ACADEMIA International Journal for Social Sciences
Volume 4, Issue 4, 2025 ISSN-L (Online): 3006-6638

# A Study of Cybersecurity Frameworks in Organizations of Pakistan

**Syed Muhammad Irfan**
smirfan2025@gmail.com
Department of Criminology, University of Karachi

**Dr. Naima Saeed**
naima.saeed7@gmail.com
Chairperson Department of Criminology, University of Karachi
Corresponding Author: * **Syed Muhammad Irfan** smirfan2025@gmail.com

**Received:** 16-08-2025 **Revised:** 21-09-2025 **Accepted:** 26-10-2025 **Published:** 05-11-2025

## ABSTRACT

*This study examines the adoption and the effectiveness of cybersecurity frameworks within various organizational types in Pakistan. Even though the importance of the protective and securing digital assets and the role of these cybersecurity frameworks cannot be overstated, the adoption and implementation in developing countries remains significantly under discussed. In this research, studies the adoption of cybersecurity frameworks such as ISO 27001, NIST, etc and aims to close the gap. It also examines the effectiveness of frameworks regarding the issues of mitigating cyber threats and employee adherence to the organization's cybersecurity policies. The researcher used qualitative methodology and conducted semi-structured interviews. The participants are cybersecurity professionals and information technology (IT) experts. There are Eight key sectors covered for the collection of data. Thematic analysis used for the interpretation of data findings analysis. The Situational Crime Prevention Theory, Control Theory, and Routine Activity Theory are used as the analytical frameworks. The findings of the research revealed a stark difference to which the regulated and unregulated sectors are implementing cybersecurity frameworks in their respective organizations. This study addresses the need for flexible tailored cyber security frameworks by regulatory authorities like OGRA, SECP and PTA, etc. The study concludes that Pakistan's organizations are not ready to face the cyber security challenges and securing sensitive and critical information. The enforcement for cyber security programs in organization from regulating authorities is a dire need of time. Organizations across every sector need to adopt cybersecurity frameworks that fit to their organization's needs. The tailored global cybersecurity frameworks that suit the specific threat landscape, resource realities, and socio-cultural context can also be an effective approach to build genuine cyber resilience.*

**Keywords:** *Cybersecurity Frameworks, Thematic Analysis, NIST, ISO 27001, COBIT 2019, Organizational Compliance, Cybersecurity policy, Situational Crime Prevention Theory, Control Theory, Routine Activity Theory.*

## INTRODUCTION

### The Global Cybersecurity Landscape

The exponential growth of cyberspace has unveiled imminence that transcends the conventional geographical boundaries. The internet is an unbounded global network that allows the cybercriminals to compromise any nation that have inadequately secured computer systems. The internet technologies are advantageous and revolutionizing the industries across many sectors that include, finance, education, healthcare, defence, etc. Cybercriminals understand the potential of internet for their illegal activities. The exponential growth of information and communication technologies (ICT) is immense throughout the last several decades (Awan et al., 2016).

The landscape of cyber threats is evolving and changing in the contemporary era as the governments and organizational dependence on digitally interconnected computer networks is increasing (Safdar, 2020). The worldwide dependence on internet and technologies is exponentially increasing the risk of cybercrimes, which might result in significant harm to nations (Syed, Khaver & Yasin, 2019).

### The Pakistani Context

The cybersecurity losses have increased to billions of dollars, state secrets leak, sensitive data theft, and critical infrastructure disruption is routine (Syed, Khaver & Yasin, 2019). Pakistan as a nation is confronting the similar cyber threats and challenges like hacking, cyber fraud, cyber attacks on infrastructure and financial institutions, etc (Rafiq, 2017). In Pakistan cyber attacks like ransomware, spyware, social engineering and modification of physical devices is quite common (Syed, Khaver & Yasin, 2019). Attacks like malware, disgruntled insiders, phishing and zero-day attacks are in routine (Awan et al., 2016).

Pakistan also has the challenges of cyber warfare, cyber terrorism, cyber propaganda, cyber harassment, cryptocurrencies fraud and the reliance on foreign devices increases the risks significantly (Khan, 2019). In Pakistan cyber attacks have increased on financial institutions and critical infrastructure, for instance, hackers in 2018, infiltrated the security system of a private bank and acquired thousands of credits and debit cards details. The cyber attacks are a stark reminder of the vulnerabilities inherent in cybersecurity programs in organizations of Pakistan against the increasing cyber threats (Siddiqui, 2020).

In Pakistan, like many other nations of the world, the increasing dependence on internet technology raises the extreme concern for organizations and government authorities as well. According to reports by Pakistan Telecommunication Authority (PTA), there are increase in cyber crimes like financial and data breaches in Pakistan (PTA, 2021). Pakistan has significant lack in focus, planning and legislations for cybersecurity capacity building. The implementation of 2017 Digital Pakistan Policy is inadequate. Pakistan is positioned 107th among 131 nations globally in terms of innovation capacity. Pakistan total score is 64.88% in organizational and cooperative criteria which is not satisfactory Cyber Security Global Index Report (2021).

According to Microsoft Digital Defence Report 2018-2019, the monthly malware attacks rate in Pakistan is 18.94% that makes the country second most impacted nation by malware attacks globally.

### Problem Statement

The Global Cyber Security Index (2018) report on cybersecurity listed five areas where countries need to improve their overall cyber security posture, that include, technical skills, laws, organizations, cooperation, and training. It ranked countries into three levels based on their commitment in improving overall cyber security scenario i.e. high, medium, and low. The UK, USA, and France showed the highest among the nations who showed dedication while Pakistan's commitment was rated as moderate. In the 2017 rankings, Singapore, the US, and Malaysia were the top three countries. Pakistan was ranked 66th, which is much lower than its neighbours like India (23rd) and China (32nd), who are considered as leading nations. The report found that while these top countries have made good laws against cybersecurity, they still lack a strong enough ability to combat cyber attacks.

According to the Global Cyber Security Exposure Index (2020) report, countries vary greatly in their exposure to cybercrime. Finland was reported to be the safest country, followed by Denmark, Luxembourg, Australia, and Estonia. The United States also ranked in the top ten country. On the other end of the list, Pakistan and India were reported as highly vulnerable countries to cyber attacks, ranking 76th and 55th respectively. Afghanistan was ranked as the most vulnerable country out of all 108 nations studied (Frisby, 2020). Although Pakistan and India are neighbouring countries but usually engage in cyber attacks on different sector and challenge on other's authority (Safdar, 2020). This is a consistent cyber threat to Pakistan as India may launch offensive cyber operations against Pakistan (Rafiq, 2017).

This research aims to analyse the cybersecurity environment of organizations in different sectors in Pakistan by studying the current cybersecurity frameworks in place. This study will provide insights into vulnerable areas which needs measure to increase or adjust cybersecurity program. This research will analyse the cybersecurity frameworks in organizations and their effectiveness in protecting networks, systems and information. The research will also examine the issues like employee's adherence to cyber security policies in organizations and role of regulatory bodies in developing a cybersecure hygiene in Pakistan.

This research will identify best practices of cybersecurity frameworks like ISO/IEC 27000 series, COBIT, NIST CSF, etc, that can be adopted by organizations to strengthen their cybersecurity environment (Chen & Liu, 2016). The recommendations and insights will serve as guidelines to organizations in improving their cybersecurity program. This research will contribute to the existing body of knowledge on cybersecurity by discussing evolving nature of cybersecurity threats and frameworks capabilities. This research will contribute and provide valuable guidance to organizations, policymakers and cybersecurity professionals.

### Research Objectives & Questions

This research is intended to fulfill a largely unmet need to assess the deployment and efficiency of cybersecurity frameworks in organizations in Pakistan. Their effectiveness in reducing cyber risk, and in improving these organizations' overall cybersecurity posture, is one of the objectives of this research. Also, of primary interest is whether organizations inside Pakistan are adopting or conforming to these purportedly beneficial cybersecurity models, frameworks, or standards. Although several frameworks, models, or standards for achieving desired outcomes in cybersecurity exist, not all organizations necessarily find them efficacious or worthwhile. This research evaluates the role of frameworks in mitigating diverse nature of cyber threats and effectiveness of frameworks in mitigation of cybersecurity incidents. This research will also examine the compliance level of employees to cybersecurity polices and procedures and the issues face by them in compliance.

**RQ1**: To identify the cybersecurity frameworks adopted by organizations in various sectors of Pakistan.

**RQ2**: To evaluate the perceived effectiveness and maturity level of implementation of these frameworks.

**RQ3**: To investigate the critical challenges and drivers influencing the adoption and implementation process.

## LITERATURE REVIEW

In the past, technical measures were the main focus of attempts to manage security related risks. Nowadays, it is well acknowledged that human factors account for the increase of data breaches (Stewart & Jurjens, 2017; Constantino et al, 2018). As a result, a secure organization requires a combination of technology and non technological measures, relying solely on technological measures is insufficient (Kayworth & Whitten, 2012; Singh et al, 2014). There is a greater awareness of the significance of using organizational and people centered strategies to avoid information security events (Werlinger, 2009; Stewart & Jurjens, 2017). Nonetheless, some businesses continue to prioritize technical security, leaving them open to dangers related to non technological information security (Hashim & Razali, 2019).

Information security is defined as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" by the NIST. The process of managing information security activities is known as information security management, or ISM. To protect information assets and guarantee their confidentiality, integrity, and availability, there exist frameworks and standards for best practices that comprise collections of rules, processes, and technological tools, etc.

By implementing a cybersecurity framework in organization that offers a structure and process for safeguarding vital organizational assets is the only way to provide acceptable cybersecurity protection, which includes holistic information security solutions (Syafrizal, Selamat, & Zakaria, 2020). The framework can be centered on providing essential services within the company or it can be used to control cybersecurity risk throughout the whole enterprise. The framework offers cybersecurity outcomes along with a techniques to assess and manage them. It also offers a way to prioritize and identify actions that can lower or mitigate cyber risk (Calder, 2018).

The organizations will not be able to achieve the wider organizational goals if it has not a well-structured cybersecurity framework to protect its resources, assets, and procedures. Without the appropriate cybersecurity framework, a cybersecurity plan cannot be carried out successfully (Dedeke & Masterson, 2019). Because of their flexibility, cyber security frameworks can decrease the implementation costs and assist in safeguarding critical infrastructure and other governmental and commercial sectors that are critical to the national economy and security.

There are several cybersecurity frameworks available, with prices ranging from free to premium. Frameworks that best fit the unique business needs are carefully chosen by organizations. There are variations in each Cyber security frameworks that rely on the context or framework setting. Because every framework has its own special features or situations. There are certain commonalities throughout the frameworks, despite the fact that there are different viewpoints and situations. (Azmi, Tibben, & Win, 2018).

## Review of Major Global Frameworks

### NIST Cyber Security Framework (CSF)

NIST CSF is a voluntary guidance, that is based on existing guidelines standards, procedures and practices for organizations to manage and mitigate cybersecurity risk, is how NIST defines the NIST Cybersecurity Framework. It is intended to promote cybersecurity risk management communications among internal and external stakeholders in organization along with assisting companies in managing and lowering risks and threats.

The framework's core is made up of cybersecurity-related activities and educational resources arranged according to certain goals.

### Overview of the CSF Core

Set of cybersecurity results, which are grouped by Function, Category, and Subcategory. The defined steps necessary to achieve an outcome will be different depending on the organization and use case, as will the person in charge of those steps. These results are not a list of things to do. Furthermore, the

chronology and importance of achieving the Functions, Categories, and subcategories in the Core are not implied by their size or order.
To achieve the best possible cybersecurity results, the CSF Core Functions are: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER.

### ISO/IEC 27001

The ISO 27001 cybersecurity standard has developed and grown over time as a result of the introduction of new and innovative technologies and the rise in system complexity. The most recent iteration of "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems — Requirements", which was released in October 2022 under the new title. After the initial release of ISO 27001 in October 2005, BS7799-2 was essentially superseded as an audit standard for assessing the efficacy and maturity of information management systems (Cook, 2022). The 2013 publication of the 2nd edition (ISO/IEC 27001:2013) was improved upon by the current version.

### Security Objectives and Protection Goals

The primary security and protection aim of ISO 27001 standard are confidentiality, integrity, and availability. The goal of confidentiality is to guarantee that only authorized person may access system and information. Integrity assures that data is only change or altered in ways that are permitted, protecting the company from both inadvertent technological mistakes and hackers who try to change or alter the data. Availability guarantees that system or data is always accessible to the system or authorized personals. Organizations must secure essential assets against all three security objectives, which ISO 27001 can assist them achieve (Calder & van Bon, 2017).

### COBIT Framework

The audit and control of IT is where the Control Objectives for Information and Related Technology (COBIT) framework got its start. It makes it possible for IT to be managed and controlled holistically for the entire organization, taking into account the interests and needs of both internal and external stakeholders in relation to IT while encompassing the entire end-to-end business operations and IT functional areas of responsibility (ISACA, 2012).

IT auditing began in 1967 when a group of US experts in charge of internal control in various corporations realized how important computers were to their businesses' operations. In order to exchange information on this topic, they established the Electronic Data Processing Auditors Association (EDPAA) in 1969. In 1994, the organization changed it to ISACA (Information Systems Audit and Control Association). Currently, ISACA is group of professionals or an association that unites about 150,000 professionals from 75 countries and look after topics beyond audit and control. To address many facets of IT governance, ISACA founded the Information Technology Governance Institute (ITGI) in 1998.

The first version of Control Objectives, which served as the primary reference for control and auditing procedures, was released in 1977 under the auspices of ISACA and ITGI. The initial iteration of the COBIT architecture, which included 271 control goals and 32 processes. The second version of COBIT, known as COBIT 2, was released in 1998. It has 302 control goals and 34 processes. The publication of COBIT 3 in 2000 included 318 specific control goals along with additional management-related components, including as metrics, a maturity assessment methodology, and essential success criteria, which operate as management recommendations. The COBIT 4.0 version, which covers IT governance (215 control goals), was released in 2005. In 2006, a framework for value management (Val-IT) was included.

With 210 control goals, the COBIT 4.1 version was released in 2007. In 2009, a risk management framework (Risk-IT) was included. Version 5 of COBIT, which was released in 2012, incorporates all of these frameworks along with a number of international standards, including ISO/IEC 38500. 15 governance practices and 195 management practices are included in COBIT 5, which is still being finished with more contributions. ISACA suggested a new version of “COBIT 2019” at the end of 2018, which frames management and governance within the digital transformation that businesses are going through. It includes some new parts and distinguishes between the Governance System and the Governance Framework (Steuperaert, 2019). The goal of the most current COBIT update is to enable a more adaptable, customized implementation of efficient Enterprise Governance of Information and Technology (EGIT)" (De Haes, Van Grembergen, Joshi, & Huygh, 2020).

### Center for Internet Security (CIS) Controls Framework

Center for Internet Security (CIS) and SANS institute approached the National Security Agency (NSA) with the proposal to create a scaled down version of security controls that would identify and prevent the majority of attacks, CIS Controls was developed. Businesses and organizations joined the campaign that CIS and SANS had launched. At last, in 2009. CIS Controls' initial edition was released. Since controls are evaluated annually, the most recent version, 7.1, was released in April 2019. In 2015, prior to being handed to the Council on Cyber Security (CCS) and then to the Center for Information Security (CIS), the CIS Controls were originally owned by SANS institute, who referred to them as 20 important security controls. CIS Control v8 was introduced in 2021.

### PCI DSS Framework

Before the implementation of PCI DSS, payment card organizations such as Visa, Mastercard, JCB, American Express, and Discover depended on their own policies for the secure processing and storage of payment card data. Before the inaugural publication of the standard, the Payment Card Industry Security Standards Council was established, which amalgamated various distinct rules, culminating in the issuance of PCI DSS v 1.0 in Dec 2004. The initial stage of standards development exhibited several deficiencies, which were later corrected in version 1.2.1.

This version introduced many requirements to resolve those shortcomings and, in the process, offered much better guidance on the specific technologies, such as encryption, virtualization and wireless, that had become increasingly important (Bhargav, 2014). The PCI DSS 2.0 standard was first released in 2010 and became an industry standard in 2011. Although there were no major modifications relative to v1.2.1. (Chuvakin & Williams, 2014) in their research documented the differences in framework versions and highlighted the important aspects. The way PCI DSS 2.0 addressed wireless network security and risk management among other things, were a noticeable improvement.

Published in November 2013, PCI DSS 3.0 was fully enacted in January 2015. It continues the framework of its preceding versions while providing a robust guide for scoping the current version and presenting successful implementation strategies. The framework PCI DSS v4.0 was officially published in March 2022. Over the years, PCI DSS has progressed and matured to keep pace with the rapidly evolving payment card industry and its technologies. Its strength and reason for being lie in the enormous payoffs from its being implemented uniformly around the world. Those payoffs are in the form of protection from breaches of cardholder data and a much higher level of security as an ongoing effort.

### SOC2 Framework

Systems and Organization Controls 2, or SOC 2, introduced a new framework. The updated version of SOC 2, published in October 2022, seeks to make the actual audits more effective and more relevant, in part by clarifying terms used in the framework. SOC 2 was created by the American Institute of CPAs (AICPA) as a way to gauge the controls that service organizations use to protect client data. It has become a necessary assurance mechanism in a digital world for not just consumers but also internal and external partners and stakeholders. Unlike SOC 1, which is an audit largely required by the Internal Revenue Service, SOC 2 pertains to "non-financial data used by the service organization."

The goal for SOCs framework is to provide an opportunity to assess not just the operational effectiveness of the organization but the effectiveness of security controls as well. Point of Focus (PoFs), represent a way of exemplifying what SOC 2 is trying to accomplish for organizations. The updated version has changes in the PoFs from the first version of SOC 2. It can be tailored according to the needs and risks environment of organizations. The updated version is more specific to current security realities through the introduction of new PoFs.

### HITRUST Framework

The Health Information Trust Alliance (HITRUST) was established in 2007. It focuses on the secure handling of health information. Its main intent was to help organizations and business associates to comply with the Health Insurance Portability and Accountability Act (HIPAA) and other mandates. Since then, HITRUST has been extending its focus beyond health information security to several other industries, including financial services and defense contracting. In January 2023, HITRUST updated its Security Framework. The latest update, called HITRUST CSF version 11, aims to beef up protections against new forms of cyber attacks, broaden the types of sources it uses to achieve maximum security and facilitate those using the framework to "elevated levels of assurance." This latest version employs AI-driven techniques to enrich both current and new authoritative sources used in the framework. The HITRUST CSF itself is not intended for the certifiable component, yet it provides a pathway to certifiability.

### The Cloud Controls Matrix (CCM) Framework

The Cloud Security Alliance (CSA) established the Cloud Controls Matrix (CCM) in 2009, to provide a straightforward and consistent framework of controls for cloud environment (Saxena, 2013). Its basic aim is to help enterprises assess the overall security posture of the cloud infrastructure and services. The first version of the CCM sought to address the special security issues in the cloud environment. It presented an extensive listing of control objectives arranged across several domains.

The most recent edition of the Cloud Controls Matrix (CCMv4) was made available in 2021. Enhancements on some of its features are notable. CAIQ, the CCM, and the Consensus Assessment Initiative Questionnaire (CAIQ) are now part of one document. Controls are compatible with prominent cybersecurity standards such as ISO 27001 and NIST. The Control Objectives now cover 17 critical domains with 197 control objectives, essentials to cloud technology and its risks and benefits.

## Theoretical/Conceptual Framework

### Introduction Routine Activity Theory in Cybersecurity

Routine Activity Theory was first articulated by (Cohen & Felson, 1979), and since then, it has become a preeminent theory in one of the pathways of crime opportunity. Most of the other criminological theories focus on the offender and the various determinants of criminal motivation. In contrast, RAT does not attempt to address these questions; rather, it postulates that three particular conditions must be present in order for a crime to occur. These conditions are, a motivated offender, a suitable target, and a lack of capable guardians. The criminological viewpoint has become more relevant in recent times, especially in cybersecurity research, when it comes to understanding the types of cyber threats that can penetrate systems but also the organizations behind them. Understanding the identifiable vulnerabilities of an organization both in terms of its daily operations and in terms of what makes an organization a suitable cyber target.

### Core Principles of Routine Activity Theory

(Cohen and Felson's, 1979) in their seminal work, established three necessary elements for the causation of crime that include:

1. A motivated offender
2. A suitable target
3. The absence of a capable guardian

The theory emphasize that crime rates change when everyday activities change which lead to the convergence of the three elements of the criminal event (Felson & Eckert, 2018). Unlike traditional criminological theories that focus on the criminal and the criminal's social environment, routine activity theory (RAT) focuses on the conditions under which crimes happen and emphasizes the importance of opportunity.

### Application to Cybersecurity Context

The application of Routine Activity Theory (RAT) in organizations' cybersecurity context, requires careful consideration like, how its core elements relevant in digital environments.

#### 1. Motivated Offenders

In organizations, malicious insider threats from employees and contractors are common along with hackers operating outside an organization (Willison & Warkentin, 2013). Hacking tools are easy to acquire and entrance barriers into the world of cybercrime have decreased. These factors have increased the number of prospective criminals in cyber world.

#### 2. Suitable Target

The value of digital assets has made them a target for cyber attackers and thieves. The ease of access and visibility even more establishes this attraction. Ineffectively managed cyber security within an organization risks the compromise of sensitive information, interconnected digital frameworks, transactional bank systems, systems involving employee passwords, and several other systems. (Felson and Eckert 2018)

#### 3. Capable Guardianship

It is always difficult to penetrate the system or network of any organizations who have deployed technical controls like firewall, DLP and antimalware, etc. The cybersecurity controls like technical, administrative, people and physical serve as capable guardians.

### Situational Crime Prevention in Cybersecurity

### Introduction

In 1992, (Ronald V. Clark, 1992), articulated Situational Crime Prevention (SCP) theory. This theory focuses on reducing criminal opportunities by making changes to the environment or situations where potential criminal activities may occur. Initially applied to conventional crimes, SCP has recently started to gain popularity in the context of cybersecurity.

### SCP Application to Organizational Cybersecurity

1. **Technical Implementation**
   a) Deployment of multiple technical controls
   b) Network segmentation
   c) Behavioral analytics
   d) Data encryption
   e) User access management

2. **Policy Framework**
   1. Effective cybersecurity policies and procedure should incorporate SCP principles
   2. Clear BYOD policies
   3. Mandatory cybersecurity awareness training
   4. Incident reporting systems and protocols

3. **Physical-Digital Hybrid Measures**
   a) SCP recognizes the intersection of physical and digital security
   b) Secure elimination of storage devices
   c) Biometric access management
   d) Visitor management systems

### Control Theory in Organizational Cybersecurity

### Introduction

Control Theory, also known as Social Bond Theory by (Travis Hirschi's, 1969), provides a useful lens to understand compliance level within the context of organizational cybersecurity. Control Theory suggests that individuals are less likely to engage in deviant or noncompliant behavior when they maintain strong bonds with the people around them and they have strong internal controls and cybersecurity mindset. Control Theory helps explain why a strong culture and a strong set of internal controls work together to produce a compliance mindset that helps prevent cyber security policies violations and cyber misconduct.

### Theoretical Foundations of Self Control Theory (SCT)

(Hirschi's, 1969) original formulation identified four key social bond elements that prevent deviance

1. **Attachment:** Emotional bond to other employees who value conformity
2. **Commitment**: Investment in conventional society and its rewards
3. **Involvement:** Time spent in legitimate activities
4. **Belief:** Endorsement of societal norms and rules

Subsequent advancements in Self-Control Theory (Gottfredson & Hirschi, 1990) added the self regulation capacity dimension that is so integral to individual differences in self control. These theoretical frameworks have shown considerable relevance in organizational context (Willison & Warkentin, 2013).

### Research Methodology

Research methodology constitutes the foundation of criminological research. It offers systematic frameworks to examine conventional crime, cybercrime, criminal behaviour and criminal justice system. Scholars in Criminology use many research methods that include quantitative analysis of crime statics and qualitative evaluation. In depth interviews in qualitative methods are essential for understanding the contextual and subjective dimensions of cybercrimes which is not possible with quantitative data analysis.

### Qualitative Exploratory Design

In this research a qualitative research approach is employed to examine the application of cybersecurity frameworks in organization of Pakistan. This methodology is appropriate for the research as the cybersecurity frameworks adoption entails intricate and context dependent (Creswell & Poth, 2018). Qualitative methods were employed to understand how the particulars of an organization, its culture, leadership, and decision-making about resources, affect the implementation of the Cybersecurity Framework like ISO 27001, NIST, etc (Yin, 2018). It is important to note that rigidly structured research methodologies may overlook the unexpected challenges during the implementation of cybersecurity framework (Stallings & Brown, 2018).

### Rationale for Interview-Based Methodology

The semi structured interviews are the main approach to primary data collection in this research. As it is well established that interviews offer detailed accounts that help a researcher capture the subtleties of the different components of a cybersecurity framework in interpretation and operationalization (Braun & Clarke, 2006). The semi structured interviews allow researcher to explore unforeseen themes and issues raised by participants. The research emphasizes on the implementation aspects that are usually unaddressed in the policy documents of the organizations and lacks in the survey data (Patton, 2015). This encourages the discussion during the interview of more difficult, and possibly more hidden, organizational cybersecurity practices that cybersecurity professionals may feel uncomfortable sharing openly (Siponen & Oinas-Kukkonen, 2007). This method has the advantage of eliciting detailed accounts of particular security events and the subsequent changes made to their security frameworks (Kharraz et al., 2019).

### Purposive Sampling Strategy

The researcher utilized purposive sampling method to identify those with the needed knowledge and understanding of the frameworks and implementations of cybersecurity. The sample includes executives in cybersecurity such as CISOs, Directors of Security, IT Managers, and cybersecurity consultants who understand cybersecurity frameworks along with the relevant technologies.

### Recruitment Protocols and Gaining Access

Due to the delicate characteristics of the proceedings, the researcher provided an integrated recruitment design. This includes the use of professional networks, for example, ISACA chapters, for identifying potential participants. Identifying new interviewees through LinkedIn and former participants’ referrals to Cybersecurity practitioners. Occasionally, the researcher has used industry events, e.g., Black Hat, for outreach to potential participants. During the recruitment process, trust is primarily built through the voluntary nature of participation and assurance of confidentiality and complete anonymization of the data through pseudonyms.

## FINDINGS AND ANALYSIS

Cybersecurity frameworks are essential for safeguarding organizational information assets. However, the effectiveness of cybersecurity frameworks in developing countries such as Pakistan remains understudied (Khan et al., 2021). In this part, the researcher examines the interview data of 32 professionals from eight different sectors in Pakistan to study the adherence to internationally accepted cybersecurity frameworks.

**Respondent Distribution by Sector (N=32)**

| **Sector** | **Sector Code** | **Number of Respondents** | **Percentage (%)** | **Respondent IDs** |
|---|---|---|---|---|
| Banking & Financial Services | BFS | 4 | 12.5% | R6, R20, R28, R32 |
| E-commerce & Retail | EC&R | 4 | 12.5% | R1, R4, R5, R11 |
| Education & Research | EDU&R | 4 | 12.5% | R2, R7, R27, R29 |
| Energy & Utility | E&UT | 4 | 12.5% | R3, R14, R16, R26 |
| Government & Critical Infrastructure | G&CI | 4 | 12.5% | R10, R15, R21, R22 |
| Healthcare | HC | 4 | 12.5% | R19, R23, R24, R31 |
| Manufacturing & Supply Chain | M&SC | 4 | 12.5% | R8, R17, R18, R25 |
| Telecommunications & IT | T&IT | 4 | 12.5% | R9, R12, R13, R30 |
| **Total** | | **32** | **100%** | |

**Cybersecurity Frameworks Adoption by Sectors**

1. **Overall Adoption Rates**

**Framework Adoption by Sector**

| **Adoption Status** | **% of Organizations** | **# of Respondents** |
|---|---|---|

| Adoption Status | % of Organizations | # of Respondents |
|---|---|---|
| No Framework | 59% | 19/32 |
| ISO 27001 Certified | 18% | 6/32 |
| Following Guidelines* | 12% | 4/32 |
| Other Certifications | 6% | 2/32 |

*Guidelines: Unofficially following ISO/NIST without certification

**Sector-Wise Breakdown**

**Sector Wise Breakdown**

| Sector | ISO 27001 | PCI DSS | NIST | No Framework | Partial/Planned Adoption |
|---|---|---|---|---|---|
| **BFS** | 3/4 | 3/4 | 2/4 | 1/4 | R28 (Pursuing ISO 27001) |
| **T&IT** | 2/4 | 1/4 | 3/4 | 2/4 | - |
| **G&CI** | 2/4 | 1/4 | 2/4 | 2/4 | R21 (Partial PCI DSS) |
| **E&UT** | 1/4 | 0/4 | 0/4 | 3/4 | - |
| **HC** | 0/4 | 0/4 | 0/4 | 4/4 | - |
| **EDU&R** | 0/4 | 0/4 | 0/4 | 4/4 | - |
| **EC&R** | 1/4 | 0/4 | 0/4 | 3/4 | R5 (Unofficial Guidelines) |
| **M&SC** | 0/4 | 0/4 | 1/4 | 4/4 | R18 (Unofficial NIST) |

**Key Findings**

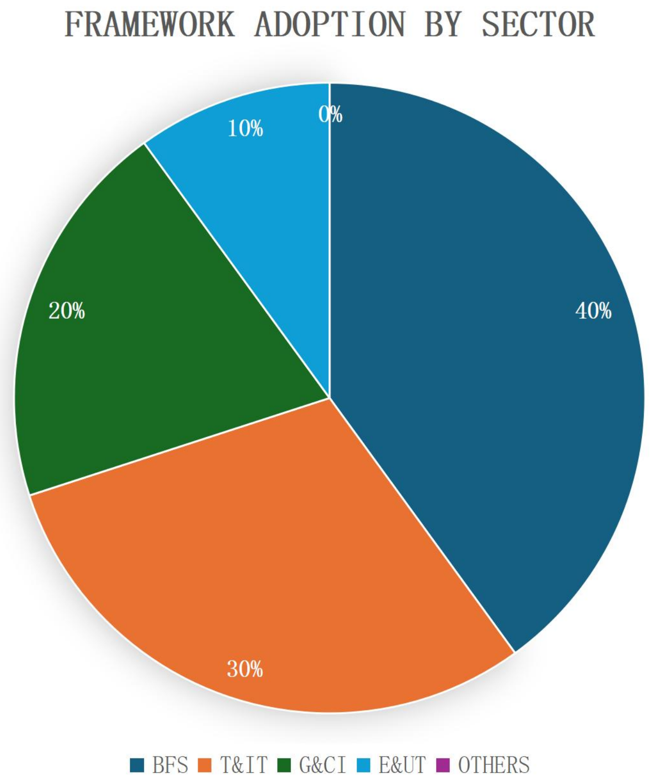
1. **Regulated Sectors Lead Adoption**:
   - **BFS**: 100% use frameworks (ISO 27001/PCI DSS/NIST) - *"State Bank regulations compel compliance" (R28)*
   - **T&IT**: 50% certified (ISO 27001), 75% use NIST guidelines
2. **Critical Gaps**:
   - **Zero Adoption**: HC (0/4), EDU&R (0/4), M&SC (0/4 certified)

- **Partial Implementation**: "We follow NIST but can't afford certification" (R18-M&SC)

3. **Emerging Trends**:

- Hybrid approaches (R15-G&CI: ISO+NIST guidelines)
- Custom frameworks (R6-BFS, R10-G&CI)

**A. Framework Adoption Heatmap**



**Framework Effectiveness Analysis**

**Framework Effectiveness**

**1. Adoption vs. Perception of Frameworks Effectiveness**

| Sector | % Using Frameworks | Key Frameworks | Perceived Effectiveness | Representative Quote |
|---|---|---|---|---|
| **BFS** | 100% | ISO 27001, PCI DSS, NIST | High | *"Frameworks reduce vulnerabilities against evolving attacks" (R28)* |
| **T&IT** | 75% | ISO 27001, | High | *"Comprehensive* |

| Sector | % Using Frameworks | Key Frameworks | Perceived Effectiveness | Representative Quote |
|---|---|---|---|---|
| | | NIST | | *foundation for regional threats" (R30)* |
| **G&CI** | 50% | ISO 27001, PCI DSS (Partial) | Moderate | *"Essential but not 100% secure" (R21)* |
| **Non-Adopters** (HC/EDU&R/M&SC) | 0% | N/A | N/A | "No budget for frameworks" (R23-HC) |

**A. Risk-Based Approach**

- "ISO 27001 systematically identifies and mitigates threats" (R14-E&UT)
- Most cited benefit: Structured risk management (6/10 framework users)

**B. Compliance & Standards**

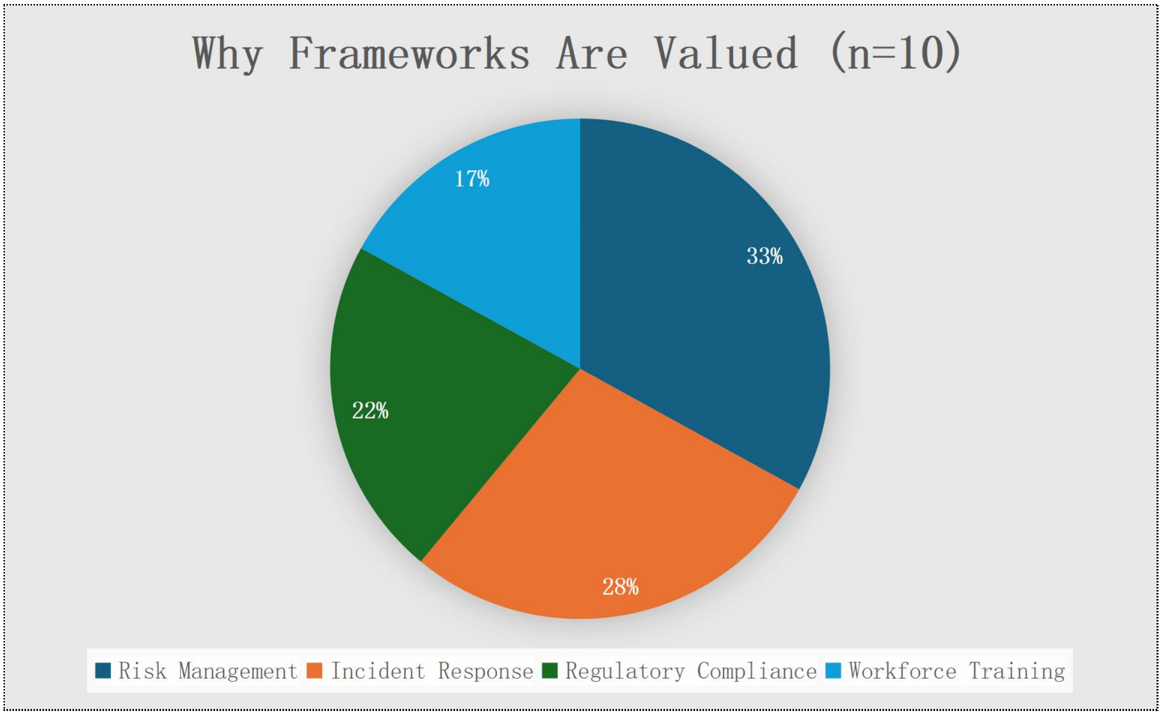
- "PCI DSS ensures payment data protection" (R20-BFS)
- Secondary benefit: Regulatory alignment (4/10)

**C. Limitations**

- *"No framework guarantees absolute security" (R14, R21, R28)*
- Common challenge: Scope limitations (e.g., R4's limited ISO implementation)

**Sector-Specific Insights**

| Sector | Unique Value Proposition | Caveats |
|---|---|---|
| **BFS** | Financial Standards (PCI DSS) + general frameworks like ISO 27001 | High implementation costs |
| **T&IT** | Adapts global cybersecurity frameworks like NIST to local threats | Requires skilled employees |
| **G&CI** | Prioritizes critical infrastructure protection | Slow bureaucratic adoption |
| **Non-Adopters** | N/A | Proactive vs Reactive security |



**Key Findings**

1. **Adoption-Confidence Correlation**:
   - Organizations who have implemented cybersecurity frameworks shows 100% more confidence in the mitigation of Cyberthreats (BFS/T&IT vs. Remaining organizations)
2. **Implementation Gaps**:
   - 60% of organizations implemented cyber security frameworks partially.
3. **Skepticism Balance**:
   - All cybersecurity framework users acknowledge limitations in flawless cybersecurity (e.g., R14: *"No 100% security"*)

**Cybersecurity Framework Implementation Challenges**

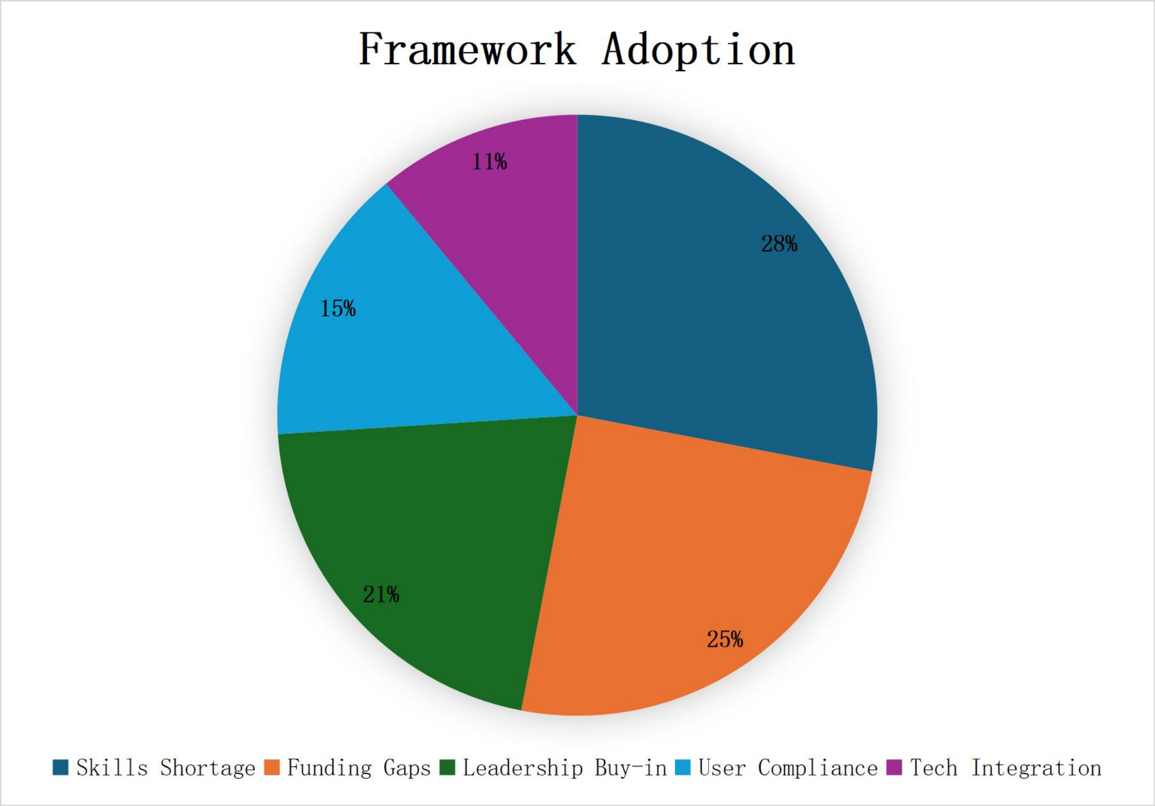
**1. Primary Obstacles (Ranked by Frequency)**

| Challenge | % Reporting | Most Affected Sectors | Example Quote |
|---|---|---|---|
| **Lack of Skilled Professionals** | 68% (22/32) | HC, EDU&R, M&SC | *"their is no cybersecurity department"* (R16-E&UT) |
| **Budget Constraints** | 62% (20/32) | HC, EDU&R, M&SC | *"No allocated budget for cybersecurity measures"* (R23-HC) |
| **Management Apathy** | 53% (17/32) | HC, EDU&R, EC&R | *"Cybersecurity is not a priority for leadership"* (R25-M&SC) |
| **Employee Resistance** | 37% (12/32) | M&SC, T&IT, G&CI | *"employees bypass cybersecurity protocols"* (R8-M&SC) |
| **Bureaucratic Hurdles** | 25% (8/32) | G&CI, E&UT | *"Multi-layer approval delays"* (R15-G&CI) |

**Sector-Specific Complications**

| Sector | Unique Challenges | Root Cause |
|---|---|---|
| **Healthcare** | Pirated software usage (4/4) | Budget constraints (R31) |
| **Education** | Zero cybersecurity staff (4/4) | HEC non-mandate (R29) |
| **Manufacturing** | Leadership underestimates risks (4/4) | No regulatory pressure (R18) |
| **Government** | Ad-hoc security measures (3/4) | No national authority (R21) |
| **BFS** | Brain drains of experts (2/4) | Global competition (R28) |

**Implementation Pain Points**



**Consequences of Unaddressed Challenges**

1. **Security Debt**:
   - HC: *"Using cracked Windows 7 in 2023"* (R31)
2. **Regulatory Risks**:
   - EDU&R: *"HEC may impose fines post-breach"* (R27)
3. **Attack Surface Expansion**:
   - M&SC: *"There are many unsecure IoT devices in the organization"* (R17)

**Positive Outliers**

- **BFS (R20)**: Cross-trained IT staff in cybersecurity
- **T&IT (R30)**: Monthly security drills for employees
- **G&CI (R10)**: Air-gapped critical systems

## DISCUSSION

This study provides important insights into the varied and intricate aspects of the cybersecurity frameworks associated with different organizations within Pakistan. There is a huge difference in the adoption and implementation of cybersecurity frameworks. As regulated sector like banking and financial sector adopt 100% cybersecurity frameworks while sectors which have no pressure from regulators avoid adopting and implementing cybersecurity framework in their organizations, like IT&T, Education etc. The implementation of global cybersecurity frameworks is a challenge for the developing nations like Pakistan.

It is important to note that organizations who have implemented cybersecurity frameworks showed their concern regarding emerging cyber threats. They admitted that securing an organization from cyber-attacks is very challenging and need dedication, leader commitment and resources as well. The unregulated sectors showed concern regarding cyber threats but their leadership is complacent with the vulnerable environment. A worrying challenge arises from the marked disparities involving different sectors. 65% of participants cited budgetary constraints while 71% cited a shortage of skilled cybersecurity professionals. Under-resourced sectors will not implement a cybersecurity framework, and will thus remain highly exposed, which discourages any investment in cybersecurity. The healthcare sector is an example of budgetary constraints driving an organization to self-destructive and dangerous compromises. The use of pirated and outdated software in the healthcare sector can compromise patient safety and jeopardize the confidentiality of sensitive data. Even among organizations utilizing cybersecurity frameworks, 60% only execute them partially, leaving many security gaps unaddressed. Furthermore, the study found that partially implementing a framework may pose a greater risk than not utilizing a cybersecurity framework at all due to the false sense of security it provides. This is especially the case in the manufacturing industry, where attempts to implement the NIST Cybersecurity Framework have not adequately resolved the specific cybersecurity risks related to operational technologies prevalent in the industry. In this study the emergence of human element in cybersecurity effectiveness is of prime importance. It is revealed that employee’s resistance and management indifference are substantial barriers in effective cybersecurity program. Employees resistance that is 39% and management commitment that is 55%, cannot be overcome with technical frameworks alone. This finding supports the growing recognition in the literature that change to an organization's culture is a prerequisite for achieving cybersecurity. Organizations such as Banking and Financial (BFS) that cross-train IT staff and T&IT firms that conduct security drills with staff demonstrate the importance of the human involvement in cybersecurity program.

In conclusion this study state that the adoption of cybersecurity frameworks in Pakistan’s organizations is characterized by an intricate set of regulation, resources, organizational culture, and situational fit. The analysis carried the implication that advocating for the adoption of frameworks without addressing the problems of resources and realistic implementation will not generate any substantial returns in security. The context of Pakistan demands an integrated security approach of regulation and culturally determining organizational change. The study suggests that future work investigate how Pakistan, and other developing countries, may establish frameworks that integrate best practice cybersecurity operations while considering the contextual constraints given in this study.

## RECOMMENDATIONS

The following recommendations are proposed to increase cybersecurity resilience in organization in Pakistan

### Development of Sector-Specific Cybersecurity Guidelines

National authorities like the Pakistan Telecommunication Authority (PTA) and the Ministry of IT should collaborate with sectoral regulators (e.g., State Bank of Pakistan for BFS, DRAP for Healthcare, HEC for Education) to create tailored cybersecurity frameworks. These cybersecurity frameworks should address sector related cyber threats. That includes, for example, Operational Technology (OT) security for Energy & Utilities and data protection legislations and policies for patient health information (PHI) in healthcare.

### Implementation of Tiered Compliance Model

Phased implementation of cybersecurity frameworks should be suggested especially for Small and Medium-sized Enterprises (SMEs) and under-resourced sectors. This would allow organizations to achieve baseline security controls.

### Foster Public-Private Partnerships for Capacity Building

It is a dire need of time to establish nationally funded cybersecurity training and certification programs to address the critical skills shortage i.e. (71%). These types of initiatives could include subsidized cybersecurity training, university curricula development, and creating a national cybersecurity apprenticeship program to manage the "brain drain" identified in the BFS and T&IT sectors.

### Adopt a Risk-Based, Phased Implementation Strategy

Organizations in Pakistan should start implementing cybersecurity program with a vulnerability and risk assessment instead of attempting to achieve full cybersecurity certification right away. Organizations should assess the critical and vulnerable assets then prioritize the implementation of the framework's controls. The organization should prioritize the assets and mitigate the most likely cyber threats and the ones that can most harm the organization.

### Integrate Cybersecurity into Organizational Culture

Leadership in the organizations must champion cybersecurity program as a strategic priority, not just an IT issue. This can be achieved by incorporating security metrics into performance reviews, conducting trainings, and fostering accountability.

### Conduct Regular Workaround Audits

The findings suggest organizations should conduct internal and third-party audit for their cybersecurity program. It should be done at least once in a year.

### Employees Training and Awareness

leaders must embrace the phenomenon of employee resistance, which can be approximated at 39%. There should be scheduled training and awareness programs regarding cybersecurity best practices and emerging threats. It will help the employees to understand how to adhere cybersecurity policies and improving cyber hygiene of the organization.

### Limitation of Study

The are few limitations observed during the research which are as follows.

### Generalizability

This research adopts a qualitative methodology which, while rich in depth, limits the statistical generalizability of the findings. By focusing on cybersecurity professionals in formal roles, the practices of smaller, informal, and, especially, unregistered organizations in Pakistan may be overlooked.

### Potential for Social Desirability Bias

This data is collected from the professionals who hold the responsibility of cybersecurity program for organizations. It is plausible that the respondents may have exaggerated their efforts for cyber security programs in organizations, to present a positive organizational image.

### Cross-Sectional Nature

This research captures a specific perspective of the cybersecurity landscape. To gain a complete picture of the evolution of the adoption of a cybersecurity framework and its long-term impacts on cyber threat mitigation in Pakistan, a longitudinal study can be undertaken.

### Lack of Quantitative Corroboration

This research has not quantitatively linked the adoption of a framework with any of the specific variables that determine incident response time, reduction in loss incurred, and other indicators of security program performance. It would be beneficial in subsequent work, if research were to incorporate the quantitative aspect alongside the qualitative to bolster the present study.

### Concluding Statement

The complex and contradictory practices regarding the adoption of cybersecurity frameworks in Pakistani organizations have remained poorly understood. This work clarifies the state of cybersecurity in the country. Research findings suggest that organizations in Pakistan are on a cybersecurity journey that is neither straight nor easy. While the regulated sectors resemble a well-resourced, compliant path, other important, but under-resourced, sectors seem to be stuck in an endless cycle of cyber vulnerability. This gap poses a significant risk and may increase the likelihood of under-resourced unregulated sectors becoming targets for cyber criminals.

## REFERENCES

Awan, J. H., Memon, S., Shah, M. H., & Awan, F. H. (2016). Security of E-government services and challenges in Pakistan. In *2016 SAI Computing Conference (SAI)*. IEEE. https://doi.org/10.1109/SAI.2016.7556133

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy*, 3(2), https://doi.org/ 10.1080/23738871.2018.1513051

Bhargav, A. (2014). *PCI compliance: The definitive guide* (1st ed.). CRC Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), https://doi.org/10.1191/1478088706qp063oa

Calder, A. (2018). *NIST cybersecurity framework: A pocket guide*. IT Governance Publishing.

Calder, A., & van Bon, J. (2017). Implementing information security based on ISO 27001/ISO 27002: A management guide. Van Haren Publishing.

Chen, X., & Liu, Y. (2016). Best practices in cybersecurity management. *Cybersecurity Journal*, 18(4).https://doi.org/ 10.1080/ 12345678.2016. 1234567

Chuvakin, A., & Williams, B. (2014). *PCI compliance: Understand and implement effective PCI data security standard compliance* (4th ed.). Syngress Publishing.

Clarke, R. V. (1992). *Situational crime prevention: Successful case studies*. Harrow and Heston.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), https://doi.org/ 10.2307/2094589

Cook, L. (2022). *The evolution of ISO 27001* Cyjax. https://www.cyjax.com /2022/07/22/the-evolution-of-iso-27001/

Costantino, G., La Marra, A., Martinelli, F., & Matteucci, I. (2018). CANDY: A social engineering attack to leak information from infotainment system. *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. https://doi.org/ 10.1109/VTCSpring.2018.8417879

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). Enterprise governance of IT, alignment, and value. In *Enterprise governance of information technology*. Springer, Cham. https://doi.org/10.1007/978-3-030-22062-6_1

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information & Computer Security, 27*(3), https://doi.org/10.1108/ICS-09-2018-0110

Felson, M., & Eckert, M. A. (2018). *Crime and everyday life* (6th ed.). SAGE Publications.

Frisby, J. (2020). *Global cyber security exposure index*. PasswordManagers.co. https://passwordmanagers.co/cybersecurity-exposure-index/#global

International Telecommunication Union (ITU). (2017). *Global cybersecurity index 2017*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

International Telecommunication Union. (2021). *Global cybersecurity index 2020*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Hashim, R., & Razali, R. (2019). Contributing factors for successful information security management implementation: A conceptual model. *International Journal of Innovative Technology and Exploring Engineering, 9*(2) . https://doi.org/ 10.35940/ijitee.B7214.129219

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT*.

Kayworth, T., & Whitten, D. (2012). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive, 11*(3), https://ssrn.com/abstract=2058035

Khan, M. A., Saleem, F., & Zaidi, S. S. H. (2021). Cybersecurity challenges in Pakistan: A stakeholder perspective. *Computers & Security, 104*, 102221. https://doi.org/10.1016/j.cose.2021.102221

Khan, M. I. (2019). Cyber-warfare: Implications for the national security of Pakistan. *NDU Journal*.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2019). Cutting the Gordian knot: A look under the hood of ransomware attacks. *Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses* . https://doi.org/10.2478/popets-2019-0029

Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27*(5), 644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Pakistan Telecommunication Authority. (2021). *Annual report 2020*. https://www.pta.gov.pk/media/annual_reports/PTA%20Annual%20Report%202020.pdf

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5). https://doi.org/10.1007/s10488-013-0528-y

Paternoster, R. (2010). How much do we really know about criminal deterrence? *The Journal of Criminal Law and Criminology, 100*(3).

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE Publications.

Qadeer, M. A. (2020). The cyber threat facing Pakistan. *The Diplomat*. https://thediplomat.com/2020/06/the-cyberthreat-facing-pakistan/

Rafiq, A. (2017). Challenges of securitising cyberspace in Pakistan. *Strategic Studies, 37*(4).

Safdar, A. (2020). The emerging threat of Indian cyber warfare against Pakistan. *Daily Times*. https://dailytimes.com.pk/660092/the-emerging-threat-of-indian-cyber-warfare-against-pakistan/

Saxena, S. (2013). Ensuring cloud security using cloud control matrix. *International Journal of Information and Computation Technology, 3*(5).

Siddiqui, N. (2020). Indian cyber attack targeting gadgets of govt officials, military personnel identified: ISPR. *Dawn*. https://www.dawn.com/news/1574034

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 38*(1). https://doi.org/ 10.1145/1216218.1216224

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

Steuperaert, D. (2019). COBIT 2019: A significant update. *EDPACS, 59*(1). https://doi.org/10.1080/07366981.2019.1583149

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security, 25*(5). https://doi.org/10.1108/ICS-07-2016-0054

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, 12*(3).

Syed, R., Khaver, A. A., & Yasin, M. (2019). *Cyber security: Where does Pakistan stand?* Sustainable Development Policy Institute.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1). https://doi.org/ 10.1108/09685220910944722

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee compliance with organizational cybersecurity policies. *Computers & Security, 78*. https://doi.org/10.1016/j.cose.2018.06.001

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.