cybersecurity for financial institutions. Through the exploration of the broad information that is available on the approaches and the measures that are taken by cybersecurity, the specified information has collected (Seo, et al., 2019). This is conducted through the application of a questionnaire survey from financial institutes regarding the options that are available to them related to cybersecurity (Rust, et al., 2017).

The reason for choosing inductive reasoning is due to the intensive and first-hand data that it provides. Due to inductive reasoning, more elaborative results were generated that provide more close and prominent reasoning of the research results (Kral, et al., 2019). The mixed-method approach was opted to understand the core elements of the research through quantitative and qualitative means. Through inductive reasoning, a more crucial and broad result of the study is

available (Kennedy, 2019). The inductive approach provided broad and widening results to the problem as it explored various literature articles that are analysed for the potential strategies acquired by cybersecurity for the financial institute (McAbee, et al., 2017).

Collection of Results

The data collection method for current research is both secondary and cases occurred recently. The second part of the data collection process is through secondary data that is recently published.

The secondary data will include the literary articles that have been published regarding the approaches that are used by cybersecurity for financial institutions (McAbee, et al., 2017). The reason for the two kinds of data collection method for the research is to analyse the research through broad and multiple approaches. The two approaches have enabled the researcher to explore the researcher with the help of collecting effectual and relevant data for the research (Mobily, and Morris, 2018).

Sample size

The sample size for the current study is done through snowball sampling size. The sampling technique chosen for the current study is selected due to the relevance that the population have with the research (Janssens, et al., 2018). The sample size for the research is around 100 participants.

Inclusion and exclusion criteria

The potential articles included in the study were relevant to the research aim. The articles included in the study were published after the year 2017 (Hayes, and Heit, 2018). This provided the research with the latest data to be collected and analysed. Those articles were excluded from the study that was not well structured. Those articles were also excluded that were not sourced and well structured.

Ethical considerations

There are certainly ethical considerations that are needed to be followed, with the potential considerations to be kept in mind. The research ensured that the data collected from the research has kept in mind the entire ethical consideration (McAbee, et al., 2017). These included giving the authors their due credit whilst citing them in the research (Yao, et al., 2018). The authors included in the research has been well quoted, and any element that was not part of the initial sources has been omitted from the research. The participants that were part of the data collection process were communicated regarding the aim of the research and the reason for collecting data (Seo, et al., 2019). They were asked prior to collecting data from them, and if they decided to refrain from providing their data, then their wishes were honoured (Rust, et al., 2017). The information of the participants was kept confidential as well to ensure that their data were not used for any unethical means.

The exploration of cyberspace is digitally vulnerable, especially in Pakistan with uprising challenges. Some of the sites have become restricted with the available objectionable data such as various torrents and YouTube, which have become easily accessible with the help of different

software. There are robust websites PTA (Pakistan Telecommunication Authority) have designed with the government agency towards maintaining the establishment or maintenance. However, the threatening or illegal have regulated the whole communication by setting up for the betterment of various cybersecurity reasons. Moreover, in 2013 around 14,000 websites were blocked due to the objectionable data by banning by the agency. Therefore, government accessibility has shown a more significant failure. With 14 billion pieces of email, fax, phone communications have intercepted by making Pakistan the second highest country observed with the NSA after Iran.

CHAPTER FOUR: RESULTS, ANALYSIS AND EVALUATION

The current research has observed that with the amplified use of internet services to improve integration, governments are migrating their centralised services to internet services. The use of Internet services in government programs increases the risk of destruction of internal security systems (Firdous, 2018). Based on reports published and published at the conference on US Online, professionals can create networks, slow down or mitigate attacks on cyber services or services related to government documents. The study further developed that cybersecurity organisations are taking notice of the potential cybercrimes that are taking place. This was established in Syed and Javed, (2017) that Agencies are also concerned about the safety, stability, and integrity of the public property and public services, as other increasingly severe attacks for private Information pose another threat to the economy national security (Bukht, 2017).

Digital Financial Services (DFS) is an excellent opportunity to analyse financial resources' integration and improve people's lives (Baloch, 2018). Cybercrime, for example, is a significant problem in financial markets in developing countries, threatening to disrupt developing countries

in other sectors, including financial markets (Haq and Atta, 2019). The rapid growth of the internet and technology has impacted South Asia with high volume markets. Although telephone numbers are most commonly used in the Asian market, they are at risk of cybersecurity attacks for office fees. In 2016, a series of attacks hit financial institutions in Bangladesh, Indonesia, Japan, the Philippines, Taiwan and Vietnam. Cybercrime is on the rise in sub-Saharan Africa and Latin America, and crime is growing faster in these two regions than in any other (Pomerleau, and Lowery, 2020). An explanation for this situation might be that DFS applications are widely used to use effective techniques to protect the security of financial transactions for DFS to work with clients. As governments develop better defenses against cyberbullying, hackers don't seem to be shifting their focus to the DFS market for vulnerable future exploits.

The current study established Information related to the extent to which technology has evolved in Pakistan as this has led to the increase in cybercrimes as well. Pakistan is one of the non-industrial countries where many associations use innovative data in their offices. Major governments are showing a willingness to use them (Ullah, et al., 2019). The types of processing and services in plan. Structures NADRA (National Registration and Database Service) is Pakistan's leading certification body, which uses banks, Visa workstations, offices, telephones, and the FBI (Federal Bureau of Investigation), among others. Update population data in a timely manner (Syed, and Javed, 2017).According to a report, NADRA is one of the largest associations in the world as it benefits from the latest advances in governance. European countries are currently using the Security Content Automation Protocol (SCAP) calculation for their National Vulnerability Database (NVD), which provides Information for risk assessment, security assessment and compliance. Experts have identified attempts to infiltrate private data (Baloch, 2018).In such a case, NADRA may become the target of suppressed on the basis of fear of

reprisals, closure, or damage to their main services, ignoring people's secrets and using them to motivate them (Daugėlienė, 2019).

A research stated that Speculation is a financial market for buying and selling long-term loans or businesses. This type of capital helps associations and governments pay their bills and protect them from misinformation (Ullah et al., 2019). Commercial electronics have supplanted this important market (Tariq, 2018). These assets include cash transactions, venture banks, financial institutions, and government agencies. This shows that there are some online and financial services organisations in use in Pakistan (Firdous, 2018).

Pakistan is a non-industrial country that is starting to advance cybersecurity. So, confidentiality is a fundamental issue for society. For example, a space for interpersonal interaction provides a stage in which clients can communicate and share individual data with their peers (Daugėlienė, 2019). However, attackers encourage these websites to collect personal Information, including. According to security experts (Threat Track Security 2014), typical cyber threats of 2015 A large number of APTs and a small number of undetectable cellular threats (Bukht, 2017). In addition, very terrible attacks again showed 23%, while short attack periods and internal threats reached 13.5% (Syed, and Javed, 2017). The volume of potential organisational threats in 2015, CPR and SQL Infusion are 28%, the latter is 23% probability, and the other is 25-17%. It was also found that most of the online services were intercepted in 2015, as shown in the photos above (Pomerleau, and Lowery, 2020).In addition, Pakistani lawmakers must again prepare for a secure future.

Cyber Security Guidelines in Pakistan

Currently, no law enforcement in Pakistan can counter cyber threats. Legislative requirements in Pakistan are certainly low, and there is no link to online threats (Khan, and ANWAR, 2020). the research concluded that there is a need for cyber law enforcements to take proper action in Pakistan (Haq and Atta, 2019). As several studies stated that as they would morid of all cybercrime and led to a wide range of cybercrimes and cyber problems such as Hacking (data access), data resistance and mechanical frame conditions, in particular, linear attacks of online fraud against ICT, offices, illegal blackmail by people in general, massive fraud, as well as virus abuse and danger in testing ICT framework conditions (Tariq, 2018).These crimes cannot be adequately solved or denied under the watchful eye of the law.

The research studied that these unique and bizarre crimes require a different and broader approach, targeting individuals / associations on the Internet (Syed, and Javed, 2017).The regulatory bodied in Pakistan by establishing a Cybercrime Unit (CCU) to combat crime, take action and create a Computer Emergency Response Team (CERT) to carry out its tasks (Khan, and ANWAR, 2020).Tanzania lost $ 6 million in various aircraft, forcing them to redesign the CCU and CERT. The authorities discussed $ 455 million lost annually due to cybercrime and computer theft (Bukht, 2017).It has been shown that a large amount of corroborated intelligence has been ignored. Thus, for example, the created countries, Pakistan, must promote laws on enemy crime in non-industrial countries (Ullah, et al., 2019).In January 2015, the Pakistani National Assembly passed the Crime Prevention Act 2015, which was approved by the Minister of Information and Communication Technology Afshan and others. (2018) and addressed key complementary issues (Syed, and Javed, 2017).

The research studied that the country improved the ability to use new discoveries for available applications. The study evaluated that guidelines for the preparation of electronic guarantees, orders for the maintenance of electronic wills, transmission of street data (Firdous, 2018).In order to investigate online crimes in general, it is necessary to collect real data under certain conditions and with different forces (Tariq, 2018). The completely new idea of a new power needed to investigate and suppress these crimes requires their capacity and human peace of mind to be realised to ensure that they can be informed in accordance with the Constitution (Baloch, 2018).This can be done very well by strengthening protective measures and installing new guards, especially in view of the new forces and the crisis (Syed, and Javed, 2017).

The introduction of this new law will ensure crime and public safety by creating and creating a protected climate of risks for ICTs, administrators and Internet businesses (Ullah et al., 2019).In addition, there is another significant insurance for the transfer of these measures and for a range of measures to ensure the safety of residents (Bukht, 2017). As a result, no attempt was made to open up to locals to get rid of the threats posed by all cybercriminals at home and abroad. It is the most important government measure to prevent cybercrime and improve public safety on the Internet (Ahmed, 2019).However, various requirements need to be added to ensure the safety of Pakistani authorities and residents (Bukht, 2017).

Cybersecurity approaches to Prevent Cyber Threats in Financial Institutions

As the research evaluated the approaches of cybersecurity, cybercrime is was analysed the most. Criminal behavior has been linked to cybercrime, with the use of personal computers as an important source of preparation and search (Firdous, 2018).Cybercrime is generally a crime

involving the use of computers and the internet to collect individual data, search by search engines, and search for data (Pomerleau, and Lowery, 2020).Because today's innovation is so important to human life, crime is linked to innovation. Malware attacks occur simultaneously between devices, programming elements and pieces of correspondence, as well as abuse of the current image. Cyberattacks are an immediate attack on an online association that uses the internet to counterfeit, hack, delete, and illegally use massive IT equipment Khan, et al., 2018). Cybersecurity has a positive effect on hierarchical execution. Unwanted PCs are a serious problem in many areas (Syed, and Javed, 2017).

A research stated that it is generally accepted that cyber fear suppressors have a strong interest and have had the ability to attack, uncover and attack various specialised service associations such as intelligence for executives (Khan, and ANWAR, 2020).The security, flexibility, and resiliency of national IT and tax-deductible organisations is another challenge to manage as the number of threatening attacks poses a threat. public safety, financial disasters and other important information (Pomerleau, and Lowery, 2020). By 2020, it is estimated that 38.5 Block Making Innovations will be permanently connected to the internet to create and distribute classified data around the world (Bukht, 2017).In this case, two new problems arise, Data not related to the availability of various cases. One is a great dataset that varies depending on the type of article and standard usage guidelines, as well as various data-sharing guidelines (Haq and Atta, 2019).At the same time, there are many possibilities for incorporating different realities and activities into data and correspondence structures.

Pomerleau, and Lowery, (2020) stated that Information and records of 19,864 cards held by 22 banks in Pakistan presented the downside, according to a Pakistani study of the PakCERT budget. It all started in mid-October 2018, when some Islamic bank clients received warning

messages about monetary transactions they were not receiving (Khan, and ANWAR, 2020).Due to unprecedented $ 2.6 million exchanges, Islami Bank closed its global rate cap on October 27, 2018. The scammers traded through ATMs around the world. Use of bank statements (Syed, and Javed, 2017).When PakCERT investigated cybersecurity, it was determined that the 20,000 bank card data could be tampered with.

Another study stated that the news may further clarify what some have recently received from your banks. The card has been excluded from global exchange for security reasons. On October 26, 2018, duplicate Information and data for over 8,000 bank cards was posted on a dirty website (Baloch, 2018).At a time when everyone thought the storm was violent on October 31, 2018, more than 12,000 darknet cards were issued in the second round of the world, including 12,000 Pakistani bank cards (Daugėlienė, 2019). The Islamic Bank was the largest bank open to the entire world. However, the complaint indicated that most of the 24 bank control cards were available over the counter (Firdous, 2018).

It has been stated that Pakistan has faced recent cyber attacks. Shortly before the 70th anniversary of Pakistan's autonomy, targets of the Ministry of Defense, the Ministry of Water Resources and Energy, the Ministry of Information, the Ministry of the Environment and the Ministry of Food Security were attacked (Ahmed, 2019).These events have led to embarrassment and exposure of the guilt of the whole world. This was a similar example in 2010, but several attacks were reported, including 36 guest suites (Ullah, et al., 2019).In 2018, the attack took place in government offices, and Karim was asked to call scouts into the territory. The attack compromised data from a dataset of 14 million customers from different countries, including Pakistan. The data shows that email id, customer data, traffic, and phone numbers have changed

(Baloch, 2018).Cybersecurity exists in many banks and is generally on the rise in Pakistan (Haq and Atta, 2019).

Another study that the Federal Investigation Agency (FIA) explained that almost all Pakistani banks were attacked by cybersecurity attacks in 2018, and that their records indicate financial disasters (Firdous, 2018).As a result, the state bank of Pakistan, which controls all banking operations, voted to violate cybersecurity. It is not clear what bullying means and how to deal with it (Pomerleau, and Lowery, 2020).Cyberattacks are in jeopardy of a final deal for all banks operating in Pakistan.

In the area of global finance, there are two key points of contention. First, exchange Information that changes the car using different methods and clear matching rules. Second, many loops require a lot of Information and expertise to enter Information and correspondence (Daugėlienė, 2019).The Delegation of Tanzania and Pakistan plans to establish a Cybercrime Unit (CCU) to tackle violations, set standards and establish a Computer Emergency Response Team (CERT) to enforce it (Tariq, 2018).Tanzania lost $ 6 million due to a series of benches that limited the development of CCU and CERT.

Authorities say they lost $ 450 million a year ago due to cybercrimes and online theft (Syed, and Javed, 2017).In addition, a large number of records of agricultural countries were made in error. Thus, for example, the nations created must support Pakistan and the most incredible countries in the crime-fighting system (Haq and Atta, 2019). To save innocent people, we ask you to place appropriate global orders based on reality (Khan, and ANWAR, 2020). In addition, the new guarantees are expected to guarantee global protection (Syed, and Javed, 2017).This is an important step in talking to you. In countries where a wide range of equipment is used, especially electronic surveillance of the territory, reconnaissance, and aircraft, such as voice recording,

satellite measurements can be carried out as needed.Open the message and delete the messages. Spills, radio surveillance and vulnerable IT correspondence transmit private data and other complex media confidentially or transparently (Ahmed, 2019).

The study further stated that Pakistan's financial institutions include banks, turnkey event companies (DFI), microfinance banks (MFB), non-bank organisations (NBFC), insurance agencies, Modarabas and other financial funds (Ullah, et al., 2019). Banks are mainly Pakistani financial institutions because they hold most of their monetary value in the form of GDP levels (Zhou et al., 2019). The State Bank of Pakistan (SBP) regulates banks, DFIs and MFB-registered organisations, while the Securities and Exchange Commission of Pakistan (SECP) manages NBFC, insurance agencies and Modaraba organisations (Syed, and Javed, 2017).

The risks in Financial Institutions in Pakistan regarding cyber-attacks

As discussed during the literature review, it is clear that cyber-attacks are criminal actions to access data, which is confidential, the facts' security obtained through a company utilising any framework that is designed to identify (Ahmed, 2019). Cyber-attacks from various point of view are essential to suppress them. There are various attacks' forms, although the most commonly known are discussed in the following paragraph.

Several Forms of cyber attacks

Some attacks are particularly utilised to contempt particulate assets, for instance, an internet server for operators. Such attacks are commonly witnessed every year. It is a contest for error and trial to identify the passcode of the system. One of the fourth attacks on networks is an effort to brute force. In such an attempt, software of the computer was utilised to give various

combinations of passwords (Awan, Memon and Burfat, 2019). Another category is browser attacks, which are targeted at users on the internet. Such attempts can additionally motivate them to save the virus deprived of realising it. These attacks utilised fake application software has to replace, upgrade, or implement. Websites are additionally required to save malware. Approaches of high quality are to bypass complete networks based on browsers attacks to upgrade web browsers repetitively (Shad, 2019). Another type of attack addresses the Bash vulnerabilities, a comprehensive line of command shell of Linux and UNIX systems. As various installation is never upgraded, the susceptibilities yet are available on the internet. The issue is that Shellshock is all networks' target.

The external procedures' interruptions are completed by a distributed denial-of services damage of the attack to the webpage. The overflow externally of demands to a site on the internet server is yet known interruption event's type has the possibility needed and disturbing. For instance, a broad company that manufactures commercial furniture whose site buy web page will note is manifested for more than 18 hours; thus, events of this type may also establish an issue in the store based on the internet (Khalil, Usman and Manzoor, 2020). Another type of attack is to intercept data transferred over a connection, which is encrypted. Such attacks lucratively occupy data deprived of encryption.

These are identified by Hussain et al. (2017) as the most commonly found attacks today. The internal processes' disruption is additionally performed through a multipoint elimination internally that regulates the data by users, eradication, and encryption of the prime systems. Attacks backdoor are utilised for safeguarding general authentication for access remotely. Such attacks are included in the program software utilising the theme. These are included in the programs or established utilising an existing application. The rear doors are not such common

attacks. On the other hand, Thieves use botnet attacks (Shad, 2019). More than one or one malicious actors are thus from a distance controlling the systems of information.

Attackers utilised such attacks for activities, which are malicious or engage botnets to conduct activities, which are dangerous for the users. At the time, getting botnets computer systems in millions can be maintained (Ahmed, 2019). The perpetrators attempt to control users' data, data website accounts, social media, and other vital information. The user accounts' hacking is insignificant just in customer accounts on social media, which are not focused on their systems. Through this rationale, such interruption activities have very minute coverage in contrast to the rest of the interruption events (Haq and Atta, 2019). The internal operations' interruption has very small coverage in contrast to the rest of the interruption events. Internal operations' interruption takes place by denial of services of an internet network. In few scenarios, such interruption may consume time to be reoccupied in days, months, and weeks comprehensively.

Advanced regulations the networks' disposition to shift the malicious code amongst the linked computers' network to change at the same time it deteriorates the computers' operating system, erasing the files, controls the service routines and work to destroy the peripherals (Haq and Atta, 2019). The access, which is unauthorised rights, has a network to abolish a physical framework amongst the physical and digital world, in addition to underlining an exposure to the comprehensive framework, which can save existing life. Such type of activity needs comprehensive information of the framework and its network with important assets and structures of management shown in figure 1 below.

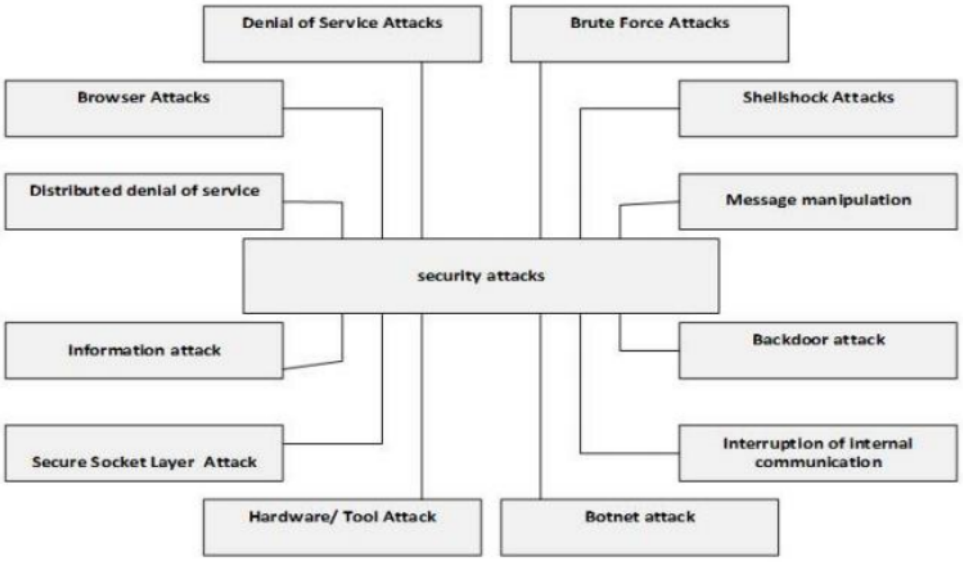

Figure 1 Management structure

The data and information on various amounts of cards that are among the clients of more than twenty-two financial institutions in Pakistan provide the signal to the dark side, as research by Alghazo, Kazmi and Latif (2017). It all begins at the end of 2018; at the time, few clients of Islamic banks obtained warning through text message cautioning them against the exchange of cash, that they did not. In an irregular trade amounting to the rest USD 18500, Islamic Bank congested its payment plans internationally at the end of the same year (Alghazo, Kazmi and Latif, 2017). Hackers carried out some international automatic teller machine transactions with debit cards issued by the banks.

The effectiveness of cybersecurity strategies in preventing cyber threats

In reality, when the researchers examined the cyberattacks, it recognised that data regarding twenty thousand cards were negotiated. Moreover, it can elucidate the news that a few users have received from their banks, who have currently shown that the car cards been blocked for transactions internationally for reasons of safety. During late 2018, data and information's copy with nearly 1000 debit cards was mentioned on the dark web. At the time everyone understood storm was more than the end of the October of the same year, the second landfill of more than 10000 cards on the darknet was the issue, encompassing more than 10000 cards from banks in Pakistan (Awan, Memon and Burfat, 2019). The Banks in Pakistan went public; nevertheless, the report showed that a huge number of control cards from more than twenty various banks were available for buying on the dark web (Hussain et al., 2017). This part of the web is famous as a criminal movement's hotbed and cannot be restored deprive of software and nameless communique.

The information came after the cyber-attack on banks of Pakistan seven days' earlies, taking a minimum of twenty thousand dollars out of their bank accounts. The cost of the deal for such debit cards has grown from thirteen thousand to twenty-two thousand. Habib Bank Limited (HBL), of all banks, is the biggest banks of Pakistan was the most knowingly pretentious through more than eight thousand cards, after the United Bank Limited, and according to Alghazo, Kazmi and Latif (2017), "Standard Chartered Bank, MCB and Meehan Bank, each with over 1,000 cards. Alfalfa Bank, Islamic Bank and the Bank of Punjab were among the banks that saw over 500 of their cards thrown into the dull network or web.

The pirated copies of credit card information can be accessed in two configurations. First, someone for illegal online purchases can easily use credits such as full name, address, phone

number, card number, and expiration date. The second configuration is represented by the scanned dumps. This means that the hacker was physically willing to check and scan the details of the credit card an ATM or a compromised commercial computer or trade machine for illegal trade." In addition to customer data in Pakistan, non-Pakistan banks' maps such as the commonwealth bank of Australia, national bank of Abu Dhabi, Citibank USA, Abu Dhabi Islamic Bank and Emirates ND were visitor data, which was discarded when they were in Pakistan and used the ATMS or the telling machines (Awan and Memon, 2016).

The mother bank in Pakistan, named as State Bank of Pakistan, mentioned that banks their selves were note hacked as it mentioned. "It has been noted with concern news things detailing that the information of most banks has been hacked. SBP completely rejects such reports". It is, moreover, assisted through a report by the research that details out the scale and timeline of leaks of data. It assisted the state bank's claim and mentioned that the data was surely cheated through scanning of cards (Bukht et al., 2020). Devices such as Carcardimmers can be used to collect and copy the information in the magnetic stripe of credit card they came into an exchange with. Utilising this data found wrongfully, hackers can exploit frauds on credit cards, as manifested in the following figure.

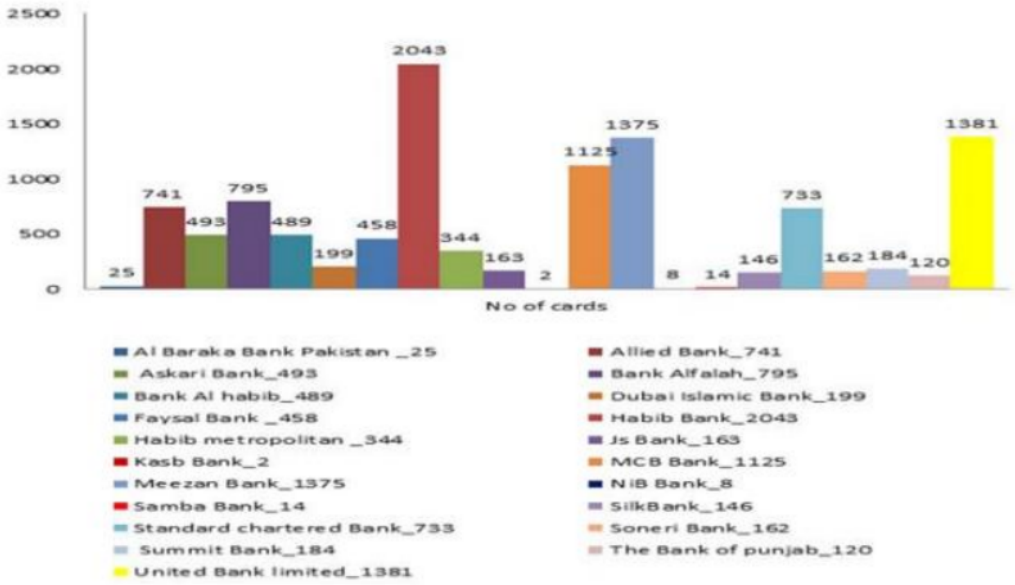

Figure 2 Credit card

When someone thinks regarding cybersecurity, the initial thing, which comes to mind, is cyberattacks that grow considerably. Cybercrime is a term for any activity, which utilises a computer as the main source of education and theft. Generally, cybercrime can be described as a crime by utilising the internet on the computer to steal the identity of a person, information, and victims' track down. A detailed technology has a vital role in the life of a person; such crime will grow with advancements in technology. Conventional attacks of malware happen at a single point on the surface amongst equipment of hardware, software section, and layers of the network, utilising the current projectile wrongly (Malik and Islam, 2019). Such cybercrimes attacks are aimed by cyberspace at a company, which utilised the internet by the malicious control, deactivation, destruction, and disorder of the IT infrastructure of organisation. According to

estimations, more than thirty-eight billion devices were connected to the internet to create and disperse sensitive data around the world.

Improving cybersecurity in Financial Institutions

The description mentioned above can be intellectual as a cybernetic cycle of defence encompassing four tools discerningly forensic reaction, detection, and prevention—these four fundamental techniques to detect, cope and deal with them; table 1 details the discussion.

Table 1: Solutions to manage cyber-attacks, phase detail

SNo	Method / Phases	Details
1	**Prevention**	Prevention is better than cure. It's better to avoid an attack before it takes place. High-quality security software needs to be installed on your computers to report your work and your private virus data.
2	**Detection**	Detection can identify security incidents. It is also used to monitor and redirect network traffic to protect a System.
3	**Reaction**	Reaction happened when cyber-attack successfully happened, it has to be quickly clarified whether and to whom the accident has to be reported. This obligation may be primarily due to the data protection act13.
4	**Forensics**	When an attack is eliminated and the System heals, this Phase is used13.

The section of prevention is accountable for consistent monitoring the device to detect any incorrect configuration or vulnerability inside. The detection section utilises IDs, for instance, "Network IDS, Host base IDS, Signature-based IDS, and Anomaly-based IDS". Experts can utilise Wireshark to identify traffic in a server that is also assistive to know about the perpetrator (Tariq, 2018). The phase of reaction is utilised to give immediately remove the attack. At the time, an attack removed, and the system heals after that, the phase of forensic is utilised. The monitored system is utilised for safeguarding the system, information of central monitoring, encompassing the configuration and topology of resources of the network. Such scenarios consist of signals of

intrusion, hardware installations, software updates etc. Few examples of this device are FW, AV, and IDS. Receipt's acknowledgement countermeasures such as closing UDP/TCP ports, redirecting traffic, which is incoming, implementing a route etc. Monitor or measure susceptibilities reaction additionally characterises data on vulnerabilities (More and Nalawade, 2015). System modal shoulders that the data accumulated the supervised system, for instance, the topology of the network.

Atomic technical solution is data which has not been converted and prepared in actions of correction will recognised the countermeasures' knowledge, a sequence of promising countermeasure will be made, and an effort will be made to amalgamate the remedies made above in the discussion to prevent the attacks. The thread model is dependent on susceptibility checks, and the system model, a threat model manifesting models of attack, was attempted. In the process of selecting an action, few measures to counter attacks are chosen through balancing the conversation amongst the phases of the safety of the machine and the reaction is cost. Especially, a problem like this is not generally a monetary value' matter the probable reduction in the availability of various sources (Syed, Khaver and Yasin, 2019). To safeguard the data is essential to utilise advanced and secured software for attack's detection.

According to Syed, Khaver and Yasin (2019), "We can also use Wireshark for detection of the attacker the source IP address. In this way, we can protect our data by block incoming viruses and attack. Cybersecurity is a global field designed to protect and monitor networks, computers, data, and programs from unauthorised access or misuse. The most important task of a cyber-security analyst is to protect a network from damage." In their study, they showed data related to cyber-attacks, threats, prime challenges and also gave little solution to suppress the crime. The researcher also introduced and discussed the importance of cybersecurity attack.

Attackers utilised such attacks for activities, which are malicious or engage botnets to conduct activities, which are dangerous for the users. At the time, getting botnets computer systems in millions can be maintained (Rasool, 2015). The perpetrators attempt to control the personal data of users, data website accounts, social media and other vital information. The user accounts' hacking is insignificant just in customer accounts on social media, which are not focused on their personal systems. Through this rationale, such activities of interruption have very minute coverage in contrast to the rest of the interruption events.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

Cybersecurity is international fields established to safeguard and monitor programs, data, computer and monitor networks from misuse and unauthorised access. The most vital task of cybersecurity analysis is to save a network from damage. In this study, it is shown that data related to cyber-attacks, threats, prime challenges and also give little solution to suppress the crime. Moreover, this researcher introduced and discussed the importance of cybersecurity. Furthermore, it analysed the security of information, cyber-attacks, and cybercrime. This research also evaluated the targeted cyber-attacks of attacks in financial institutions in Pakistan happened. Pakistan is the improving state and future of South Asia day by day. The government of the country is attempting to develop few policies to combine security measures to enhance the existing systems' capabilities to safeguard future cyber targets. Through this method, the chance for the banks' security, critical infrastructure, and major sectors are considered and requires more study in the privacy and security of such deployed systems of Pakistan.

Digital conflicts are a real threat to public influence and protection, as they have far-reaching consequences that are exacerbated at home, around the world and abroad. Just as there is no digital activity between countries, this makes it difficult to identify an opponent. In the case of Pakistan, the internet has spread to banking institutions, education, as well as the military, as well as to the government. In any case, Pakistan is lagging behind when it comes to limiting its position. Pakistan's financial sector has expanded the excellent quality of its computer network and started putting financial offices online, but executives are not encouraged to try illegal transfers. In the financial district, ATM fraud has become commonplace. Programmers are introducing ATMs to hack into the card economy and extort other documents. The government does not see a significant need in this area, and therefore, they do not spend more on it. As a result, Pakistan has been

experiencing a sharp economic downturn for some time. At the time, Kamran Ali Qureshi, the director of the Office of Science and Innovation, told the Pakistani Commission that Japan was burning a 25% budget for research and innovation, while Pakistan was spending less than 1%. Law has not yet been passed because it is not interested in the government. Pakistan currently has some laws on cybersecurity, but many of them are not strict, and others are not enforced. This is a major reason for Pakistan's digital warfare. Pakistan has a digital platform called Public Cybercrime Response Point. Its main task is to combat digital hidden words related to data collection, financial problems, and illegal stimuli. In fact, it is not very economical due to the digital ignorance of the Pakistani people. People have no idea how to break crutches, and others think it could make it harder for them, so they are stuck. However, government research institutes also cover Facebook, Twitter, Google, Skype and other similar cybercrime. It is gratifying to draw attention is not so realistic.

The Pakistani framework cannot fight against or prevent illegal entry. In addition, there are a number of panicked organisations operating in Pakistan that point to a more difficult security situation in Pakistan. Lack of attention to digital technology in humans is also becoming an increasingly serious challenge. People do not know how to protect their information against hackers or illegal access because they are being abused. Many Pakistani programmers claim that Pakistan's official database and registration authority are insecure. NADRA information is, in fact, public and therefore, it must take effective steps to keep the website secure. Because Pakistan is such a convenient place, there is a unique knowledge of Pakistan and, therefore, a real threat to NADRA. This requires existing methods to ensure the security of the information they develop. Hacktivism is not controlled in Pakistan, programmers in the current plan are destroying many

official destinations in the Pakistani administration, and it is completely inappropriate for a government agency to do so as they lack innovations to prevent these digital attacks.

Many countries are adopting radio services, and Pakistan is one of the developing countries where many organisations are using information technology in their facilities. Top governments are showing their willingness to use these. NADRA is Pakistan's official state-of-the-art certification body used by banks, passport offices, electoral departments, telephone, and the FBI, among others. Maintain population information. According to the report, NADRA is one of the world's leading organisations due to its use of advanced service technologies. Currently, European countries are using the SCAP algorithm for their NVDs, which data that allows risk assessment, security measurement, and compliance. Experts have observed attempts to breach confidential information. Meanwhile, NADRA may be the target of a terrorist attack to close down or harm its central services, violate people's confidential information, and use it for their purposes.

Pakistan has faced cyberattacks in recent years. On the eve of the 70th anniversary of Pakistan's independence, the Ministry of Defence's websites, the Ministry of Water and Energy, the Ministry of Information, the Ministry of Environment, and the Ministry of Food Security were attacked. Those events took a long time to shame and expose the scarcity of the world. In 2010, it was a similar pattern, but several attacks were recorded, including the collapse of 36 visitor websites. In 2018, the attack was on not only government departments but also Kareem's request, designed to call travellers, and was made on the website. As a result of the attack, information on the database of 14 million users from different countries, including Pakistan, was compromised. The information indicates that email ID, customer information, traffic, and phone numbers have changed. Similarly, cyberattacks at many banks have emerged and are frequently increasing in Pakistan.

Officials say they lost $ 450 million last years from cybercrime and online theft. In addition, hundreds of millions of documents from developing countries have been produced incorrectly. In this regard, developed countries such as Pakistan should encourage and the more prominent countries a plan to fight crime. To save the lives of innocent people, we encourage you to make proper international orders based on real life. In addition, new protections are needed to protect global privacy. It is an essential step in communicating with IT. In countries that use a wide range of equipment, especially electronic location monitoring, surveillance, and aircraft such as voice recording, satellite measures can be taken as required. Open the message and delete the emails. Leakage, radio surveillance, and weak IT communication secretly or openly transmit confidential information and other complex media.

Pakistan's financial institutions include banks, financial development, microfinance banks, non-banking companies, insurance companies, Modarabas, and other financial institutions. Pakistan's financial institutions are mainly made up of banks because they hold most of its monetary value as a percentage of GDP. Pakistan's State Bank controls banks, DFIs, companies listed by MFBs, while Pakistan's Securities and Exchange Commission regulates NBFCs, insurance companies, and Modaraba companies. With stops in many countries, these areas can facilitate cross-border, rapid system management and share regional practices, threats, and best practices with other regions of the world. Another benefit of regional sites is their ability to connect to the internet in many developing countries, providing support, information, and tools that may not be available at the regional level. For example, the central cybersecurity zone in West Africa could pose a serious threat to cyber support in Europe. Several European and African participants are working to create and improve such " natural resources'. At present, there are very few attempts to support workers in many countries and facilitate dialogue and sharing borders.

One example is the FS-ISAC Threat Distribution Network, which expands globally to form regional regions in Asia and Europe. Most of the world's efforts seem to be globalisation and the sharing of industrial services; they are very familiar with the type of services provided. Young and middle-aged donors and governments with limited resources and capacity are critical of these efforts to address. They need a general store that allows them to access professional services and share information with their community affiliates. To effectively support the DFS sector's growth in developing countries, more international efforts are urgently needed to provide costly and efficient services to the financial services sector.

With a high data high-data-rate, organisations need credit protection for data breaches. A well-thought-out strategy may include protecting a website with single security that includes all protections - firewall, antivirus, anti-spyware, and malware - as security software from multiple clients can ultimately work together. In addition, employees should be trained to prevent cybercrime - for example, not to open emails, radio, or media from suspicious or anonymous people. Combining good security with business insurance helps to protect the company's financial position and its reputation, and public trust. Moyle saw buyers and sellers of accurate money information. He saw security leaders advising on stupid water conservation methods. The control system must require the financial component to provide the appropriate information and data storage measures to ensure the reliable delivery of the product and the service component, protect the data services and its processes, and the efficient use of facilities. With advanced businesses covering the financial system through numbers and remote financial solutions, it is also responsible for supporting the group in risk management. As non-partisans, international organisations and development workers can promote public-independent dialogue, support constitutional initiatives,

and help build support structures that enable the sector to move forward with the rapid change of environment.

REFERENCES

Afshan, S., Sharif, A., Waseem, N. and Frooghi, R., 2018. Internet banking in Pakistan: An extended technology acceptance perspective. *International Journal of Business Information Systems*, *27*(3), pp.383-410.

Ahmed, N., 2019. Key Cyber Attacks Facing Financial Institutions in Pakistan. *Defence Journal*, *23*(5), p.23.

Alghazo, J.M., Kazmi, Z. and Latif, G., 2017. Cybersecurity analysis of internet banking in emerging countries: User and bank perspectives. In *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICES)* (pp. 1-6). IEEE.

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W. and Orgun, M.A., 2019. Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health informatics journal*, *25*(2), pp.315-329.

Awan, J.H., Memon, S., Khan, R.A., Noonari, A.Q., Hussain, Z. and Usman, M., 2017. Security strategies to overcome cyber measures, factors and barriers. *Eng. Sci. Technol. Int. Res. J*, *1*(1), pp.51-58.

Awan, J.H., Memon, S., Memon, S., Pathan, K.T. and Arijo, N.H., 2018. A defensive model to mitigate cyber activities. *Mehran University Research Journal of Engineering & Technology*, *37*(2), pp.359-366.

Awan, J.H., Memon, S., Pathan, S.M., Usman, M., Khan, R.A., Abbasi, S., Noonari, A.Q., Hussain, Z., 2017b. A user friendly security framework for the protection of confidential information. Int. J. Comput. Sci. Netw. Secur 17, 215–223.

Awan, J. and Memon, S., 2016. Threats of cybersecurity and challenges for Pakistan. In *International Conference on Cyber Warfare and Security* (p. 425). Academic Conferences International Limited.

Awan, J.H., Memon, S. and Burfat, F.M., 2019. Role of Cyber Law and Mitigation Strategies in Perspective of Pakistan to Cope Cyber Threats. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *9*(2), pp.29-38.

Baloch, R., 2018 Cyber Warfare Trends, Tactics and Strategies: Lessons for Pakistan.

Barclay, K., Voyer, M., Mazur, N., Payne, A.M., Mauli, S., Kinch, J., Fabinyi, M. and Smith, G., 2017. The importance of qualitative social research for effective fisheries management. *Fisheries Research*, *186*, pp.426-438.

Bukht, T.F.N., Raza, M.A., Awan, J.H. and Ahmad, R., 2020. Analysing cyber-attacks targeted on the Banks of Pakistan and their Solutions. *IJCSNS*, *20*(2).

Bukit, TFN, 2017 Malik, M.H. and Ahmad, R., Importance of Cybersecurity and its sub-domains.

Daugėlienė, R., 2019 ASSESSMENT AND ENHANCEMENT OF CYBERSECURITY RISKS IN PAKISTAN.

Firdous, M.A., 2018. Formulation of Pakistan's Cyber Security Policy. *CISS Insight Journal*, *6*(1), pp.70-94.

Gcaza, N., Von Solms, R., 2017. A strategy for a cybersecurity culture: A South African perspective. The Electronic Journal of Information Systems in Developing Countries 80, 1–17.

Glavee-Geo, R., Shaikh, A.A., Karjaluoto, H., 2017. Mobile banking services adoption in Pakistan: are there gender differences? International Journal of Bank Marketing.

Gupta, B.B., 2018. Computer and cyber security: principles, algorithm, applications, and perspectives. CRC Press.

Hayes, B.K. and Heit, E., 2018. Inductive reasoning 2.0. *Wiley Interdisciplinary Reviews: Cognitive Science*, *9*(3), p.e1459.

Haq, U. and Atta, Q., 2019. Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network & Information Security*, *11*(1).

Hussain, E., 2019. CPEC: Governance and security challenges—Implications for the Belt and Road Initiative. Chinese Political Science Review 4, 135–147.

Hussain, E., 2019. CPEC: Governance and security challenges—Implications for the Belt and Road Initiative. *Chinese Political Science Review*, *4*(1), pp.135-147.

Hussain, Z., Das, D., Bhutto, Z.A., Hammad-u-Salam, M., Talpur, F. and Rai, G., 2017. E-banking challenges in Pakistan: An empirical study. *Journal of Computer and Communications*, *5*(2), pp.1-6.

Irfan, M., Iqbal, J., Iqbal, A., Iqbal, Z., Riaz, R.A., Mehmood, A., 2017. Opportunities and challenges in control of smart grids–Pakistani perspective. Renewable and Sustainable Energy Reviews 71, 652–674.

Janssens, K.A., Bos, E.H., Rosmalen, J.G., Wichers, M.C. and Riese, H., 2018. A qualitative approach to guide choices for designing a diary study. *BMC medical research methodology*, *18*(1), pp.1-12.

Khalil, K., Usman, A. and Manzoor, SR, 2020. Effect of Cyber Security Costs on Performance of E-banking in Pakistan. *Journal of Managerial Sciences*, *14*.

Khan, A., Mubarik, M.S. and Naghavi, N., 2018 What matters for financial inclusions? Evidence from emerging economy. *International Journal of Finance & Economics*.

Khan, U.P. and ANWAR, M.W., 2020. Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward. *Cyberpolitik Journal*, *5*(10), pp.205-218.

Kral, P., Valjaskova, V. and Janoskova, K., 2019. Quantitative approach to project portfolio management: proposal for Slovak companies. *Oeconomia Copernicana*, *10*(4), pp.797-814.

Kennedy, K.M., 2019. Promoting the qualitative research approach in the discipline of forensic and legal medicine: Why more qualitative work should be promoted and how that can be achieved. *Journal of forensic and legal medicine*, *62*, pp.72-76.

Malik, M.S. and Islam, U., 2019. Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime*.

McAbee, S.T., Landis, R.S. and Burke, M.I., 2017. Inductive reasoning: The promise of big data. *Human Resource Management Review*, *27*(2), pp.277-290.

Mobily, K. and Morris, H., 2018. Qualitative approach to evaluating TR definitions. *Therapeutic Recreation Journal*, *52*(3), pp.237-253.

More, D.M.M. and Nalawade, MPJDK, 2015. Online banking and cyber-attacks: the current scenario. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper.

Noor, U., Anwar, Z., Amjad, T., Choo, K.-K.R., 2019. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems 96, 227–242.

Pomerleau, P.L. and Lowery, D.L., 2020. The Evolution of the Threats to Canadian Financial Institutions, the Actual State of Public and Private Partnerships in Canada. In *Countering Cyber Threats to Financial Institutions* (pp. 47-85). Palgrave Macmillan, Cham.

Rahman, S.U. and Shurong, Z., 2017. Analysis of Chinese economic and national security interests in China-Pakistan Economic Corridor (CPEC) under the framework of One Belt One Road (OBOR) initiative. *Arts and Social Sciences Journal*, *8*(4), pp.1-7.

Rasool, S., 2015. Cybersecurity threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal*, *12*, pp.21-32.

Rust, N.A., Abrams, A., Challender, D.W., Chapron, G., Ghoddousi, A., Glikman, J.A., Gowan, C.H., Hughes, C., Rastogi, A., Said, A. and Sutton, A., 2017. Quantity does not always mean quality: The importance of qualitative social science in conservation research. *Society & Natural Resources*, *30*(10), pp.1304-1310.

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: a survey. *Future Internet*, *11*(4), p.89.

Seo, S., Lee, J.M., Yang, H. and Kim, S., 2019, August. Can AI Tell Emerging Technologies: Evaluating the Importance of Quantitative Features of Technology. In *2019 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 1-5). IEEE.

Shad, M.R., 2019. The cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, *39*(1), pp.1-19.

Shah, A.R., 2018. How Does China–Pakistan Economic Corridor Show the Limitations of China's 'One Belt One Road'Model. Asia & the Pacific Policy Studies 5, 378–385.

Shah, S.B.H., Mu, Y., Abbas, G., Pavase, T.R., Mohsin, M., Malik, A., Ali, M., Noman, M., Soomro, M.A., 2018. An economic analysis of the fisheries sector of Pakistan (1950-2017): Challenges, opportunities and development strategies. International Journal of Fisheries and Aquatic Studies 6, 515–524.

Syed, F.Z. and Javed, S., 2017. Deterrence: A Security Strategy against Non Traditional Security Threats to Pakistan. *International Journal of Social Sciences and Management*, *4*(4), pp.267-274.

Syed, R., Khaver, A.A. and Yasin, M., 2019. Cyber Security: Where Does Pakistan Stand?.

Tariq, N., 2018. Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, *23*(2), pp.1-11.

uddin Ahmed, S., Ali, A., Kumar, D., Malik, M.Z., Memon, A.H., 2019. China Pakistan Economic Corridor and Pakistan's energy security: A meta-analytic review. Energy policy 127, 147–154.

Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M.A., Al-Tudjman, F. and Mostarda, L., 2019. Cybersecurity threats detection in internet of things using deep learning approach. *IEEE Access*, *7*, pp.124379-124389.'

Valasai, G.D., Uqaili, M.A., Memon, H.R., Samoo, S.R., Mirjat, N.H. and Harijan, K., 2017. Overcoming electricity crisis in Pakistan: A review of sustainable electricity options. *Renewable and Sustainable Energy Reviews*, *72*, pp.734-745.

Venkatachary, S.K., Prasad, J., Samikannu, R., 2018. Cybersecurity and cyber terrorism-in energy sector–a review. Journal of Cyber Security Technology 2, 111–130.

Wolf, S.O., 2020. The China-Pakistan Economic Corridor of the Belt and Road Initiative. Springer.

Yao, H., Chan, C.H.Y. and Chan, C.L.W., 2018. Childbearing importance: A qualitative study of women with infertility in China. *Research in nursing & health*, *41*(1), pp.69-77.

Zhou, D., Shah, T., Ali, S., Ahmad, W., Din, I.U., Ilyas, A., 2019. Factors affecting household food security in rural northern hinterland of Pakistan. Journal of the Saudi Society of Agricultural Sciences 18, 201–210.

Dissertation

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

< 1%

★ medicinegarden.com

Internet Source

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Dissertation

GRADEMARK REPORT

FINAL GRADE

/1000

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

PAGE 39

PAGE 40

PAGE 41

PAGE 42

PAGE 43

PAGE 44

PAGE 45

PAGE 46

PAGE 47

PAGE 48

PAGE 49

PAGE 50

PAGE 51

PAGE 52

PAGE 53

PAGE 54

PAGE 55

PAGE 56

PAGE 57

PAGE 58

PAGE 59

PAGE 60

PAGE 61

PAGE 62

PAGE 63

PAGE 64

PAGE 65

PAGE 66

PAGE 67